Gestion de la sécurité Xanadu

Dernière mise à jour: 12/11/2024

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

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

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

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

Traduction automatique

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

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Sommaire

Opérations de sécurité 5
- Explorer Opérations de sécurité 7
- Now Assist pour Opérations de sécurité 13
  - Explorer Now Assist pour Opérations de sécurité 15
  - Configurer Now Assist pour Opérations de sécurité 17
  - Utilisation Now Assist pour Opérations de sécurité pour résoudre des incidents de sécurité 24
- Applications de surface d'attaque 28
  - Réponse aux vulnérabilités 30
  - Application Vulnerability Response 814
  - Réponse aux vulnérabilités pour conteneurs 1022
  - Conformité de la configuration 1094
  - Vulnerability Response commun 1368
  - Réponse aux vulnérabilités Espaces de travail 1376
  - Nomenclature logicielle 1547
- Applications de gestion des tickets de sécurité d'entreprise 1576
  - Réponse aux incidents de sécurité 1577
  - Renseignements sur les menaces 3104
- Contrôle de la posture de sécurité 3362
  - Explorer Contrôle de la posture de sécurité 3364
  - Utilisation de l'espace de Contrôle de la posture de sécurité travail 3374
  - Cas d'utilisation, exemples de politiques et connecteurs du graphe de services pris en charge dans Contrôle de la posture de sécurité 3392
- Tableau de bord de direction de cybersécurité 3407
  - Adhésion aux scores de point de référence 3425
  - Définir des cibles 3426
  - Intégration de la simulation et de la formation de sécurité pour les opérations de sécurité 3427
  - Tableau de bord des risques et de la conformité pour GRC : Mesures 3429
- Threat Intelligence Security Center 3439
  - Explorer Centre de sécurité des renseignements sur les menaces 3441
  - Séparation de domaine et Threat Intelligence Security Center 3443
  - Configurer Threat Intelligence Security Center 3445
  - Afficher la page d'accueil de Threat Intelligence Security Center 3447
  - Intégration de Threat Intelligence Security Center 3450
  - Administration 3509
  - Utilisation des importations de données 3552
  - Importer Threat Intelligence 3554
  - Console d'analyste de menaces 3563
  - Centre de sécurité des renseignements sur les menaces Bibliothèque 3578

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MITRE-ATT&CK™ Dépôt 3709
Gestion et conservation des données 3718
Flux fonctionnel de traitement des données TISC 3727
Data Loss Prevention Incident Response 3729
Explorer Data Loss Prevention Incident Response 3730
Installation et configuration DLP IR d'Incident Response 3733
Administration de Réponse aux incidents DLP 3734
Data Loss Prevention Incident Response Gestion des incidents 3788
Intégration entrante pour Data Loss Prevention Incident Response 3806
Intégrations DLP 3809
Opérations de sécurité Fonctionnalité commune 3862
Créer et définir des groupes de filtres dans Security Operations 3865
Transformation des données partagées 3866
Opérations de sécurité Traitement des e-mails 3870
Opérations de sécurité Mappage de champs 3881
Opérations de sécurité Transformations de valeurs de champs 3885
Opérations de sécurité Mappage des données d'enrichissement 3887
Opérations de sécurité Escalade définie par l'utilisateur 3890
Créer des remplacements de propriété séparés par domaine 3891
Créer un groupe de systèmes d'exploitation 3892
Configurer des groupes et des balises de sécurité 3894
Annotations de sécurité 3898
Composants installés avec Security Support Common 3900
Rechercher Opérations de sécurité 3901
Référence de Security Operations Integrations 3901
Opérations de sécurité Déclencheurs de workflow 4014
Orchestration de Security Operations 4016

Traduction automatique

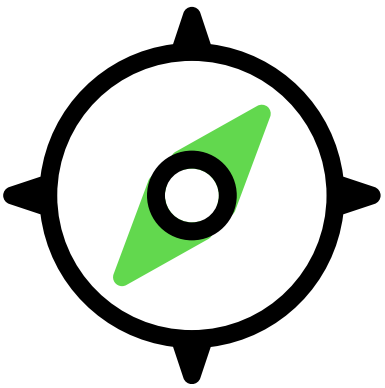
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opérations de sécurité

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

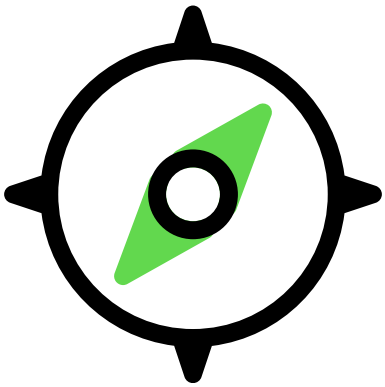
Choisissez l'une des vignettes suivantes pour commencer.

Explorer les applications Security Operations et leurs espaces de travail



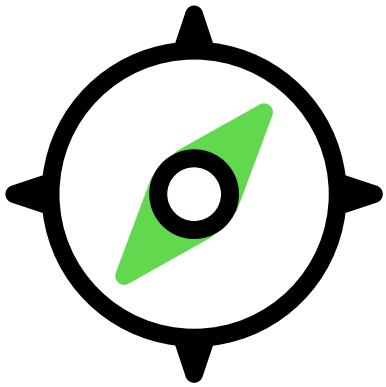
Découvrez comment les Opérations de sécurité applications peuvent vous aider à améliorer votre posture de sécurité.

Explorer Now Assist pour Security Operations



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

Explorer les applications de surface d'attaque

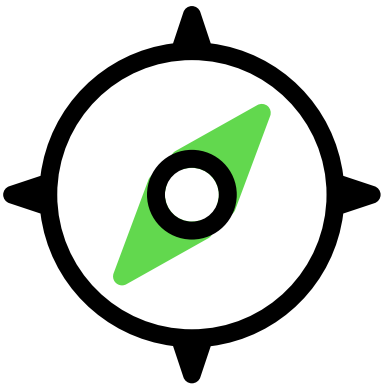


Découvrez les applications de Vulnerability Response qui vous aident à identifier et à corriger les vulnérabilités sur votre surface de cyberattaque.

Traduction automatique

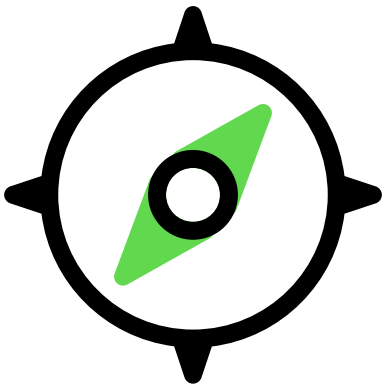
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer les applications de gestion des tickets de sécurité d'entreprise



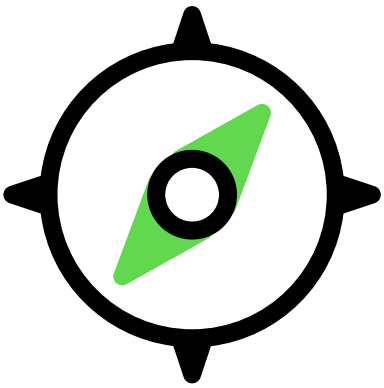
Découvrez les applications de Réponse aux incidents de sécurité qui vous aident à analyser, isoler et corriger les incidents de sécurité critiques à mesure qu'ils évoluent.

Explorer les applications de contrôle de la posture de sécurité



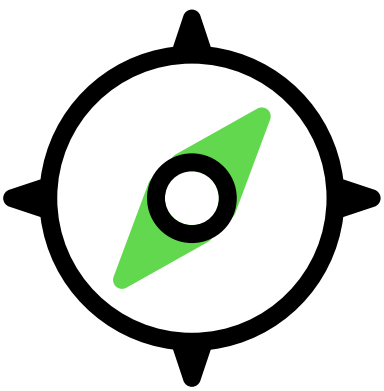
Découvrez les applications qui vous aident à mieux comprendre votre posture de sécurité globale.

Explorez le tableau de bord de direction de cybersécurité



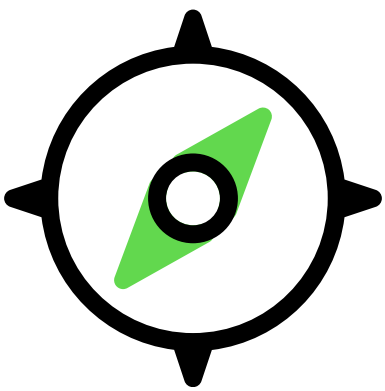
Découvrez comment le tableau de bord de direction de cybersécurité consolide les données des différents produits SecOps dans un tableau de bord unifié.

Explorer le centre de sécurité Threat Intelligence



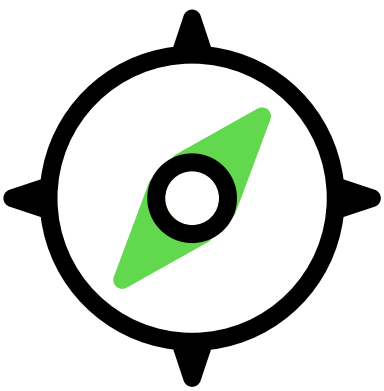
Découvrez comment la plateforme (TISC) fournit des solutions technologiques pour l'agrégation Centre de sécurité des renseignements sur les menaces et la gestion de la connaissance des menaces.

Explorer Data Loss Prevention Incident Response



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

Explorer les applications partagées Security Operations

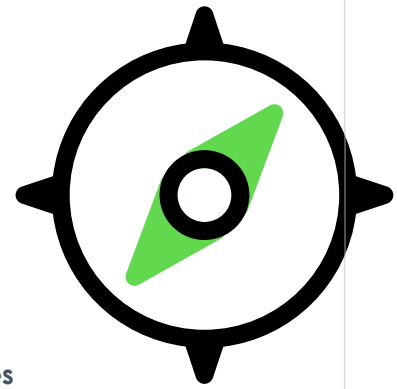


Découvrez les fonctionnalités et modules qui fournissent des fonctionnalités communes à .Opérations de sécurité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer les scénarios et les exemples



Apprenez-en davantage sur la façon d'obtenir Opérations de sécurité des applications à partir de et ServiceNow® Store des scénarios pour les applications que vous pouvez utiliser tout en utilisant les produits.

Dépannage et demande d'aide

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

Explorer Opérations de sécurité

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

Vue d'ensemble de Opérations de sécurité

La Opérations de sécurité suite d'applications vous aide à protéger vos actifs en améliorant votre posture de sécurité globale. Par exemple, en intégrant des applications telles que Réponse aux incidents de sécurité, Réponse aux vulnérabilitéset Contrôle de la posture de sécurité avec vos outils de sécurité existants, les analystes, les responsables et les équipes informatiques de votre centre des opérations de sécurité (SOC) peuvent :

- Répondez à l'évolution rapide des menaces de cybersécurité et de sécurité
- Identifier, classer par ordre de priorité et corriger les vulnérabilités
- Afficher votre inventaire complet d'actifs
- Déterminer la couverture globale de votre outil de Security
- Résolvez les incidents de sécurité plus rapidement grâce à des workflows intelligents et ServiceNow à des compétences d'IA générative (GenAI). Consultez Now Assist pour Opérations de sécurité pour plus d'informations.

Traduction automatique

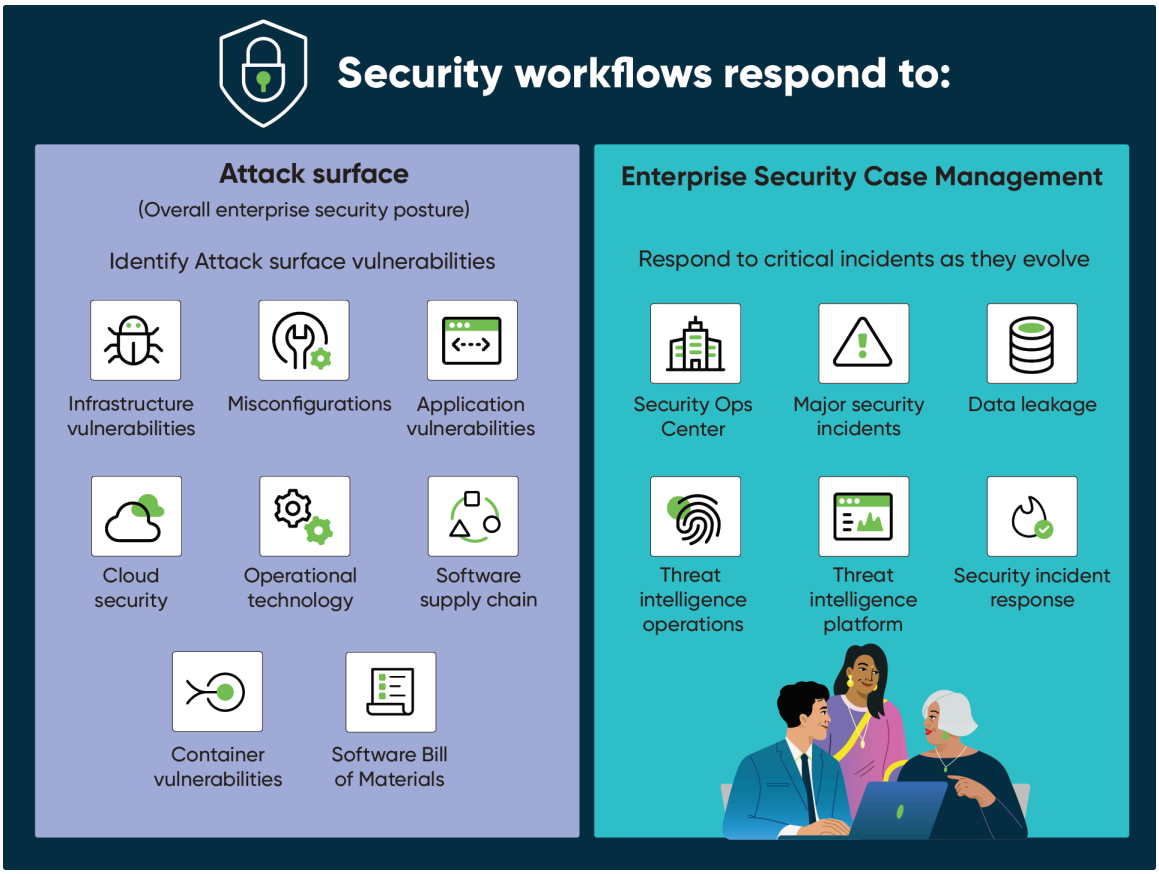
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opérations de sécurité Applications pour les flux de travail

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

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

Workflows de sécurité



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

Avantages des Opérations de sécurité applications

Affichez Opérations de sécurité les applications et les données à l'aide d'interfaces utilisateur (espaces de travail) de nouvelle génération. Grâce aux espaces de travail, les analystes de sécurité, les responsables du centre des opérations de sécurité (SOC) et les spécialistes du rattrapage de votre organisation peuvent surveiller et gérer les types de workflows suivants à partir d'un seul emplacement :

- Le cycle de vie des incidents de sécurité, de l'analyse initiale à l'émancipation, à l'éradication et à la reprise
- Les vulnérabilités qui leur tiennent le plus à cœur afin qu'ils puissent décider stratégiquement des vulnérabilités qu'ils envoient aux équipes informatiques pour qu'elles les corrigent.
- Des aperçus clés et des cas d'utilisation clés pour la couverture des outils de sécurité et l'hygiène des actifs qui signalent et surveillent les informations importées sur vos actifs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications de surface d'attaque

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

Application	Description	Utilisateurs
Contrôle de la posture de sécurité	Obtenez un aperçu de la façon dont les outils de sécurité sont déployés et de la couverture de vos actifs en fonction d'un inventaire des actifs et des données importées. Les connecteurs du graphe de services et les produits ServiceNow tels que Gestion des actifs matériels (HAM) et Détection ITOM sont pris en charge pour les importations de données. Les audits basés sur des politiques vous aident à hiérarchiser la correction des combinaisons à haut risque telles que l'exposition à Internet et les vulnérabilités connues. Créez des politiques et des aperçus personnalisés pour surveiller la conformité des actifs avec les normes de configuration de votre outil de Security interne.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Ingénieur des opérations informatiques • Propriétaire de service (profil du propriétaire de la réconciliation)
Réponse aux vulnérabilités	Les analyseurs de vulnérabilité et les outils d'évaluation tiers vous aident à identifier les risques que les vulnérabilités posent pour les types d'actifs suivants : • Infrastructure (hôte) • Conteneur • Applications • Nomenclatures logicielles Les vulnérabilités identifiées par ces outils se traduisent par des risques pour les équipes de sécurité et informatiques responsables de la maintenance et de la sécurisation des actifs d'une organisation.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Ingénieur des opérations informatiques • Propriétaire de service (profil du propriétaire de la réconciliation)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

Application	Description	Utilisateurs
Conformité de la configuration	Vérifiez votre conformité aux politiques de sécurité ou d'entreprise. Identifiez, classez par ordre de priorité et corrigez les éléments de configuration non conformes grâce aux résultats des tests obtenus à partir d'intégrations tierces de Secure Configuration Assessment (SCA).	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Ingénieur des opérations informatiques • Propriétaire de service (profil du propriétaire de la réconciliation)

Applications de gestion des tickets de sécurité d'entreprise

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

Application	Description	Utilisateurs
Réponse aux incidents de sécurité	Simplifiez le processus d'identification des incidents critiques en appliquant de puissants workflows et outils d'automatisation qui accélèrent la correction. Intégrez vos outils SIEM (Security Information and Event Manager) existants aux Réponse aux incidents de sécurité applications Security Operations pour importer des données sur les menaces à partir de différentes sources et créer automatiquement des incidents de sécurité prioritaires.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Analyste Threat Intelligence
Gestion des incidents de sécurité majeurs	Les options majeures de gestion des incidents de sécurité fonctionnent avec les capacités existantes du produit Security Incident Response. Cela inclut la possibilité pour un analyste de sécurité d'escalader un incident de sécurité standard en un incident de	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Ingénieur des opérations informatiques

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

Application	Description	Utilisateurs
	sécurité majeur, de sorte que les nouvelles options du produit soient disponibles pour prendre en charge le processus de correction. Suivez la progression d'un incident de sécurité majeur (MSI), de la détection à l'analyse. Proposer des solutions, promouvoir et lier les incidents de sécurité et la fermeture.	• Propriétaire de service (profil du propriétaire de la réconciliation) • Conseil général
Data Loss Prevention Incident Response	Data Loss Prevention Incident Response (DLP IR) vous permet d'examiner et de gérer le workflow de rattrapage des incidents DLP à partir de plusieurs sources, telles que les points de terminaison, le réseau, la messagerie électronique et le cloud.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité
Renseignements sur les menaces	Permet aux équipes de réponse aux incidents d'automatiser les recherches, les recherches et la corrélation des menaces. L'intégration avec MITRE ATT&CK vous permet de mesurer et de comprendre la couverture de détection et d'atténuation et vous aide à rechercher les menaces.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Analyste Threat Intelligence
Centre de sécurité des renseignements sur les menaces (TISC)	Agrégez, organisez et gérez les renseignements sur les menaces provenant de plusieurs sources et gérez les tickets de renseignements sur les menaces. Suivez les campagnes, rendez opérationnels les renseignements sur les menaces et répondez aux renseignements exploitables.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Analyste Threat Intelligence

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce qu'il faut explorer ensuite

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

Espace de travail Réponse aux incidents de sécurité	**Espace de travail du gestionnaire de vulnérabilité**	**Espace de travail pour le contrôle de la posture de sécurité**
		
En savoir plus sur l'espace de travail Réponse aux incidents de sécurité	En savoir plus sur l'espace de travail du gestionnaire de vulnérabilité	En savoir plus sur l'espace de travail Contrôle de la posture de sécurité
Espace de travail de l'évaluation de la vulnérabilité	**Espace de travail de remédiation informatique**	**Espace de travail de nomenclature logicielle**
		
En savoir plus sur l'espace de travail de l'évaluation de la vulnérabilité	En savoir plus sur l'espace de travail de remédiation informatique	En savoir plus sur la nomenclature logicielle de l'espace de travail

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Espace de travail de Threat Intelligence Security Center (TISC)	Espace de travail de réponse aux incidents de la prévention des pertes de données (DLP)	Espace de travail Major Security Incident Management (MSIM)
		
En savoir plus sur l'espace de travail TISC	En savoir plus sur l'espace de travail DLP	En savoir plus sur l'espace de travail MSIM

Dépannage et demande d'aide

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

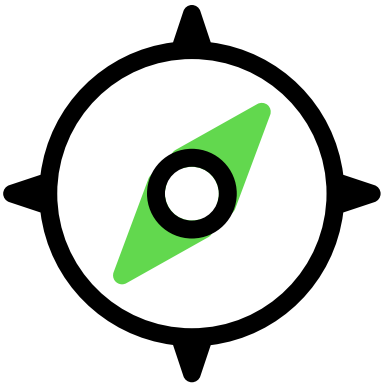
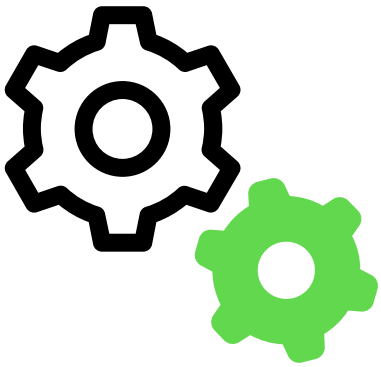
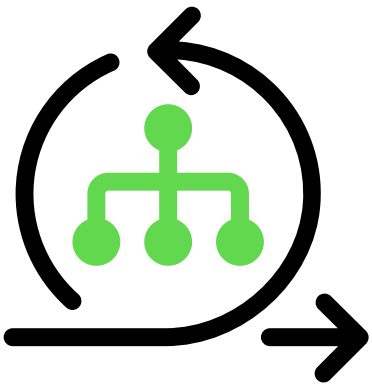
Now Assist pour Opérations de sécurité

Les analystes de sécurité peuvent utiliser des workflows intelligents et ServiceNow des compétences d'IA générative pour les aider à résoudre les incidents de sécurité. Les gestionnaires de sécurité peuvent examiner rapidement le contexte des incidents de sécurité et les notes de fermeture dans un format concis et facile à lire avec l'application Now Assist pour Opérations de sécurité .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Premiers pas

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

Important : Certains produits/fonctionnalités Now Assist ne sont actuellement pas disponibles pour les clients dans les centres de données FedRAMP, NSC DOD IL5 ou protégés par l'IRAP en Australie, les clients auto-hébergés ou dans d'autres environnements restreints. Pour en savoir plus, consultez l'article KB0743854 dans la Now Support Base de connaissances. Consultez les mises à jour de disponibilité dans les versions futures.

Dépannage et demande d'aide

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

Limitations de l'IA

Cette application utilise l'intelligence artificielle (IA) et l'apprentissage machine, des domaines d'étude à l'évolution rapide qui génèrent des prédictions basées sur des modèles de données. Par conséquent, cette application peut ne pas toujours produire des informations exactes, complètes ni appropriées. De plus, il n'y a aucune garantie que cette application ait été entièrement formée ou testée pour votre cas d'utilisation. Pour vous aider à atténuer ces problèmes, nous vous recommandons vivement de tester et d'évaluer l'utilisation que vous faites de cette application pour vérifier qu'elle est appropriée à votre utilisation, d'avoir recours à une vérification humaine le cas échéant et d'éviter de vous fier uniquement aux résultats générés par l'IA pour prendre des décisions. Cela est particulièrement important si vous déployez cette application dans des domaines

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ayant des impacts importants tels que la santé, la finance, le droit, l'emploi, la sécurité ou l'infrastructure.

Traitement des données

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

Collecte de données

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

Explorer Now Assist pour Opérations de sécurité

Vos analystes de sécurité peuvent utiliser des workflows intelligents et ServiceNow des compétences d'IA générative pour les aider à résoudre les incidents de sécurité dans le cadre de leur travail avec l'application Now Assist pour Opérations de sécurité . Grâce à leurs compétences en matière d'IA générative, ils peuvent examiner rapidement le contexte et les notes de clôture des incidents de sécurité dans un format concis et facile à lire.

Vue d'ensemble de Now Assist pour Opérations de sécurité

Vos analystes de sécurité ont la possibilité de résumer les détails de l'incident de sécurité et de générer des notes de fermeture avec l'IA générative. Ils peuvent partager des résumés et des notes de clôture avec d'autres analystes, gestionnaires et parties prenantes clés.

Now Assist pour Opérations de sécurité utilisateurs

Utilisateurs

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

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Now Assist pour Opérations de sécurité avantages

Fonctionnalités de Now Assist pour Opérations de sécurité

Avantage	Fonctionnalité	Utilisateurs
Accélérez le triage des incidents de sécurité avec de longs flux d'activité en examinant rapidement les notes de travail et les informations contextuelles dans un format concis et facile à lire.	Générer des résumés pour les incidents de sécurité qui incluent les informations suivantes : • Problème • Détails • Observations • Principales mesures prises • Détails de fermeture	• les analystes de la sécurité • Gestionnaires de la sécurité
Générez automatiquement un brouillon de notes de fermeture pour un incident de sécurité lorsqu'il est prêt à être fermé. Les analystes peuvent modifier tout contenu généré par la compétence d'IA en le modifiant, en le supprimant ou en ajoutant leurs propres notes avant de fermer l'incident de sécurité.	Générer des notes de clôture d'incident de sécurité	• les analystes de la sécurité • Gestionnaires de la sécurité
Découvrez rapidement les détails d'un incident de sécurité en accédant aux résumés et aux notes de fermeture à partir du Now Assist panneau.	Accédez au résumé de l'IA générative et aux notes de fermeture à partir du Now Assist panneau. Saisissez des demandes d'informations plus basiques sur les incidents de sécurité dans le panneau.	• les analystes de la sécurité • Gestionnaires de la sécurité
Personnalisez les compétences de l'IA générative pour les résumés et les notes de clôture en fonction de vos besoins.	Copiez une compétence et modifiez-la Sélectionnez les champs de table connexes, définissez la disponibilité de la compétence, puis choisissez où la compétence est affichée.	administrateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce qu'il faut explorer ensuite

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

- Configurer Now Assist pour Opérations de sécurité
- Résumer un incident de sécurité avec Now Assist pour Opérations de sécurité
- Générer des notes de fermeture pour un incident de sécurité avec Now Assist pour Opérations de sécurité
- Référence : entrées et déclencheurs de Now Assist pour Security Operations

Informations de prise en charge pour Now Assist pour Opérations de sécurité

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

Versions prises en charge

- Pour legacy l'interface utilisateur (UI16) : Réponse aux incidents de sécurité application principale, v13.5.1
- Pour le Espace de travail de la Réponse aux incidents de sécurité (SIR Workspace), v1.6.0

Interfaces utilisateur prises en charge

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

Now Assist pour Opérations de sécurité Interfaces et compétences prises en charge

Interface	Fonctionnalités
Réponse aux incidents de sécurité	• Synthèse des incidents de sécurité • Génération de notes de fermeture • Panneau Now Assist
legacy Interface utilisateur UI16	• Synthèse des incidents de sécurité • Génération de notes de fermeture • Panneau Now Assist

Configurer Now Assist pour Opérations de sécurité

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

Vue d'ensemble de la configuration

En partageant des données avec le programme de développement de l'IA, vous fournissez des données pertinentes pour améliorer la précision des prédictions, l'expérience

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow® utilisateur, adapter les produits à vos besoins professionnels et réduire les hallucinations pour vos compétences activées Now Assist .

Vous pouvez choisir de vous désabonner d'une ServiceNow instance du partage de données à partir de la Now Assist Admin console si vous ne souhaitez pas participer. Consultez Refuser le partage de données pour Now Assist . Répétez le processus de désabonnement pour toutes les instances qui utilisent la Now Assist fonctionnalité.

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

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

Now Assist pour Opérations de sécurité Fonctionnalités et compétences de la Now Assist Admin console

Produit de technologie Now Assist	Compétences en matière d'incidents de sécurité
Opérations de sécurité	Synthèse des incidents de sécurité **Remarque :** La synthèse des incidents prend en charge les incidents de sécurité dans tout état autre que **brouillon**.
	Génération de notes de résolution.

1. Installer Now Assist modules d'extension .

   Installez l'application Now Assist pour Opérations de sécurité (sn_sec_gen_ai).

2. Configurer et activer une compétence pour Now Assist pour Opérations de sécurité

   Configurez et passez en revue les détails d'une compétence. Vous activez une compétence à partir du Configuration guidéefichier .

Utilisation Configuration guidée pour implémenter Now Assist pour Opérations de sécurité

Configuration guidée fournit une séquence de tâches qui vous aident à configurer Now Assist pour Opérations de sécurité sur votre ServiceNow instance. Pour ouvrir le Configuration guidée formulaire , Now Assist pour Opérations de sécuritéaccédez à **Tout** > **Administrateur Now Assist** > **Fonctionnalités**.

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

Configurer et activer une compétence pour Now Assist pour Opérations de sécurité

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

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Administrateur Now Assist** > **Fonctionnalités**.
2. Une fois **Technologie** sélectionnée dans le panneau de navigation, sélectionnez **Security Operations** dans la liste.
   Les compétences d'incident de sécurité suivantes sont affichées sur la carte d'incident de sécurité :
   - Synthèse des incidents de sécurité
   - Génération de notes de résolution
3. Sélectionnez **Afficher les détails**.
4. Sélectionnez **Activer la compétence** correspondant à la compétence souhaitée.
5. Suivez les étapes de configuration et d'activation d'une compétence à l'aide du Configuration guidée.

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

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

   Vous préférerez peut-être laisser ces modèles d'entrée dans leurs paramètres par défaut jusqu'à ce que vous vous familiarisiez avec le fonctionnement des compétences Now Assist pour Opérations de sécurité .

   Toutefois, vous pouvez modifier certains des champs de table connexes, tester l'invite sur un incident de sécurité, définir la disponibilité de la compétence et choisir l'emplacement où la compétence est affichée.

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

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

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

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

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	(Optional) Utilisez le créateur de conditions pour définir vos conditions.

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

Option	Description
Intégré au produit	Now Assist Les compétences sont affichées sur les formulaires et dans les espaces de travail.
Panneau Now Assist	Now Assist Les compétences sont disponibles dans le Now Assist panneau. **Remarque :** Si vous ne voyez pas cette option, vous devez activer le panneau Now Assist. Pour plus d'informations, consultez Activer le Now Assist panneau .

12. Sélectionnez **Enregistrer et continuer** pour passer à l'étape suivante.
13. Passez en revue vos choix et sélectionnez **Activer** pour terminer la configuration de la compétence.
14. Sélectionnez **Revenir à l'incident de sécurité**.
    La compétence est affichée dans la section Compétences actives.

Personnaliser une compétence Now Assist pour Opérations de sécurité

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

Avant de commencer

Rôles requis : admin

Procédure

1. Accédez au **Tout** > **Administrateur Now Assist** > **Fonctionnalités** de la Now Assist Admin console.
2. Une fois **Technologie** sélectionnée dans le panneau de navigation, sélectionnez **Security Operations** dans la liste.
   Les compétences d'incident de sécurité suivantes sont affichées :
   - Synthèse des incidents de sécurité
   - Génération de notes de résolution
3. Créer une copie d'une compétence et personnaliser les champs d'entrée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

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

c. Sélectionnez **Faire une copie**.

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

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

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

g. Sélectionnez **Choisir une entrée**.

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

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

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

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

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

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

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

- **Sélectionner l'affichage** :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Intégré au produit	Affichez la synthèse des incidents de sécurité dans tous les produits de sécurité. Now Assist Les compétences sont affichées sur les formulaires et dans les espaces de travail.
Panneau Now Assist	Now Assist Les compétences sont disponibles dans le Now Assist panneau. **Remarque :** Si vous ne voyez pas cette option, vous devez activer le panneau Now Assist. Pour plus d'informations, consultez Activer le Now Assist panneau .

j. Sélectionnez **Enregistrer le modèle** pour enregistrer les changements apportés au modèle Travail en cours.

k. Sélectionnez le modèle Réviser.

l. Continuez à modifier les champs modifiables dans les modèles Révision et Fermé avec des conditions de filtrage, comme décrit dans les étapes précédentes.

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

n. Sélectionnez **Enregistrer le modèle** pour enregistrer les changements que vous avez apportés à un modèle.

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

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

Entrées et déclencheurs pour Now Assist pour Opérations de sécurité

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

Vue d'ensemble

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

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

Compétence de synthèse des incidents de sécurité

Les entrées pour la compétence de synthèse des incidents de sécurité identifient la table et les champs utilisés lorsqu'un résumé d'incident de sécurité est généré. Le tableau suivant répertorie les entrées pour la compétence de synthèse des incidents de sécurité à partir de la page Choisir une entrée de la Now Assist Admin console.

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

Compétence de génération de notes de résolution

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

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

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation Now Assist pour Opérations de sécurité pour résoudre des incidents de sécurité

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

Vue d'ensemble de Now Assist pour Opérations de sécurité

Vos analystes de sécurité ont la possibilité de résumer les détails de l'incident de sécurité et de générer des notes de fermeture avec des compétences d'IA générative avec Now Assist pour Opérations de sécurité. Ils peuvent partager ces résumés et notes de clôture avec d'autres analystes, gestionnaires et parties prenantes clés.

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

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

1. Résumer un incident de sécurité avec Now Assist pour Opérations de sécurité

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

2. Générer des notes de fermeture pour un incident de sécurité avec Now Assist pour Opérations de sécurité

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

3. Demander des compétences d'IA générative dans le Now Assist panneau pour Now Assist pour Opérations de sécurité

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

4. Personnaliser une compétence Now Assist pour Opérations de sécurité

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

Résumer un incident de sécurité avec Now Assist pour Opérations de sécurité

Comprenez le contexte d'un incident de sécurité avec la compétence d'IA générative de résumé des incidents de sécurité.

Avant de commencer

Vous pouvez résumer un incident de sécurité dans l'interface legacy utilisateur principale (UI16) et dans le Espace de travail de la Réponse aux incidents de sécurité. Les champs utilisés pour les données d'entrée afin de résumer un incident à l'aide de l'IA générative doivent comporter un minimum de 200 mots. Pour plus d'informations sur les champs d'entrée, reportez-vous à Entrées et déclencheurs pour Now Assist pour Opérations de sécurité.

Rôles requis : si_analystsn, si.manager ou sn_si.basic

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

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

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

Option	Description
Afficher les détails du résumé	Sélectionnez l'icône d'informations (ⓘ) en regard de l'incident de sécurité résumé par Now Assist.
Enregistrer les informations de résumé en les ajoutant aux notes de travail de l'incident	**a.** Sélectionnez **Partager dans les notes de travail**. **b.** Vérifiez l'exactitude du contenu généré par l'IA dans le modal et apportez les modifications nécessaires. **c.** Sélectionnez **Enregistrer dans les notes de travail**.
Agrandir ou réduire le résumé	Sélectionnez l'icône de développement (⌄) ou l'icône de réduction (⌃) en regard de **Partager dans les notes de travail** pour développer ou réduire le résumé.
Fournir des commentaires	Sélectionnez l'icône Utile (👍) pour obtenir des commentaires positifs. Sélectionnez l'icône Inutile (👎) si le résumé n'a pas été utile. **Remarque :** Les commentaires améliorent le modèle d'IA générative et peuvent contribuer à optimiser les futures versions de cet habillage.
Copier le résumé	Sélectionnez l'icône Copier (⧉) pour copier le résumé dans le presse-papiers.

Générer des notes de fermeture pour un incident de sécurité avec Now Assist pour Opérations de sécurité

Générez automatiquement un brouillon des notes de fermeture d'un incident de sécurité lorsque vous le fermez. Le brouillon est modifiable et est révisé avant la clôture de l'incident

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de sécurité. Il peut être utilisé ou modifié selon les besoins. Les notes de fermeture fournissent des informations sur la résolution d'un incident de sécurité à d'autres analystes, gestionnaires et personnes concernées clés.

Avant de commencer

Rôles requis : si_analystsn, si.manager ou sn_si.basic

Procédure

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

Option	Description
Fermer l'incident de sécurité dans legacy Core UI16	**a.** Remplacez le champ **État** par **Fermé**. Le modal d'exécution pas à pas s'affiche. **b.** Passez en revue chaque étape et sélectionnez **Suivant**. **c.** Sélectionnez **Fournir les détails de la résolution**. **Remarque :** Avant de fermer l'incident de sécurité, vous voudrez peut-être examiner le texte généré et vous assurer qu'il est exact. Modifiez les notes ou supprimez-les pour fournir les vôtres. **d.** Mettez à jour le code de fermeture et sélectionnez **Fermer l'incident**. Le résumé de la résolution est affiché dans la section Informations sur la résolution de l'enregistrement d'incident de sécurité.
Fermer l'incident de sécurité à partir du Espace de travail de la Réponse aux incidents de sécurité	**a.** Dans l'onglet **Détails** de l'espace de travail, définissez le champ **État** sur **Fermé**. Le modal d'exécution pas à pas s'affiche. **b.** Passez en revue chaque étape et sélectionnez **Suivant**. **c.** Sélectionnez **Fournir les détails de la résolution**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Vous souhaitez peut-être examiner le texte généré et vous assurer qu'il est exact avant de fermer l'incident de sécurité. Modifiez les notes ou supprimez-les pour fournir les vôtres. **d.** Mettez à jour le code de fermeture et sélectionnez **Fermer l'incident**. Le résumé de la résolution est affiché dans l'onglet **Détails** de l'enregistrement d'incident de sécurité dans l'espace de travail.

Demander des compétences d'IA générative dans le Now Assist panneau pour Now Assist pour Opérations de sécurité

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

Avant de commencer

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

Rôles requis : si_analystsn, si.manager ou sn_si.basic

Procédure

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

Option	Description
Générer des notes de résolution	Dans le panneau Now Assist, sélectionnez **Générer des notes de résolution**. Les notes de fermeture générées dans le panneau sont identiques à celles générées lorsque vous fermez un incident de sécurité à partir d'un enregistrement. Les notes de fermeture des incidents de sécurité sont créées en fonction des mesures prises pour le rattrapage et le confinement, en plus des autres détails pertinents liés à leur fermeture.

Traduction automatique

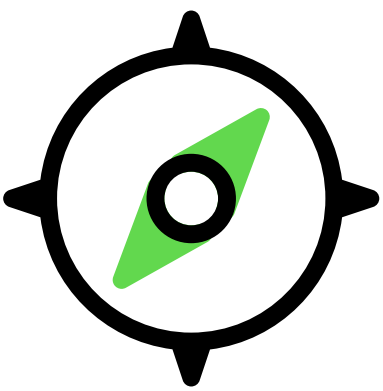
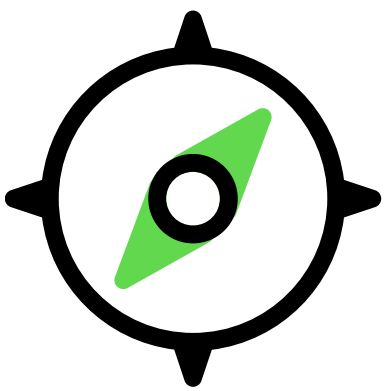
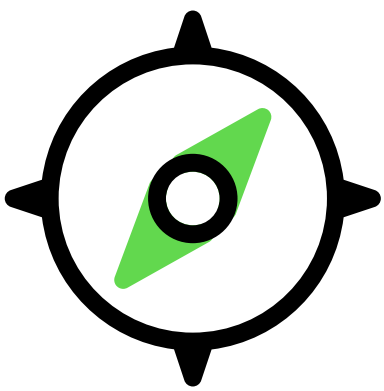
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Vous souhaitez peut-être examiner le texte généré et vous assurer qu'il est exact avant de fermer l'incident de sécurité. Modifiez les notes ou supprimez-les pour fournir les vôtres.
Résumer un incident de sécurité	Dans le panneau Now Assist, sélectionnez **Résumer un enregistrement**. Le résumé généré dans le panneau est identique à celui que vous générez à partir d'un enregistrement d'incident de sécurité. Les résumés générés par l'IA peuvent manquer des détails clés. Vous préférerez peut-être vérifier l'exactitude et l'exhaustivité du résumé avant de poursuivre.

Applications de surface d'attaque

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

Réponse aux vulnérabilités applications

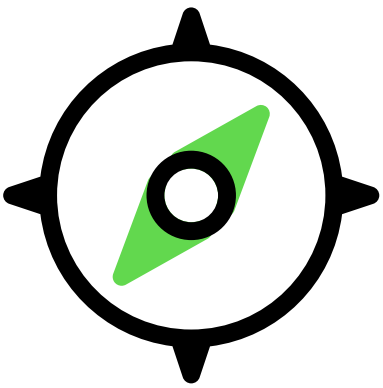
Réponse aux vulnérabilités	Application Vulnerability Response	Conteneur Vulnerability Response
		
En savoir plus sur l'application Vulnerability Response	En savoir plus sur l'application Application Vulnerability Response	En savoir plus sur l'application Container Vulnerability Response

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

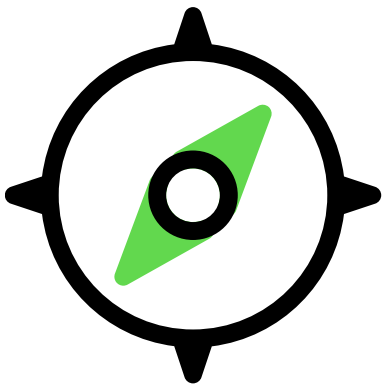
Réponse aux vulnérabilités applications (suite)

Configuration Compliance



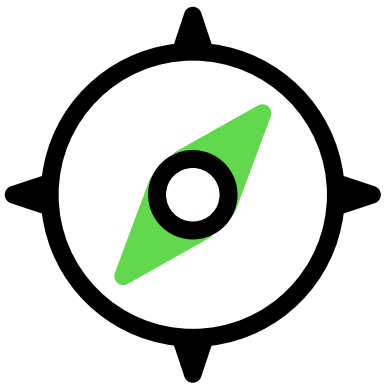
En savoir plus sur l'application Configuration Compliance

Nomenclature logicielle



En savoir plus sur les applications de nomenclature logicielle

Fonctionnalités partagées des applications Vulnerability Response



En savoir plus sur les fonctionnalités partagées entre les applications Vulnerability Response

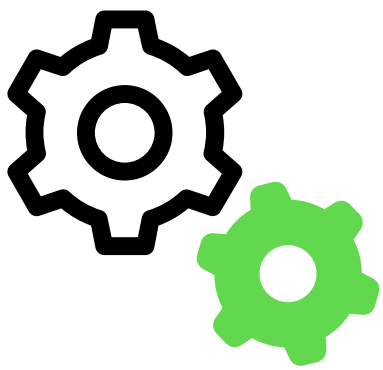
Réponse aux vulnérabilités Espaces de travail

Espace de travail du gestionnaire de vulnérabilité



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

Espace de travail de remédiation informatique



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

Espace de travail de l'évaluation de la vulnérabilité



En savoir plus sur l'espace de travail de l'évaluation de la vulnérabilité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

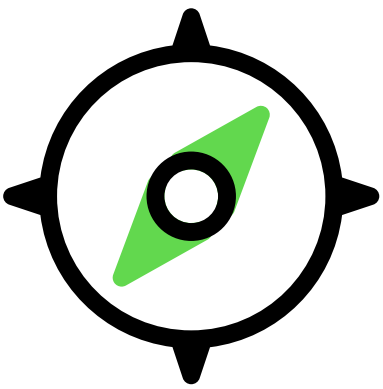
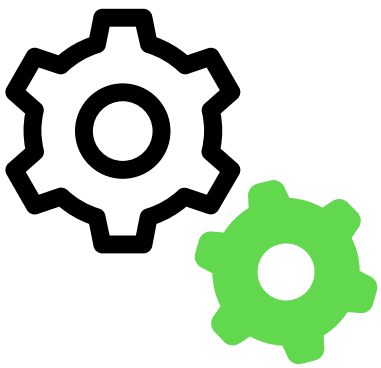
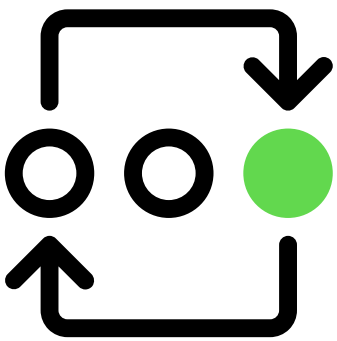
Dépannage et demande d'aide

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

Réponse aux vulnérabilités

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

Réponse aux vulnérabilités

Explorer	Installation et configuration	Intégrer
		
En savoir plus sur les fonctionnalités de Vulnerability Response	Installer et configurer votre application Vulnerability Response	Étendre Vulnerability Response en l'intégrant à d'autres applications

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

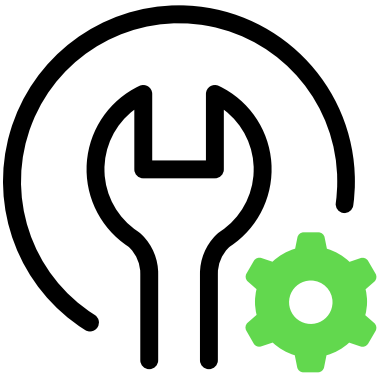
Réponse aux vulnérabilités (suite)

Explorer et utiliser les espaces de travail Vulnerability Response



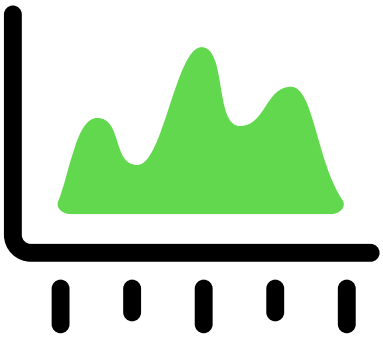
Apprenez à utiliser le Gestionnaire de vulnérabilité et les espaces de travail de remédiation informatique

Corriger



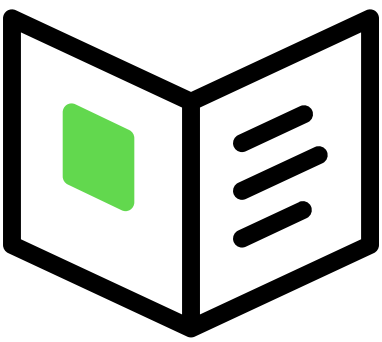
Utilisez les fonctionnalités de Vulnerability Response pour corriger vos vulnérabilités et protéger vos actifs

Analyse et génération de rapports



Surveiller la progression du rattrapage

Référence



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

Traduction automatique

Exploration de l'application Réponse aux vulnérabilités

L'application ServiceNow® Réponse aux vulnérabilités importe et regroupe automatiquement les éléments vulnérables en fonction de règles qui vous permettent de corriger rapidement les vulnérabilités. Les données de vulnérabilité sont extraites de sources

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

externes, telles que la base de données de vulnérabilité nationale (NVD) et des intégrations tierces, et traitées avec des applications développées par ServiceNow®.

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

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

Réponse aux vulnérabilités et l'environnement de votre entreprise

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

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

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

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

- Quelles vulnérabilités identifiées doivent être examinées en premier ?
- Qu'est-ce que ces vulnérabilités identifiées signifient pour notre organisation ?
- Qui doit être responsable des risques identifiés et s'en approprier ?
- Qui devrait mettre la main à la pâte pour résoudre ou atténuer ces risques ?
- Comment pouvons-nous atténuer efficacement les vulnérabilités identifiées avec les ressources dont nous disposons ?
- Quels sont les résultats inattendus potentiels de la réduction des vulnérabilités identifiées ?
- Quel processus suivons-nous pour corriger les vulnérabilités, suivre les étapes que nous avons suivies et assurer un suivi pour nous assurer que nos actions ont fonctionné ?
- Comment pouvons-nous savoir si nous faisons des progrès dans la réduction de notre situation globale en matière de risque ?

Réponse aux vulnérabilités et le Now Platform®

Réponse aux vulnérabilités est l'un des membres de la Opérations de sécurité suite d'applications. Ensemble, ces applications connectent la sécurité à votre service

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

informatique, augmentent la vitesse et l'efficacité de votre réponse et vous donnent une vue définitive de votre posture de sécurité.

Vue d'ensemble des opérations de sécurité

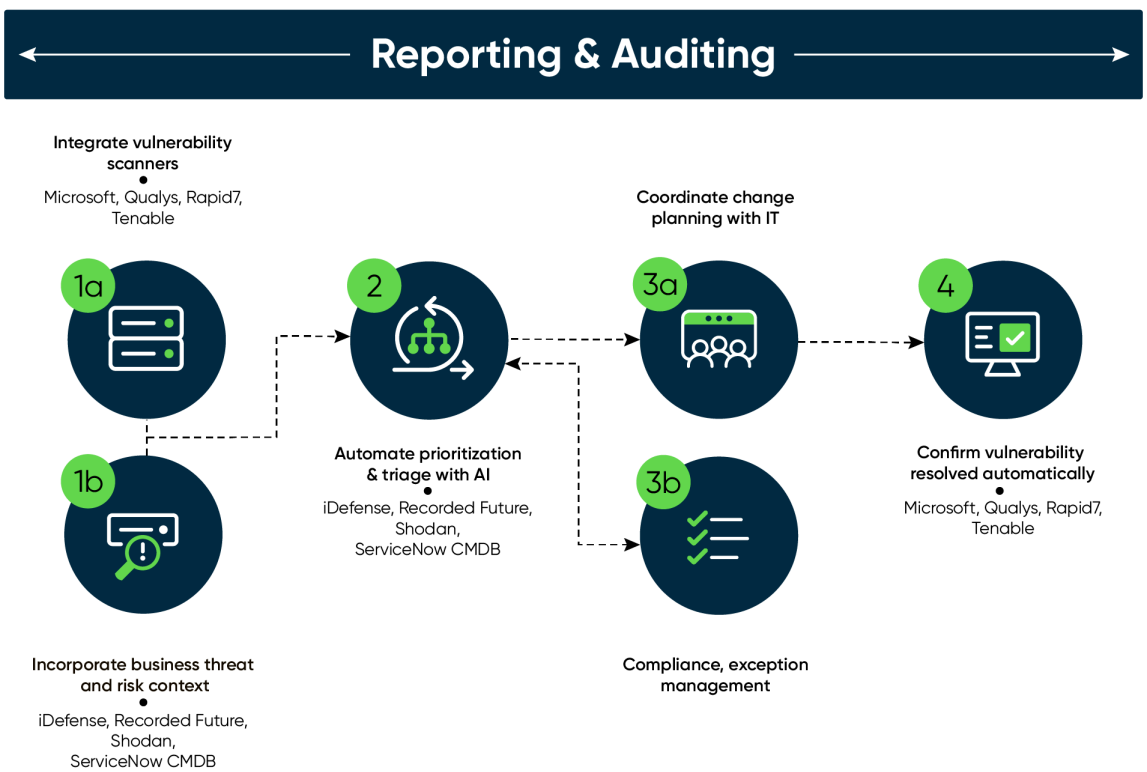


L'application ServiceNow Réponse aux vulnérabilités a deux objectifs principaux :

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

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

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



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

Qui pourrait être utilisé Réponse aux vulnérabilités dans votre organisation

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

Analyste de vulnérabilité

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

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

Propriétaire de la résolution

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

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

Réponse aux vulnérabilités des applications

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

Versions disponibles

Pour obtenir un glossaire des termes et d'autres références qui incluent des liens, des dépannages, des articles de la base de connaissances, ainsi que des données de champ sur

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

les formulaires et les enregistrements trouvés dans , reportez-vous Réponse aux vulnérabilités Informations de référenceà Réponse aux vulnérabilités.

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

Installation et prise en charge des Réponse aux vulnérabilités applications

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

Tâches pour la configuration de base

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

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

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

- Vous pouvez également sélectionner, installer et configurer une ou plusieurs intégrations tierces prises en charge à partir de l'Assistant de configuration. Ces intégrations récupèrent les données de vulnérabilité auprès de systèmes et de fournisseurs externes. Pour en savoir plus sur le fonctionnement des intégrations et sur les intégrations prises en charge par Réponse aux vulnérabilités, reportez-vous à Intégrations de Réponse aux vulnérabilités.
- Avant d'implémenter des intégrations tierces, exécutez la tâche planifiée d'intégration NVD et CWE dans le cadre de votre configuration initiale de Réponse aux vulnérabilités.

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

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

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

- Sélectionner une application de solutions, le cas échéant. Solution Management vous aide à corréler les vulnérabilités de votre environnement avec les solutions susceptibles

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'y remédier. [Facultatif] Installer l'application Gestion des solutions pour Réponse aux vulnérabilités.

Remarque :

- Lorsque l'application Gestion des solutions pour vulnérabilités est activée, les et les Microsoft Security Response Center Solution Integration peuvent être modifiés dans l'Assistant Intégration de solution Red Hat de configuration.
- Gestion des solutions pour vulnérabilités nécessite un abonnement distinct. Pour plus d'informations, consultez Gestion des solutions pour vulnérabilités.

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

Autres tâches de configuration que vous pouvez effectuer

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

Tâches avancées en dehors de la configuration de base

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

Réponse aux vulnérabilités Profils et rôles granulaires

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

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

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

Remarque :

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

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

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous avez déjà attribué des rôles à l'aide de l'Assistant de configuration et que vous souhaitez gérer les affectations de rôles granulaires pour tous les utilisateurs et groupes à partir du module Administration des utilisateurs, reportez-vous à la section Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités pour plus d'informations.

Rôles de profil et rôles granulaires commençant

Termes clés.

Rôle

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

Groupe

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

Rôle de profil

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

Rôles hérités

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

Liste de contrôles d'accès (ACL)

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

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

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

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

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

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

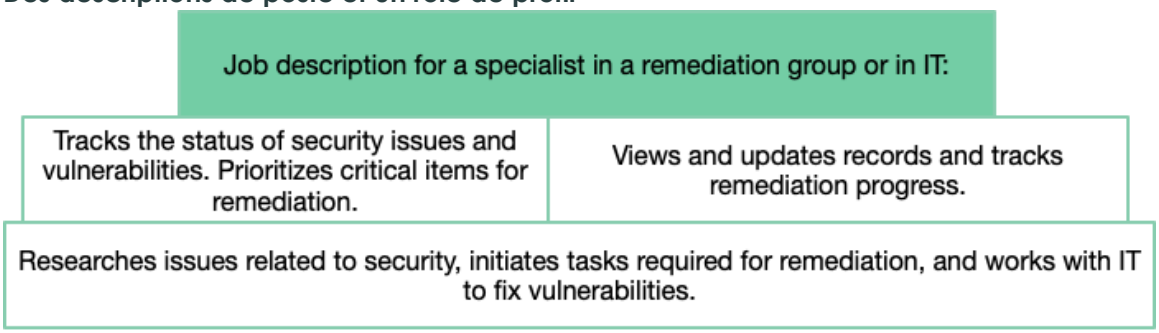
Rôles granulaires et rôles de profil

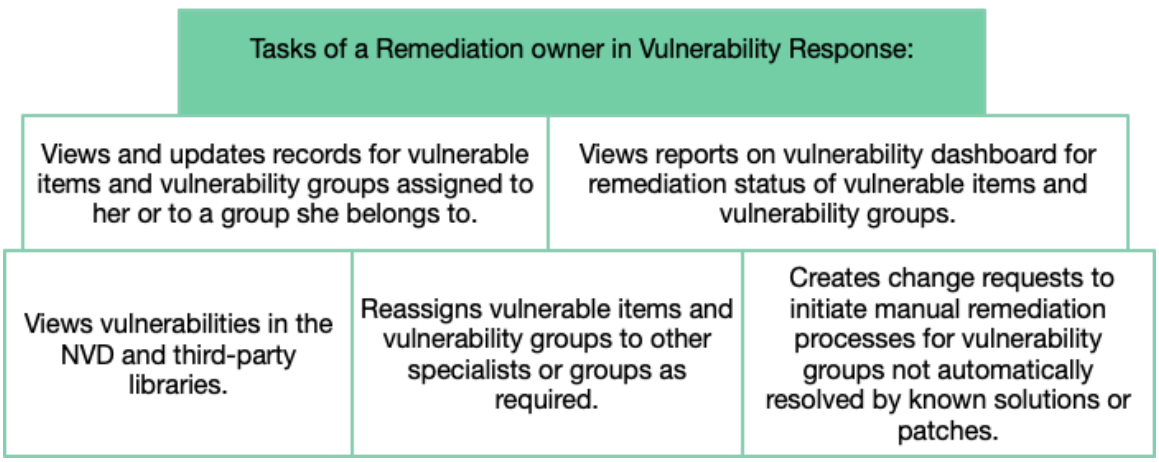
Une façon d'envisager les rôles de persona est d'examiner comment leurs descriptions peuvent être liées aux descriptions de poste pour divers postes informatiques ou de rattrapage de vulnérabilités dans votre organisation. La figure suivante illustre une description de poste possible pour un spécialiste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

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Des descriptions de poste et un rôle de profil





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

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

Les rôles granulaires définissent les tâches

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

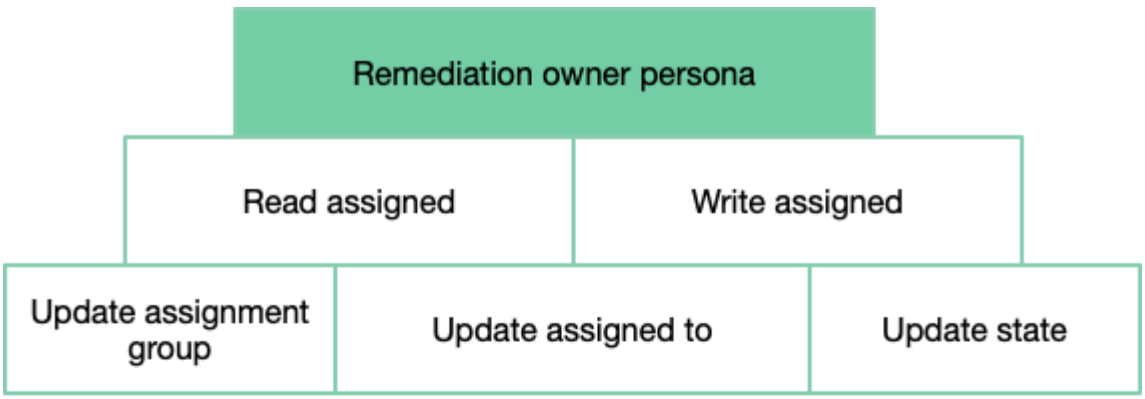
Traduction automatique

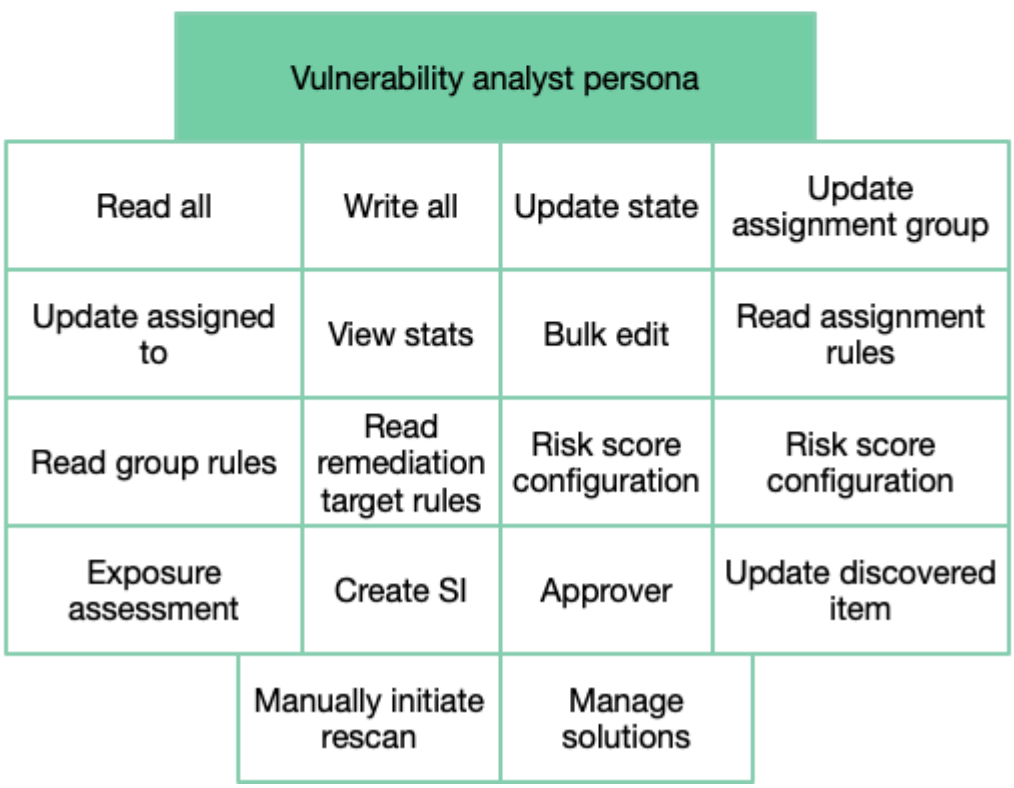
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

localisez le rôle que vous souhaitez. Les rôles qui sont automatiquement hérités lorsqu'un rôle est affecté sont répertoriés. En outre, lorsqu'un rôle dépend d'autres affectations de rôles, tous les rôles requis sont également répertoriés.

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

Rôles granulaires et profils de propriétaire de rattrapage et d'analyste de vulnérabilité





Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

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

Rôles granulaires dans le module Administration utilisateurs

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

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

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

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

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

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

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

Utilisez la règle d'affectation et les informations sur le type d'affectation pour identifier les tickets dans lesquels les règles d'affectation n'ont pas trouvé de correspondance correcte pour le destinataire prévu. Vous pouvez également utiliser ces informations pour identifier les règles ayant le plus de réaffectations.

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

Remarque : Pour rendre Rapid7 InsightVM les balises d'actifs disponibles pour une utilisation dans le filtre de condition des règles d'affectation, vous devez exécuter l'intégration de la Rapid7 InsightVM liste des actifs avant les autres Rapid7 InsightVM intégrations.

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

Affectation automatique des éléments vulnérables

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

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

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

Processus d'évaluation des règles d'affectation

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

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

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

  Une fois que l'élément vulnérable a été affecté, la règle de tâche de rattrapage appropriée utilise l'affectation comme l'un de ses critères pour placer les éléments vulnérables dans une tâche de rattrapage. Voir Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage et Filtrage au sein de Réponse aux vulnérabilités pour plus d'informations.

  Remarque : La règle par défaut est celle dont la valeur d'ordre d'exécution est la plus élevée. Une dernière règle à utiliser qui est un bon fourre-tout est `active=true`. S'il n'y a pas de règle par défaut, le VIT reste non affecté lorsque la règle de tâche de rattrapage effectue l'affectation.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réapplication des règles d'affectation

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

Remarque :

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

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

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

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

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

Pour activer la propriété système :

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

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

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

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

Pour activer la règle métier :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Tout** > **Définition du système** > **Règles métier**.
2. Ouvrez le lien vers la règle métier des tâches de remédiation.
3. Cochez la case **Actif** pour activer la règle métier.

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

Remarque :

- Les éléments vulnérables sont supprimés des groupes sans que ceux-ci ne soient supprimés.
- Seuls les éléments créés à l'aide des règles de tâche de rattrapage ou de l'effort de rattrapage sont supprimés.
- Le regroupement s'effectue automatiquement uniquement lorsque le groupe d'affectation change dans le cadre d'une règle d'affectation et non lorsqu'il est modifié manuellement.

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

Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage

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

Suivi des nombres de reports pour les éléments vulnérables et les tâches de rattrapage

Suivez le nombre de fois où un élément vulnérable, un élément vulnérable d'application, un élément vulnérable de conteneur ou une tâche de rattrapage est différé. Une tâche planifiée, **définie sur les nombres de reports**, s'exécute quotidiennement pour publier les nombres des enregistrements qui sont différés plus d'une fois dans la colonne Nombre de reports. Les enregistrements s'affichent dans les modules Reports multiples pour VR, AVR et CVR.

Actualisation automatique des éléments vulnérables

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

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

Par défaut, lorsque la tâche de rattrapage quitte l'état **Ouvert** , la case n'est pas cochée. Si vous voulez que les éléments vulnérables continuent d'être ajoutés à la tâche de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

rattrapage, quel que soit leur état, désactivez la *Set auto refresh vulnerable items* règle métier.

Vous pouvez cocher à nouveau la case manuellement à partir de l'état En cours d'examen. **La mise à jour automatique des éléments vulnérables connexes** n'est pas désactivée lorsque la tâche de rattrapage passe à l'état **En attente d'implémentation** . Une fois l'état En attente d'implémentation atteint, aucun nouvel élément vulnérable ne peut être ajouté à la tâche existante, et les éléments vulnérables existants ne peuvent pas non plus être supprimés.

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

Actualisation manuelle des éléments vulnérables

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

Les tâches de rattrapage créées manuellement à l'aide des types **de filtres Condition** ou **Groupe de filtres** sont actualisées une fois par heure.

Présentation des règles de tâche de rattrapage

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

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

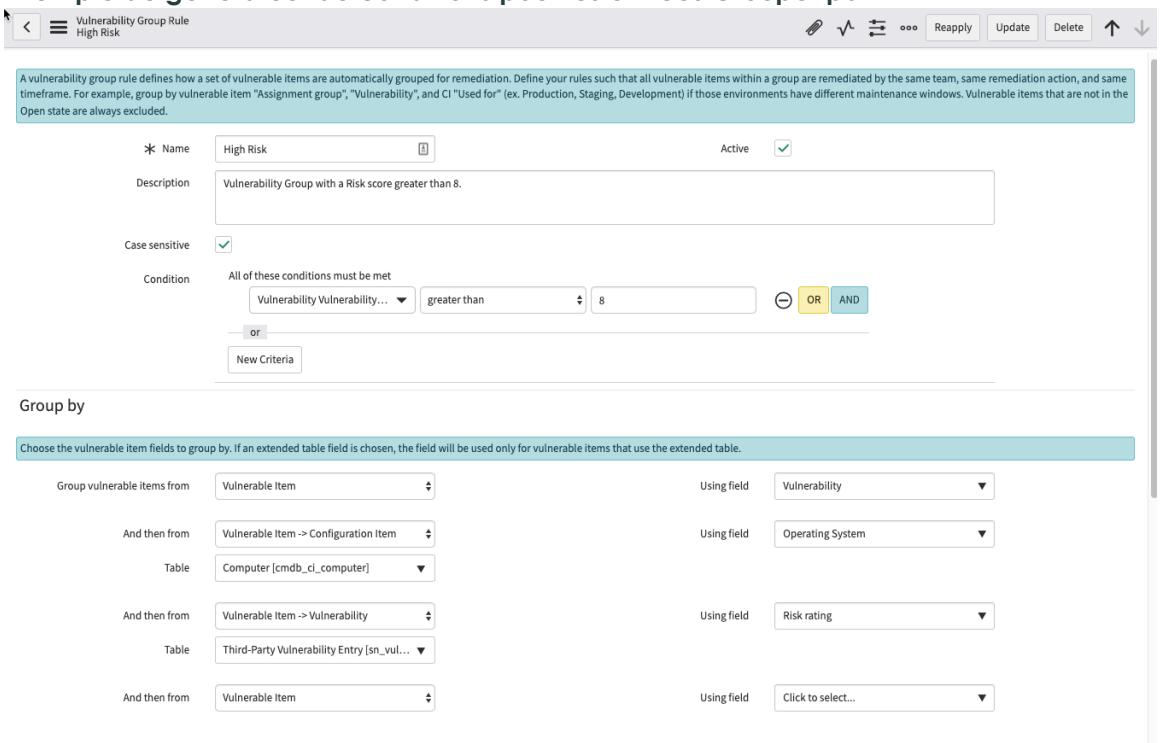
Remarque : Pour rendre Rapid7 InsightVM les balises d'actifs disponibles pour une utilisation dans le filtre de condition pour les règles de tâche de rattrapage, vous devez exécuter l'intégration de la Rapid7 InsightVM liste des actifs avant les autres Rapid7 InsightVM intégrations.

Par exemple, vous pouvez regrouper vos éléments vulnérables par centre de coûts du CI vulnérable ou par vecteur d'attaque de la vulnérabilité. Vous pouvez avoir une règle de tâche pour les vulnérabilités de faible gravité ou les CI à faible risque. Vous pouvez avoir une autre règle de tâche pour les serveurs critiques et les vulnérabilités avec des exploits, c'est-à-dire des éléments vulnérables qui exposent l'entreprise à davantage de risques.

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

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de générateur de conditions pour les entrées Grouper par



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

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

- Pour chaque règle de tâche de rattrapage, le VI est comparé au filtre de règle de tâche de rattrapage.

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

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

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

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

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

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

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

Lorsqu'une règle de tâche est supprimée de la vue de formulaire ou de liste, vous avez la possibilité de supprimer toutes les tâches **ouvertes** créées par cette règle. Les tâches qui ne sont pas **ouvertes** sont exclues.

Réapplication des règles de tâche de rattrapage

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

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

Réponse aux vulnérabilités Règles de cibles de rattrapage

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

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

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

Les analystes et gestionnaires de vulnérabilité peuvent voir la date cible de rattrapage dans le formulaire d'élément de vulnérabilité et les vues de liste, tant que les éléments vulnérables ne sont pas à l'état **Différé**, **Résolu** ou **Fermé** . Les règles de cible de rattrapage sont exécutées lors de l'importation et réexécutées si un VI est rouvert.

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

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

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

Les règles de cibles de rattrapage peuvent être désactivées ou supprimées

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

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

Scénario de règle de cible de rattrapage

Lorsque plusieurs règles de cible de rattrapage sont appliquées au même élément vulnérable, la règle la plus restrictive est appliquée.

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

À partir de la version 17.1, les cibles de rattrapage sont calculées à partir **de la cible à partir de (date).** La valeur par défaut demeure **Date de dernière ouverture**.

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

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

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

Dans ce scénario, la règle de cible de rattrapage 2 s'applique à l'élément vulnérable, car il comporte la date la plus restrictive. 10 jours depuis que l'élément vulnérable a été identifié pour la première fois contre 15 jours.

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

À propos de la tâche planifiée Évaluer les cibles de rattrapage

`Evaluate remediation targets` Fonctionne une fois à 4:00:00 tous les jours.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

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

- ne sont pas dans un état **Fermé**, **Différé** ou **Résolu** .
- N'a pas de date cible de rattrapage.
- Avoir une date cible de rattrapage qui est postérieure à la date indiquée dans la règle de cible de rattrapage.

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

Une fois les *Evaluate remediation targets* exécutions, les notifications disponibles sont envoyées.

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

À partir de la Réponse aux vulnérabilités version 19.0, la propriété, lorsqu'elle *sn_sec_cmn.evaluate_targetmissed_records* est activée, empêche la tâche planifiée d'évaluer les *Remediation Target Rules* VI manqués. Cette propriété est activée par défaut.

Réapplication des règles de cibles de rattrapage

Lorsque vous modifiez une règle de cible de rattrapage, utilisez le bouton **Appliquer les changements** de la page de liste Règles de cibles de rattrapage pour réexécuter toutes les règles modifiées sur tous les VI ouverts actifs, à l'exception de ceux à l'état **Fermé**, **Différé** ou **Résolu** . Selon le nombre d'éléments vulnérables que vous avez, cela peut prendre du temps.

Remarque :

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

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

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

Information associée

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

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

Créer ou modifier des notifications de cibles de rattrapage

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupes et règles de classification de vulnérabilité

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

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

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

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

Remarque :

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

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

Solutions d'apprentissage machine pour Réponse aux vulnérabilités

Recommandations d'affectation de vulnérabilité utilise ServiceNow® Intelligence prédictive l'apprentissage machine pour recommander des groupes d'affectation pour les éléments vulnérables (VI) et les tâches de rattrapage (VUL ou RT). Vous pouvez réduire le temps que vous consacrez à l'identification des propriétaires des résultats de vulnérabilité non affectés ou mal affectés. En outre, vous pouvez afficher un score de confiance généré par le système qui évalue si le groupe d'affectation recommandé est adapté pour résoudre la vulnérabilité.

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

Pour en savoir plus, consultez Intelligence prédictive .

Recommandations d'affectation de vulnérabilité

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

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

Pour en savoir plus, consultez Intelligence prédictive .

Scores de confiance

Utilisez l'application Recommandations d'affectation de vulnérabilité pour générer le score de confiance qui indique le niveau de confiance des groupes d'affectation recommandés pour les RT ou VI sélectionnés. Le score de confiance évalue si le système est convaincu

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que le groupe d'affectation recommandé est apte à résoudre la vulnérabilité. Jusqu'à 10 recommandations s'affichent. Ces recommandations sont basées sur la probabilité la plus élevée de réussite des affectations. La première recommandation de la liste signifie que le système a la plus grande confiance dans le fait qu'il s'agit du bon groupe d'affectation.

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

Information associée

- Intelligence prédictive
- Créer et former une solution de classification
- Créer et former une solution de similarité
- Créer et former une solution de mise en grappe
- Configuration des paramètres avancés pour vos solutions ML

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

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

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

Au fur et à mesure que les actifs sont importés, une recherche est d'abord effectuée sur la liste **des éléments détectés** à l'aide d'ID tiers pour trouver des correspondances avec des éléments de configuration (CI) à partir d'importations précédentes. Lorsqu'une correspondance d'ID d'hôte est trouvée, elle est utilisée comme champ **d'élément de configuration** dans l'enregistrement d'élément vulnérable.

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

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

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

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

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Pour éviter toute correspondance sur des éléments de réseau de bas niveau, si un CI correspondant est l'un des `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic` ou `cmdb_ci_ip_address`, le CI parent est renvoyé.

Une propriété système permettant d'exclure les classes CI est disponible. Cette propriété n'est pas disponible avec la mise à niveau. Consultez la section Ignorer les classes CI pour obtenir des informations sur la mise à niveau et des instructions sur la définition de la propriété.

Pour faciliter la recherche de problèmes correspondants, lorsqu'une correspondance est trouvée, la règle de recherche de CI utilisée pour la trouver est ajoutée à l'enregistrement d'élément détecté dans le champ **Règle de correspondance de CI** . Les règles de recherche sont évaluées en fonction de la valeur **d'ordre** la plus basse en premier.

Ces Qualys règles de recherche de CI sont fournies avec le système de base.

- ID D'HÔTE QUALYS
- FQDN
- NetBIOS
- DNS
- IP

Ces Rapid7 règles de recherche de CI sont fournies avec le système de base.

- MacAddress
- FQDN
- Nom d'hôte
- IP

Ces règles de recherche de CI Tenable.io sont fournies avec le système de base.

- FQDN
- NETBIOS
- NOM D'HÔTE
- MacAddress
- DNS

Ces règles de recherche de CI Tenable.sc sont fournies avec le système de base.

- MacAddress
- FQDN
- NETBIOS

Remarque : Les règles, une fois supprimées, ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

L'importation de données de vulnérabilité peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas soigneusement construites. La logique utilisée pour itérer et effectuer une correspondance au sein de peut CMDB entraîner de longs délais de traitement. Pour éviter toute dégradation potentielle des ressources ou toute complication des performances, testez les règles de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

recherche de CI écrites sur mesure ou les modifications apportées aux **règles de recherche de CI prédéfinies**. Pour plus d'informations sur la prévention des enregistrements orphelins en double, la suppression des données et le nettoyage des données, consultez la rubrique Étapes pour empêcher les enregistrements en double ou orphelins après l'exécution de Réponse aux vulnérabilités règles de recherche de CI .

Remarque : Pour plus d'informations sur la correspondance des CI, reportez-vous à la section KB0998706 .

Réapplication des règles de recherche de CI mises à jour

Lorsque vous modifiez une règle de recherche de CI, cliquez sur **Appliquer les changements** sur la page de liste Règles de recherche de CI pour réexécuter toutes les règles sur les éléments détectés qui :

- Ont été appariés par les règles mises à jour
- Ne sont assortis à aucune règle

Si l'élément de configuration (CI) change après la réapplication des règles de recherche, les éléments détectés sont mis à jour avec le nouveau CI. Les détections impactées et les éléments vulnérables sont également mis à jour. Pour plus d'informations, reportez-vous à la section Réappliquer des règles de recherche de CI sur les éléments détectés sélectionnés.

Matériel non classé

Si un actif ne trouve pas de correspondance dans les règles de Base de données de gestion des configurations (CMDB) recherche par CI, il est qualifié de matériel non classé.

Lorsque des données sont importées à partir d'intégrations ServiceNow créées, Réponse aux vulnérabilités les données de l'hôte sont automatiquement utilisées pour rechercher des correspondances dans le CMDBfichier . Les règles de recherche de CI sont utilisées pour identifier les éléments de configuration (CI) et les ajouter à l'enregistrement d'élément vulnérable pour faciliter la correction. Si les actifs sont introuvables dans le CMDB, le moteur Identification et réconciliation (IRE) exécute ses propres règles d'identification définies sur la classe de matériel et tous ses enfants, et crée un CI dans une classe de matériel non classé. Lorsqu'il Découverte trouve cet actif, au lieu de reclasser le matériel non classé existant, il crée un CI. Cela est dû au fait que la règle d'identification repose sur le nom du CI matériel.

Si le moteur Identification et rapprochement (IRE) est activé, l'option de reclassification à partir des éléments détectés n'est pas prise en charge.

Les extraits suivants montrent la charge utile IRE pour la création d'un CI dans Unclassed Hardware via Réponse aux vulnérabilités et Découverte respectivement.

```
"className": "cmdb_ci_unclassed_hardware",

"values": {
        "name": "asset01.company.com",//from NetBios,
        "mac_address": "1a:5e:2c:0e:42:f3",
        "fqdn": "asset01.company.com",
        "ip_address": "133.10.3.123"
    }

"settings": {
        "updateWithoutSwitch": true
    }
```

```
"className": "cmdb_ci_cmdb_ci_win_server"
```


© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
"values": {
        "name": "asset01",
        "mac_address": "1a:5e:2c:0e:42:f3",
        "fqdn": "asset01.company.com",
        "ip_address": "133.10.3.123",
        "os_domain": "company"
    }

"settings": {
        "updateWithoutSwitch": false
    }
```

Dans ce cas, le CI matériel non classé existant n'est pas reclassé dans le serveur Windows, mais un nouveau CI sous le serveur Windows est créé. Cela s'explique par le fait que la règle d'identification repose sur le nom du CI matériel. Si vous remarquez les charges utiles, le nom dans la charge utile à partir de Réponse aux vulnérabilités est le même que FQDN/NETBIOS, mais il s'agit simplement du nom d'hôte de la charge utile à partir de Découverte.

Information associée

Reclassifier le matériel non classé

Ci sans correspondance

Les éléments de configuration (CI) sont automatiquement mis en correspondance avec les CI lorsqu'ils Base de données de gestion des configurations (CMDB) sont importés. Par défaut, l'option **Security Operations** > **CMDB** > **Éléments détectés** répertorie les éléments de configuration sans correspondance.

Si vous pensez qu'un CI sans correspondance appartient à une classe existante dans la CMDB, passez en revue vos règles de recherche de CI. Sinon, envisagez de reclassifier l'élément de configuration.

Remarque : Le filtre par défaut de cette liste est défini sur **Sans correspondance**. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Si le moteur Identification et rapprochement (IRE) est activé, l'option de reclassification à partir des éléments détectés n'est pas prise en charge.

Information associée

Afficher et reclasser des éléments de configuration sans correspondance

Rapprocher les éléments détectés sans correspondance

Étapes pour empêcher les enregistrements en double ou orphelins après l'exécution de Réponse aux vulnérabilités règles de recherche de CI

Déduplication d'éléments de configuration existants

Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement

Vous pouvez créer des éléments de configuration (CI) dans le Base de données de gestion des configurations (CMDB) à l'aide de l'API du moteur Identification et réconciliation (IRE). En utilisant l'API IRE pour créer des CI, vous pouvez empêcher la création de CI en double et vous pouvez rapprocher les attributs de CI en autorisant uniquement les sources de données de référence à écrire vers CMDB.

Une classe CI (table) est le nom de table d'origine dans la base de données de l'instance. CMDB contient des classes système de base qui stockent des données sur les CI.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation d'IRE pour la création de CI

Avant la Réponse aux vulnérabilités version 12.2, si un CI correspondant n'est pas trouvé dans la liste des éléments détectés ou CMDB, un CI est créé dans la classe de CI sans correspondance (`sn_sec_cmn_unmatched_ci`). Pour plus d'informations, consultez CI sans correspondance.

À partir de la version 12.2 et de Réponse aux vulnérabilités la version 18.0, si aucune correspondance n'est trouvée lors de l'application des règles de recherche de CI, les informations sur l'actif sont envoyées à IRE et un CI est créé dans l'une des classes *`Matériel non classé`* et *`Appareil identifié IP incomplète`*. À partir de la Réponse aux vulnérabilités version 18.0, une nouvelle classe, *`Cloud Resource`*, est également incluse. Pour en savoir plus sur la configuration de la catégorisation des ressources cloud inégalées dans votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

CMDB Classes CI

Remarque : Pour utiliser les nouvelles classes, activez le module d'extension Modèles de CMDB classes CI. Dans le cas contraire, les CI sont créés dans la classe CI sans correspondance.

Si l'hôte que vous avez importé à partir d'un scanner tiers est introuvable dans la liste des éléments détectés ou CMDBs'il est créé dans l'une des nouvelles CMDB classes CI suivantes.

CMDB Classes CI

CMDB **Classe CI**	**Description**
Adresse IP incomplète de l'appareil identifié (*`cmdb_ci_incomplete_ip`*)	Le CI est créé dans cette table si seule l'adresse IP est disponible dans les informations d'hôte reçues de l'analyseur.
Matériel non classé (*`cmdb_ci_unclassed_hardware`*)	Le CI est créé dans cette table si l'une des informations suivantes est disponible dans les informations de l'hôte reçues du scanner : • Nom d'hôte • Adresse IP • DNS • NETBIOS • Adresse MAC **Remarque :** Si l'adresse MAC est disponible, l'entrée de la carte réseau est créée et associée au CI matériel non classé. Si les adresses IP et MAC sont disponibles, le CI d'adresse IP est également créé et associé au CI matériel non classé.
Ressource dans le cloud (*`cmdb_ci_cmp_resource`*)	Le CI est créé dans cette table s'il *`Cloud Resource ID`* est disponible dans les informations d'hôte reçues du scanner.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

CMDB Classes CI (suite)

CMDB **Classe CI**	**Description**
	Remarque : Si le type d'actif d'une intégration de scanner est *hybride* et que la *sn_sec_cmn.unmatched_cloud_resource_enabled* propriété système est false, les CI sont créés dans la classe *de matériel non classé*, mais pas dans la classe *de ressources cloud*.

Si le moteur Identification et rapprochement (IRE) est activé, l'option de reclassification à partir des éléments détectés n'est pas prise en charge.

Le système utilise automatiquement une classe CI sans correspondance si l'une des situations suivantes se produit :

- Le CMDB module d'extension Classe CI n'est pas activé.
- IRE lève une exception lors de la création d'un CI.

  Pour plus d'informations, consultez CI sans correspondance.

Information associée

Application de stockage CMDB CI Class Models

Moteur Identification et réconciliation (IRE)

Mise à jour de la classe CI pour les actifs cloud sans correspondance

À partir de la Réponse aux vulnérabilités version 20.0, vous pouvez classer les actifs cloud sans correspondance des Qualysscanners , Rapid7 et Tenable dans la catégorie *Matériel non classé* à l'aide de la *sn_sec_cmn.unmatched_cloud_resource_enabled* propriété système.

Cette propriété système dont la valeur par défaut est « `faux` » est fournie avec le système de base. Elle classe les actifs cloud sans correspondance dans une classe *de matériel non classé* (*cmdb_ci_unclassed_hardware*) ou *de ressource dans le cloud* (*cmdb_ci_cmp_resource*) pour les intégrations qui apportent à la fois des actifs d'infrastructure et de cloud.

À partir de la Réponse aux vulnérabilités version 20.0, la colonne Type d'actif est ajoutée à la table Intégrations tierces (`sn_sec_int_integration`) pour identifier les intégrations qui prennent en charge à la fois les actifs d'infrastructure et de cloud. La colonne Type d'actif a la valeur *Hybride* pour les scanners qui importent à la fois des actifs d'infrastructure et de cloud. Par exemple, Qualysles intégrations , Rapid7 et Tenable ont la valeur *Hybride* dans la colonne Type d'actif.

- Pour la nouvelle installation de v20.0 et versions ultérieures Réponse aux vulnérabilités , tous les actifs dans le cloud sans correspondance sont classés comme suit :
  - *Classe de matériel non classé* par défaut.
  - *Cloud Resources*, si vous remplacez la *sn_sec_cmn.unmatched_cloud_resource_enabled* propriété système par `true`.
- Pour les mises à niveau vers Réponse aux vulnérabilités la version 20.0 :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si la classe *de ressources dans le cloud* comprend des actifs, la propriété système *sn_sec_cmn.unmatched_cloud_resource_enabled* est définie sur vrai afin que les actifs cloud sans correspondance continuent de s'ajouter à la classe *de ressources dans le cloud* (*cmdb_ci_cmp_resource*).
- Dans le cas contraire, la propriété système *sn_sec_cmn.unmatched_cloud_resource_enabled* est définie sur false afin que les actifs cloud sans correspondance soient classés dans la classe *Matériel non classé*.

Remarque : Si vous modifiez la valeur de la *sn_sec_cmn.unmatched_cloud_resource_enabled* propriété système, assurez-vous de supprimer les éléments de configuration sans correspondance sur la classe CI précédemment ciblée, puis réappliquez les règles de recherche. Pour en savoir plus sur la façon de supprimer les CI existants et de réappliquer des règles de recherche de CI afin que les nouveaux CI soient créés dans la classe appropriée, consultez KB1533376 .

Éléments détectés

Les actifs sont automatiquement mis en correspondance avec des éléments de configuration (CI) dans lorsqu'ils Base de données de gestion des configurations (CMDB) sont importés à l'aide des **règles de recherche de CI**. Les éléments détectés vous donnent une visibilité sur la façon dont l'identification des actifs est mappée aux CI dans le CMDB.

Les éléments détectés sont considérés comme **correspondants**, **sans correspondance** ou **reclassés**. Les CI identifiés sont dans l'état **En correspondance** .

Pour faciliter la recherche de problèmes de correspondance potentiels, la règle de recherche de CI correspondant au CI apparaît dans le champ **Règle de correspondance de CI** .

Par défaut, l'option **Security Operations** > **CMDB** > **Éléments détectés** Liste les éléments de configuration sans correspondance. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour obtenir une description des champs dans Éléments détectés, reportez-vous à la section Champs du formulaire Éléments détectés. Pour plus d'informations sur le rapprochement des éléments détectés sans correspondance et la réapplication des règles de recherche de CI sur les éléments détectés sélectionnés, consultez Rapprocher les éléments détectés sans correspondance respectivement et Réappliquer des règles de recherche de CI sur les éléments détectés sélectionnés

Changements de CI pour les éléments détectés

Lorsqu'un élément de configuration (CI) sur un élément détecté (DI) change, les détections impactées et les éléments vulnérables (VI) sont mis à jour. Le score de risque, les règles d'affectation, les règles de groupe et la règle de cible de rattrapage sont réévalués.

Si un VI existe avec la même vulnérabilité et le même CI, les détections sont mises à jour avec le VI existant et le VI actuel est fermé avec le sous-état `invalidCI`. Des notes de travail sont ajoutées pour les raisons suivantes :

- Lorsque les détections sont déplacées d'un VI à un autre.
- Lorsqu'un VI en double est fermé.

Si vous ne souhaitez pas mettre à jour le CI pour le VI existant, définissez la propriété `sn_sec_cmn.update_on_ci_change` sur `faux`. Ensuite, lorsqu'un CI change, un nouveau VI est créé et l'élément existant est fermé en tant que `CI non valide`.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La valeur par défaut de la propriété `sn_sec_cmn.update_on_ci_change` est `vrai`.

Réévaluation des éléments détectés

Lorsque de nouvelles données sont reçues sur un élément détecté, l'élément détecté n'est pas immédiatement réévalué. Lors de la réception de nouvelles données, l'option *`reevaluate_ci`* est définie sur *`true`* Par défaut.

La tâche *`Re-apply CI Lookup Rules on the Changed Discovered items`* planifiée évalue tous les éléments détectés dont les données sources sont en cours de modification par le scanner. Il traite à nouveau les éléments détectés et met à jour les éléments vulnérables liés à l'élément détecté dont les données sources sont modifiées. La valeur de cette tâche planifiée est *`On Demand`* par défaut.

Remarque : Vous pouvez également choisir d'exécuter cette tâche planifiée quotidiennement.

Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables

Avec l'application Réponse aux vulnérabilités , vous pouvez utiliser le modèle d'état pour afficher l'état d'une tâche de rattrapage, à tout moment. Savoir comment chaque état est lié et s'affecte les uns les autres vous aide à déterminer quand et comment corriger vos éléments vulnérables (VI).

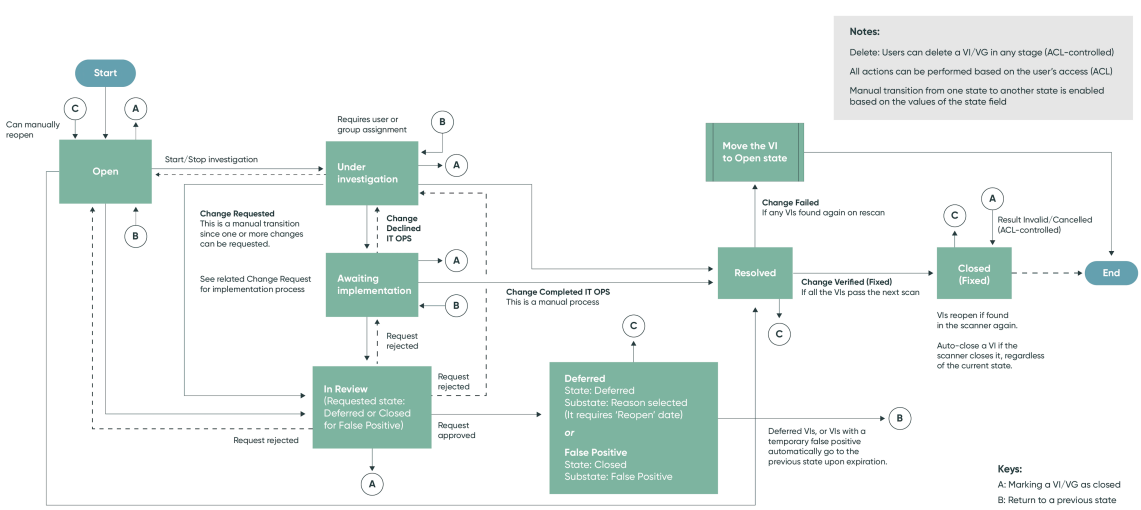
États des tâches de résolution

Des cas d'utilisation complexes peuvent parfois entraîner un élément vulnérable dans un état différent de celui de sa tâche de correction. Comprendre le fonctionnement des états permet d'expliquer ce comportement et peut aider à créer des tâches de rattrapage et à créer ou modifier des règles de tâches de rattrapage.

Remarque : À partir de la version 23.0 de , le workflow **Approbation de l'état de l'élément vulnérable** est déconseillé et remplacé par le flux Changement de l'état d'approbation de Réponse aux vulnérabilitésla vulnérabilité dans le concepteur de flux.

Les tâches de rattrapage ont de nombreux états possibles, comme le montre le diagramme suivant.

Flux d'état Vulnerability Response



Remarque : Chaque formulaire de tâche contient des boutons **Suivre** et **Mettre à jour** qui sont standard pour ServiceNow les tâches.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les états de la tâche de rattrapage et les actions que vous pouvez effectuer sur celle-ci dans un état respectif, reportez-vous à la section Réponse aux vulnérabilités États des tâches de résolution.

Pour plus d'informations sur les états des détections, des tâches de rattrapage et des éléments vulnérables, reportez-vous à la section États des détections, des tâches de rattrapage et des éléments vulnérables.

Pour plus d'informations sur la tâche de rattrapage et les états des VI, consultezTâches de rattrapage et états des éléments vulnérables .

Pour plus d'informations sur l'état de la tâche de rattrapage pour les VI de plusieurs groupes, reportez-vous à la section État de la tâche de rattrapage pour les éléments vulnérables (VI) dans plusieurs groupes.

Calcul et affichage de l'âge de l'élément vulnérable

L'âge des éléments vulnérables (VI) est affiché dans l'application Réponse aux vulnérabilités avec plus de détails.

Vue d'ensemble

L'âge de l'élément vulnérable (VI) est affiché au format Jours/heures/Minutes dans la colonne Âge de la vue de liste Éléments vulnérables et dans les champs Âge et Âge fermé des enregistrements VI (VIT). L'âge affiché en chiffres plus significatifs peut vous aider à effectuer les activités suivantes avec plus de précision :

- Configurez des règles dans le module Règles de suppression automatique pour cibler et supprimer des enregistrements de VI spécifiques par jours/heures/minutes. La suppression d'enregistrements avec plus de précision peut augmenter vos performances, en particulier si vous avez un grand nombre d'enregistrements de VI dans votre instance.
- Affichez les rapports contenant des détails plus spécifiques dans Analyse des performances pour l'application Réponse aux vulnérabilités .
- Créez des filtres qui identifient uniquement les VI souhaités.
- Élaguez les vues de listes pour afficher uniquement les VI souhaités.
- Remontée pas à pas plus facilement.

Une tâche planifiée a calculé l'âge et mis à jour tous les VI actifs. Dans les instances avec un grand nombre d'enregistrements de VI, ce processus peut être lent et avoir un impact négatif sur les performances. L'âge VI est calculé plus efficacement à la demande et affiché avec des chiffres plus significatifs avec une colonne Âge améliorée. La colonne Âge améliorée est automatiquement ajoutée lorsque vous installez ou mettez à niveau l'application Réponse aux vulnérabilités .

Remarque : Si vous effectuez une mise à niveau et que l'âge de la VI n'est pas affiché dans la vue de liste des éléments vulnérables et dans les champs Âge et Âge fermé des enregistrements de VI actifs (VIT) au format Jours/heures/Minutes (9 jours, 18 heures, 29 minutes), la colonne Âge n'est pas à jour dans votre instance. Pour en savoir plus sur la résolution de ce problème après une mise à niveau, consultez KB0749231 .

La colonne Âge et les champs ne sont pas modifiables. Un gestionnaire de vulnérabilités ayant l'autorisation sn_vul.vulnerability_read ou le profil d'administrateur de vulnérabilité peut voir cette valeur, et les propriétaires de rattrapage informatique disposant du rôle sn_vul.remediation_owner peuvent l'afficher sur les enregistrements qui leur sont affectés.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

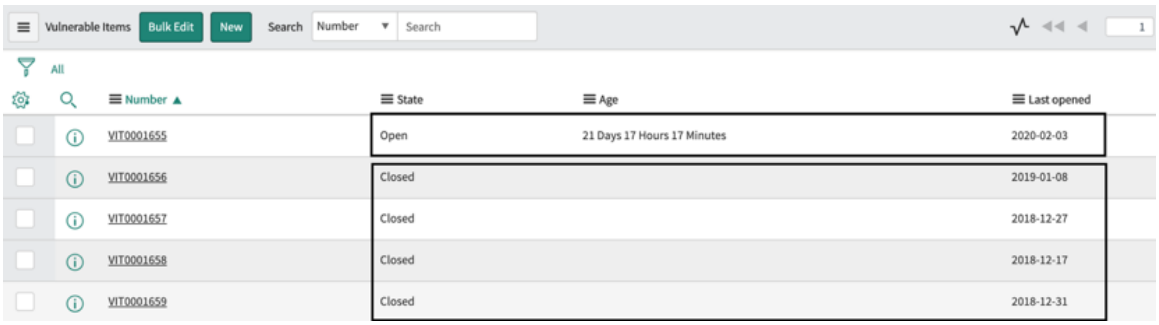
Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

L'âge VI est affiché comme illustré dans les images suivantes.

Liste des éléments vulnérables

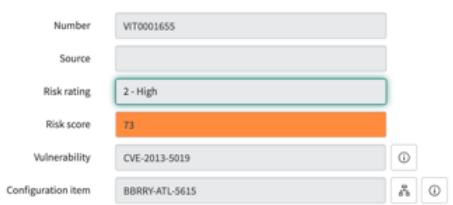
Comme le montre la figure suivante, dans la vue de liste Éléments vulnérables, l'âge est affiché dans la colonne Âge en jours/heures/minutes (21 jours 17 heures 17 minutes) uniquement pour les VI actifs. Les VI actifs sont des VI dans un état autre que « Fermé ». Cette valeur d'âge représente le nombre de jours pendant lesquels le VI a été actif.

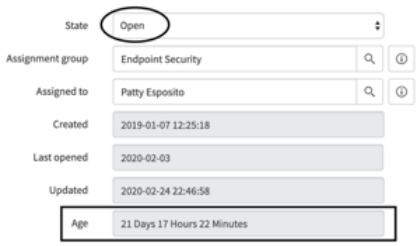
L'âge n'est pas affiché pour les VI à l'état « Fermé ». Pour les VI précédemment à l'état « Fermé » puis rouverts, la valeur représente le nombre de jours pendant lesquels le VI a été actif depuis la date de sa dernière ouverture.



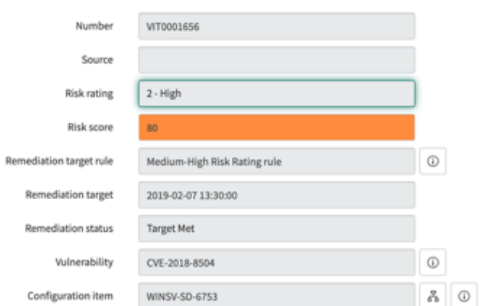
Âge sur les enregistrements de VI

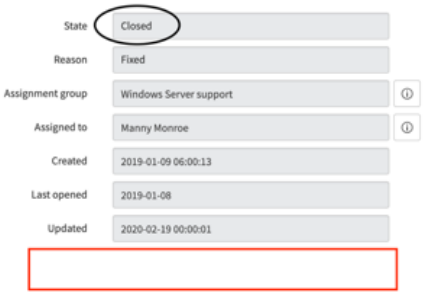
Sur les enregistrements de VI, la valeur de la colonne Âge dans la vue de liste est visible pour les VI actifs dans le champ Âge.





La valeur de la colonne Âge ne s'affiche pas pour les enregistrements de VI à l'état « Fermé ».



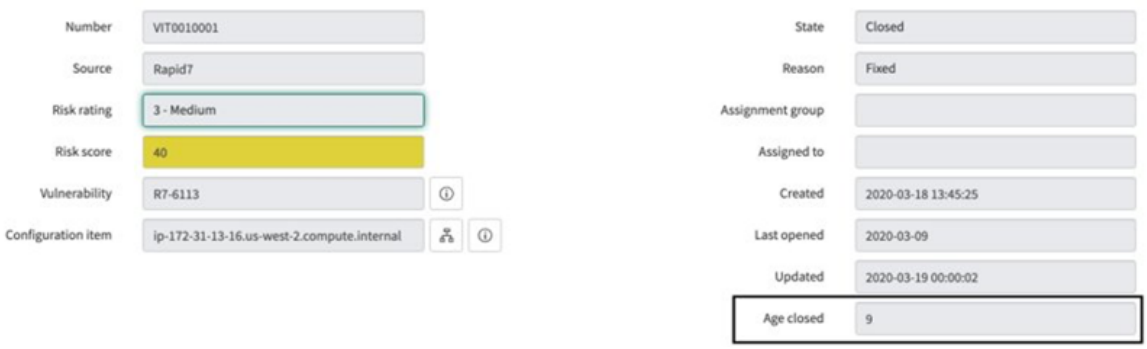


Traduction automatique

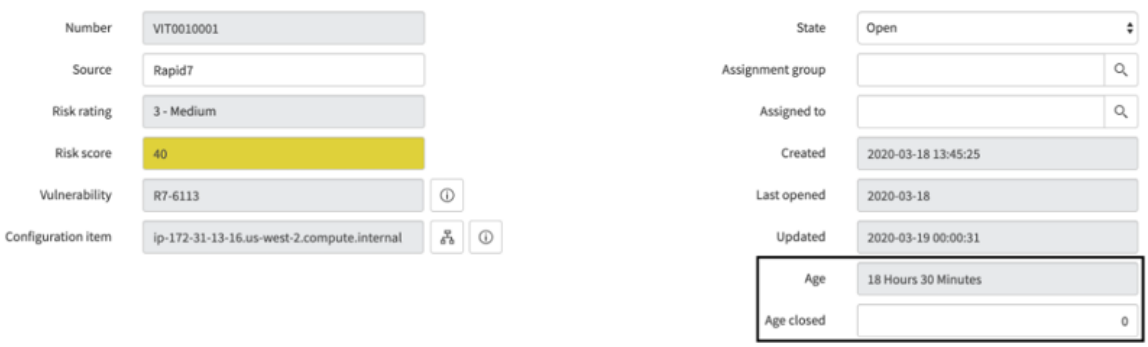
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Âge sur la liste des éléments vulnérables et les enregistrements de VI lorsqu'un VI est mis à jour

Lorsqu'un VI est à l'état « Fermé », le champ Âge n'est pas affiché. Lorsque le VI passe à l'état « Fermé », la valeur en nombre de jours à partir de la colonne Âge s'affiche dans le champ Fermé par âge (9), comme illustré dans la figure suivante. Cette valeur représente le nombre de jours pendant lesquels le VI a été actif avant de passer à l'état « Fermé ». Par exemple, dans l'image suivante, ce VI a été actif pendant 9 jours, 18 heures et 29 minutes, mais seul le nombre de jours (9) est affiché sur l'enregistrement fermé.



Si ce VI est rouvert, lorsque l'état du VI repasse à « Ouvert », le champ Âge fermé est réinitialisé à 0. Étant donné que le VI est à nouveau actif, l'âge en jours/heures/minutes s'affiche dans la vue de liste dans la colonne Âge et dans le champ Âge du VIT.



Suppression des affectations des éléments vulnérables et des tâches de rattrapage

Vous pouvez effacer les champs Affecté à et **Groupe d'affectation** des éléments vulnérables directement à partir des enregistrements d'élément vulnérable (VIT) et de tâche de rattrapage qui, selon vous, pourraient être affectés de manière incorrecte à vous ou à vos groupes.

Vue d'ensemble

À partir de la version 16.5, les propriétaires de rattrapage peuvent mettre à jour les enregistrements pour la réaffectation à l'aide du bouton **Annuler l'affectation** dans Réponse aux vulnérabilités les Réponse aux vulnérabilités des applications applications.

Cas d'utilisation

Si vous déterminez que les VI ne sont pas dans votre champ d'application pour le rattrapage, ou si vous pensez que les enregistrements ont été affectés de manière incorrecte à vous ou à vos groupes, vous pouvez vous retirer, vous ou vos groupes, des champs Affecté à et **Groupe d'affectation** sur les enregistrements d'éléments vulnérables et de tâches de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désaffecter le module

Le bouton **Annuler l'affectation** s'affiche sur les enregistrements suivants dont l'état n'est pas Fermé ou Résolu :

- Tâches de remédiation (VUL) dans l'environnement classique et les Réponse aux vulnérabilités espaces de travail. Si une tâche de rattrapage est mise à jour avec cette fonctionnalité, les champs **Affecté à** et **Groupe d'affectation** de tous ses VI associés sont également effacés.
- Éléments vulnérables (VIT) dans l'environnement classique et les Réponse aux vulnérabilités espaces de travail.
- Éléments vulnérables de l'application (AVIT).

Tous les enregistrements que vous mettez à jour à l'aide du bouton d'interface utilisateur ou manuellement sont affichés dans le module Non affecté sous leurs modules respectifs.

Pour savoir comment réaffecter des enregistrements à l'aide de l'action d'interface utilisateur, reportez-vous à la *Unassigned*section Supprimer les affectations des éléments vulnérables.

Modifier en bloc

Vous pouvez effacer les champs d'affectation de plusieurs VI d'une liste. Une fois que vous avez sélectionné les VI et sélectionné **Modifier en bloc**, dans la boîte de dialogue qui s'affiche, cochez la case **Annuler l'affectation** .

Propriété système et notifications

Si vous êtes un administrateur disposant du rôle sn_vulc.vulnerability_admin, lorsque vous cliquez sur **Annuler l'affectation** d'un enregistrement, par défaut, la *sn_vul.unassign_vr.approval_required*propriété système déclenche le flux d'approbation et crée un enregistrement d'approbation de changement d'état à l'état Révision et une demande d'approbation est émise pour l'approbateur qui s'affiche dans la liste **Mes approbations** .

> **Remarque :** En tant qu'administrateur de vulnérabilité, vous pouvez définir la *sn_vul.unassign_vr.approval_required*propriété système sur **false** pour désactiver le processus d'approbation.

- Si l'approbateur approuve la demande, *sn_vul.default_assignment_group* il efface les champs **Affecté à** et **Groupe d'affectation** et renseigne le **champ Type d'affectation** avec **Non affecté.** En tant qu'administrateur de vulnérabilité, vous pouvez modifier la valeur de la *sn_vul.default_assignment_group* propriété système afin que les champs d'affectation soient effacés et qu'un groupe spécifique soit ensuite affecté. Par exemple, si un utilisateur clique sur **Annuler l'affectation** d'un enregistrement et que vous souhaitez le rediriger vers un groupe spécifique pour révision, vous pouvez ajouter un ID système pour le groupe de votre choix dans le champ de valeur de la propriété système.

  > **Remarque :** Si vous modifiez cette valeur, les notifications de tous les VI, AVIT et CVIT qui ne sont pas affectés sont envoyées au groupe que vous spécifiez.

- Si l'approbateur rejette votre demande, le motif du rejet s'affiche dans l'onglet **Notes** .

S'il *sn_vul.default_assignment_group* n'est pas configuré pour un groupe spécifique, par défaut, les utilisateurs que vous ajoutez au groupe d'utilisateurs de notification Annuler l'affectation sont avertis lorsque les enregistrements ne sont pas affectés. La

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sn_vul.default_assignment_group propriété système détermine les notifications envoyées à ce groupe.

Le type d'affectation, qu'il soit **manuel**, **de règle** ou **non affecté**, est disponible dans les enregistrements de VI et la vue de liste. Le type **d'affectation non affecté** s'affiche dans les enregistrements une fois que les champs **Affecté à** et **Groupe d'affectation** sont effacés par la propriété système de la fonctionnalité.

Surveillance de vos règles d'affectation avec la tâche planifiée pour cette fonctionnalité

Une tâche planifiée quotidienne compte les enregistrements lorsqu'ils passent au type **d'affectation Non affecté** . Grâce à ce nombre, les analystes de vulnérabilité peuvent surveiller et ajuster toutes les règles d'affectation susceptibles de ne pas être performantes en fonction des règles d'affectation qui ont un nombre plus élevé de VI non affectés.

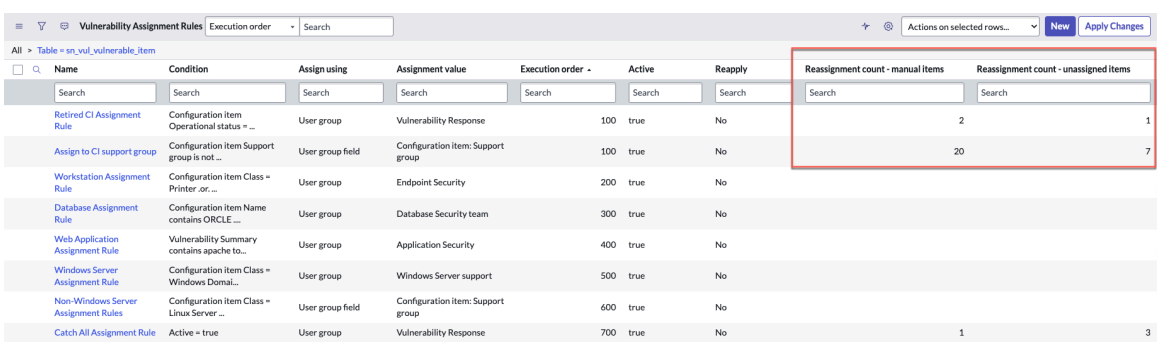
La *Reassignment count for assignment rules* tâche planifiée s'exécute quotidiennement et publie le nombre total de VI qui ne sont pas affectés par cette fonctionnalité pour une règle d'affectation particulière.

Les nombres rassemblés par cette tâche s'appliquent aux éléments vulnérables et aux règles d'affectation uniques pour Réponse aux vulnérabilités et Réponse aux vulnérabilités des applications. Les nombres sont affichés par règle d'affectation dans chaque liste de règles d'affectation pour chaque module.

La tâche compte également tous les enregistrements qui ne sont pas affectés manuellement. Les décomptes manuels et les décomptes recueillis par cette fonctionnalité sont affichés dans la liste Règles d'affectation de vulnérabilité dans deux colonnes : *Reassignment count - manual items* et *Reassignment count - unassigned items*.

1. En tant qu'administrateur de vulnérabilité, pour afficher ces nombres, accédez à **Réponse aux vulnérabilités** > **Administration** > **Règles d'affectation**.
2. Cliquez sur l'icône d'engrenage dans le coin supérieur droit de la liste, puis sélectionnez le *Reassignment count - manual items*, et *Reassignment count - unassigned items* pour affichage.
3. Tout VI qui a été affecté à l'origine par une règle, mais qui a ensuite été réaffecté automatiquement ou manuellement, contient une référence à la règle d'origine dans la vue de liste.

L'exemple suivant montre les nombres de réaffectations pour deux règles d'affectation.



Name	Condition	Assign using	Assignment value	Execution order	Active	Reapply	Reassignment count - manual items	Reassignment count - unassigned items
Retired CI Assignment Rule	Configuration item Operational status = ...	User group	Vulnerability Response	100	true	No	2	1
Assign to CI support group	Configuration item Support group is not ...	User group field	Configuration item: Support group	100	true	No	20	7
Workstation Assignment Rule	Configuration item Class = Printer .or. ...	User group	Endpoint Security	200	true	No		
Database Assignment Rule	Configuration item Name contains ORCLE	User group	Database Security team	300	true	No		
Web Application Assignment Rule	Vulnerability Summary contains apache to...	User group	Application Security	400	true	No		
Windows Server Assignment Rule	Configuration item Class = Windows Domai...	User group	Windows Server support	500	true	No		
Non-Windows Server Assignment Rules	Configuration item Class = Linux Server ...	User group field	Configuration item: Support group	600	true	No		
Catch All Assignment Rule	Active = true	User group	Vulnerability Response	700	true	No	1	3

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité

Les calculateurs de vulnérabilité automatisent le calcul des valeurs initiales pour les champs des éléments vulnérables. La condition de chaque calculateur est évaluée dans l'ordre, et le premier calculateur correspondant est utilisé.

Calculateurs de vulnérabilités

Le Réponse aux vulnérabilités système de base comprend deux calculateurs de vulnérabilité qui définissent le **score de risque** de base sur l'élément vulnérable.

- **Calculateur de risque par défaut**
- **Gravité de la vulnérabilité**

Les calculateurs de vulnérabilité peuvent être conçus pour classer par ordre de priorité et évaluer l'impact des éléments vulnérables en fonction de n'importe quel critère à l'aide de filtres de condition. Qu'il s'agisse de l'impact sur l'entreprise de la vulnérabilité, de la classe de l'élément de configuration (CI) ou de l'âge de l'élément vulnérable, vous pouvez créer des calculateurs de vulnérabilité supplémentaires pour définir d'autres champs sur les éléments vulnérables. Vous pouvez également personnaliser les calculateurs de vulnérabilité existants. Un calculateur peut être écrit pour refléter n'importe quel ensemble de priorités. Voir Créer un Réponse aux vulnérabilités calculateur et Filtrage au sein de Réponse aux vulnérabilités pour plus d'informations.

En outre, vous pouvez utiliser des attributs dans le configuration_item [cmdb_ci] dans Base de données de gestion des configurations (CMDB) pour vous aider à créer une logique pour vos calculateurs de risque de Vulnerability Response. Si, par exemple, vous déterminez que les CI qui sont orientés vers l'extérieur dans votre organisation sont plus vulnérables et peuvent nécessiter une correction immédiate, vous pouvez affecter des attributs tels que *Internet Facing* pour ces CI. Cet attribut, ainsi que d'autres, sont répertoriés dans les notes de publication de Common Service Data Model pour la version de famille Orlando. Pour obtenir des informations et des conseils à jour sur le CMDB, consultez les rubriques suivantes :

- Modèle conceptuel de modèle de données de service commun
- Modèle de schéma CMDB

Chaque calculateur contient une liste de règles de calcul, avec une condition déterminant quand l'appliquer. Lorsque le calculateur est exécuté, la condition de chaque règle de calcul est évaluée dans l'ordre, et la première règle de calcul correspondante est utilisée.

Le calculateur **de gravité** de la vulnérabilité calcule le **score de risque** pour les éléments vulnérables en utilisant la gravité de vulnérabilité normalisée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Un seul calculateur par champ cible (**score de risque**) peut être actif à la fois. **La gravité de la vulnérabilité** est désactivée par défaut.
- À partir de la version 23.0 de Réponse aux vulnérabilités, chaque fois que le score de risque est mis à jour sur un VIT, la section **Notes** est mise à jour avec les détails suivants :
  - Nom du groupe de calculateurs
  - Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre parenthèses. Pour modifier ou afficher la base de la règle du calculateur, cliquez sur n'importe quelle règle et activez la case à cocher Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. Si le modèle est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si Script est sélectionné, vous pouvez ajouter ou mettre à jour le script existant.

Tous les calculateurs de vulnérabilité activés définissent les champs sélectionnés chaque fois qu'un élément vulnérable est créé, lorsqu'un CI ou une vulnérabilité associés, ou lorsque le lien connexe **Calculer le score de risque** dans un élément vulnérable est utilisé. Par exemple, le score de risque est automatiquement mis à jour sur les enregistrements d'éléments vulnérables lorsque la valeur de gravité est mise à jour sur une vulnérabilité importée. Une fois qu'une importation de vulnérabilité a mis à jour un score de vulnérabilité, le marqueur de recalcul est activé pour cette vulnérabilité. Les scores de risque des éléments vulnérables pour lesquels le marqueur de recalcul est activé (vrai) avec cette vulnérabilité sont recalculés.

À partir d'un élément vulnérable existant, si vous cliquez sur le lien connexe **Calculer le score de risque** et que l'un des calculateurs est activé, le champ Score de **risque** de l'élément vulnérable est mis à jour.

Remarque :

- Le lien connexe **Calculer le score de risque** est uniquement visible lorsqu'au moins un calculateur de vulnérabilité est activé.
- À partir de la version 22.0 de , vous pouvez mettre à jour le score de risque d'un élément vulnérable dans et en sélectionnant le bouton Calculer le score de Réponse aux vulnérabilités**risque** dans sa vue d'enregistrement Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT.
- À partir de la version 23.0 de Réponse aux vulnérabilités, chaque fois que le score de risque d'un VIT change, les détails suivants sont documentés dans la section Notes du VIT :
  - Nom du groupe de calculateurs
  - Nom du calculateur
  - Valeurs de champ avec leur pondération et leur contribution au score de risque
  - Score de risque final

Règle du calculateur de vulnérabilité

Le **calculateur de risque par défaut** du système de base contient la règle**Règle de risque par défaut**, une règle de calcul de vulnérabilité spécialisée appelée **règle de risque**. Il calcule le **score de risque** en fonction de plusieurs valeurs :

- Gravité de la vulnérabilité
- Informations sur l'exploitation

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Criticité
- Exposition externe du CI avec la vulnérabilité
- Scores de l'EPSS

Vous pouvez ajuster les valeurs à utiliser dans la **règle de risque par défaut** et le poids à donner à chacune de ces valeurs. Les pondérations sont utilisées pour ajuster l'importance de chaque élément lors de la définition du **score de risque** de base.

Vous pouvez personnaliser les critères de la règle de risque par défaut. Pour plus d'informations, consultez Définir des champs et des poids pour la règle de risque pour les calculateurs de risque de Vulnerability Response.

Pour obtenir un exemple de la façon dont les scores de risque sont déterminés pour les calculateurs de règles de risque, reportez-vous à Exemple de calcul du score de risque pour Réponse aux vulnérabilités.

Affectation d'un pourcentage de pondération

Vous pouvez également affecter un pourcentage de pondération (0-100) au niveau de la valeur de champ. Par exemple, vous pouvez affecter un pourcentage de pondération à chaque niveau de gravité (aucun à critique).

Si la pondération de gravité est de 50 pour la règle de risque et que les valeurs de pondération suivantes sont affectées au niveau de gravité :

Gravité de la vulnérabilité	Score du risque
Critique	100
Élevé	50
Moyen	20
Aucun	0

Si la gravité est critique, la pondération équivalente est de 50. Si la gravité est élevée, la pondération équivalente est de 25, et si la gravité est moyenne, la pondération équivalente est de 10. Si la gravité est Aucune, la pondération équivalente est de 0. Pour plus d'informations, reportez-vous à la Exemple de calcul du score de risque pour Réponse aux vulnérabilitéssection .

Paramètres de règle du calculateur de vulnérabilité

Chaque règle possède un paramètre **d'ordre** . Toutefois, le premier à correspondre aux conditions met à jour le champ **Score de risque** dans l'élément vulnérable. Pour en savoir plus sur les paramètres des règles du calculateur de vulnérabilité, reportez-vous à la section Créer un Réponse aux vulnérabilités calculateur. Les règles de calculateur non scriptées ont généralement moins d'impact sur les performances que les règles de calculateur scriptées.

Le calculateur de **gravité de vulnérabilité** du système de base contient des règles de calcul qui attribuent à chaque niveau de gravité (aucun à critique) une valeur (0-100) pour **le score de risque** en fonction de la gravité. **Gravité inconnue** se voit automatiquement attribuer un score de risque de 100. Ces valeurs peuvent être ajustées et, comme le **calculateur de risque par défaut**, de nouvelles règles de calcul ou de nouvelles règles de risque peuvent être créées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Poids du score du risque de vulnérabilité

Un score de risque et une évaluation sont attribués à toutes les vulnérabilités en fonction de facteurs tels que la gravité, la criticité, les informations d'exploitation, etc. La règle *`Update Risk Rating from Risk Score`* métier de la table des éléments vulnérables est responsable du calcul de la cote de risque. Chaque fois que le score de risque change, la cote de risque est calculée et renseignée sur les éléments vulnérables. Avant la version 17.1 de l'application Réponse aux vulnérabilités (VR), les évaluations de risque suivantes étaient fournies dans le cadre du script `include VulnerabilityUtils`, qui étaient codés en dur.

Valeur (cote de risque)	Poids (score de risque)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

À partir de la version 18.0 de Réponse aux vulnérabilités,

- Les types de cote de risque sont envoyés dans la table de base en tant que vr_risk_rating. Ces types sont transmis dans le cadre de la règle métier sur chaque table où la cote de risque est calculée.
- Le script est modifié afin que vous puissiez interroger les entrées dans les valeurs de la table Poids du score de risque pour le calcul de la cote de risque.
- Ajoutez des entrées supplémentaires pour un type existant ou créez un nouveau type. Lorsque vous créez un nouveau type, assurez-vous d'ajouter les étiquettes pour la nouvelle cote de risque et de modifier les scripts et règles métier connexes. Vous devez également ajouter un nouveau style pour le nouveau score de risque.
- Modifiez le script pour interroger les enregistrements dans la table de base.

Vous pouvez accéder à la table des poids de score de risque en saisissant sn_sec_cmn_risk_score_weight dans le navigateur de filtre.

En outre, le score de risque est automatiquement recalculé dans les scénarios suivants :

- Lorsqu'un élément de configuration (CI) passe d'un mode non accessible sur Internet à un mode accessible sur Internet.
- Lorsque les vulnérabilités et expositions communes (CVE) ou les entrées tierces (TPE) associées sur les éléments de vulnérabilité (VI) sont liées à une vulnérabilité d'exploitation connue CVE (KEV).

Intégration de vulnérabilité tenable et règle de risque tenable

La règle de risque tenable est disponible avec le Tenable Vulnerability Integrationfichier . L'évaluation de priorité de vulnérabilité (VPR) est un attribut du produit Tenable qui est importé et utilisé avec un nouveau calculateur de risque par défaut dans Réponse aux vulnérabilités. La règle de risque Tenable est installée avec l'application dans le Intégration de Réponse aux vulnérabilités à Tenable cadre du calculateur de risque par défaut dans les calculateurs de vulnérabilité à partir de Réponse aux vulnérabilités.

Cette règle de risque est désactivée par défaut. Consultez Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités Détections d'éléments vulnérables à partir d'intégrations tierces

Affichez toutes les informations collectées par les analyses tierces dans votre Now Platform® instance. Affichez les résultats renvoyés des analyses sur les enregistrements de détection et d'éléments vulnérables (VI) de votre instance tels qu'ils sont affichés sur les scanners.

Vue d'ensemble

L'application Réponse aux vulnérabilités prend en charge les intégrations tierces qui récupèrent les données des éléments vulnérables de votre environnement d'entreprise. Les données détaillées sur les détections, c'est-à-dire les occurrences uniques et distinctes des vulnérabilités signalées par les analyseurs de vos intégrations tierces, sont importées et affichées à la fois sur les enregistrements de détection et les enregistrements d'éléments vulnérables dans votre instance Now Platform.

Les intégrations tierces récupèrent les données de détection des éléments vulnérables. Les détections sont des occurrences distinctes de vulnérabilités telles que signalées par les scanners. Les données de détection sont couplées à des éléments vulnérables et l'état de VI est mis à jour en fonction de l'état des détections. Si aucun VI n'est trouvé, un nouveau VI est créé. Les détections ne sont ouvertes ou fermées que par des données trouvées directement par un scanner.

Dans les versions précédentes de , les détections d'éléments Réponse aux vulnérabilitésvulnérables, la relation entre un CI (actif) dans votre environnement et une vulnérabilité importée à partir d'un scanner tiers, créait un élément vulnérable unique dans votre instance Now Platform.

La granularité des données d'origine fournies par le scanner est préservée. Avec les détections, les données de détection sont couplées à des éléments vulnérables. Lors d'une ingestion, si aucun élément vulnérable n'est trouvé, un nouvel élément vulnérable est créé.

À partir de la version 21.1.2 de Réponse aux vulnérabilités, une propriété *sn_vul.show_last_open_detection* système est fournie dans le système de base. Par défaut, la valeur de cette propriété est définie sur false et le comportement actuel d'agrégation des valeurs de la détection initiale au VI reste inchangé. Toutefois, si elle est définie sur vrai, un VI est automatiquement mis à jour avec la dernière détection ouverte après une ingestion. Les champs tels que adresse IP, SSL, port, protocole, NetBIOS et Preuve sont mis à jour pour les détections de VI. Si nécessaire, vous pouvez personnaliser les champs de détection qui doivent être mis à jour en modifiant le script `DetectionBase` .

Pour afficher les valeurs de la dernière détection ouverte, accédez à l'onglet **Dernière détection ouverte** sur la vue du formulaire VI. Pour mettre à jour tous les VI ouverts au cours de l'année écoulée avec les dernières valeurs de détection ouvertes, vous pouvez exécuter la tâche *Update Last Open Detection Value To VITs* planifiée sur demande. Cette tâche planifiée est également fournie dans le système de base.

Remarque : Lorsqu'un élément de configuration (CI) change sur un élément détecté, les mises à jour correspondantes sont également reflétées dans les détections. Par conséquent, les détections peuvent être déplacées d'un élément vulnérable à un autre. En fonction de ce changement et de la valeur de la *sn_vul.show_last_open_detection* propriété, les valeurs des détections sont déployées sur les VI source et cible.

Versions prises en charge de Réponse aux vulnérabilités

Pour en savoir plus sur l'installation ou la mise à jour de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations tierces prises en charge

Une intégration tierce prise en charge avec votre Réponse aux vulnérabilités application est requise pour les détections d'éléments vulnérables. Les intégrations tierces suivantes sont prises en charge par l'application pour les Réponse aux vulnérabilités détections d'éléments vulnérables :

- Intégration de la détection d'hôte Qualys
- Entrepôt de données Rapid7 :
  - Intégration d'éléments vulnérables
  - Intégration de résolution des éléments vulnérables
- Intégration de résolution des éléments vulnérables Rapid7 (InsightVM)
  - Intégration d'Insight VM
  - Intégration d'éléments vulnérables : API
- Tenable Vulnerability Integration
- Gestion des menaces et des vulnérabilités par Microsoft Defender

Ces intégrations tierces sont disponibles avec un abonnement distinct à partir du ServiceNow Store. Pour plus d'informations sur ces intégrations, consultez Intégrations de Réponse aux vulnérabilités et pour plus d'informations sur l'obtention d'autorisations.

Pour vérifier que votre scanner tiers est configuré pour l'importation, consultez Installer et configurer l'application Rapid7 Integration for Security Operations et Installer Qualys Vulnerability Integration.

Termes clés pour la détection des éléments vulnérables

Vulnérabilité

Données sur les faiblesses des logiciels, des systèmes d'exploitation et des ressources importées de sources internes et externes. Ces données sont importées et comparées aux actifs existants (éléments de configuration, CI) répertoriés dans la CMDB.

Élément vulnérable

Un élément vulnérable est créé ou mis à jour lorsqu'une vulnérabilité importée correspond à un CI dans la CMDB.

Détection

Une occurrence unique et distincte d'une vulnérabilité signalée par un scanner, appelée détection d'élément vulnérable dans l'environnement Now Platform . Une détection inclut des données enrichies sur une vulnérabilité et tous les éléments vulnérables correspondants. Ces données sont affichées dans l'enregistrement de détection (VID#) et dans la vue de liste des éléments vulnérables qui comprend les détails suivants :

- Premier trouvé (données)
- Dernier trouvé (date)
- Nom DNS
- Nom du BIOS net
- Adresse IP
- Port

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Protocole
- Preuve
- SSL
- Durées trouvées

Remarque : L'ajout d'une règle métier à la table de détection impacte les performances de l'ingestion.

Clé de détection

Une combinaison hachée de champs qui fournit un moyen d'identifier et de lier une détection à un élément vulnérable. Les clés de détection sont spécifiques à l'intégration.

Configurations des clés de détection

Scanner	Vulnérabilité	Port	Protocole	ID de l'actif	Preuve	Carte réseau
Qualys	Oui	Oui	Oui	Oui	Non	N/A
Tenable	Oui	Oui	Oui	Oui	Non	N/A
Rapid7	Oui	Oui	Oui	Oui	Oui (il n'est pas sensible à la casse)	Oui

Remarque :

- Si la clé de détection n'est pas spécifiée, ou pour les versions antérieures à Réponse aux vulnérabilités la version 14.0, la clé de détection est une combinaison de l'entrée de vulnérabilité, du port, du protocole, de l'ID d'actif et de la preuve.
- À partir de la version 19.0 de , une nouvelle carte réseau de clé de Réponse aux vulnérabilitésdétection est ajoutée pour Rapid7 InsightVM, qui est activée par défaut. Les détections existantes sans carte réseau sont mises à jour avec la première carte réseau entrante dans la charge utile à partir de Rapid7. La clé de détection est recalculée et renseignée sur la carte réseau de détection incluse. De nouvelles détections sont créées si des détections similaires sont observées avec des valeurs de carte réseau différentes. Ces données ne sont pas déployées dans la table Élément vulnérable. La valeur NIC est stockée dans une nouvelle colonne de la table sn_vul_detection_key_config et sn_vul_detection.

De dup

Le processus utilisé par l'application de la Réponse aux vulnérabilités réduction des détections individuelles en un seul VI lorsque les données répondent à certains critères codés en dur.

ID externe VI

Valeur stockée dans le champ ID externe de la table des VI. Cette valeur est un hachage composé de la combinaison de clés au sein d'un VI qui représente ce qui le rend unique au sein de l'application. Il est composé d'un CI et d'une entrée vulnérable.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rouvrir les éléments vulnérables résolus

Les éléments vulnérables définis sur **Résolu** dans votre Now Platform instance, mais pas sur **Fermé/Résolu** par les exécutions d'intégration suivantes, sont rouverts s'ils sont détectés lors des nouvelles analyses.

Les VI fermés avec un sous-état **Fixe** ou **Périmé** sont rouverts si une nouvelle détection est créée et les VI peuvent être mis en correspondance avec la nouvelle vulnérabilité.

Selon l'include de script, *`DetectionBase_shouldReOpenVI()`*, si le VIT a été **précédemment fermé** avec **le** sous-état Fixe, **Périmé** ou **CI désactivé**, il est rouvert et la détection est mappée au VIT existant.

Par exemple, supposons que la date de fermeture d'un VIT soit postérieure à la date de last_found d'une détection. Vous pouvez vous attendre à ce que ces enregistrements VIT restent fermés. Toutefois, si vous voyez une VIT précédemment fermée rouverte, cela signifie que la VIT a été fermée par une détection antérieure et que la vulnérabilité a été détectée à nouveau lors d'une analyse ultérieure. Lorsqu'une nouvelle détection est trouvée qui correspond au VIT fermé qui présente la même vulnérabilité sur l'élément de configuration du VIT, le VIT est rouvert.

Pour Rapid7 les détections, une option est désormais disponible sur la page de configuration Rapid7 de votre instance pour rouvrir les VI résolus par âge. Si cette option est activée, les VI définis sur **Résolu** , mais qui ne sont pas ensuite transférés à **l'état Fermé/Corrigé** par les analyses suivantes, reviennent à **l'état Ouvert** après le nombre de jours que vous entrez.

Pour Qualys les détections, si le scanner continue de rechercher des VI qui ont été définis sur **Résolu** mais qui ne sont pas ensuite passés à **l'état Fermé/Fixe** par les analyses suivantes, ces VI reviennent à l'état **Ouvert** lorsque la dernière date de recherche est postérieure à la date de résolution.

Afficher les données de détection

Vous affichez les données importées à partir des détections d'éléments vulnérables sur l'enregistrement VI. Pour plus d'informations, consultez Afficher les Réponse aux vulnérabilités données de détection des éléments vulnérables et Vérifier Réponse aux vulnérabilités les données de détection d'éléments vulnérables sur les enregistrements d'exécution de l'intégration (VINTRUN).

Gestion des solutions pour vulnérabilités

Corrélez automatiquement les vulnérabilités de votre environnement avec les solutions susceptibles d'y remédier. Identifiez les actions de rattrapage qui s'appliquent à vos vulnérabilités et classez-les par ordre de priorité en fonction de la plus grande réduction du risque de vulnérabilité.

Gestion des solutions pour vulnérabilités

Les équipes de sécurité et informatiques consacrent souvent beaucoup de temps à la recherche des résultats de vulnérabilité afin d'identifier les traitements les plus efficaces pour leur environnement. Compte tenu du volume et de la complexité des vulnérabilités dans les grandes organisations, la traduction des résultats de vulnérabilité en tâches de correction est un processus manuel, fastidieux et sujet aux erreurs.

Avec Gestion des solutions pour vulnérabilités, vous pouvez corréler automatiquement vos résultats de vulnérabilité avec les solutions qui y remédient. Identifiez les correctifs logiciels, les mises à jour de configuration et les autres contrôles qui ont le plus d'impact sur votre organisation sans les frais généraux manuels.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration requise pour le Gestion des solutions pour vulnérabilités

Gestion des solutions pour vulnérabilités est une fonctionnalité disponible dans l'application Réponse aux vulnérabilités . Gestion des solutions pour vulnérabilités Nécessite un abonnement distinct.

Pour plus d'informations sur l'obtention d'autorisations pour les applications à partir de , reportez-vous à .ServiceNow Store Pour en savoir plus sur l'installation de l'application après l'avoir téléchargée sur votre instance, reportez-vous à la rubrique Installer l'application Gestion des solutions pour Réponse aux vulnérabilités .

Une fois installé, Gestion des solutions pour vulnérabilités il vous permet d'accéder aux données de la Microsoft Security Response Center solution à Red Hat partir Réponse aux vulnérabilitésde .

Remarque :

Vous pouvez configurer les deux applications de solution à partir de l'assistant de configuration. Consultez Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'Assistant de configuration.

Voir Présentation de Microsoft Security Response Center Solution Integration et Présentation de Intégration de solution Red Hat pour plus d'informations sur les solutions importées.

Versions disponibles

Pour la version la plus récente de Gestion des solutions pour vulnérabilités, vérifiez que vous disposez de la version la plus récente de Réponse aux vulnérabilités installée.

Version de Gestion des solutions pour vulnérabilités	**Versions compatibles de** Réponse aux vulnérabilités	**Notes de publication**
Gestion des solutions pour vulnérabilités v10.3	Réponse aux vulnérabilités v18.0	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

À propos des solutions et du remplacement

Une mise à jour remplacée est un remplacement complet d'une ou de plusieurs versions précédentes. Par exemple, une mise à jour de correctif d'urgence peut être remplacée par un Service Pack. Les solutions sont liées aux vulnérabilités. Les solutions peuvent également se rapporter à d'autres solutions d'une chaîne de remplacement. Les solutions corrigent les vulnérabilités des solutions précédentes et elles sont cumulatives. Gestion des solutions pour vulnérabilités Associe automatiquement les vulnérabilités des solutions précédentes aux solutions de remplacement. Si une vulnérabilité plus ancienne est détectée, n'importe quelle solution de remplacement supérieure peut la résoudre, mais la solution de remplacement la plus élevée est préférée, car c'est la plus cumulative.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Solutions potentielles par rapport aux solutions privilégiées

Une solution potentielle est une solution qui pourrait remédier à une vulnérabilité. Les vulnérabilités ont souvent de nombreuses solutions potentielles. Une solution privilégiée est la solution unique ciblée pour la remédiation d'une vulnérabilité ou d'un élément vulnérable (VI). Il communique l'intention et permet d'obtenir des mesures de déploiement plus détaillées.

Solutions privilégiées

Gestion des solutions pour vulnérabilités définit automatiquement la solution la plus efficace (**solution privilégiée**) pour la vulnérabilité détectée en fonction de la priorité la plus élevée lorsqu'il n'existe qu'une seule solution de remplacement la plus élevée. S'il existe plus d'un remplacement le plus élevé pour la vulnérabilité, aucune valeur n'est fixée. Dans Réponse aux vulnérabilités, une **solution privilégiée** correspond à la Microsoft Security Response Center solution ou Red Hat présentant le remplacement le plus élevé dérivé des solutions associées à la vulnérabilité.

Les valeurs de la solution préférée peuvent être définies sur l'élément vulnérable ou sur la vulnérabilité. Lorsqu'ils sont définis directement sur la vulnérabilité, tous les éléments vulnérables associés à la vulnérabilité héritent de cette solution. Modifiez les valeurs **de la solution privilégiée** pour plusieurs éléments vulnérables à l'aide de la fonctionnalité de modification en bloc. Lorsqu'il est modifié en bloc, seule la **solution privilégiée** sur l'élément vulnérable est mise à jour, car définir la **solution privilégiée** au niveau d'entrée de vulnérabilité définira la **solution privilégiée** pour tous les nouveaux éléments vulnérables à venir. La modification en bloc s'applique uniquement aux éléments vulnérables actuels.

Remarque : S'il existe plusieurs solutions de remplacement le plus élevé pour une vulnérabilité, les valeurs **de solution privilégiée** au niveau de la vulnérabilité sont effacées, car cette solution dépend de l'actif affecté. Lorsqu'il existe plusieurs solutions de remplacement le plus élevé pour une vulnérabilité, définissez une **solution préférée** sur l'élément vulnérable. Vous pouvez définir une solution différente à **l'aide** de la liste de recherche du formulaire **Élément vulnérable** .

Toutes les solutions privilégiées pour les éléments vulnérables dans une tâche de rattrapage se trouvent dans une liste connexe de l'enregistrement **de la tâche de rattrapage** .

Toutes les importations de solutions n'entraînent pas une actualisation complète des données. Le processus de remplacement est mis à jour lorsque :

- Un élément vulnérable est créé.
- Les données ont changé sur un VI actif.

  Remarque : À partir de la version 22.0 de Réponse aux vulnérabilités, les solutions ne sont pas mises en file d'attente dans les deux cas ci-dessus.

- Un nouveau mappage est créé pour une entrée tierce avec les CVE.
- De nouvelles données de solution ont été publiées depuis la dernière importation, une solution existante est mise à jour.

Amélioration de la gestion des solutions et optimisation des performances

Les solutions proviennent de diverses intégrations, notamment Microsoft et Redhat. Le premier fournit des mises à jour mensuelles et établit une chaîne de dépendances pour suivre la solution préférée pour les vulnérabilités. Cependant, d'autres intégrations ne suivent pas ce format de mise à jour et n'ont pas besoin d'établir une chaîne de dépendances pour elles. Auparavant, une logique de traitement était utilisée qui impliquait la création

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'un graphique pour maintenir la priorité et identifier les solutions de remplacement les plus élevées. Ces solutions ont été suggérées comme étant la solution privilégiée pour les vulnérabilités. Cependant, comme la construction du graphique prend du temps, les autres intégrations sont exclues de ce processus. Pour améliorer les performances, à partir de la v22.0 de Réponse aux vulnérabilités, la méthode *`utility.processNonGraphSolutions()`* est appelée dans la *`Process Vulnerability Solutions Metrics Queue`* tâche planifiée. Cette méthode gère les solutions issues d'intégrations autres que Microsoft.

Deuxièmement, les solutions sont mises en file d'attente à partir de diverses sources à l'aide de la tâche *`Process Vulnerability Solutions Metrics Queue`*planifiée. Cette tâche planifiée implique le déploiement de solutions à partir d'entrées NVD vers des entrées tierces, le remplissage des solutions préférées sur les vulnérabilités et la mise à jour des mesures d'état de rattrapage sur les solutions. Dans les scénarios suivants, seules les mesures d'état de rattrapage doivent être mises à jour :

- Lorsque la solution préférée change en fonction des vulnérabilités
- Lorsque les VIT sont créés ou supprimés
- Lorsqu'une importation VIT est terminée

Bien que les solutions soient mises en file d'attente pour mettre à jour uniquement les mesures d'état de rattrapage, elles tentent toujours de déployer des solutions à partir d'entrées NVD vers des entrées tierces et de renseigner les solutions privilégiées. Pour optimiser ce processus, la colonne Statut de mise **à jour** est introduite dans la table Solution de vulnérabilité. Lorsque les mesures d'état de rattrapage des solutions doivent être mises à jour sans nécessiter le déploiement ou le remplissage des solutions privilégiées, les solutions ne sont plus en file d'attente. Au lieu de cela, la colonne **Mettre à jour l'état** est directement mise à jour en tant que vrai. Cette approche permet de traiter les tickets où seules les mesures d'état de rattrapage doivent être mises à jour, ce qui permet de réaliser des économies de temps et de ressources. Dans la tâche planifiée, une fois le traitement des solutions en file d'attente terminé, les solutions marquées avec un état de mise à jour défini sur vrai sont identifiées. Ensuite, ces solutions sont itérées, en calculant les nombres et en mettant à jour les mesures d'état de rattrapage en conséquence. Cette étape joue un rôle important dans l'amélioration des performances de la tâche planifiée, car le nombre de solutions à mettre en file d'attente est réduit. Pour afficher les mesures d'état de rattrapage, accédez à la table Solution de vulnérabilité [sn_vul_solution] et sélectionnez une solution de vulnérabilité. Ensuite, sélectionnez l'onglet **État du rattrapage** . Cet onglet renseigne les champs suivants :

Mesures de l'état du rattrapage

Champ	Description
Cibles de solutions préférées : état de rattrapage des VI pour lesquels il s'agit de la solution préférée	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
CI restants	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre d'éléments vulnérables actifs et fermés pour lesquels cette solution est

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures de l'état du rattrapage (suite)

Champ	Description
	préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
CI totaux	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
% des VI rattrapés	Pourcentage complet pour le rattrapage d'éléments vulnérables (VI). S'applique aux éléments vulnérables pour lesquels cette solution est préférée. Ce nombre exclut les éléments vulnérables différés.
% des CI rattrapés	Pourcentage complet pour le rattrapage de CI. S'applique aux éléments vulnérables pour lesquels cette solution est préférée. Ce nombre exclut les éléments vulnérables différés.
Cibles de solutions privilégiées (inclut les éléments différés) : état de rattrapage des VI, y compris les éléments différés, pour lesquels il s'agit de la solution privilégiée	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est préférée pour le rattrapage.
CI restants	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre d'éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage.
CI totaux	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage.
% des VI rattrapés	Pourcentage complet pour le rattrapage d'éléments vulnérables (VI). S'applique aux éléments vulnérables pour lesquels cette solution est préférée.
% des CI rattrapés	Pourcentage complet pour le rattrapage de CI. S'applique aux éléments vulnérables pour lesquels cette solution est préférée.
Cibles potentielles de la solution : état de rattrapage de tous les éléments vulnérables présentant une vulnérabilité liée à cette solution	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est une solution possible pour le rattrapage. Ce

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures de l'état du rattrapage (suite)

Champ	Description
	nombre exclut les éléments vulnérables différés.
CI restants	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est une solution possible pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
Cibles potentielles de solutions (y compris les éléments différés) : état de rattrapage pour tous les VI, y compris les éléments différés, avec une vulnérabilité liée à cette solution	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est une solution possible pour le rattrapage.
CI restants	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est une solution possible pour le rattrapage.

Troisièmement, la disponibilité d'une solution privilégiée pour les vulnérabilités et les VIT doit être assurée pour remédier aux vulnérabilités. Toutefois, dans les situations où plusieurs solutions de remplacement supérieures existent pour une vulnérabilité, une solution privilégiée n'est pas renseignée en raison de l'ambiguïté. Pour faire face à ce scénario, une approche est implémentée qui implique d'exécuter la logique de traitement et de renseigner la solution préférée lorsqu'elle est disponible. Dans les cas où il n'existe qu'une seule solution de remplacement supérieure, elle est renseignée comme solution privilégiée. Lorsqu'il existe plusieurs solutions de remplacement supérieures, le champ de solution privilégiée reste vide. Cependant, l'objectif est de renseigner la solution de remplacement la plus élevée, qui est publiée comme la plus récente, en tant que solution privilégiée. Pour ce faire, une propriété *sn_vul.latest_solutions* système est introduite. Par défaut, cette propriété est définie sur faux. Si vous souhaitez activer la possibilité de renseigner les dernières solutions en tant que solution préférée lorsqu'aucune solution privilégiée n'est disponible, vous pouvez activer cette propriété. Une fois activée, la colonne **Type de solution** est mise à jour dans la table de vulnérabilité avec les options suivantes :

- Préféré : lorsque la solution préférée est renseignée
- Dernière : lorsqu'aucune solution privilégiée n'est disponible, la solution la plus récente de l'ensemble des solutions de remplacement les plus élevées est sélectionnée en fonction de la valeur de la date de publication. Le champ à sélectionner comme dernière solution peut être personnalisé à l'aide de la *sn_vul.latest_solutions* propriété système. Par défaut, la valeur est définie sur « date de publication », mais elle peut être changée en « dernière modification » pour sélectionner la solution en fonction de la dernière colonne modifiée dans les solutions.
- Manuel : lorsque le type de solution préféré est mis à jour manuellement. La priorité pour ce type de solution est la plus élevée.

Dans certains scénarios, la solution préférée sur un élément vulnérable (VIT) peut différer de la solution préférée sur la vulnérabilité correspondante. Cela se produit lorsque la solution privilégiée est mise à jour manuellement sur un VIT et non sur la vulnérabilité. Dans ce cas, le champ **Type de solution** est masqué dans le VIT.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Qu'est-ce que Gestion des solutions pour vulnérabilités

- Associe automatiquement les nouveaux éléments vulnérables (VIT) et les tâches de rattrapage aux solutions pendant Microsoft Security Response Center Solution Integration et Intégration de solution Red Hat l'importation.

  MSRC Les solutions sont associées au dernier bulletin dans lequel la solution apparaît.

- Associe automatiquement les éléments vulnérables et les tâches de rattrapage à des solutions lorsque les enregistrements de vulnérabilité sont associés manuellement à des solutions.

  Remarque : Les éléments vulnérables réaffectés manuellement à une autre solution ne sont pas automatiquement mis à jour avec les changements de solution au niveau de la vulnérabilité.

- MSRC: crée des chaînes de remplacement pendant l'importation que vous pouvez afficher dans la liste connexe de la solution.
- Indique si une solution est une solution de remplacement le plus élevé ou non.
- Répertorie le **score de risque** de la solution associé à chaque solution afin de vous fournir les plus grandes opportunités de réduction des risques.

- Gère **l'état de rattrapage** des solutions sur **les entrées de vulnérabilité**, les **tâches de rattrapage** et les enregistrements de solutions de **vulnérabilité** tiers afin que vous puissiez suivre la progression du rattrapage.

  Il contient :

  - Nombre d'éléments vulnérables par pourcentage rattrapé, pour les VI avec des solutions privilégiées, avec et sans les VI à l'état Différé.
  - Nombres d'éléments de configuration (CI) par pourcentage rattrapés, pour les VI avec des solutions privilégiées, avec et sans les VI à l'état Différé.
  - Nombre d'éléments vulnérables par pourcentage rattrapé, pour les éléments vulnérables avec des solutions potentielles, avec et sans ces éléments vulnérables à l'état Différé.
  - Nombre d'éléments de configuration par pourcentage rattrapé, pour les VI avec des solutions privilégiées, avec et sans les VI à l'état Différé.

Traduction automatique

Ce que vous pouvez faire avec Gestion des solutions pour vulnérabilités

- Créez, mettez à jour, affichez ou supprimez des solutions associées à des vulnérabilités, afin de pouvoir suivre les solutions de vulnérabilité qui ne sont pas couvertes par le contenu de solution tiers. L'intégration de la solution à l'entrepôt de données Rapid7 n'est pas prise en charge.
- Associez des vulnérabilités tierces et des entrées NVD à un enregistrement de solution.
- Supprimez et associez à nouveau les éléments vulnérables et les tâches de rattrapage à une solution.
- **Affichez la solution préférée** applicable à une vulnérabilité donnée dans les formulaires de vulnérabilité et d'élément vulnérable.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Affichez une liste **connexe Solutions préférées** sur les formulaires de tâche de rattrapage qui répertorie toutes les solutions qui ont été préférées par au moins un VI actif au sein de ce groupe.
- Affichez les détails de **l'état du rattrapage** d'une solution qui montrent la réduction du risque associée au déploiement de la **solution privilégiée** sur la vulnérabilité, l'élément vulnérable, les tâches de rattrapage et les formulaires de solution.
- Affichez les vulnérabilités applicables à une solution donnée sur le formulaire de solution.
- MSRC: affichez les solutions de remplacement pour une solution donnée sur une vulnérabilité, afin de trouver la dernière mise à jour à déployer ou une mise à jour antérieure, plus ciblée et plus efficace.
- Affichez des listes de solutions triées en fonction de leurs différentes caractéristiques.
  - Toutes : solutions triées par date de publication et par nombre.
  - MSRC: Priorité la plus élevée : solutions comportant des éléments vulnérables actifs et non différés. **Trié par priorité la plus élevée**, **date de publication** et **nombre**.
  - Avec éléments vulnérables : solutions avec des éléments vulnérables actifs et non différés. Trié par **remplacement le plus élevé** ou **préféré**, **score de risque** et **nombre**. En cas de déploiement, les entrées supérieures de la liste offrent la réduction de risque la plus importante pour les actifs de votre environnement.

Enregistrement de solution Score de risque et cote de risque

Remarque : Le score de **risque** et la **cote de risque** de l'enregistrement de la solution sont distincts des champs utilisés pour les vulnérabilités, les éléments vulnérables et les tâches de rattrapage.

Le score de **risque** de l'enregistrement de solution est un calcul pondéré basé sur le **score de risque** de l'élément vulnérable et un nombre d'éléments vulnérables actifs avec cette solution comme **solution potentielle**. Le **score de risque** de la solution fournit une estimation de la réduction du risque attendue par la solution.

Le **score de risque** de l'enregistrement de solution est calculé comme suit :

- Il commence par prendre 85 % du **score de risque** le plus élevé ou le plus élevé d'un élément vulnérable actif avec cette solution potentielle.
- Le score de **risque** de l'enregistrement de solution compile ensuite le nombre total d'éléments vulnérables avec cette solution potentielle. Pour chaque plage du nombre d'éléments vulnérables, il ajoute des points et arrive à un total.
  - 0–09 éléments vulnérables n'ajoute aucun point
  - 10–99 objets vulnérables ajoute 5 points
  - 100–999 éléments vulnérables ajoute 10 points
  - 1 000 et au-delà des éléments vulnérables ajoute 15 points

  Par exemple, pour un score de **risque** d'élément vulnérable de 80, le **score de risque** de l'enregistrement de solution commencerait à 68. S'il y avait 200 éléments vulnérables actifs au total avec cette solution potentielle, le **score de risque** final de la solution serait de 78.

La cote de **risque** de l'enregistrement de solution sépare le **score de risque** de l'enregistrement de solution en plages allant de Critique à Aucun. **L'évaluation du risque** de la solution évalue la réduction du risque pour les éléments vulnérables corrigés par cette solution.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Jusqu'à VR v16.1, les évaluations des risques séparaient le **score de risque** de solution obtenu dans les plages suivantes :

- 1 — Critique (**90+ score de risque de la** solution)
- 2 — Élevé (70-89 Score de risque de l'enregistrement **de la** solution)
- 3 — Moyen (30-69 Score de risque de l'enregistrement de **la** solution)
- 4 — Faible (1-29 Enregistrement de **solution Score de risque**)
- 5 — Aucun (0 **Enregistrement de solution Score de risque**)

À partir de VR v16.1, les évaluations des risques séparent le **score de risque** de solution obtenu dans les plages suivantes pour la gestion des solutions :

- 1 — Critique (**90+ score de risque de la** solution)
- 2 — Élevé (70-89 Score de risque de l'enregistrement **de la** solution)
- 3 — Moyen (40-69 Score de risque de l'enregistrement **de la** solution)
- 4 — Faible (1-39 Enregistrement **de solution Score de risque**)
- 5 — Aucun (0 **Enregistrement de solution Score de risque**)

Cas d'utilisation

Affichez l'état de progression du déploiement d'un cycle de correctif actuel à l'aide du module de priorité la plus élevée, trié par date.

Affichez les solutions à valeur élevée à l'aide du module Avec éléments vulnérables, triées par score de risque.

Les listes de solutions communiquent les détails clés des solutions, les scores de risque et les mesures de déploiement. Utilisez le **score de risque** et le nombre de VI actifs pour établir des priorités. Découvrez quelles solutions du cycle de correctif actuel ne progressent pas, ce qui peut indiquer un prérequis de déploiement manqué.

Remarque : Ajoutez **%VI rattrapés(percent_nd_pref_vis_remediated)** à partir du menu **Personnaliser les colonnes de la liste** pour connaître l'avancement du rattrapage sur le formulaire Solutions de vulnérabilité.

Présentation de Microsoft Security Response Center Solution Integration

Examiner et mettre en œuvre les solutions d'assainissement proposées par le Microsoft Security Response Center Solution Integration.

Microsoft Security Response Center Solution Integration est inclus dans la Gestion des solutions pour vulnérabilités fonctionnalité de Réponse aux vulnérabilités, disponible par abonnement distinct. Pour plus d'informations sur la façon d'intégrer Réponse aux vulnérabilités des solutions, consultez la section Gestion des solutions pour vulnérabilités

Microsoft Security Response Center examine les rapports de vulnérabilités de sécurité affectant les produits et services Microsoft et fournit des informations sur les solutions pour aider à gérer les risques de sécurité. Les solutions sont des mesures correctives connues importées dans votre Microsoft Security Response Center Solution Integration à partir du Microsoft Security Response Center produit.

Contient des Microsoft Security Response Center Solution Integration points d'entrée vers Microsoft Security Response Center le produit, invoqués en tant que travaux planifiés. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités. Les travaux

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

planifiés s'exécutent automatiquement et dans l'ordre spécifié. Vous pouvez également exécuter manuellement des travaux planifiés individuels.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Versions disponibles

Pour la version la plus récente de Gestion des solutions pour vulnérabilités et Microsoft Security Response Center des solutions, vérifiez que vous avez installé la version Réponse aux vulnérabilités la plus récente.

Pour plus d'informations sur l'installation, la configuration Gestion des solutions pour vulnérabilités et l'intégration de solutions, consultez Installer l'application Gestion des solutions pour Réponse aux vulnérabilités et Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'Assistant de configuration.

Version de Réponse aux vulnérabilités	**Version de** Gestion des solutions pour vulnérabilités	**Notes de publication**
Réponse aux vulnérabilités v15.0	v10.3	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Rôles

Microsoft Security Response Center Solution Integration Les tâches impliquent les rôles suivants.

- sn_vul.vulnerability_admin ou sn_vul.admin (obsolète) : peut lire, écrire et supprimer des enregistrements.
- sn_vul.vulnerability_write : peut lire et écrire des enregistrements.
- sn_vul.vulnerability.read : peut lire les enregistrements.
- sn_vul.remediation_owner : peut lire et écrire des notes internes sur les enregistrements affectés au groupe ou à l'individu spécialiste du rattrapage. (Contenu dans le rôle itil.)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Microsoft Security Response Center Solution Integration

Pour afficher le Microsoft Security Response Center Solution Integration, accédez à **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.

L'intégration suivante est incluse dans le système de base.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Microsoft Security Response Center Solution Integration

Intégration	Description
Microsoft Security Response Center Solution Integration	Récupère les solutions et le mappage de la base de données de vulnérabilité nationale (NVD) pour associer les solutions aux vulnérabilités, aux éléments vulnérables et aux tâches de rattrapage. **Remarque :** Il Microsoft Security Response Center Solution Integration n'apporte pas de solutions avant 2016.

Solutions

Pour afficher les solutions importées dans une liste, reportez-vous à la section Afficher une solution.

Présentation de Intégration de solution Red Hat

Vous pouvez examiner et implémenter les solutions de rattrapage proposées fournies par le Intégration de solution Red Hat dans l'application Réponse aux vulnérabilités .

Intégration de solution Red Hat est inclus dans la Gestion des solutions pour vulnérabilités fonctionnalité de Réponse aux vulnérabilités, disponible par abonnement distinct. Pour plus d'informations sur la façon d'intégrer Réponse aux vulnérabilités des solutions, consultez la section Gestion des solutions pour vulnérabilités

Intégration de solution Red Hat examine les rapports de vulnérabilités de sécurité affectant les Red Hat produits et services, et fournit des informations sur les solutions pour aider à gérer les risques de sécurité. Les solutions connues sous le nom de rattrapages sont importées dans votre Intégration de solution Red Hat formulaire .Red Hat

À partir de la version 21.0 de Réponse aux vulnérabilités, Red Hat transmet les charges utiles au format CSAF (Common Security Advisory Framework) plutôt qu'au format CVRF (Common Vulnerability Reporting Framework). La CSAF, une norme basée sur XML, diffère à la fois de la structure et du format de la CVRF. Pour tenir compte de ce changement, un nouvel analyseur CSAF a été développé. Cet analyseur interprète le format CSAF, en extrayant les champs requis pour remplir les tables en conséquence.

Remarque : Par défaut, vous recevrez la charge utile au format CSAF.

Les extraits suivants montrent le script d'intégration pour l'analyse de Red Hat la charge utile reçue dans les formats CSAF et CVRF respectivement.

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in
 the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is
 expected
return new sn_vul.RedHatSolutionIntegration(true);
})(integrationProcessGr);
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in
 the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is
 expected
return new sn_vul.RedHatSolutionIntegration(false);
})(integrationProcessGr);
```

Intégration de solution Red Hat contient des points d'entrée vers le produit Red Hat, invoqué en tant que tâche planifiée. La tâche planifiée simplifie le cycle de vie de la correction des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités. Il s'exécute automatiquement. Vous pouvez également exécuter la tâche planifiée manuellement.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Versions disponibles

Pour la version la plus récente de Gestion des solutions pour vulnérabilités et Red Hat des solutions, vérifiez que vous avez installé la version Réponse aux vulnérabilités la plus récente.

Pour plus d'informations sur l'installation, la configuration Gestion des solutions pour vulnérabilités et l'intégration de solutions, consultez Installer l'application Gestion des solutions pour Réponse aux vulnérabilités et Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'Assistant de configuration.

Version de Réponse aux vulnérabilités	**Version de** Gestion des solutions pour vulnérabilités	**Notes de publication**
Réponse aux vulnérabilités v15.0	v10.3	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Rôles

Intégration de solution Red Hat Les tâches impliquent le rôle suivant : sn_vul.configure_rhsa_integration

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Intégration de solution Red Hat

Pour afficher le Intégration de solution Red Hat, accédez à **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.

L'intégration suivante est incluse dans le système de base.

Intégration Red Hat

Intégration	Description
Intégration de solution Red Hat	Récupère les solutions et le mappage de la base de données de vulnérabilité nationale (NVD) pour associer les solutions aux vulnérabilités, aux éléments vulnérables et aux tâches de rattrapage.

Solutions

Pour afficher les solutions importées dans une liste, reportez-vous à la section Afficher une solution.

Rapid7 Gestion des solutions

Les solutions sont des rattrapages connus qui sont importés dans votre Intégration des vulnérabilités Rapid7 à partir de l'entrepôt Rapid7 de données ou Rapid7 InsightVM Rapid7 . L'entrepôt de données importe à la fois des solutions et des solutions de remplacement. Avec Rapid7 InsightVM, vous obtenez des solutions dans le cadre de l'API Rapid7 Vulnerable Item Integration.

À partir de la version 21.0 de Réponse aux vulnérabilités, il y a un changement dans la façon dont les solutions sont créées par Rapid7 InsightVM. Au lieu de s'appuyer sur **des champs solution_summary**, **solution_fix** ou **solution_type** , Rapid7 InsightVM crée désormais des solutions à l'aide des solution_id fournies par le scanner. Cela signifie que même si ces champs sont vides, une solution est créée tant qu'un ID de solution est disponible.

Pour afficher les solutions importées sous forme de liste, accédez à **Rapid7** > **Solutions**.

Si le module d'extension Gestion des solutions pour vulnérabilités est activé, la dernière version de Intégration des vulnérabilités Rapid7 fournit les fonctionnalités clés suivantes concernant les solutions :

- La Rapid7 gestion des solutions est déplacée vers la gestion des solutions de vulnérabilité.
- Une nouvelle intégration Rapid7 Prerequisite Solution Management pour l'entrepôt de données est introduite. L'intégration récupère la solution prérequise à partir de l'entrepôt Rapid7 de données.
- La liste connexe de Rapid7 (solution) sur les entrées tierces (TPE) est masquée.
- Les données précédemment importées peuvent être visualisées dans le nouveau modèle de données. Les solutions Rapid7, le remplacement de la solution et la carte de solutions en matière de vulnérabilité sont réimportés et le champ **Importer depuis** est défini sur vide. Le champ est renseigné dans Gestion des solutions.
- Les détections sont mises à jour pour renseigner le champ de solution. Les détections montrent les solutions telles qu'elles font partie de Vulnerability Solution Management.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Rapid7 obtient une préférence plus élevée par rapport à d'autres solutions tout en définissant la solution préférée sur TPE pour Rapid7 l'entrepôt de données.
- Les solutions sont déployées sur les éléments vulnérables (VI) à partir des détections pour Rapid7 InsightVM.

Remarque : Si vous n'avez pas activé le module d'extension Gestion des solutions pour vulnérabilités , l'application fonctionne telle quelle.

Vulnerability Solution Management

Si vous avez activé le module d'extension Gestion des solutions pour vulnérabilités , les solutions pour l'entrepôt Rapid7Rapid7 de données et Rapid7 InsightVM la table Solutions en matière de vulnérabilité [sn_vul_solution]. Toutefois, si vous n'avez pas activé le module d'extension Gestion des solutions pour vulnérabilités , alors Intégration des vulnérabilités Rapid7 fonctionne tel quel et importe les solutions dans la table personnalisée [sn_vul_r7_solution].

Pour afficher la table des solutions en matière de vulnérabilité, accédez à **Tout** > **Réponse aux vulnérabilités** > **Solutions en matière de vulnérabilité** où vous pouvez afficher et comparer les solutions de différents fournisseurs. Pour afficher les solutions importées dans la table personnalisée, accédez à **Tout** > **Rapid7 Vulnerability Integration** > **Solutions**.

Remarque : Regrouper par source pour afficher les solutions en fonction des fournisseurs.

Intégration de Rapid7 Prerequisite Solution Management

Si vous avez activé le module d'extension Gestion des solutions pour vulnérabilités , un script correctif est exécuté et modifie l'ordre des intégrations. La nouvelle intégration de solutions préalables Rapid7 pour Rapid7 l'entrepôt de données mappe les solutions avec les solutions prérequises. Les intégrations s'exécutent dans la séquence suivante :

1. Rapid7 Intégration de solution
2. Rapid7 Solution prérequise
3. Rapid7 Intégration de solution de remplacement
4. Rapid7 Intégration de la carte de solution de vulnérabilité
5. Rapid7 Intégration de la solution VI (à partir de la version 19.0 de Réponse aux vulnérabilités)

Remarque : Si vous exécutez les intégrations manuellement, commencez par l'intégration de la Rapid7 solution. Ne modifiez pas la chaîne d'intégration suivante dans l'intégration Rapid7 . La séquence est définie dans la colonne Intégration suivante.

Liste connexe Rapid7 (Solutions) sur TPE

Si vous avez activé le module d'extension Gestion des solutions pour vulnérabilités , vous pouvez effectuer les opérations suivantes :

- Vous pouvez afficher les TPE en accédant à **Tout** > **Réponse aux vulnérabilités** > **Tiers**.
- Vous ne pouvez pas voir la liste connexe Solutions (Rapid7), qui était disponible dans les versions antérieures.
- Vous pouvez voir les solutions liées à Rapid7 dans la liste connexe des solutions, ainsi que les solutions d'autres sources, telles que RedHat, Microsoft (MSRC), etc.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous n'avez pas activé le module d'extension Gestion des solutions pour vulnérabilités , les événements suivants se produisent :

- La fonctionnalité des listes connexes reste la même.
- Vous pouvez consulter la liste connexe Solutions (Rapid7).
- La liste connexe Solutions est masquée.

Solution privilégiée sur les TPE et les VI

Rapid7 obtient la solution de l'entrepôt de données au niveau de l'entrée tierce (TPE) et Rapid7 InsightVM au niveau de la détection.

Pour un Rapid7 entrepôt de données, la solution est gérée de la manière suivante :

- La solution privilégiée est définie sur le TPE en fonction de la vulnérabilité et du mappage de la solution.
- Si la vulnérabilité de a Rapid7 une seule solution de remplacement la plus élevée de Rapid7, alors elle est définie comme la solution préférée, quelles que soient les autres solutions des fournisseurs attachés à cette vulnérabilité.
- Dans tous les autres cas, le flux de la solution privilégiée reste le même. Pour en savoir plus sur le comportement par défaut des solutions privilégiées, reportez-vous à la section Gestion des solutions pour vulnérabilités.

Pour Rapid7 InsightVM, la solution est gérée de la manière suivante :

- La solution privilégiée est déployée des détections aux VI.
- S'il n'existe qu'une seule détection et une seule solution à partir de Rapid7, la solution est déployée jusqu'à VI.
- S'il existe plusieurs détections et qu'elles ont toutes la même solution à partir de Rapid7, la solution est déployée jusqu'à VI.
- Si plusieurs détections ont plusieurs solutions à partir de Rapid7, la dernière solution est déployée sur le VI.

À partir de la version 19.0 de Réponse aux vulnérabilités, la solution privilégiée, générée par Rapid7 Data Warehouse, est directement renseignée sur les éléments Rapid7 vulnérables en contournant le besoin de Gestion des solutions pour vulnérabilités. Ce changement permet d'éliminer toute incertitude quant aux solutions potentielles pour ces éléments vulnérables.

Pour atteindre cette population directe par le biais Rapid7de , les mesures suivantes sont prises :

- Une nouvelle intégration, Rapid7 VI Solution Integration, est établie et intégrée dans le workflow existant de Rapid7 Vulnerability Integration.
- Une nouvelle table [sn_vul_r7_rapid7_vi_solution_import] est créée.
- Une nouvelle carte de transformation Rapid7 VI Solution Transform est créée.
- L'include de script Rapid7AssetsImportProcessor est modifié pour exclure le traitement des solutions générées par Rapid7 dans Gestion des solutions pour vulnérabilités.

Lors de l'exécution de l'intégration de la solution Rapid7 VI, les données non traitées obtenues à partir de Rapid7 sont stockées dans la table nouvellement créée. Par la suite, la transformation de la solution Rapid7 VI est déclenchée, traitant ces données et renseignant la solution préférée directement dans la table des éléments vulnérables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'intégration de la solution Rapid7 VI renseigne la solution préférée exclusivement lorsque le module d'extension Gestion des solutions pour vulnérabilités a été installé.

À partir de la version 22.0 de , les solutions de ne sont plus mises en file d'attente lors de Réponse aux vulnérabilitésRapid7 l'exécution de la tâche *Process Vulnerability Solutions Metrics Queue*planifiée. Cette tâche planifiée implique le déploiement de solutions à partir d'entrées NVD vers des entrées tierces, le remplissage des solutions préférées sur les vulnérabilités et la mise à jour des mesures d'état de rattrapage sur les solutions. Dans les scénarios suivants, seules les mesures d'état de rattrapage doivent être mises à jour :

- Lorsque la solution préférée change en fonction des vulnérabilités
- Lorsque les VIT sont créés ou supprimés
- Lorsqu'une importation VIT est terminée

Bien que les solutions soient mises en file d'attente pour mettre à jour uniquement les mesures d'état de rattrapage, elles tentent toujours de déployer des solutions à partir d'entrées NVD vers des entrées tierces et de renseigner les solutions privilégiées. Pour optimiser ce processus, la colonne Statut de mise **à jour** est introduite dans la table Solution de vulnérabilité. Lorsque les mesures d'état de rattrapage des solutions doivent être mises à jour sans nécessiter le déploiement des solutions à partir des entrées NVD vers les entrées tierces ou le remplissage des solutions privilégiées, elles ne sont plus en file d'attente. Au lieu de cela, la colonne **Mettre à jour l'état** est directement mise à jour en tant que vrai. Cette approche permet de traiter les tickets où seules les mesures d'état de rattrapage doivent être mises à jour, ce qui permet de réaliser des économies de temps et de ressources. Dans la tâche planifiée, une fois le traitement des solutions en file d'attente terminé, les solutions marquées avec un état de mise à jour défini sur vrai sont identifiées. Ensuite, ces solutions sont itérées, en calculant les nombres et en mettant à jour les mesures d'état de rattrapage en conséquence. Cette étape joue un rôle important dans l'amélioration des performances de la tâche planifiée, car le nombre de solutions à mettre en file d'attente est réduit.

Chaîne de remplacement de solution importée d'un entrepôt de données Rapid7 pour une vulnérabilité

Vous pouvez afficher les solutions de remplacement d'une solution en sélectionnant une solution de vulnérabilité et en sélectionnant la liste connexe Solutions de remplacement. Vous pouvez afficher les solutions précédentes en sélectionnant la liste connexe Solutions précédentes. Lorsque vous attachez une solution au TPE, la solution de remplacement de cette solution est attachée à ce TPE.

Modifier la profondeur maximale de la chaîne de remplacement de solution dans un graphique par propriété système

La chaîne de remplacement de la solution reçue dans le Rapid7 modèle de données est trop longue pour créer le graphique lors du remplissage de la solution préférée. Ainsi, pour limiter la profondeur de la chaîne, une propriété système nommée *sn_vul.max_recursion_depth* avec une valeur 500 est créée. Si la profondeur de la chaîne est supérieure à 500, le reste de la chaîne est ignoré. Pour modifier la profondeur maximale de la chaîne, accédez à la table [sys_properties] et modifiez la valeur de la propriété.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise à niveau de l'application Rapid7

Si vous mettez à niveau le Intégration des vulnérabilités Rapid7 module d'extension et que vous ne l'avez pas encore activé Gestion des solutions pour vulnérabilités , l'application fonctionne telle quelle.

Que vous activiez le module d'extension Gestion des solutions pour vulnérabilités avant ou après la mise à niveau de l'application Rapid7 , le champ **Importer depuis** reste vide pour les intégrations suivantes :

- Intégration de la solution de remplacement Rapid7
- Intégration de la carte de solutions de vulnérabilité Rapid7
- Intégration de la solution Rapid7

> **Remarque :** À partir de l'exécution de l'intégration suivante, les données sont renseignées dans la table de solution de vulnérabilité.

Pour Rapid7 InsightVM, les données sont reçues au niveau de la détection. Lorsque l'intégration s'exécute Rapid7 InsightVM , les solutions sont importées dans la table des solutions de vulnérabilité.

Cadre de travail générique pour ingérer des données provenant de n'importe quel fournisseur de solution

Un cadre de travail générique pour l'intégration de l'intelligence des solutions est disponible pour prendre en charge l'ingestion de données dans différents formats de fichiers auprès des fournisseurs de solutions. Ces formats accélèrent l'échange et le traitement de l'information et facilitent le partage d'informations critiques liées à la sécurité dans un format de rapport normalisé.

Les formats de fichier pris en charge sont les suivants :

CVRF (Common Vulnerability Reporting Framework)

Le Common Vulnerability Reporting Framework (CVRF) est un langage basé sur XML. Les principaux fournisseurs tels que Oracle, Red Hat, Cisco, et Microsoft prennent en charge le format CVRF.

Cadre consultatif de sécurité commun (CSAF)

Le Cadre commun consultatif de sécurité (CSAF) est une norme open source qui fournit des avis de sécurité structurés et lisibles par machine basés sur JSON. Les principaux fournisseurs tels que Siemens, Red HatHitachi et Schneider prennent en charge le format CSAF.

La gestion des solutions prises en charge par le CVRF ou le CSAF comprend les fonctionnalités clés suivantes :

- Configuration via l'assistant de configuration
- Prise en charge de l'importation de données CVRF ou CSAF par le biais de l'importation de fichiers
- Prise en charge de l'importation de données CVRF ou CSAF par le biais d'une URL CVRF ou CSAF
- Prise en charge de l'importation de données CVRF ou CSAF par le biais d'avis
- Mappage des solutions avec les vulnérabilités associées

Le module d'extension Vulnerability Response prend en charge la mise à jour des statuts des mesures de la solution créée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

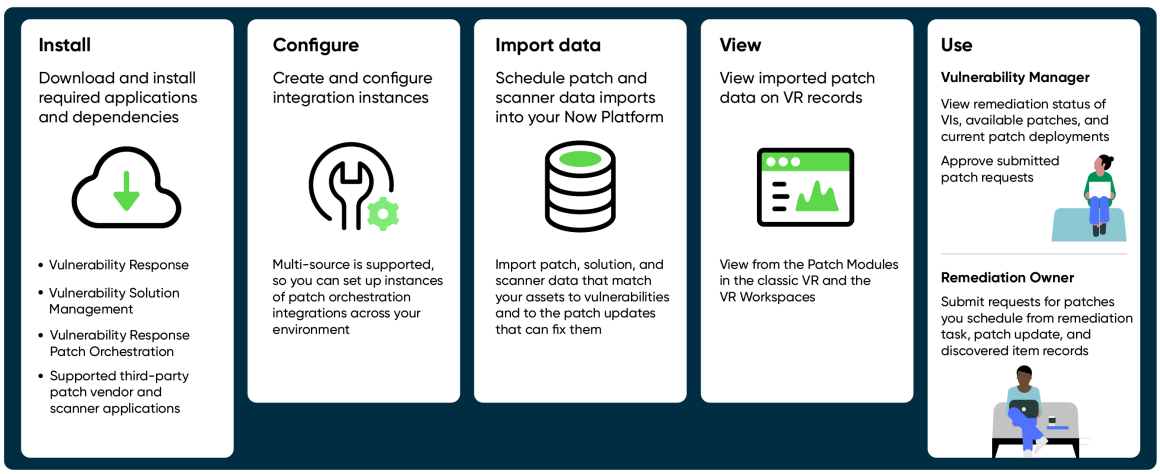
Pour en savoir plus sur la configuration des fournisseurs de solutions, reportez-vous à la section Configurer les fournisseurs de solutions en matière de vulnérabilité.

Orchestration des correctifs avec Réponse aux vulnérabilités

Vous pouvez gérer les correctifs et les déploiements de correctifs pour les vulnérabilités critiques de grands groupes de vos actifs avec l'orchestration de correctifs avec Réponse aux vulnérabilités. Réponse aux vulnérabilités Patch Orchestration et les intégrations Patch Orchestration sont disponibles sur le ServiceNow® Store.

Comprendre l'orchestration des correctifs avec Réponse aux vulnérabilités

Patch orchestration with Réponse aux vulnérabilités utilise les données des importations planifiées provenant d'intégrations de solutions tierces, de fournisseurs de correctifs et d'analyseurs de vulnérabilité. Ces données sont corrélées dans l'application Réponse aux vulnérabilités . Cette organisation des données vous permet d'effectuer les étapes du cycle de rattrapage de vulnérabilité. Commencez par identifier les vulnérabilités, puis appliquez des correctifs et des mises à jour, et enfin fermez les éléments vulnérables à l'aide de données d'analyseurs tiers, le tout à partir de votre Now Platform® instance.



L'orchestration des correctifs est Réponse aux vulnérabilités prise en charge à la fois dans l'environnement classique et dans les Réponse aux vulnérabilités espaces de travail.

Pour en savoir plus sur l'orchestration des correctifs dans les espaces de travail, reportez-vous à la section Appliquer des correctifs à Orchestration avec les Réponse aux vulnérabilités espaces de travail.

Avec l'orchestration des correctifs dans Réponse aux vulnérabilités, les gestionnaires et analystes de vulnérabilités et les spécialistes de la remédiation informatique peuvent effectuer les tâches de remédiation suivantes :

- Pour en savoir plus sur les types de correctifs et les fournisseurs qui les composent, consultez plus de contexte et d'informations sur les types de correctifs et les fournisseurs qui composent leurs solutions (correctifs).
- Affichez et surveillez les données de vulnérabilité et de solution, ainsi que la progression du rattrapage des vulnérabilités à partir d'enregistrements dans les Réponse aux vulnérabilités espaces de travail ou dans l'environnement classique.
- Déployez des correctifs pris en charge par les fournisseurs de solutions tiers pour leurs Windows, CentOS MacOSOracleet d'autres actifs à intervalles réguliers et planifiés. Vous pouvez programmer des correctifs en dehors des heures de travail pour éviter les conflits avec les personnes au travail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- À l'aide des données de détection importées fournies par des scanners tiers, identifiez les actifs qui présentent des vulnérabilités et qui ne sont pas corrigés ou qui ne sont pas mis à jour correctement par les correctifs planifiés.
- Lancez et planifiez les correctifs disponibles pour les actifs qui nécessitent des mises à jour à partir d'enregistrements de mise à jour de correctifs, de tâche de rattrapage et d'éléments détectés dans l'application Réponse aux vulnérabilités .
- Surveillez les déploiements de correctifs avec un processus d'approbation facultatif pour les demandes de correctifs soumises par vos spécialistes du rattrapage.

Termes clés

Élément de configuration (CI)

Les CI sont les actifs existants répertoriés dans votre Base de données de gestion des configurations (CMDB).

Élément vulnérable (VI)

Une vulnérabilité importée qui correspond à un actif existant dans votre CMDB. Les éléments vulnérables (VIT) sont regroupés en tâches de rattrapage, ou listes, en fonction de certains critères qui spécifient des actions de rattrapage pour les VI.

Instance

Fait référence à un compte distinct d'une application du fournisseur de solutions. Par exemple, chaque compte d'utilisateur peut être une instance de l'application HCL BigFix. Ce terme désigne également une adresse Web unique et sécurisée pour une Now Platform® instance.

Solution

Il existe deux types de solutions dans le cadre de cette intégration, potentielles et préférées. Une solution potentielle est une solution qui pourrait remédier à une vulnérabilité. Les vulnérabilités ont souvent de nombreuses solutions potentielles. #Une solution privilégiée correspond à la solution la plus efficace pour une vulnérabilité spécifique détectée.

Correctif

Mises à jour logicielles qui corrigent les vulnérabilités. Les fournisseurs de correctifs utilisent leur propre nom pour les correctifs, par exemple, dans l'application HCL BigFix, les correctifs sont appelés fixlets.

Correctif préféré

Les correctifs préférés sont les mises à jour logicielles destinées à corriger des vulnérabilités spécifiques. Les correctifs, une fois déployés, sont mappés aux éléments vulnérables liés à des vulnérabilités spécifiques et corrigent-les.

Déploiement

Aux fins de cette intégration, le déploiement désigne le moment où vous appliquez, lancez ou planifiez un correctif sur un ordinateur.

Le déploiement dans le Now Platform peut également faire référence à une intégration qui prend en charge plusieurs sources. Une existence d'intégration unique est appelée un déploiement de votre intégration. Un déploiement fait référence aux intégrations et aux produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements d'un scanner tiers ou d'une intégration de fournisseur de solution dans votre environnement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions disponibles des applications et dépendances requises pour l'intégration d'orchestration de correctifs

- L'application Vulnerability Response et les modules d'extension de dépendance, Security Support Common et Security Support Orchestration.
- Gestion des solutions pour vulnérabilités.
- Réponse aux vulnérabilités Application Patch Orchestration disponible dans le ServiceNow® Store.
- Une application de fournisseur de correctifs tiers prise en charge, telle que l'intégration d'orchestration de correctifs Vulnerability Response avec HCL BigFix ou l'intégration d'orchestration de correctifs de Vulnerability Response avec Microsoft SCCM.
- Intégrations de scanners tiers prises en charge avec Vulnerability Response.

Rôles requis

Les utilisateurs ont besoin de rôles spécifiques à l'intégration d'orchestration de correctifs que vous utilisez pour afficher les données et planifier les correctifs à partir de l'application Réponse aux vulnérabilités . Consultez les informations de configuration des intégrations prises en charge que vous utilisez et qui sont répertoriées ci-dessous pour en savoir plus.

- Présentation de l'intégration de l'orchestration des correctifs HCL BigFix avec Réponse aux vulnérabilitéset l'intégration de l'orchestration des correctifs Vulnerability Response à Microsoft SCCM.
- Dans les Réponse aux vulnérabilités espaces de travail et l'environnement classique, le rôle sn_vul_patch_orch.read_patch, qui permet aux utilisateurs d'afficher des données mais pas de les modifier, est hérité des rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst.

  Les rôles que vous devez affecter pour configurer les connexions aux fournisseurs de correctifs et planifier les correctifs sont spécifiques à l'intégration. Consultez Configurer l'intégration d'orchestration de correctifs Réponse aux vulnérabilités avec HCL BigFix et configurez Orchestration des correctifs de réponse aux vulnérabilités avec MS SCCM pour plus d'informations.

Il existe un processus de soumission et d'approbation pour les demandes de correctifs incluses dans les applications. Par défaut, une propriété système est activée [**sn_vul_patch_orch.patch_approval_required**] dans l'application Vulnerability Response Patch Orchestration dans votre Now Platform instance.

Cette propriété système est activée de sorte que, lorsque des déploiements de correctifs sont planifiés, ils sont soumis pour examen et approbation aux utilisateurs affectés au groupe d'approbation de mise à jour de correctif de niveau 1. Si vous souhaitez que les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch planifient des correctifs sans approbation, vous pouvez désactiver la propriété [**sn_vul_patch_orch.patch_approval_required**]. Vous préférez peut-être laisser les approbations activées afin que les correctifs planifiés n'entrent pas en conflit avec les heures de travail normales. Si vous désactivez la propriété système d'approbation, tout utilisateur disposant du rôle sn_vul_patch_orch.configure_patch peut planifier et déployer des correctifs sans examen ni approbation.

Pour en savoir plus et savoir comment désactiver cette propriété système, consultez la rubrique de configuration de votre intégration prise en charge.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Configurer l'intégration d'orchestration de correctifs Réponse aux vulnérabilités avec HCL BigFix.
- Configurer l'orchestration des correctifs de réponse aux vulnérabilités avec Microsoft l'intégration SCCM.

Planifier les correctifs à partir des Réponse aux vulnérabilités enregistrements

Les spécialistes de la correction peuvent planifier des mises à jour de correctifs pour résoudre les éléments vulnérables et surveiller la progression du rattrapage, le tout à partir d'enregistrements dans l'application Réponse aux vulnérabilités .

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- Mise à jour du correctif
- Tâche de rattrapage
- Élément détecté

Enregistrements qui déploient des nombres de VI actifs dans Réponse aux vulnérabilités

Pour éviter d'éventuels problèmes de performances lors du déploiement de tous les correctifs sur toutes les vulnérabilités, la tâche planifiée qui récupère les changements ne modifie que le nombre de VI actifs. Ces changements de nombre et les données connexes sont déployés dans les enregistrements suivants dans l'application Réponse aux vulnérabilités :

- VIT (élément vulnérable)
- RT (tâche de rattrapage)
- Solution de vulnérabilité
- Mise à jour du correctif

Pour plus d'informations sur l'affichage des données de correctifs et du déploiement des données de correctifs dans les enregistrements, ainsi que sur l'affichage des correctifs sans solutions, consultez les rubriques suivantes.

- Déploiement des données et de l'état des correctifs pour l'orchestration des correctifs dans Réponse aux vulnérabilités.
- Affichage des données de correctifs et planification des correctifs dans Réponse aux vulnérabilités.
- Afficher les correctifs sans solution dans Réponse aux vulnérabilités.

Modifier en bloc les éléments vulnérables avec des correctifs

Vous pouvez modifier en bloc les éléments vulnérables de l'environnement classique qui ont des correctifs de l'environnement classique. Pour en savoir plus sur le fonctionnement de la modification en bloc, reportez-vous à la section Modifier les éléments vulnérables en bloc dans Réponse aux vulnérabilités. Les correctifs préférés pour tous les VI sélectionnés pour la modification en bloc. Cette option de modification ne fonctionne que si des correctifs préférés sont mappés à tous les VI sélectionnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble de la gestion des exceptions

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive de sécurité ou de gestion des vulnérabilités publiée, vous pouvez demander une exception. La gestion des exceptions implique de demander, examiner, approuver ou rejeter des exceptions à un élément vulnérable (VI) ou à une tâche de rattrapage (RT) qui ne peuvent pas être corrigés conformément à la politique.

Certaines vulnérabilités peuvent ne pas disposer d'un correctif, d'un correctif ou d'une solution existante. Lorsqu'une exception est approuvée, cela signifie également que vous acceptez un risque, car vous reconnaissez et acceptez les conséquences de ne pas corriger la vulnérabilité.

Cycle de vie d'une exception

Définition d'une exception

Une exception est une demande de différer le rattrapage d'un VI ou d'un RT pour une période spécifiée. Par exemple, en tant que propriétaire du rattrapage, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine.

Demande d'une exception

En tant que propriétaire du rattrapage, vous pouvez demander une exemption pour un VI ou un RT à l'aide du processus de gestion des exceptions. Une fois que l'approbateur d'exceptions a approuvé cette demande, le VI ou le RT passe à un état **Différé** .

Approuver une demande d'exception

Les éléments vulnérables ou les éléments vulnérables qui ne peuvent pas être corrigés immédiatement sont examinés par des analystes de vulnérabilité, évalués pour déterminer leur risque et approuvés pour être reportés jusqu'à ce qu'ils puissent être corrigés. L'approbation d'une demande d'exception peut être un workflow à deux niveaux. Si seul l'approbateur de premier niveau est présent, l'exception peut être demandée et approuvée. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Consultez Ajouter un approbateur d'exception pour plus d'informations.

Remarque :

- À partir de la Réponse aux vulnérabilités version 15.0, si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas le repasser en workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et des faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

  Une fois qu'une demande d'exception pour un VI ou un RT est approuvée, vous pouvez effectuer les actions suivantes :

  - Rouvrir
  - Supprimer
  - Mettre à jour les champs **Affectation à** ou **Groupes d'affectation**
- À partir de la version 23.0 de , le workflow **Approbation de l'état des règles d'exception**Réponse aux vulnérabilitésest déconseillé et remplacé par l'approbation des règles d'exception du flux dans le concepteur de flux.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

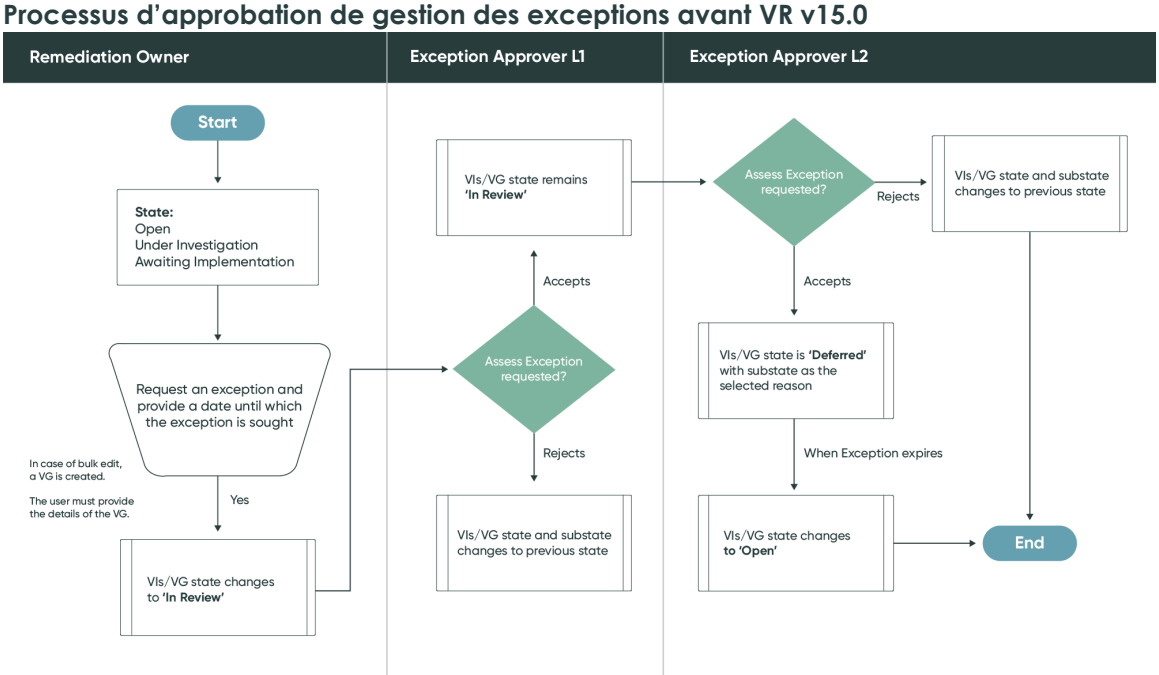
Suivi d'une demande d'exception

Après avoir déclenché l'exception, vous pouvez suivre son état à l'aide de l'onglet **Approbations de changement d'état** du VI ou du RT. Si une action est effectuée sur un RT, vous ne pouvez pas suivre l'état des VI individuels dans ce RT.

Expiration d'une demande d'exception

Lorsqu'une demande d'exception pour un VI ou un RT particulier expire, le VI ou le RT impacté revient à son état **Ouvert** .

Processus d'approbation de gestion des exceptions avant VR v15.0



Si un seul VI ou tous les VI d'un RT passent lors de l'analyse suivante, les VI et, le cas échéant, le champ **État** RT basculent sur **Fermé** avec le sous-état **Fixe**.

Reports multiples

Suivez le nombre de fois où un enregistrement ou une tâche de rattrapage est différé. Une tâche planifiée, *`set deferral counts`*, s'exécute quotidiennement pour publier les nombres des enregistrements qui sont différés plus d'une fois dans la colonne Nombre de reports du module Plusieurs reports pour VR. Tous les décomptes des enregistrements associés à une tâche de rattrapage sont collectés et publiés si une tâche de rattrapage est reportée plusieurs fois.

Information associée

Demander des exceptions pour les tâches et les enregistrements de rattrapage auprès du Espace de travail du gestionnaire de vulnérabilités

Demander une exception dans le Espace de travail de remédiation IT

Demander une exception à l'aide GRC : gestion de la politique et de la conformité de Espace de travail de remédiation IT

Vue d'ensemble des règles d'exception

Les règles d'exception vous Réponse aux vulnérabilités permettent d'automatiser le processus de report pour les éléments vulnérables (VI). Demandez une exception pour les éléments vulnérables (VI) qui ne peuvent pas être corrigés ou différés immédiatement, en identifiant les vulnérabilités, éléments de configuration (CI) ou VI impactés. Différer les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

éléments vulnérables correspondants en fonction de la règle lorsque le système les identifie en automatisant le processus de report des éléments vulnérables.

Utilisation des règles d'exception dans votre organisation

Utilisez les règles d'exception pour différer automatiquement les VI nouveaux et existants pour une période spécifique s'ils correspondent à la condition de règle approuvée. L'automatisation minimise le risque de manquer les accords sur les niveaux de service et facilite la gestion de plusieurs éléments, car vous éliminez les interventions manuelles.

Les règles de report prennent en charge la fonction de classement, c'est-à-dire que la règle ayant la priorité la plus élevée est exécutée en premier. Lorsqu'une règle de priorité élevée est appliquée à un élément vulnérable, aucune règle subséquente n'est réappliquée à celui-ci, même si la condition correspond au élément vulnérable.

Remarque :

- Vous ne pouvez créer des règles que si vous les sélectionnez Réponse aux vulnérabilités dans la configuration Gestion des exceptions. Pour plus de détails, voir Configurer la gestion des exceptions pour Réponse aux vulnérabilités.
- Lorsque les VI sont différés par une règle d'exception, ils sont copiés dans le groupe de vulnérabilité de report (VG) créé. Les VI continuent de faire partie des groupes de vulnérabilité dont ils faisaient partie auparavant.

Le cycle de vie d'une règle d'exception est le suivant :

- Création d'une règle d'exception
- Approuver une demande de règle d'exception
- Activation d'une règle d'exception
- Différer une règle d'exception
- Expiration d'une règle d'exception

Création d'une règle d'exception

Vous pouvez créer une règle d'exception pour différer automatiquement les VI qui correspondent aux conditions définies pour la période spécifiée. Après avoir créé une règle d'exception, soumettez-la pour approbation.

Approuver une demande de règle d'exception

L'approbation d'une demande de règle d'exception est un processus à deux niveaux. Si seul l'approbateur de premier niveau est présent, la règle d'exception peut être évaluée et approuvée par une seule approbation. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une approbation de règle d'exception ne peut pas être approuvée. Une fois la règle approuvée, une tâche de rattrapage (RT) est créée. Consultez Approuver une demande de règle d'exception pour plus d'informations.

Remarque :

À partir de la Réponse aux vulnérabilités version 15.0, si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas le repasser en workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et des faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois qu'une demande de règle d'exception est approuvée, vous pouvez effectuer les actions suivantes :

- Annuler
- Supprimer

Activation d'une règle d'exception

Après l'approbation d'une règle d'exception, une tâche de rattrapage est créée à l'état Différé par défaut. À partir de la date de début de validité, la règle d'exception s'exécute sur tous les VI créés, ainsi que sur ceux qui passent de l'état Fermé à l'état Ouvert.

Remarque : Si vous activez l'option Exécuter sur les données existantes, une tâche planifiée s'exécute une fois sur les données existantes à la date de début de validité.

Différer une règle d'exception

Vous pouvez différer les VI qui correspondent aux conditions définies dans cette règle d'exception, jusqu'à la date « Reporté jusqu'à » définie pour la règle. À cette date, la tâche de rattrapage que vous avez créée pour la règle d'exception est fermée et tous les VI de ce groupe reviennent à l'état Ouvert. Des règles de groupe leur sont à nouveau appliquées pour les allouer aux RT requis.

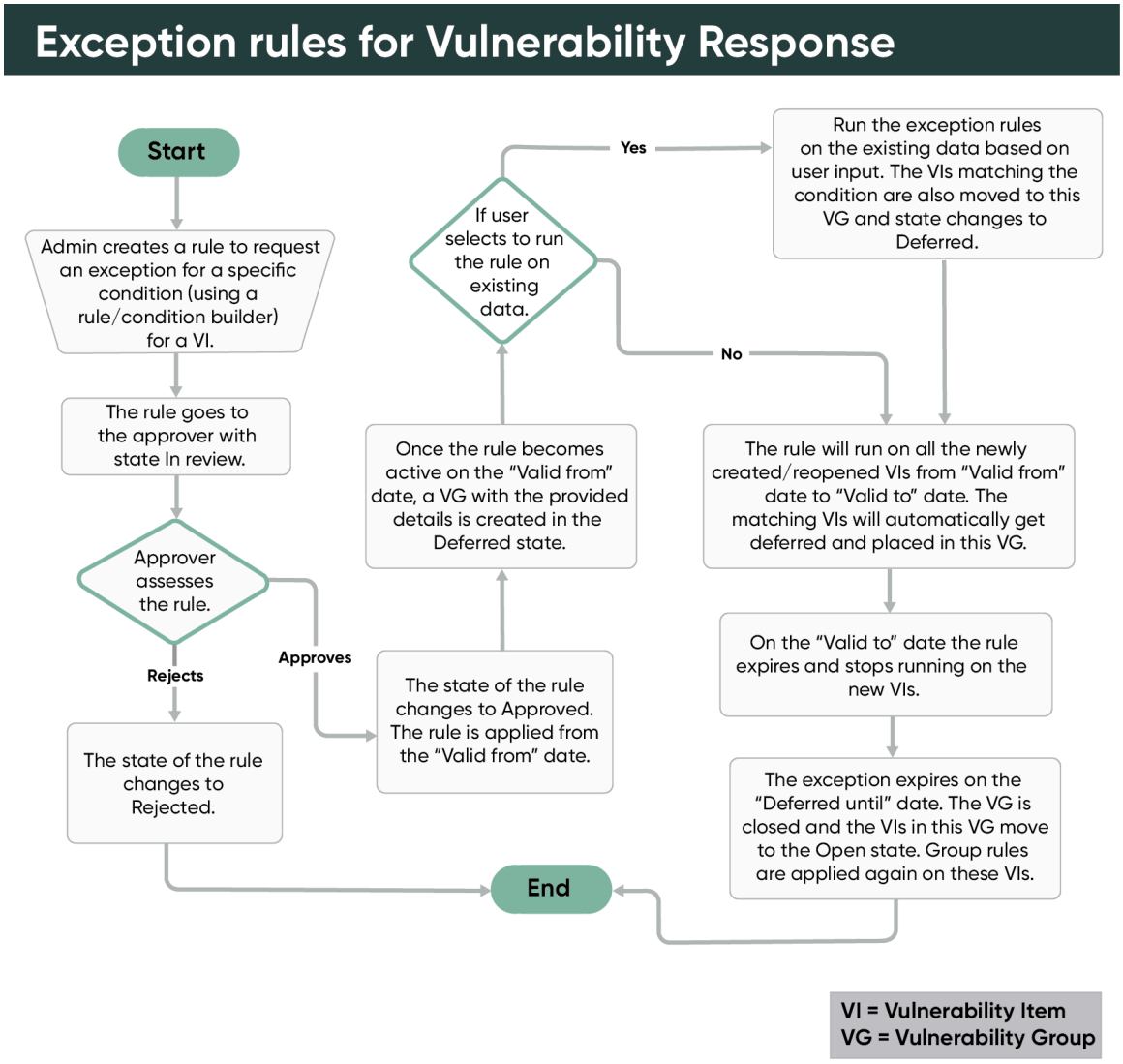
Expiration d'une règle d'exception

Une fois la règle d'exception expirée, elle ne s'exécute plus sur les VI nouveaux ou rouverts. Le RT associé reste dans l'état Différé jusqu'à la date « Reporté jusqu'à ».

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de travail des règles d'exception antérieur à la version 15.0



Vue d'ensemble des règles d'exclusion

Les règles d'exclusion fournissent un moyen de filtrer ou d'empêcher les détections d'être converties en éléments vulnérables (VIT) pendant le processus d'ingestion dans Réponse aux vulnérabilités.

Ces règles peuvent être configurées pour gérer divers scénarios tels que :

- À l'exclusion des vulnérabilités de faible gravité ou de faible risque qui ne nécessitent pas de correction immédiate.
- Amélioration du processus de rattrapage en hiérarchisant les VIT les plus critiques en vue d'une action.
- Réduction du temps de traitement pendant l'importation des données en excluant un pourcentage de détections de la conversion VIT.

Pendant le processus d'ingestion des données, il existe des approches distinctes pour gérer les détections nouvelles et existantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour les nouvelles détections :
  - Si une nouvelle détection ne répond pas aux conditions d'une règle d'exclusion, une détection est créée avec les VIT.
  - Si une nouvelle détection remplit les conditions d'une règle d'exclusion, la règle est associée à la détection, mais VIT n'est pas créé. Renseignez la référence de règle d'exclusion correspondante sur l'enregistrement de détection. La colonne Règle d'exclusion est renseignée en conséquence avec une référence à la règle d'exclusion sur l'enregistrement de détection.
- Pour les détections existantes :
  - Si la détection ne répond pas aux conditions d'une règle d'exclusion, elle poursuit le workflow normal.
  - Si une détection existante correspond aux conditions d'une règle d'exclusion, le VIT associé à cette détection reste dans son état actuel, mais la règle est associée à la détection. L'état du VIT est régi par la valeur définie dans la *sn_vul.close_vit_with_excluded_detections* propriété. Par défaut, la valeur de cette propriété est définie sur Faux. Si la valeur est définie sur Faux, les détections sous un VIT sont exclues et l'état des VIT reste dans son état actuel. Toutefois, si la valeur est définie sur Vrai, les scénarios suivants peuvent se produire :
    - Si toutes les détections dans le cadre d'un VIT sont exclues, l'état du VIT est mis à jour et prend la valeur Fermé exclu.

      Remarque : À partir de la v22.1.2 d'un Réponse aux vulnérabilités nouveau sous-état appelé Exclu a été ajouté,

    - Si une détection est marquée comme fermée alors que les autres sont exclues, le VIT est désigné comme fermé fixe.
    - Si le VIT présente des détections ouvertes, il reste ouvert.

Information associée

Créer une règle d'exclusion

Vue d'ensemble des faux positifs

Un faux positif est une condition dans laquelle le scanner signale qu'une vulnérabilité existe dans le système, alors qu'en réalité il n'y a pas de vulnérabilité. Il peut y avoir plusieurs raisons telles qu'une classification incorrecte, une logique ou un algorithme incorrect dans le scanner. Le propriétaire de la remédiation peut marquer des éléments vulnérables (VI) ou des tâches de remédiation (RT) comme des faux positifs.

Important : Vous pouvez marquer les éléments vulnérables de l'hôte comme faux positifs en bloc dans le Espace de travail du gestionnaire de vulnérabilitésfichier . Pour plus d'informations sur la façon de marquer les éléments vulnérables de l'hôte comme faux positifs en bloc, reportez-vous à la section Modification en bloc pour les faux positifs dans Vulnerability Manager Workspace.

Cycle de vie d'un faux positif

Signification de faux positif

Le scanner donne parfois un avertissement, alors qu'en réalité il n'y a pas de vulnérabilité. Par exemple, si un élément de configuration a été mis hors service, mais que le scanner soulève toujours un problème qui lui est lié, marquez-le comme faux positif.

Marquage comme faux positif

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur le marquage d'un VI ou d'un RT comme faux positif, reportez-vous à la section Marquer comme faux positif.

Travailler avec le faux positif

Une fois qu'une VI ou une RT est marquée comme faux positif, l'état est mis à jour sur Fermé et le sous-état est basculé sur Faux positif. Les actions suivantes peuvent être effectuées :

- Rouvrir
- Supprimer
- Mettez à jour la date dans le champ **Jusqu'à** . Cette date est ensuite utilisée comme date d'expiration du faux positif.

Remarque : S'il n'est pas approuvé, le VI ou le RT revient à son état précédent.

Approuver un faux positif

L'approbateur peut approuver le faux positif à partir de son workflow d'approbation.

Remarque :

À partir de Vulnerability Response v15.0, si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas le repasser en workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et des faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Réouverture d'un faux positif

Un VI ou un RT dans un sous-état de faux positif peut être rouvert à tout moment.

Suivi d'un faux positif

Utilisez la section **Approbations de changement d'état** pour suivre l'état du faux positif. Une fois approuvée, l'état de la VI ou de la RT est mis à jour sur Fermé et la raison est Faux positif.

Expiration d'un faux positif

Seul l'approbateur de faux positif peut définir une date de fin pour le faux positif, pour que le VI ou le RT expire. En outre, seuls les faux positifs pour lesquels l'approbateur a fourni une date de fin peuvent expirer. Cette date peut être fournie après l'approbation du faux positif.

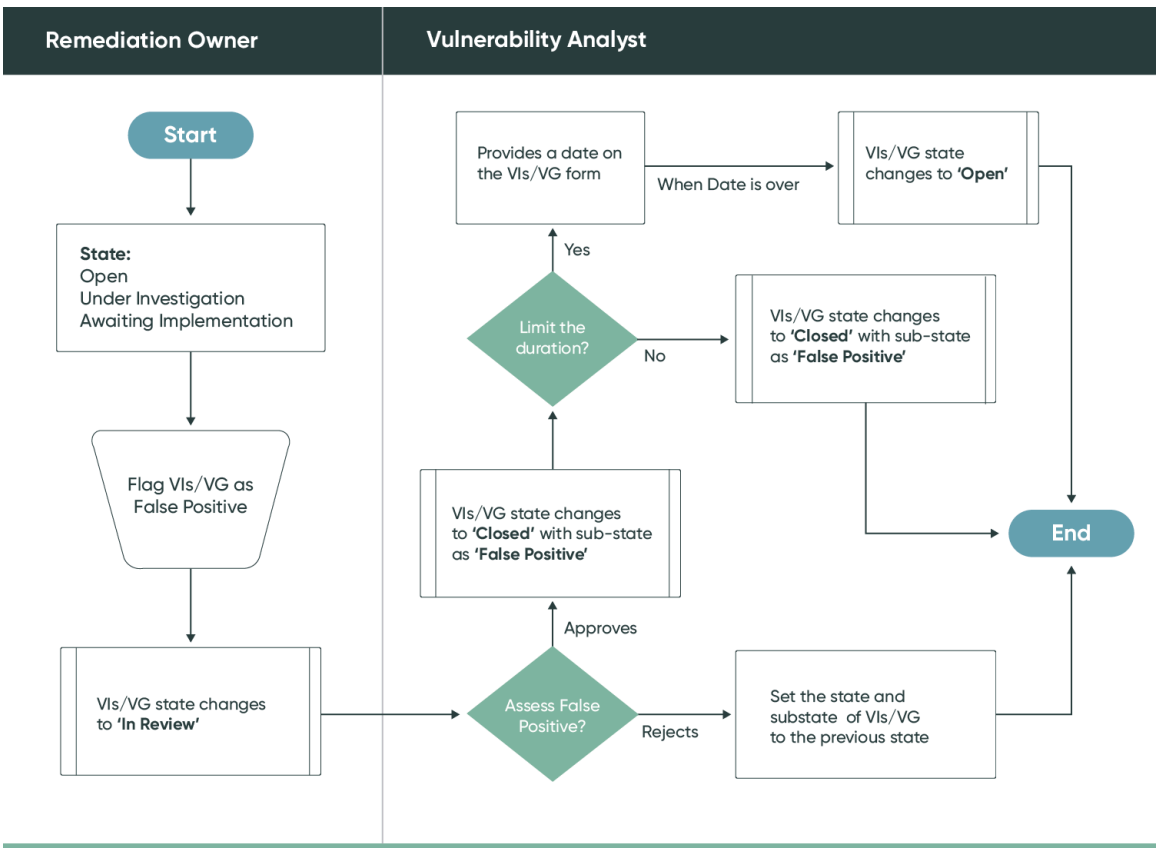
Un faux positif sans date de fin est un faux positif permanent. Après l'expiration du faux positif, l'état du VI ou du VR revient à Ouvert.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

À partir de la version 21.0 de Réponse aux vulnérabilités, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Processus d'approbation des faux positifs antérieurs à la version 15.0



Traduction automatique

Le processus d'approbation est automatique si tous les éléments vulnérables réussissent l'analyse suivante. Les VI se ferment automatiquement quel que soit leur état actuel. Les **champs VI** ou, le cas échéant, État RT basculent sur **Fermé** avec le sous-état **Fixe.**

Pour plus d'informations, consultez Marquage et approbation d'un faux positif.

Information associée

Demander un faux positif dans le Espace de travail de remédiation IT

Chien de garde pour Réponse aux vulnérabilités

Le chien de garde est utilisé pour suivre les tables en fonction des conditions que vous spécifiez. Par exemple, il peut être utilisé pour consigner les détails des échecs d'exécution de l'intégration dans Réponse aux vulnérabilités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez choisir d'être informé de ces échecs. Sur la base de cette notification, vous pouvez planifier le rattrapage. Les chiens de garde par défaut sont les suivants :

- Échec de l'exécution de l'intégration : si l'état de l'exécution de l'intégration est défini sur Terminé et que le sous-état est défini sur Échec, les utilisateurs et les groupes d'utilisateurs sont informés si la condition renvoie un nombre supérieur à 0, c'est-à-dire que l'exécution de l'intégration échoue.
- Intégrations à exécution longue : script permettant de vérifier si l'exécution de l'intégration dépasse la durée définie. Cet organisme de surveillance vous alerte de manière proactive chaque fois qu'il y a un retard dans l'exécution de l'exécution de l'intégration.

Journal de surveillance

Le chien de garde est livré avec un journal de surveillance, qui fournit un décompte du nombre de fois où la condition a été remplie.

Tableau de bord de vue d'ensemble

Utilisez le tableau de bord Vue d'ensemble pour surveiller le chien de garde au cours des 30 derniers jours. Vous pouvez créer plusieurs widgets pour suivre d'autres sujets de surveillance que vous surveillez.

À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Rapport

Nom	Description
Échec de WatchDog au cours des 30 derniers jours	Toutes les conditions remplies au cours des 30 derniers jours.

Pour plus d'informations, consultez Configurer WatchDog et Gestion des erreurs pour les détections.

Gestion des changements pour Réponse aux vulnérabilités

En tant que propriétaire de rattrapage informatique, vous pouvez créer et gérer les demandes de changement (CHG) directement à partir des tâches de rattrapage (RT) dans l'application Réponse aux vulnérabilités . Les demandes de changement vous permettent de lancer et de suivre des activités de changement sur vos actifs afin que vous puissiez corriger vos tâches de rattrapage et leurs éléments vulnérables correspondants.

Les demandes de changement et le workflow de vulnérabilité

Si vous ne connaissez pas l'application Vulnerability Response, consultez Exploration de l'application Réponse aux vulnérabilités.

L'image suivante illustre le flux d'informations pour Réponse aux vulnérabilités, depuis l'intégration (scanner) mis en place jusqu'à l'enquête, en passant par le triage automatisé.

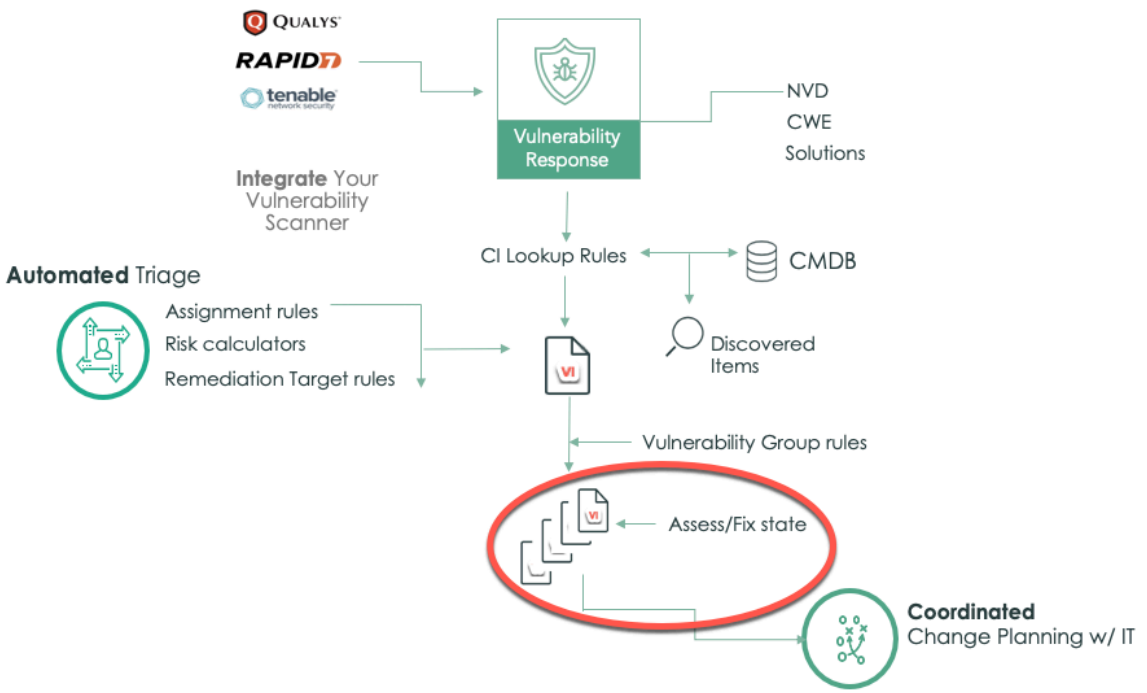
Les demandes de changement et la gestion des changements font partie du processus de rattrapage (état Évaluation/Correction) dans le Réponse aux vulnérabilités workflow illustré dans la figure suivante. Au cours de cette phase, vous pouvez utiliser des demandes de changement pour initier et suivre le rattrapage des vulnérabilités. Vous pouvez créer et

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

gérer des demandes de changement directement à partir de la tâche de rattrapage et répertorier les tâches d'investigation et de rattrapage qui incluent des solutions pour les actifs impactés pour les éléments de configuration (CI) dans votre CMDB.

Demandes de changement dans Vulnerability Response



Quand utiliser les demandes de changement dans Vulnerability Response

En tant que propriétaire du rattrapage informatique, vous pouvez créer des demandes de changement à partir d'une tâche de rattrapage si un processus manuel et contrôlé, quel qu'il soit, est requis pour la modification ou la suppression des éléments de configuration (CI) pris en charge dans votre CMDB. La création et la gestion des demandes de changement directement à partir d'un enregistrement de tâche de rattrapage vous aident à examiner et à résoudre rapidement les vulnérabilités. Les VI d'une tâche de rattrapage résolue peuvent être analysés et vérifiés lors de la prochaine analyse planifiée dans votre Now Platform et renvoyés au triage automatisé du Réponse aux vulnérabilités workflow. Les interventions manuelles qui peuvent nécessiter des demandes de changement incluent les exemples suivants :

- Un correctif logiciel, un correctif ou toute autre tâche du service informatique requise sur les éléments vulnérables avant la résolution RT.
- Vous déterminez qu'un sous-ensemble d'éléments vulnérables dans une tâche de rattrapage nécessite une enquête plus approfondie ou une réaffectation à un autre département.
- Vous déterminez qu'un sous-ensemble d'éléments vulnérables dans un RT avec un grand ensemble d'éléments vulnérables peut être déplacé vers une nouvelle tâche de rattrapage.
- Vous pouvez associer une tâche de rattrapage à une demande de changement existante pour éviter la duplication des tâches de rattrapage.

Types de demandes de changement pour un RT

L'application Réponse aux vulnérabilités utilise les trois types de changements de service pris en charge par le ITSM Gestion des changements produit sur votre Now Platform® instance :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

standard, urgent et normal. Le type de changement que vous sélectionnez détermine le modèle d'état invoqué et le processus de changement à suivre. Les demandes de changement enregistrent les informations détaillées sur le changement, telles que la raison du changement, la priorité, le risque, le type et la catégorie du changement. Reportez-vous à la section Types de changements .

En tant que propriétaire de Réponse aux vulnérabilités rattrapage informatique, vous disposez des options suivantes pour créer des demandes de changement normal, standard et urgent directement à partir d'une tâche de rattrapage :

- Vous pouvez créer des demandes de changement qui contiennent des informations pré-remplies à partir de la tâche de rattrapage pour rationaliser le processus et gagner du temps.
- Vous pouvez associer une tâche de rattrapage à une demande de changement existante pour éviter de créer des demandes de changement en double qui partagent des informations similaires et des éléments vulnérables.
- À l'aide d'un ensemble de conditions, vous pouvez filtrer un sous-ensemble d'éléments vulnérables et diviser une tâche de rattrapage. Les éléments que vous sélectionnez sont automatiquement déplacés vers un nouveau RT.

Vous pouvez filtrer les éléments vulnérables à l'aide des valeurs de n'importe quel champ d'une tâche de rattrapage et appliquer la demande de changement uniquement aux éléments qui correspondent à vos critères de filtre.

Information associée

Créer une demande de changement à partir d'une tâche de rattrapage

Associer une tâche de rattrapage à une demande de changement existante

Diviser une tâche de rattrapage

Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage

Évaluation de l'exposition logicielle à l'aide de Gestion des actifs logiciels (SAM Foundation)

Utilisez l'application Évaluation de l'exposition à la ServiceNow® vulnérabilité pour déterminer le nombre total de logiciels installés pour un package logiciel spécifique sur vos actifs. Lorsqu'elle est utilisée avec l'application ServiceNow® Software Asset Management (SAM) Foundation, évaluez votre exposition, créez des éléments vulnérables et gérez la correction des logiciels vulnérables que vous détectez.

Important : Vous pouvez effectuer l'évaluation de l'exposition par logiciel et par vulnérabilités et expositions courantes (CVE) pour tirer parti des options supplémentaires de l'espace de travail d'évaluation de la vulnérabilité. Pour plus d'informations, consultez Explorer l'espace de travail de l'évaluation de la vulnérabilité.

Déterminez votre exposition aux logiciels vulnérables en fournissant les informations sur les logiciels vulnérables (éditeur, produit, édition et version) sans utiliser la base de données CVE (Common Vulnerabilities and Exposures). Évaluez les tickets de vulnérabilités zero-day (jour actuel) du logiciel pour les cas suivants :

- Lorsque les produits n'ont pas encore de données CVE.
- Lorsqu'il y a un décalage entre le moment où une vulnérabilité devient publique et le moment où les données CVE contenant la vulnérabilité sont mises à jour dans le NVD.
- Lorsque vous en apprenez davantage sur la vulnérabilité entre les analyses planifiées de votre scanner de vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avec l'application Vulnerability Exposure Assessment, si vous connaissez l'éditeur et le produit du logiciel vulnérable, à l'aide des enregistrements qui répertorient les logiciels installés sur votre réseau créés par l'application SAM Foundation , vous pouvez évaluer votre exposition aux packages logiciels potentiellement malveillants à la demande.

Connaître l'ampleur de votre exposition à ce type de vulnérabilité vous permet de réagir de manière proactive en mettant en place une alerte rouge et en désinstallant le logiciel, ou en informant votre centre des opérations de sécurité (SOC) de rechercher un correctif spécifique. Vous pouvez créer des éléments vulnérables et affecter des tâches au spécialiste du rattrapage pour un rattrapage plus approfondi. Affichez une liste de tâches de rattrapage (VUL) pour vérifier que les éléments vulnérables que vous souhaitez sont créés et associés correctement à la VUL.

Information associée

Configurer l'évaluation de l'exposition à la vulnérabilité

Évaluer votre exposition aux logiciels vulnérables

Gestion de crise de vulnérabilité

Créez et suivez les événements de vulnérabilité critiques via le workflow Gestion des crises de vulnérabilité (VCM). Créez des enregistrements d'évaluation de la vulnérabilité, enregistrez les attributs clés de la vulnérabilité pour calculer le risque, effectuez une évaluation pour identifier le niveau d'exposition et impliquez les personnes concernées pour une réponse coordonnée et rapide aux vulnérabilités.

Gestion des événements de crise de vulnérabilité

Vulnerability Crisis Management est un workflow complet pour gérer les événements de crise de vulnérabilité avec les options suivantes.

- Identifiez efficacement les éléments de configuration vulnérables en corrélant les vulnérabilités critiques avec l'inventaire des installations logicielles à partir de l'inventaire et Nomenclature logicielle de Gestion des actifs logiciels l'inventaire (SBOM), les vulnérabilités signalées par les scanners, etcBase de données de gestion des configurations (CMDB).
- Convertissez les résultats de l'évaluation en éléments vulnérables pour le rattrapage.
- Lancez un incident de sécurité majeur afin d'assurer une réponse rapide et coordonnée à la menace.
- Engagez-vous et collaborez avec les équipes de l'ensemble de l'organisation, facilitant ainsi une réponse unifiée aux vulnérabilités.
- Fournir des rapports d'étape réguliers aux parties prenantes interfonctionnelles et aux équipes impliquées afin de maintenir la transparence et la communication tout au long de la crise.

Gestion des crises de vulnérabilité à l'aide de l'espace de travail d'évaluation de la vulnérabilité

Remarque : À partir de la version 1.0.1 de Gestion des crises de vulnérabilité, l'application est disponible sous forme d'abonnement distinct dans le magasin. Vous pouvez accéder à Vulnerability Crisis Management à partir de l'espace de travail d'évaluation de la vulnérabilité uniquement si vous disposez d'une autorisation précise ou si vous avez installé l'application à partir du magasin. Auparavant, Vulnerability Crisis Management était inclus dans le module d'extension Vulnerability Emergency Response. À partir de la version 3.2.2, le module d'extension Vulnerability Emergency Response a été renommé Vulnerability Exposure Assessment.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lors de l'identification d'une vulnérabilité d'intérêt, le gestionnaire d'événements de vulnérabilité crée un enregistrement d'évaluation de la vulnérabilité avec des informations sur la source de renseignements sur les menaces, les caractéristiques de la vulnérabilité et les produits affectés. Ces informations sont utilisées pour une analyse plus approfondie de l'impact et de l'exposition.

Une fois que l'enregistrement d'une vulnérabilité d'intérêt a été créé, une évaluation des risques est effectuée. Cette évaluation comprend une notation structurée des risques, l'examen du dossier et les observations de l'analyste effectuant la tâche. Le score de risque initial pour une vulnérabilité d'intérêt est calculé à l'aide des attributs disponibles au moment de la création de l'événement. Le score de risque de l'évaluation peut changer à mesure que des renseignements supplémentaires deviennent disponibles. Utilisez le score de risque pour déterminer l'impact potentiel de l'exploitation et établir les priorités d'intervention.

Une fois que l'évaluation d'une vulnérabilité d'intérêt a été créée et qu'il a été déterminé qu'elle présente un risque pour l'infrastructure de l'organisation, vous pouvez analyser la menace plus en détail en mettant à jour l'évaluation des risques avec une évaluation approfondie de l'exposition avec l'inventaire des installations logicielles de Gestion des actifs logiciels, Nomenclature logicielle (SBOM) l'inventaire, les vulnérabilités signalées par les scanners et Base de données de gestion des configurations (CMDB). Les applications et éléments de configuration impactés sont automatiquement identifiés par le biais de l'évaluation. D'autres éléments impactés peuvent être ajoutés manuellement.

Une fois l'évaluation terminée, il est possible de créer des éléments vulnérables ou des éléments vulnérables de l'application pour les résultats d'exposition qui n'ont pas déjà d'élément vulnérable associé. Le calculateur de score de risque des éléments vulnérables peut être exploité/configuré pour ajuster le score de risque pour les éléments vulnérables liés aux enregistrements d'évaluation de vulnérabilité. Le niveau d'exposition et la priorité de l'événement peuvent être affectés à l'enregistrement de l'évaluation de vulnérabilité. En fonction de la priorité de l'événement, le gestionnaire des événements de vulnérabilité peut choisir de proposer, promouvoir ou lier l'évaluation de vulnérabilité à un incident de sécurité majeur.

Permet Gestion des incidents de sécurité majeurs de suivre et de gérer l'activité de correction, de lier les incidents de sécurité en cours, de créer des tâches ad hoc, d'impliquer les équipes affectées, d'envoyer des rapports d'état et de collaborer à l'aide des intégrations de collaboration disponibles dans Gestion des incidents de sécurité majeurs.

ServiceNow® Gestion des actifs logicielset (SBOM) la logique d'évaluation et Nomenclature logicielle de traitement

À l'aide Gestion des actifs logiciels des données, les CPE provenant de NVD pour le CVE, puis les modèles de détection sont récupérés à l'aide de la logique de correspondance de chaînes. Après l'extraction des modèles de détection, une analyse des installations connexes est exécutée, les éléments de configuration connexes sont extraits et la table Éléments de configuration affectés est renseignée. Vous pouvez fournir des détails supplémentaires tels que l'éditeur, le produit, la version et l'édition. Sur cette base, tous les modèles de détection correspondants et les installations logicielles pour l'enregistrement sont récupérés. Ensuite, les éléments de configuration connexes sont extraits et la table Éléments de configuration affectés est renseignée.

Pour SBOM, le logiciel associé aux CVE à partir de la table connexe (m2m) (entre CVE et logiciel) est extrait. Après avoir extrait les détails logiciels, les composants SBOM connexes sont identifiés en faisant correspondre le produit et la version du composant SBOM au produit et à la version du logiciel identifiés.

Une fois les composants associés trouvés, les entités liées aux composants sont extraites. Le modèle de produit des entités et le CI connexe (le cas échéant) sont extraits et l'élément

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de configuration est enregistré dans la table Élément de configuration affecté. Si l'élément de configuration n'a pas d'éléments vulnérables, vous pouvez l'utiliser pour créer l'élément vulnérable. Si un élément de configuration n'est pas trouvé, le modèle de produit est enregistré dans la table Modèle logiciel affecté et peut être utilisé pour créer des éléments vulnérables de l'application.

Pour plus d'informations sur l'utilisation du workflow Vulnerability Crisis Management, consultez Utilisation de l'espace de travail de l'évaluation de la vulnérabilité.

Information associée

- Exploration de l'évaluation des vulnérabilités
- Explorer l'espace de travail de l'évaluation de la vulnérabilité
- Onglet Évaluation

Séparation de domaine et Réponse aux vulnérabilités

L'application Séparation de domaine est prise en charge dans Réponse aux vulnérabilités. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Standard

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Comment fonctionne Séparation de domaine dans Réponse aux vulnérabilités

Avec Domain Separation, vous pouvez standardiser les procédures de RV (Réponse aux vulnérabilités) pour l'ensemble de la clientèle que vous servez, avec des coûts d'exploitation réduits et une meilleure qualité de service.

Des espaces de travail client distincts pour les workflows, les tableaux de bord, les rapports, etc., garantissent que les données client sont séparées et ne sont jamais exposées à d'autres clients.

Prise en charge de Domain Separation dans Vulnerability Response par versions

Version	Niveau de prise en charge	Notes
Orlando	Standard	
Paris	Standard	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prise en charge de Domain Separation dans Vulnerability Response par versions (suite)

Version	Niveau de prise en charge	Notes
Québec	Standard	
Rome	Standard	
San Diego	Standard	
Tokyo	Standard	
Utah	Standard	
Vancouver	Standard	
Washingtondc (en anglais seulement)	Standard	

Séparation de domaine pour l'application Réponse aux vulnérabilités couvre les fonctionnalités du produit suivantes :

- Ingère les éléments vulnérables à partir d'analyseurs tiers (par exemple, Qualys, Rapid 7 ou Tenable) dans le domaine approprié. Les données ingèrent dans le même domaine que celui de l'utilisateur d'intégration, dont les informations d'identification sont utilisées pour l'intégration.
- Analyse à nouveau des actifs Réponse aux vulnérabilités spécifiques depuis le domaine à partir duquel la demande a été effectuée.
- Utilise le processus de recherche de CI CMDB pour s'assurer que les informations CI des scanners correspondent aux CI dans CMDB du domaine de l'utilisateur d'intégration.
- Calcule les scores de risque au niveau de l'élément vulnérable selon le calculateur de score de risque défini dans le même domaine que celui de l'utilisateur d'intégration.
- Les règles de cibles de rattrapage sont exécutées sur les éléments vulnérables conformément aux règles de cibles de rattrapage définies dans le même domaine que celui de l'utilisateur d'intégration.
- Les règles de tâche de rattrapage peuvent être définies et rester dans le même domaine que le domaine de l'utilisateur d'intégration.
- Les tâches de rattrapage créées à l'aide des règles de tâche de rattrapage restent dans le même domaine que celui dans lequel les règles de groupe sont créées.
- Le workflow du report passe par le processus d'approbation dans le même domaine pour lequel le report est demandé.
- Les rapports et les tableaux de bord affichent les états des éléments vulnérables tels que l'âge de l'élément vulnérable, les éléments vulnérables ouverts par CI, les vulnérabilités par impact et l'état de la date cible de rattrapage dans le domaine auquel ils appartiennent.
- Les connaissances provenant de scanners tiers ou de la base de données de vulnérabilité nationale (NVD) peuvent être ingérées dans le domaine mondial et les données peuvent être partagées entre plusieurs clients.

Remarque : Dans tous les cas ci-dessus, les principes fondamentaux de la séparation de la visibilité dans des domaines séparés dans la NOW Platform s'appliquent.

Pour plus d'informations sur la création et la prise en charge des importations séparées par domaine, consultez Créer des importations séparées par domaine pour une intégration et Créer et prendre en charge plusieurs domaines dans le cadre de travail des tâches en arrière-plan.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation

L'application Réponse aux vulnérabilités gère le cycle de vie d'un élément de vulnérabilité de bout en bout. Les cas d'utilisation suivants prennent en charge la séparation par domaine :

- **Ingérer** des éléments vulnérables (vulnérabilités sur l'actif) à partir de votre intégration tierce.
  - Ingérer des données à partir de plusieurs instances
  - Dédupliquer l'élément vulnérable
  - Correspondre avec le CI CMDB
- **Enrichissement** de l'élément vulnérable avec les scores de risque et les dates cibles de rattrapage
  - Enrichissement des actifs (CMDB)
  - Score du risque et enrichissement de la date cible de rattrapage
- **Regrouper** les éléments vulnérables et affecter la tâche de rattrapage
  - Regrouper automatiquement les éléments vulnérables
  - Affecter automatiquement la tâche de rattrapage
- **Corriger**
  - Tâches de rattrapage
  - Cycle de vie complet de la correction
  - Workflow du report
- **Mesurer** la posture de sécurité de l'organisation et le programme de gestion des vulnérabilités
  - Tendance de vulnérabilité, actif le plus vulnérable, vulnérabilité par âge
  - État du rattrapage par date cible de rattrapage

Configuration

La configuration de Séparation de domaine pour Réponse aux vulnérabilités ne nécessite aucune étape supplémentaire. Toutes les Réponse aux vulnérabilités tables acquièrent la colonne Domaine une fois que l'instance est séparée par domaine. Vous pouvez diriger les données d'importation d'intégration de vulnérabilité vers des domaines spécifiques. Consultez Créer des importations séparées par domaine pour une intégration pour plus d'informations.

Données séparées par domaine

Les données peuvent être séparées par domaine, ce qui signifie :

- L'élément vulnérable ingéré à partir d'analyseurs tiers reste dans le même domaine que le domaine de l'utilisateur d'intégration et n'est accessible à partir d'aucun autre domaine.
- Les vulnérabilités, les éléments vulnérables (instances) ou les actifs d'un domaine ne peuvent pas être affichés à partir d'autres domaines.
- L'algorithme de notation des risques, les règles de tâche de rattrapage et les règles de cible de rattrapage ne peuvent être consultés par aucune personne extérieure au domaine.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les informations de vulnérabilité du NVD peuvent exister dans le domaine global et être partagées avec tous les clients.
- Les tâches de rattrapage d'un domaine ne peuvent pas être affichées à partir d'un autre domaine.
- Les workflows de report créés dans un domaine ne sont pas visibles dans un autre domaine.
- Toutes les notifications par e-mail sont contenues dans le domaine auquel elles appartiennent.

Comment les analystes de vulnérabilité gèrent-ils leurs propres données d'application ?

- Les analystes créent leurs propres règles d'installation d'application, de gestion des applications multisources et de recherche de CI.
- Les analystes peuvent configurer des intégrations spécifiques exclusivement pour une utilisation au sein du domaine.
- Les analystes peuvent créer leurs propres workflows de gestion des reports et des changements.
- Les analystes peuvent créer leurs propres règles de tâche de rattrapage, une logique de notation des risques pour classer les vulnérabilités par ordre de priorité, affecter automatiquement les tâches de rattrapage et les affecter au groupe d'affectation approprié.
- Les utilisateurs du domaine créent un élément de vulnérabilité manuel, puis ferment l'élément.

Logique métier et processus qui peuvent être séparés par domaine par le propriétaire de l'instance

- Réponse aux vulnérabilités Utilisateurs et groupes
- Intégrations de Réponse aux vulnérabilités
- Configuration complète de l'installation (gestion des utilisateurs et des groupes, installation des applications, gestion des applications multisources, règles de recherche de CI, règles de tâche de rattrapage, calculateurs de risque, règles de cible de rattrapage, etc.)
- Cycle de vie complet du rattrapage, y compris le report
- Planifier des travaux

Information associée

Séparation de domaine pour les fournisseurs de services

Mappage des services dans Réponse aux vulnérabilités

Service Mapping aide les organisations à obtenir une compréhension complète de votre infrastructure IT et des relations entre les différents composants. Il permet la détection et le mappage automatiques des services, des applications et des composants d'infrastructure, fournissant une représentation visuelle des dépendances et des relations.

Dans Réponse aux vulnérabilités, la tâche *Set related CI services* planifiée établit des connexions entre les services aux entreprises affectés et les éléments de configuration (CI) qui leur sont associés. Le processus de liaison a lieu une fois l'importation de l'intégration terminée et à un moment désigné. Pour améliorer les performances de cette tâche

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

planifiée, plusieurs changements ont été implémentés à partir de la version 21.1.2 de Réponse aux vulnérabilités. Les voici :

- Calcul du score de risque : le processus de calcul des scores de risque implique l'utilisation de la *Set related CI services* tâche planifiée. Une fois le CI traité, cette tâche stocke les données nécessaires dans la table Services associés [sn_vul_m2m_ci_services]. Auparavant, dans , le Conformité de la configurationcalcul du risque impliquait d'accéder directement aux *CIUtils* de l'interface de programmation d'application Base de données de gestion des configurations (CMDB) (API) pour récupérer les services pour chaque résultat de test pendant l'importation. Toutefois, le processus actuel s'appuie sur la sortie de la tâche planifiée de la table Services associés [sn_vul_m2m_ci_services] pour calculer le score de risque dans Conformité de la configuration. En outre, le calculateur du système de base a été modifié pour utiliser la table Services associés [sn_vul_m2m_ci_services].
- Taille des services : la valeur de service dans la propriété *sn_sec_cmn.services_affected_by_CI_max_size*système, qui est liée à la *Set related CI services* tâche planifiée, passe de 1 000 à 500.
- Profondeur des services : la profondeur dans la propriété *sn_sec_cmn.services_affected_by_CI_max_depth*système, qui est liée à la *Set related CI services* tâche planifiée, est réduite de 10 à 5. La valeur de service est également diminuée, passant de 1000 à 500.
- Exclusion de CMDB classes : une propriété *sn_sec_cmn.ignoreCIClassForService* système a été introduite pour permettre la configuration des classes pour lesquelles le calcul de CMDB service doit être ignoré. Dans le système de base, cette propriété est définie sur *cmdb_ci_unclassed_hardware*, *cmdb_ci_incomplete_ipsn_sec_cmn_unmatched_ci* car ces classes sont créées par Réponse aux vulnérabilités et peuvent ne pas avoir de mappage des services. Auparavant, le calcul du service était basé sur le VIT. Toutefois, la logique a été modifiée pour utiliser l'élément détecté à la place. L'élément détecté est utilisé pour calculer le service, qui est ensuite associé au CI dans la même table.
- Tâche planifiée pour l'actualisation complète des services : une tâche *Full refresh-related CI services for VI*planifiée à la demande a été introduite pour effectuer une actualisation complète des services. Lorsque vous effectuez une mise à niveau vers la version 21.0 de Réponse aux vulnérabilités, la tâche s'exécute *Set related CI services* d'abord pendant une durée plus longue, car la table de base utilise des éléments détectés au lieu d'éléments vulnérables. Par conséquent, la tâche doit traiter tous les éléments détectés qui ont été analysés au cours des 90 derniers jours. En outre, si vous avez besoin d'actualisations de service plus fréquentes, vous pouvez y répondre en planifiant des actualisations périodiques hebdomadaires ou en effectuant une actualisation complète. Si vous avez effectué des activités qui ont entraîné des changements dans les services associés à vos CI et que vous souhaitez Réponse aux vulnérabilités refléter ces changements, vous pouvez exécuter la tâche *Full refresh related CI services for VI*planifiée sur demande. Cette tâche prend tous les éléments détectés enregistrés au cours des 90 derniers jours et actualise les services associés en conséquence.

Information associée

Mappage des services

CIUtils - Global

Implémentation de Réponse aux vulnérabilités

Suivez les étapes illustrées dans les images suivantes pour télécharger l'application Réponse aux vulnérabilités à ServiceNow Storepartir du , installez-la sur votre Now Platform® instance et configurez-la à l'aide de l'Assistant de configuration.

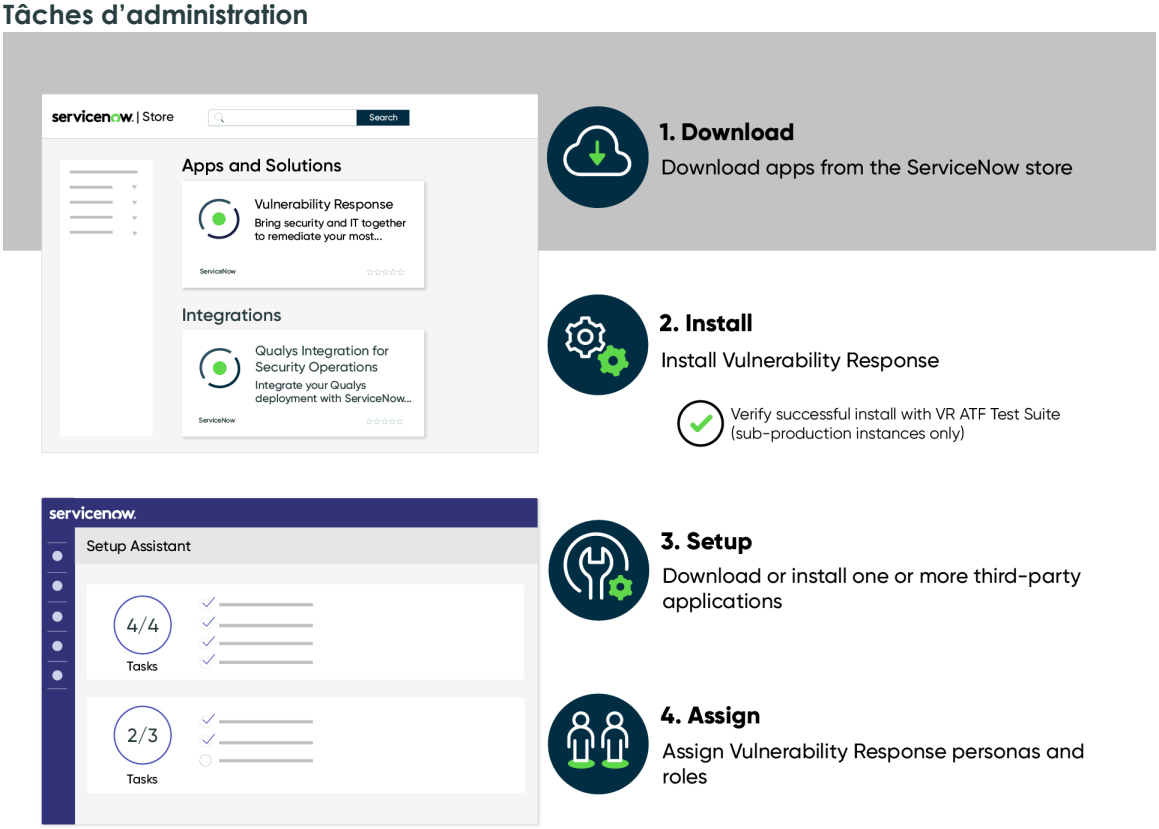
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les images suivantes présentent un exemple d'installation et de configuration pour l'installation du système de base, de l'application Réponse aux vulnérabilités et d'une application de scanner tierce, l'application Qualys . Les rôles requis et les tâches obligatoires, ainsi que les étapes facultatives, sont également répertoriés.

- Pour plus d'informations sur chaque étape illustrée dans les images suivantes et une liste de vérification avec des liens vers la documentation à l'appui, reportez-vous à la section Liste de vérification d'implémentation de l'application Réponse aux vulnérabilités.
- Vous pouvez étendre les concepts et la séquence d'étapes présentés dans cet exemple à l'installation et à la configuration d'autres applications prises en charge pour Réponse aux vulnérabilités. Pour obtenir la liste des applications prises en charge, reportez-vous à la section Installation et prise en charge des Réponse aux vulnérabilités applications.
- Le rôle administrateur est requis pour télécharger et installer l'application et l'application Réponse aux vulnérabilitésQualys de vulnérabilité utilisée pour cet exemple.
- Le rôle administrateur affecte également le personnage d'administrateur de vulnérabilité [sn_vul.vulnerability_admin] et d'autres Réponse aux vulnérabilités rôles de profil aux utilisateurs et aux groupes.

Tâches d'administration



Le rôle sn_vul.vulnerability_admin configure les applications et Qualys dans l'assistant Réponse aux vulnérabilités de configuration et vérifie les résultats attendus.

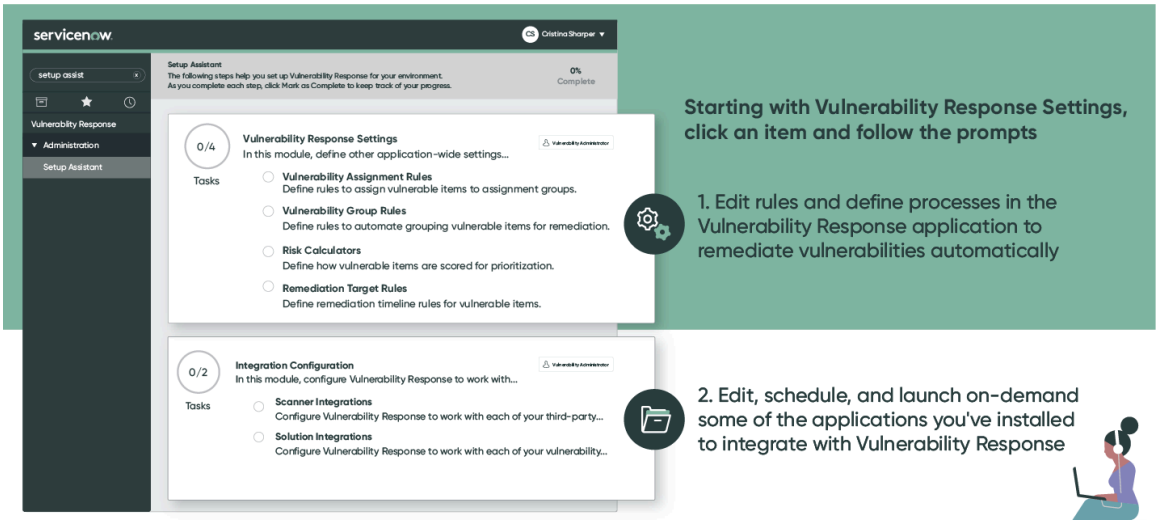
Suivez les étapes et invites de l'Assistant de configuration, en commençant par la section Paramètres de Vulnerability Response pour poursuivre l'installation et la configuration. L'examen de ces paramètres vous aide à comprendre et à vérifier les processus de la poursuite de la configuration de Réponse aux vulnérabilités votre environnement.

Rôle requis : sn_vul.vulnerability_admin ou, alternativement, admin.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de l'administrateur de vulnérabilité



Roles required: sn_vul.vulnerability_admin or admin

Passez en revue les descriptions, les paramètres par défaut et les données de démonstration que vous avez installés avec les applications dans les sections suivantes :

- Règles d'affectation de vulnérabilité : affectent automatiquement les éléments vulnérables (VI) au groupe d'affectation approprié.
- Règles de tâche de rattrapage : regroupent automatiquement les éléments vulnérables (VI) à mesure qu'ils sont importés en fonction de certaines conditions.
- Calculateurs de risque : le calculateur de risque par défaut est activé.
- Règles de cibles de rattrapage : définissez des chronologies de rattrapage pour les VI et les tâches de rattrapage (RT).
- Examinez et modifiez les paramètres des applications tierces et des solutions installées que vous avez installées, et définissez les conditions pour vos importations de données. Saisissez les informations de votre compte tiers et configurez les paramètres d'importation, les calendriers, les règles de recherche d'éléments de configuration (CI), ainsi que d'autres paramètres.

Consultez Liste de vérification d'implémentation de l'application Réponse aux vulnérabilités pour plus d'informations.

Pour plus d'informations sur la personnalisation ou l'implémentation de l'application, consultez KB1000704 Réponse aux vulnérabilités.

Installer Réponse aux vulnérabilités

Avant d'exécuter l'application Réponse aux vulnérabilités dans votre Now Platform instance, vous devez obtenir l'autorisation et télécharger l'application à partir du ServiceNow Store, l'installer sur votre Now Platform instance, puis effectuer quelques étapes d'installation dans l'Assistant de configuration.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

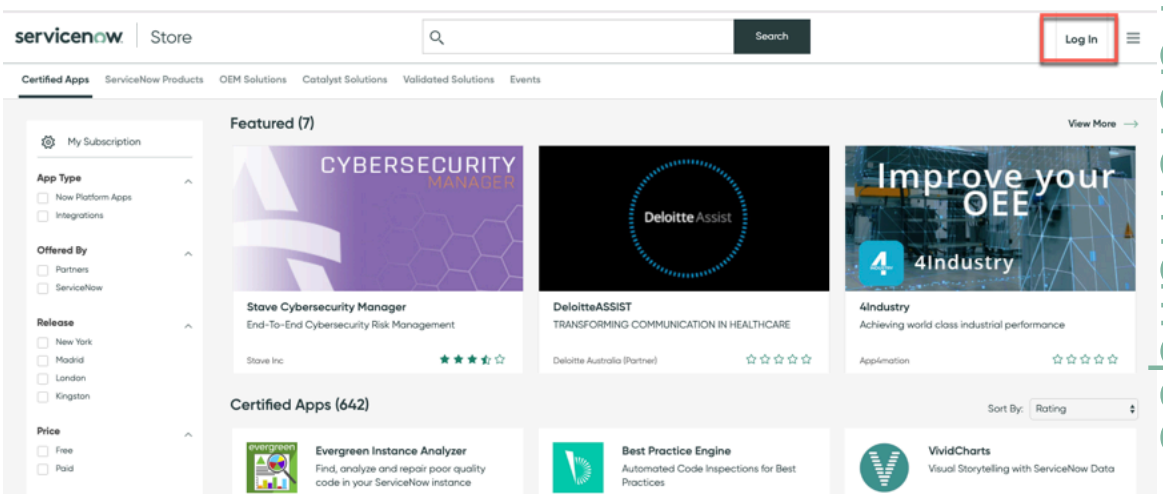
Tâches de configuration	Description
Vérifiez que les rôles requis ServiceNow vous ont été affectés à votre instance.	Le rôle administrateur est requis pour l'installation. S'il n'est pas déjà affecté, l'administrateur système [admin] affecte également le rôle Administrateur de vulnérabilité, sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)].

Rôle requis : administrateur

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

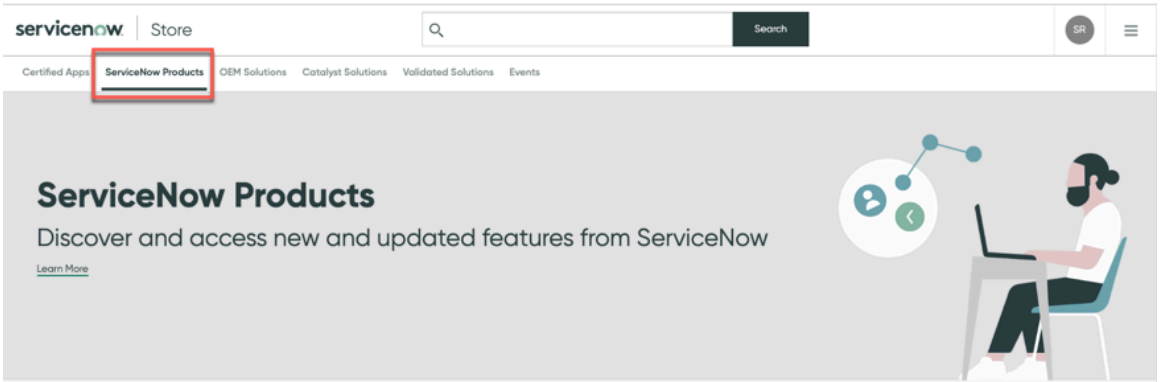
1. Pour obtenir une autorisation et télécharger l'application Réponse aux vulnérabilités principale, accédez ServiceNow Storeau .
2. En haut à droite de la page, cliquez sur **Se connecter**.



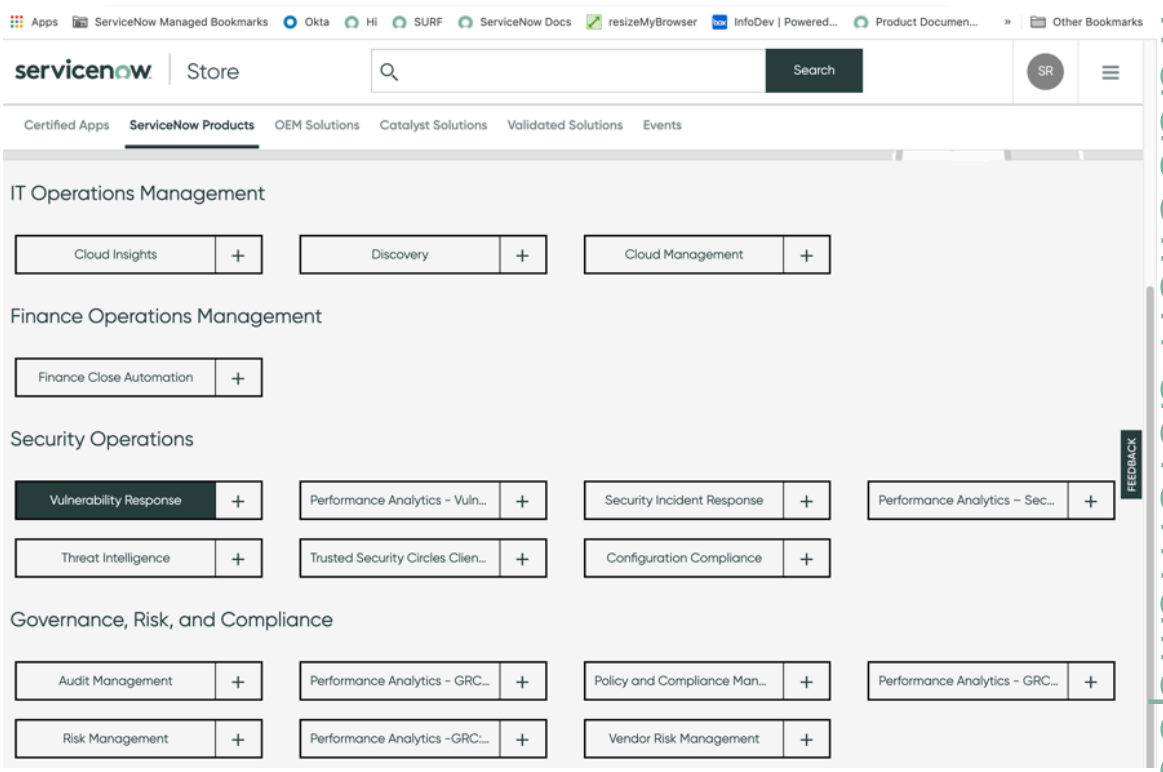
3. Dans la boîte de dialogue qui s'affiche, saisissez vos informations d'identification HI et cliquez sur **Connexion**.
4. Sur la page qui s'affiche, si elle n'est pas sélectionnée, cliquez sur l'onglet **Produits ServiceNow** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



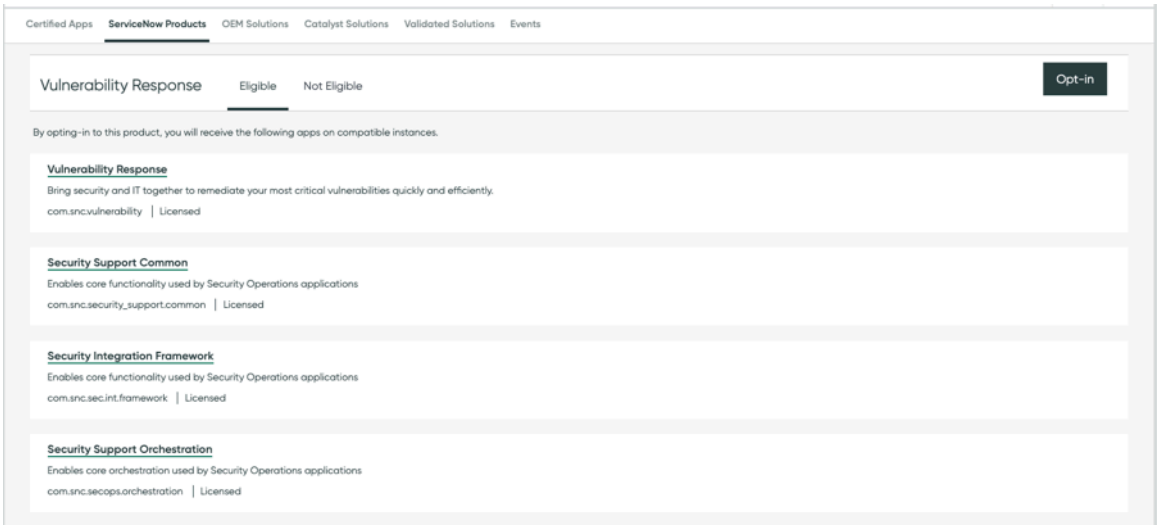
5. Pour afficher les applications associées auxquelles vous êtes éligible avec l'application, sur la page de liste des Réponse aux vulnérabilités produits, cliquez sur le produit **Vulnerability Response** .



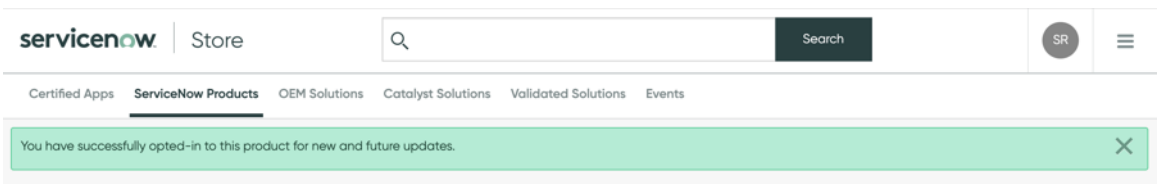
L'onglet Admissibilité répertorie toutes les demandes auxquelles vous êtes admissible si vous optez. Pour plus d'informations sur une application, cliquez sur un lien.

Traduction automatique

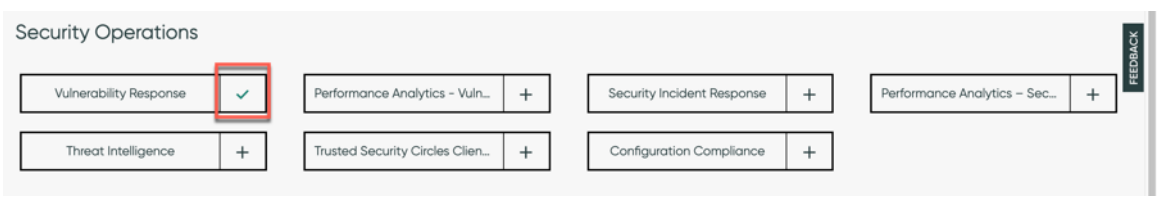
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Pour obtenir l'application Réponse aux vulnérabilités principale, cliquez sur **Adhérer**.
7. Pour accepter les termes et conditions, à l'invite, cochez la case et cliquez sur **Accepter**. Un message s'affiche qui indique que vous avez adhéré avec succès à l'application.



Lorsque l'onglet ServiceNow Produits est sélectionné et affiché, une coche verte remplace le signe plus à droite de l'application Réponse aux vulnérabilités , comme illustré dans la figure suivante.



Une fois que vous avez accepté les termes et conditions et les autorisations gérées pour l'une des applications de l'onglet **Produits ServiceNow** , sur la page Liste des produits, vous pouvez cliquer sur le signe plus (+) pour obtenir l'autorisation et l'adhésion aux autres applications de cette page en un seul clic.

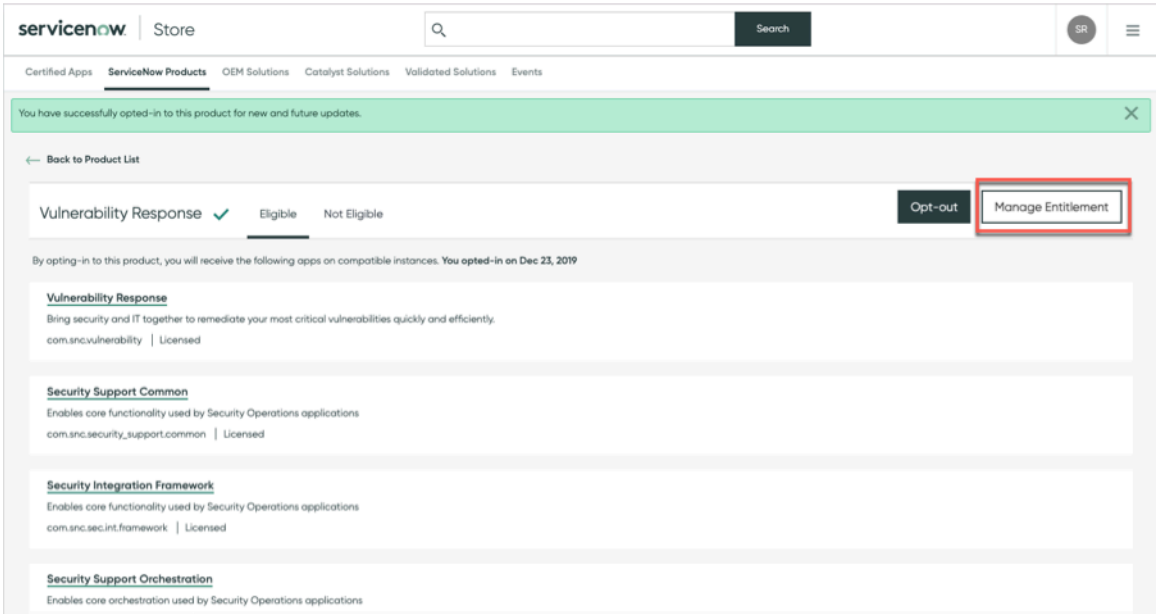
8. Passez à l'étape 10 pour installer l'application sur votre Now Platform instance.
9. Facultatif : Pour gérer votre autorisation pour l'application Réponse aux vulnérabilités sur d'autres Now Platform instances, suivez également les étapes suivantes.

   a. Si le bouton Gérer l'autorisation n'est pas affiché, cliquez sur l'application Réponse aux vulnérabilités dans la liste de produits pour l'afficher.

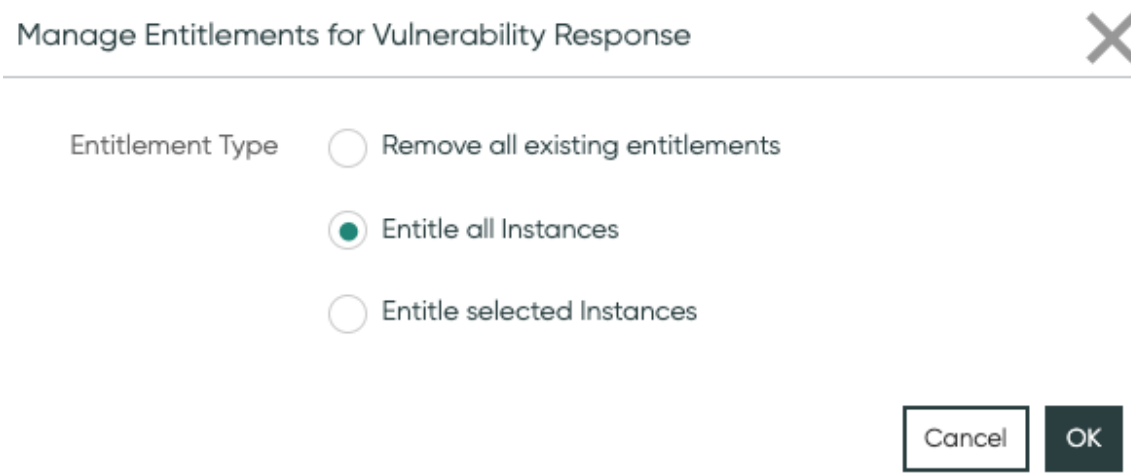
   b. Une fois l'onglet Éligible sélectionné, cliquez sur **Gérer l'autorisation**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Dans la boîte de dialogue Gérer les autorisations pour Vulnerability Response qui s'affiche, choisissez l'une des options suivantes :



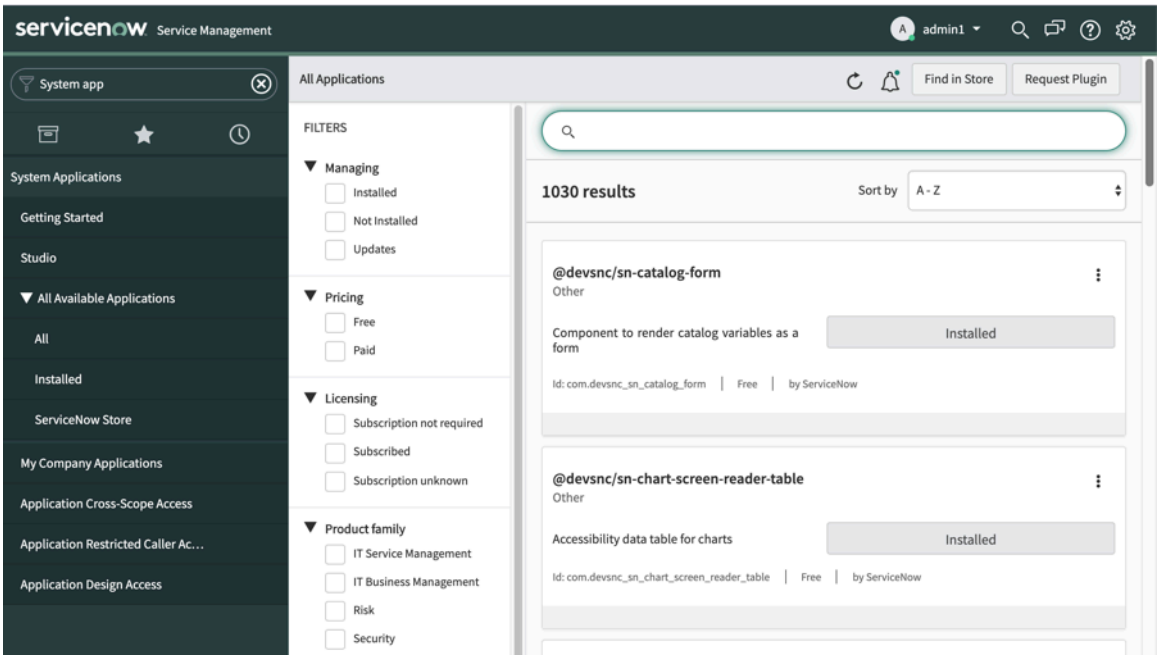
d. Cliquez sur **OK** ou **Annuler** pour continuer.
Vous êtes prêt à activer les modules d'extension et à installer l'application sur votre ou vos Now Platform instances.

10. Connectez-vous à l'instance Now Platform sur laquelle vous souhaitez installer l'application Réponse aux vulnérabilités .

11. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.

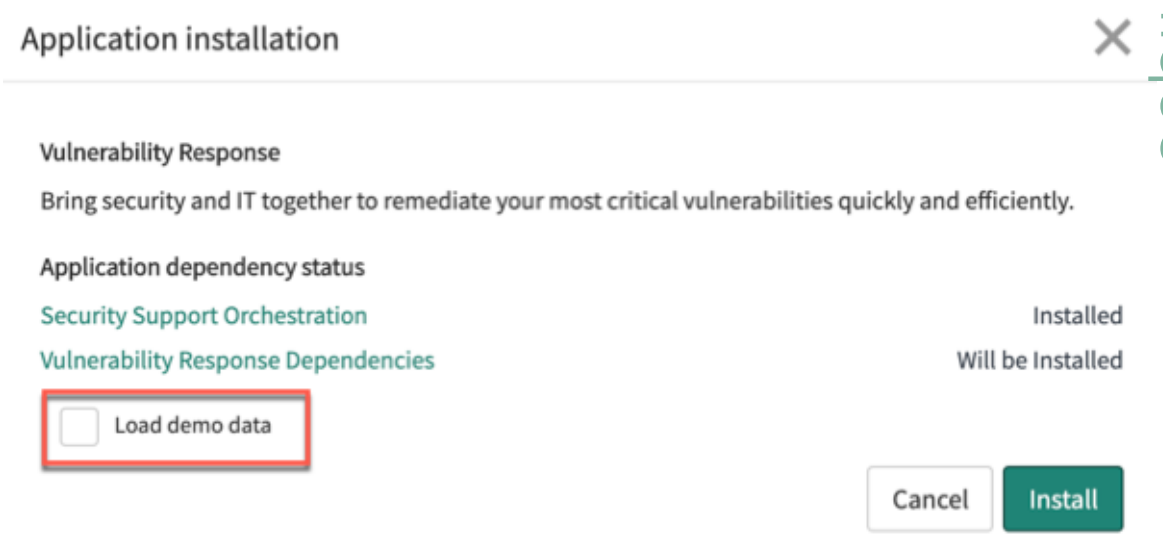
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



12. Dans la liste des applications, localisez l'application Vulnerability Response (sn_vul), sélectionnez une version dans la liste de choix, puis cliquez sur **Installer**.
La boîte de dialogue d'installation de l'application s'affiche. Toutes les dépendances qui seront installées sont affichées.
13. Facultatif : Si vous souhaitez des données de démonstration, cochez la case Charger les données de démonstration et cliquez sur **Installer**.

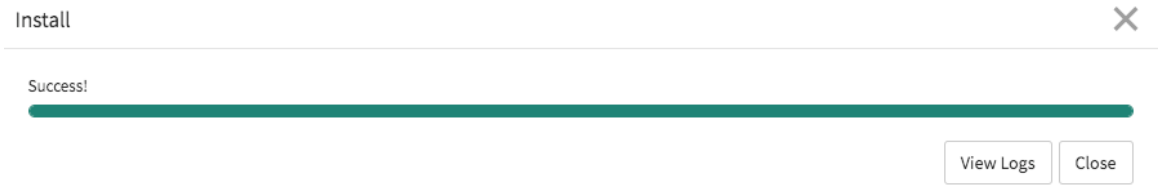
> **Remarque :** Si vous ne cochez pas la case **Charger les données de démonstration** , les données de démonstration ne peuvent pas être installées ultérieurement à partir d'Application **Manager** . Pour plus d'informations sur l'installation ou la réinstallation de données de démonstration après l'installation initiale, consultez l'article Solution de contournement pour installer des données de démonstration si l'application est déjà installée [KB0722909] dans la base de Now Support connaissances.



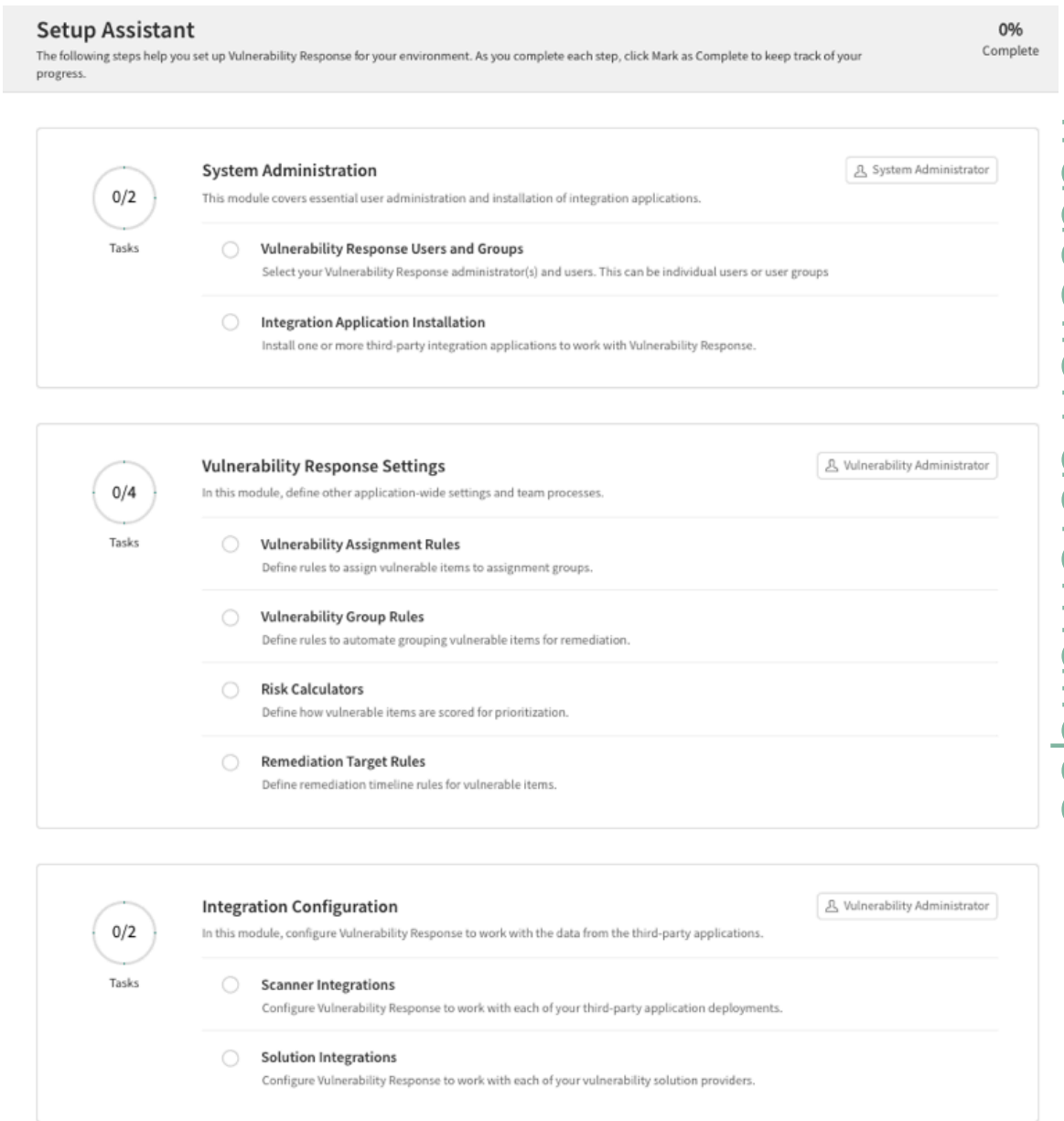
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette installation peut prendre un certain temps. Un message s'affiche dans la boîte de dialogue Installer une fois l'application installée avec succès.



14. Cliquez sur **Fermer**.
15. Une fois l'installation terminée, accédez à **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.



16. Suivez les instructions figurant sur les formulaires de chaque section.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Pour plus d'informations sur les paramètres, l'installation Réponse aux vulnérabilités d'applications, la configuration, les intégrations, les règles de groupe, les calculateurs de risque et les règles de cible de rattrapage, reportez-vous à Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration.

Composants installés avec Réponse aux vulnérabilités

Plusieurs types de composants sont installés lors de l'activation de l'application Réponse aux vulnérabilités, notamment des tables, des rôles d'utilisateur et des tâches planifiées.

Afficher les listes filtrées pour les composants installés avec une application

Filtrez la table Fichiers d'applications afin que seuls les rôles, les travaux planifiés et les tables installés avec une application s'affichent. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés sur l'instance et dans la table de métadonnées. Procédez comme suit pour afficher les listes filtrées à partir de la table Fichiers d'applications.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application. Par exemple : **Application** > **est** > **Réponse aux vulnérabilités**.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, sélectionnez **ET**, puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Rôles installés

Remarque : Les rôles, les travaux planifiés et les tables pour Réponse aux vulnérabilités des applications se trouvent dans Composants installés avec Réponse aux vulnérabilités des applications.

Titre du rôle [name]	Description	Contient des rôles
v23.0 : sn_vul.delete	Supprime les enregistrements sources et les éléments vulnérables. Avant la version 23.0, le rôle administrateur avait le privilège de supprimer les enregistrements sources.	• sn_vul_cmn.delete • sn_vul.delete_vulnerab
v23.0 : sn_vul_cmn.delete	Supprime les enregistrements sources.	
V23.0 : sn_vulc.bulk_edit	Effectue une opération de modification en bloc sur les résultats des tests.	
sn_vul.app_bulk_edit	Effectue une opération de modification en bloc sur les éléments vulnérables de l'application (AVIT).	sn_vul.app_write_all

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
sn_vul_container.container_bulk_modifier	Effectue une opération de modification en bloc sur les éléments vulnérables (CVIT) du conteneur.	sn_vul_container.write_c
sn_vul_cisa.configure_intelligence_integration	Configure les intégrations Intelligence.	
Responsables de la vulnérabilité et analystes seniors [sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)]	Mettre à jour les propriétés et les intégrations de vulnérabilité. Le rôle sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) est requis pour Réponse aux vulnérabilités l'administration, y compris les intégrations de vulnérabilité, les règles de tâche de rattrapage, les calculateurs, les règles et les tâches de cible de rattrapage, les rapports et la configuration des intégrations tierces.	• sn_vul.vulnerability_wri • sn_vul.ciso_write • sn_sec_cmn.admin • sn_vul_qualys.admin (l Vulnerability Integratio • sn_vul_r7.admin (lorsqu Vulnerability Integratio • sn_vul_shodan.admin Shodan Exploit Integra installé.) • sn_vul.configure_nvd_ (lorsque les intégration installées.) • treemap_admin (lorsq l'application Performa est installée.)
Orchestration de correctif	Configure les intégrations de fournisseurs de correctifs tiers pris en charge. Affichez et appliquez les données de correctifs et les enregistrements de correctifs.	• sn_vul_patch_orch.co Configurez et appliqu • sn_vul_patch_orch.rec Peut afficher les enreg les données de correc • sn_vul_bigfix.configure Configure l'applicatio Orchestration Integrat rôle contient les rôles g sn_vul_bigfix.read_inte connection_admin qu à l'utilisateur de se co console BigFix. • sn_vul_sccm.configure Ce rôle contient les rô sn_vul_sccm.read_inte connection_admin qu à l'utilisateur de se co console SCCM.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
		• sn_vul_bigfix.read_inte Les utilisateurs disposa peuvent afficher (en le les enregistrements de Response et de l'appli Patch Orchestration In des données d'orches correctifs. • sn_vul_sccm.read_inte Les utilisateurs disposa rôle peuvent afficher (seule) les enregistreme Vulnerability Response d'orchestration des co l'application Microsoft Orchestration Integrat
Analystes de vulnérabilités [sn_vul.vulnerability_write]	Le rôle sn_vul.vulnerability_write est requis pour gérer les tâches de rattrapage et les éléments vulnérables, et pour surveiller la progression du rattrapage.	• sn_vul.read_al • sn_sc_cmn.write • sn_vul_qualys.user (lors Vulnerability Integratio • sn_vul_shodan.write (lo Exploit Integration est i
V19.0 : gestionnaire d'événements de vulnérabilité [sn_vul_analyst.vul_event_manager]	Le rôle sn_vul_analyst.vul_event_manager permet d'évaluer l'impact d'une nouvelle vulnérabilité ou d'un nouveau logiciel, ou d'ajouter une vulnérabilité zero-day pour identifier les actifs impactés et créer des éléments vulnérables (VI).	• sn_sec_cmn.read • canvas_user • sn_vul_analyst.emerge • sn_vul.manage_expos
Autres [sn_vul.read_all] Le rôle sn_vul.vulnerability_read est déconseillé.	Le rôle sn_vul.read_all est requis pour toute personne ayant besoin d'une visibilité sur la gestion des vulnérabilités. Par exemple, les responsables informatiques et de sécurité ou toute personne qui souhaite explorer les tableaux de bord de haut niveau jusqu'aux éléments qui composent les visuels de tableau de bord.	• sn_sec_cmn.read • sn_vul_qualys.read (lor Vulnerability Integratio • sn_vul_shodan.read (lo Exploit Integration est i • pa_viewer (lorsque l'a Performance Analytics • sn_vul_tenable.read_in (lorsque l'intégration T Vulnerability est installe

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
Administrateur d'importation de systèmes VR [sn_vul.vr_import_admin]	Exécuter en tant qu'utilisateur du système. Exécute les travaux planifiés. **Remarque :** Cet utilisateur est l'utilisateur exécutable par défaut pour chaque enregistrement d'intégration. Ne changez pas.	• import_admin • sn_vul.vulnerability_wri
Propriétaire de la résolution [sn_vul.remediation_owner]	Affichez et mettez à jour les autorisations pour les éléments vulnérables, les tâches de rattrapage qui vous sont affectées ou qui sont affectées à votre groupe. Peut afficher toutes les vulnérabilités et solutions. dispose d'un accès en écriture au**champ Notes internes** sur l'enregistrement de la solution.	Contenu dans le rôle itil.
RSSI et responsables de la vulnérabilité [sn_vul.vulnerability_ciso]	Affichez le tableau de bord CISO dans Analyse des performances pour Vulnerability Response.	• sn_vul.ciso_read • sn_vul.read_all

Travaux planifiés installés

Tâche planifiée	Description
Remplir les filtres OOTB enregistrés pour l'hôte et le module d'application	Migre les modules liés aux modules Hôte et App.
Renseigner les filtres OOTB enregistrés pour le module CC	Migre les modules associés au module CC.
Renseigner les filtres OOTB enregistrés pour le module conteneur	Migre les modules liés au module de conteneur.
Actualiser les filtres enregistrés associés à l'hôte	Actualise toutes les données d'agrégation associées aux filtres enregistrés du module Hôte.
Actualiser les filtres enregistrés associés CC	Actualise toutes les données d'agrégation associées aux filtres enregistrés du module CC.
Actualiser les filtres enregistrés	Actualise toutes les données d'agrégation associées aux filtres enregistrés du module Conteneur.

Traducción automática

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
associés au conteneur	
Actualiser les filtres enregistrés associés à l'application	Actualise toutes les données d'agrégation associées aux filtres enregistrés du module d'application.
Création et exécution de déclenchement d'agrégation pour le filtre enregistré	Crée, met à jour, exécute et actualise les agrégations associées au filtre enregistré.
Version 19.0 de Vulnerability Response et v4.0 de Veracode Vulnerability Integration	L'intégration CWE Veracode récupère les données CWE (Common Weakness Enumeration) spécifiques pour obtenir des informations sur les Veracode menaces et des recommandations de correction. L'intégration de SBOM Veracode ingère les informations sur les versions, les versions et les vulnérabilités provenant des Veracode composants de vos projets logiciels. L'intégration génère des SBOM au format JSON CycloneDx et les télécharge dans votre instance L'intégration des catégories Veracode récupère les données des catégories améliorées à partir de Veracode. L'intégration Veracode DevOps permet aux utilisateurs DevOps d'afficher les détails du résumé des analyses de vulnérabilité tierces sans licence SecOps. API basées sur JSON pour les intégrations Veracode suivantes : Élément vulnérable de l'application, Synthèse de l'analyse, Liste des applications. Les versions d'API basées sur XML de ces intégrations sont déconseillées.
Associer les VI existants à la règle d'exception automatique	Associe automatiquement la règle d'exception automatique aux VI existants.
Fermer automatiquement les détections vulnérables	Ferme automatiquement les détections vulnérables périmées en fonction de la configuration définie dans la table « sn_vul_auto_close_config ».
Version 16.1 : HCL BigFix Collection, Fixlet et Actions Integrations.	Gérez les correctifs et les déploiements de correctifs pour les vulnérabilités avec les correctifs du produit HCL BigFix.
Calculer les nombres connexes	Inactif par défaut. Traite les données de solutions une fois par nuit au lieu de façon continue.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
pour toutes les solutions	À partir de la version v22.0, vous pouvez exécuter cette tâche uniquement sur demande. Comme cette tâche planifiée traite toutes les solutions, elle peut avoir un impact sur les performances. Par conséquent, il est recommandé d'exécuter cette tâche une seule fois si les données de la solution sont corrompues.
Calculer les nombres de VI connexes pour la vulnérabilité et la tâche de rattrapage	Capture les changements d'importation manuels et de VI pour la journée. Rapproche les relations de vulnérabilité et de solution et recalcule les totaux. Les données de solutions sont mises en file d'attente et traitées séparément par la tâche planifiée **File d'attente des mesures de solutions de vulnérabilité de processus** .
Vérifier le délai d'expiration du MID Server	Envoie un ping sur le MID Server et fait disparaître les erreurs au bout de 30 secondes.
V19.0 : vérifier l'exposition potentielle à la vulnérabilité	Traite les CVE delta, les logiciels et les installations pour obtenir l'exposition.
Vérifier l'état d'exécution WaitComplete	Marque une exécution d'intégration comme terminée une fois qu'elle a été vérifiée comme terminée.
Vérifier l'expiration du report des éléments et des groupes vulnérables	Envoie des notifications si des éléments vulnérables ou des vulnérabilités ont expiré (et s'ils expirent dans une semaine). Vérifie si une règle d'exception est applicable sur un VI différé et met à jour les champs **Motif** et **Jusqu'à** en fonction de la règle d'exception. L'état du VI reste Reporté jusqu'à la dernière date d'expiration.
Fermer les VIT d'annulation qui n'ont pas de CI associé	Ferme automatiquement les éléments vulnérables qui n'ont pas d'élément de configuration (CI) associé et qui n'ont pas été mis à jour depuis trois jours. L'état est défini sur Fermé/Annulé.
Fermer le VI à la suppression d'enregistrement de l'exp.	Ferme un VI lorsqu'il est supprimé.
Intégration des résultats de conformité	Importe les résultats des tests avec les politiques, les tests de configuration (contrôles) et les contenus des documents de référence avec des sources de référence pour traitement dans l'application Configuration Compliance.
Intégration du remplissage des résultats de conformité	Faisant partie d'une intégration chaînée exécutée avec l'intégration des actifs, importe les données d'évaluation de la configuration pour les actifs ignorés qui sont détectés (importés via l'intégration Tenable.io des actifs).
Synchronisation de l'état CR	Le script adapte ultérieurement toutes les tâches de rattrapage existantes aux relations CHG afin qu'elles soient synchronisées. Active la synchronisation à venir.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Version 15.0 Intégration des informations d'identification de numérisation	Importe et stocke temporairement Tenable.io en toute sécurité les informations d'identification utilisées pour accéder au scanner pour de nouvelles analyses à la demande.
Intégration complète de CWE 2000	Intégration de vulnérabilité qui extrait les informations sur les vulnérabilités à partir du jeu de données Common Weakness Enumeration (CWE), organisé par MITRE Corporation.
V18.0 : supprimer les enregistrements d'actions de division périmés	Tâche quotidienne pour nettoyer les enregistrements périmés dans les tables intermédiaires de tâches fractionnées.
Désactiver les solutions VR lorsque l'application de solutions n'est pas active	Désactive et masque la Gestion des solutions pour vulnérabilités fonctionnalité lorsque l'application Gestion des solutions pour Réponse aux vulnérabilités n'est pas installée.
Évaluer les cibles de rattrapage	Définit ou met à jour les dates cibles de rattrapage sur tous les éléments vulnérables. Détermine l'état des dates cibles de rattrapage par rapport aux règles.
• Correction des détections pour la clé mise à jour pour Rapid7 • Correction des détections pour la clé mise à jour pour Qualys • Correction des détections pour la clé mise à jour pour Tenable	Nettoie automatiquement les données de détection par une tâche planifiée spécifique à l'intégration qui est déclenchée après la mise à niveau vers Réponse aux vulnérabilités.
Version 16.1 : générer un résumé de rattrapage	Cette tâche génère automatiquement une synthèse d'e-mail pour tous les utilisateurs du groupe d'utilisateurs Propriétaire du rattrapage. La tâche est activée par défaut.
V19.0 : Insérer les CVE exploitées par CISA dans la configuration d'exposition	Insère les CVE CISA dans la table de configuration de l'exposition pour calculer l'exposition.
V18.0 : insérer des tâches de remédiation classiques dans une tâche de remédiation unifiée	Tâche planifiée unique pour insérer toutes les tâches de rattrapage créées dans l'interface utilisateur classique dans la tâche de rattrapage unifiée (sn_vul_remediation_task).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Intégration de la solution Microsoft Security Response Center	Gestion des solutions pour vulnérabilités Intégration qui récupère les solutions à partir du Microsoft Security Response Center.
Version 16.1 : intégrations de la collection, de la mise à jour des correctifs et des déploiements Microsoft SCCM	Gérez les correctifs et les déploiements de correctifs pour les vulnérabilités à l'aide Microsoft de correctifs SCCM.
Processus d'intégration accéléré de reprise	Crée le processus d'intégration pour le Intégration d'exploit Shodan.
Renseigner le texte relatif aux produits affectés	Après la mise à niveau, gère les solutions existantes pour renseigner le texte des produits affectés. Cette tâche ne s'exécute qu'une seule fois.
Renseigner la nouvelle colonne du nombre de CR	Remplit automatiquement la nouvelle colonne Nombre de CR pour les clients ayant des données existantes dans la table Tâche de rattrapage [sn_vul_vulnerability].
Traiter la file d'attente des mesures de la solution de vulnérabilité	Traite les données des solutions mises en file d'attente via : • Déploiement des solutions à partir d'entrées NVD vers des entrées tierces • le remplissage des solutions privilégiées sur les vulnérabilités, et • Mise à jour des mesures d'état de rattrapage sur les solutions En outre, il traite également les solutions qui sont marquées pour les statuts de mise à jour. **Remarque :** Si vous utilisez uniquement Rapid7, vous pouvez désactiver cette tâche planifiée pour améliorer les performances.
Renseigner les enregistrements dans la table de mappage du fournisseur de vulnérabilités Renseigner les enregistrements dans la table de mappage du fournisseur de vulnérabilités pour les vulnérabilités Rapid7	Insère des enregistrements dans la table de mappage du fournisseur de vulnérabilités pour les vulnérabilités existantes.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Rouvrir les groupes de vulnérabilité différés	Rouvre les tâches de rattrapage différées lorsque la date de report est passée.
Réappliquer toutes les règles d'affectation de vulnérabilité	Réévalue les règles d'affectation par rapport à tous les VI **ouverts** .
Version 16.5 : Nombre de réaffectations pour les règles d'affectation	S'exécute quotidiennement et publie le nombre total de VI et de tâches de rattrapage non affectés par cette fonctionnalité pour une règle d'affectation particulière.
Intégration de solution Red Hat	Gestion des solutions pour vulnérabilités Intégration qui récupère les solutions à partir du Avis de sécurité Red Hat.
V17.1 : Actualiser et résoudre les VIT en double sur la tâche de rattrapage	Trouve les éléments vulnérables en double pour les éléments de la tâche de rattrapage avec l'option « Actualiser automatiquement les VI en double » comme active.
Actualiser les éléments vulnérables associés pour la tâche de remédiation basée sur des règles de tâche autre que de rattrapage	Met à jour la tâche de rattrapage avec les éléments vulnérables correspondant aux critères Groupe de filtres et Groupes de conditions.
Réparer les éléments vulnérables erronés Dernières ouvertures et fermetures	Répare les données d'interface utilisateur existantes corrompues par des défauts précédemment corrigés.
Réexécuter les calculateurs	Réapplique les calculateurs à tous les éléments vulnérables affectés par le changement. Cela déclenche un nouveau calcul des scores de risque cumulé de leurs tâchesde rattrapage. **Remarque :** La nouvelle exécution des calculateurs peut prendre beaucoup de temps en fonction de votre environnement.
Nouvelle tentative annulée Ensembles de données à importer de l'intégration	Nouveaux essais des jeux d'importation d'intégration annulés. Réessaie 5 fois avant de renvoyer une erreur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Réessayer les processus d'intégration	Retente les processus d'intégration. Réessaie 5 fois avant de renvoyer une erreur.
Déployer les valeurs d'éléments vulnérables dans la vulnérabilité et le groupe	Calcule le score de risque, le nombre d'éléments vulnérables et l'état de la cible de rattrapage pour les tâches de rattrapage, à l'aide du calculateur de déploiement. **Remarque :** À partir de la version 23.0 de Réponse aux vulnérabilités, la tâche planifiée est améliorée pour créer des tâches en arrière-plan avec des options de multithreading. Cette mise à niveau implique de segmenter la tâche en plusieurs tâches enfants plus petites, qui sont exécutées en parallèle ou simultanément. Cette modification permet de traiter plusieurs enregistrements simultanément, ce qui accélère considérablement la tâche globale.
Exécuter le calculateur de gravité après la promotion de l'entrée de vulnérabilité	Exécute le calculateur de gravité après la mise à jour d'une vulnérabilité précédemment manquante avec son score et d'autres données provenant d'un fournisseur tiers, par exemple Qualys Cloud PlatformRapid7 Nexpose, .
V19.0 : Exécuter l'évaluation de l'exposition pour les CVE configurés	Calcule l'exposition pour tous les enregistrements CVE dans la table de configuration de l'exposition.
V19.0 : Exécuter l'exposition logicielle	Calcule l'exposition pour tous les enregistrements logiciels dans la table de configuration de l'exposition.
Processeur de source de données de vulnérabilité planifié	Vérifie la file d'attente d'importation pour les entrées à traiter et affecte une tâche d'importation planifiée en fonction des ressources disponibles.
Processus d'intégration de vulnérabilité planifié : nettoyage de pièce jointe	Supprime les pièces jointes XML d'intégration une fois qu'elles ont 14 jours. Cette durée de rétention n'est pas configurable.
Vérificateur de délai d'expiration de l'intégration de vulnérabilité planifiée	Annule les exécutions d'intégration qui prennent plus de 60 minutes.
Définir les services CI connexes pour VI	Une fois l'importation de l'intégration terminée, elle relie les services aux entreprises affectés aux CI connectés aux éléments vulnérables, à l'heure spécifiée. Pour plus d'informations, consultez Mappage des services dans Réponse aux vulnérabilités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Définir les nombres de reports	Collecte le nombre de fois où un élément vulnérable, un élément vulnérable d'application, un élément vulnérable de conteneur ou une tâche de rattrapage est différé.
Déclencher l'intégration suivante	Déclenche l'intégration suivante dans une exécution d'intégration chaînée.
Intégration de modèle	Un enregistrement de modèle unique est envoyé lors de Tenable.io la nouvelle analyse.
Mettre à jour les éléments vulnérables dégroupés	Détermine si un élément vulnérable se trouve dans une tâche de rattrapageet l'ajoute ou le supprime de la liste **Éléments vulnérables dégroupés**. **Remarque :** Cette tâche s'exécute après la mise à niveau et, en fonction de votre ensemble de données, peut prendre beaucoup de temps.
Mettre à jour la vulnérabilité sur VG	Met à jour le champ **Vulnérabilité** de la table Tâche de rattrapage (sn_vul_vulnerabilty) après la mise à niveau. Cette tâche est déclenchée une fois et inactive par la suite.
Modèle d'importation de vulnérabilité	Moteur qui traite la file d'attente d'importation. L'un des 10.
Vulnerability Response Âge fermé Mettre à jour	Met à jour la colonne Âge fermé sur la table VI.
Nombre de CI de Vulnerability Response	Calcule le nombre de CI analysés par des scanners tiers au cours des 30 derniers jours.
Mise à niveau de l'état du rattrapage et du risque de Vulnerability Response	Met à jour la cote de risque sur les données lors de la mise à niveau.
v20.0 : Vérifier l'expiration de l'atténuation des risques	Vérifie si les contrôles compensatoires ont expiré pour un élément vulnérable et une tâche de rattrapage. S'ils ont expiré, le score de risque est rétabli au score de risque d'origine et une notification par e-mail est envoyée indiquant que les contrôles compensatoires ont expiré. Envoie également une notification par e-mail si les contrôles compensatoires doivent expirer dans les 7 jours.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables installées

Table	Description
v22.0 sn_vul_cmn_auto_close_rule	Ferme automatiquement les détections obsolètes en fonction des conditions de filtre.
sn_vul_cmn_ws_saved_filter	Stocke les données du filtre enregistré.
sn_vul_licensing_usage	Contient l'actif en double, l'actif IP incomplet, le nombre total d'actifs du scanner et l'utilisation finale.
sn_vul_m2m_entry_compensating_control	Représente l'association entre les entrées de vulnérabilité et les contrôles de compensation.
v21.0 Moteur d'analyse Rapid7 [sn_vul_r7_scan_engine]	Stockez les enregistrements importés Données du moteur d'analyse responsables de la détection des actifs lors d'une analyse et de la vérification de leur vulnérabilité.
v21.0 Importation du moteur d'analyse Rapid7 [sn_vul_r7_scan_engine_import]	Utilisé par l'intégration du moteur d'analyse Rapid7 pour préparer les données d'importation avant leur traitement.
Version 19.0 : [sn_vul_veracode_cwe_import]	Étend la table de catégories Veracode des recommandations de rattrapage CWE.
Version 19.0 : [sn_vul_veracode_category_import]	Stocke les données de catégorie importées.
Version 19.0 : [sn_vul_veracode_sbom_import]	Stocke les données SBOM importées provenant de Veracode.
v17.1 : Ajouter une preuve à la clé de VI [sn_vul_proof_key_vulnerability]	Vulnérabilités Rapid7 pour lesquelles la preuve doit être incluse dans la clé de VI.
Éléments vulnérables évalués [sn_vul_m2m_exp_sw_vi]	Affecte une tâche de rattrapage à un groupe d'affectation lors de la création de la tâche de rattrapage.
Règle d'affectation [sn_vul_vgr_assignment_rule]	Affecte une tâche de rattrapage à un groupe d'affectation lors de la création de la tâche de rattrapage. Avant la version 15.0 : Affecte une tâche de rattrapage à un groupe d'affectation lors de la création d'une tâche de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Demande de changement associée [sn_vul_action_associate_cr]	Table intermédiaire utilisée pour traiter les nouvelles associations tâche de rattrapage-CHG. Avant la version 15.0 : table intermédiaire utilisée pour traiter les nouvelles associations VG-CHG.
Tâche d'élément vulnérable asynchrone [sn_vul_async_vi_job]	Contient des tâches en arrière-plan qui traitent les éléments vulnérables. Un seul type de tâche est pris en charge. Utilisé pour modifier les vulnérabilités en bloc.
Type de tâche d'élément vulnérable asynchrone [sn_vul_async_vi_job_type]	Contient les types de tâches en arrière-plan et fait référence au script pertinent. N'a qu'un seul processeur, le **VulnerabilityBulkEditProcessor**
Fermer automatiquement les détections obsolètes [sn_vul_auto_close_config]	Stocke la configuration permettant de fermer automatiquement les détections obsolètes.
Configurer la granularité des éléments vulnérables [sn_vul_action_vi_granularity_config]	Stocke le formulaire d'interface utilisateur utilisé pour activer ou désactiver Inclure le port à partir de la page de configuration dans le module Configurer la granularité VI.
Création d'une demande de changement [sn_vul_action_create_cr]	Utilisée pour créer des demandes de changement à partir de la tâche de rattrapage.
Créer des éléments vulnérables [sn_vul_action_create_vi]	Table intermédiaire qui est utilisée comme espace réservé pour les informations. Cette table ne stocke aucun enregistrement.
Collection [sn_vul_patch_orch_collection]	Stocke les données de collection provenant d'instances distinctes.
CWE [sn_vul_cwe]	Catalogue des vulnérabilités logicielles courantes de vulnérabilité et d'énumération (CWE).
Plateforme CWE applicable [sn_vul_cwe_m2m_cwe_platform]	Contient les données de plateforme CWE applicables importées.
Catégorie CWE [sn_vul_cwe_category]	Contient les données de catégorie CWE importées.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Conséquence courante CWE [sn_vul_cwe_consquence]	Contient les données de conséquence courantes CWE importées.
Référence externe CWE [sn_vul_cwe_reference]	Contient les données de référence externes CWE importées.
Exemple observé de CWE [sn_vul_m2m_cwe_cve]	Contient les données CVE CWE importées.
Plateforme CWE [sn_vul_cwe_platform]	Contient les données de la plateforme CWE importées.
Référence externe CWE [sn_vul_cwe_reference]	Contient les données de référence externes associées à CWE importées.
Relation CWE [sn_vul_m2m_cwe_relation]	Contient les données de relation CWE importées.
Vue CWE [sn_vul_cwe_view]	Contient les données de vue CWE importées.
Faiblesse CWE [sn_vul_cwe_weakness]	Contient les données de faiblesse CWE importées.
Version 16.1 : collection d'appareils [sn_vul_patch_orch_m2m_src_ci_collection]	Stocke les données de collection sur les éléments détectés.
Version 16.1 : Mise à jour de l'appareil [sn_vul_patch_orch_m2m_src_ci_update]	Stocke les données relatives aux correctifs déployés, ainsi que l'état de déploiement, qui sont affichés sur les enregistrements d'éléments détectés.
Correspondance de logiciel vulnérable de modèle de Détection [sn_vul_discovery_model_software_match]	Complète l'appariement des logiciels vulnérables à un modèle de détection.
Configuration de gestion de l'exception [sn_vul_exception_config]	Stocke les paramètres de configuration de la fonctionnalité de gestion des exceptions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Règle d'exception [sn_vul_auto_exception_rule]	Contient l'ensemble des règles évaluées pour la gestion des exceptions.
Exploit [sn_vul_exploit]	Contient les définitions des exploits : code accessible au public qui tire parti d'une vulnérabilité.
Cadre de travail de l'exploit sn_vul_exploit_framework	Contient les noms des frameworks d'exploitation, c'est-à-dire des progiciels complets capables d'exécuter de nombreux exploits.
Modèles de détection exposés [sn_vul_m2m_exp_sw_model]	Stocke le mappage entre le modèle de détection et l'évaluation de l'exposition à la vulnérabilité .
Évaluation de l'exposition [sn_vul_exp_by_sw]	Stocke les enregistrements pour l'évaluation de l'exposition.
V19.0 : manifeste d'exposition sn_vul_analyst_exposure_manifest	Table de manifeste pour le traitement delta.
Entrées de vulnérabilité d'exposition [sn_vul_m2m_entry_exp]	Stocke le mappage entre l'évaluation de vulnérabilité (sn_vul_entry) et l'évaluation de l'exposition.
Kit malware [sn_vul_malware_kit]	Contient les détails des kits de logiciels malveillants : des outils pré-écrits qui facilitent l'exécution d'un exploit ou d'un ensemble d'exploits connexes sans effectuer de travail de codage ou de configuration supplémentaire
Table d'actifs manquante [sn_vul_tenable_missing_asset]	Contient des ID d'actifs temporaires pour les données d'évaluation de Configuration Compliance ignorées avec des actifs sans correspondance.
Mise à jour de la solution du Microsoft Security Response Center [sn_vul_msrc_update]	Contient la dernière fois que les données de la solution ont été mises à jour par Microsoft. Utilisé pour comparer avec l'importation nocturne afin de déterminer les données delta à télécharger.
Microsoft Security Response Center Importation de solution [sn_vul_msrc_solution_import]	Utilisé par l'intégration de la solution Microsoft Security Response Center pour préparer les données d'importation avant leur traitement.
Microsoft Security Response Center Solution Integration [sn_vul_msrc_integration]	Étend la table d'intégration de vulnérabilité [sn_vul_integration] pour le Microsoft Security Response Center Solution Integration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Entrée de base de données de vulnérabilité nationa [sn_vul_nvd_entry]	Vulnérabilité documentée à partir de la base de données de vulnérabilité nationale du NIST.
Importation NVD CVSS [sn_vul_nvd_cvss_import]	Contient des données intermédiaires qui n'ont pas encore été transformées en schéma lors de l'importation Réponse aux vulnérabilités NVD.
Édition 16.1 [sn_vul_patch_orch.patch_approval_required]	Lorsque les déploiements de correctifs sont planifiés à partir d'une intégration de correctifs, les demandes sont soumises pour examen et approbation aux utilisateurs affectés au groupe d'approbation de mise à jour de correctif de niveau 1. Cette propriété est activée par défaut.
Version 16.1 : Déploiement des correctifs [sn_vul_patch_orch_deployment]	Stocke des informations sur les correctifs déployés, sur les collections et les CI.
Version 16.1 : Mise à jour du correctif [sn_vul_patch_orch_update]	Stocke des informations sur les correctifs disponibles sur des instances distinctes.
Version 16.1 : Correctif potentiel [sn_vul_patch_orch_m2m_vuln_patch]	Stocke des données sur les correctifs et les vulnérabilités qui identifient les correctifs qui peuvent être utilisés pour résoudre une vulnérabilité.
V19.0 : Exposition potentielle à la vulnérabilité sn_vul_analyst_m2m_pot_exp_sw_model	Tableau d'évaluation de l'exposition pour CVE.
Catégorie de produits [sn_vul_product_category]	Contient les données de la catégorie de produits importée.
Avis de sécurité Red Hat [sn_vul_rhsa_update]	Compare les Red Hat solutions par rapport à la tâche nocturne pour déterminer les données delta à importer.
Red Hat Importations de solutions [sn_vul_rh_solution_import]	Utilisé par les données d'importation intermédiaire avant leur Intégration de solution Red Hat traitement.
Intégration de solution Red Hat [sn_vul_rh_integration]	Étend la table d'intégration de vulnérabilité [sn_vul_integration] pour le Intégration de solution Red Hat.
Services d'entreprise connexes [sn_vul_m2m_ci_services]	Relie les CI aux services d'entreprise pour la recherche des services impactés. Contient

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	un marqueur indiquant s'il a été ajouté par Mappage des services.
V18.0 : Nombre d'efforts de rattrapage [sn_vul_daily_count_re]	Nombre quotidien d'efforts de rattrapage. Cette table est mise à jour quotidiennement.
V18.0 : Enregistrement de l'effort de rattrapage [sn_vul_remediation_effort_record]	Suit la progression du rattrapage pour les efforts de rattrapage (RE). Contient des références aux ER.
Règle de cible de rattrapage [sn_vul_ttr_rule]	Définit le délai prévu pour le rattrapage d'un élément vulnérable. Prolonge le fichier d'application.
V18.0 : Tâche de rattrapage [sn_vul_remediation_task]	Stocke toutes les tâches de rattrapage pour les groupes VR, AVR, CVR et résultats des tests.
Intégrations REST [sn_vul_rest_integration]	Étend la table Intégration de vulnérabilité [sn_vul_integration] pour les intégrations basées sur REST.
Détection de vulnérabilité NVD SAM [sn_vul_sam_config]	Contient quels CI et vulnérabilités sont surveillés avec SAM NVD et si la détection de vulnérabilité SAM NVD est activée ou non.
Pool d'importation planifiée [sn_vul_sched_import_pool]	Collecte des enregistrements de jeux d'importation planifiée utilisés pour faciliter les importations simultanées de sources de données.
Sélectionner l'élément vulnérable [sn_vul_action_select_vi]	Table intermédiaire de base utilisée pour gérer les VG divisés, créer des CHG et associer des CHG
État de la configuration [sn_vul_setup_status]	Interne uniquement : utilisé par l'assistant de configuration. Chaque fois que l'assistant de configuration est ouvert, il affiche l'état des étapes terminées et le pourcentage dans le coin supérieur droit provient de ce tableau.
Carte de gravité [sn_vul_severity_map]	Contient les mappages de la gravité de la source à la gravité normalisée.
Mappage de l'analyse de la solution [sn_vul_solution_scanner_mapping]	Mappe le fournisseur, le scanner et les mots clés pour l'exclusion ou l'inclusion.
Diviser le groupe de vulnérabilité [sn_vul_action_split_vg]	Table intermédiaire utilisée pour diviser les tâches de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Entrée de vulnérabilité tierce [sn_vul_third_party_entry]	Vulnérabilité documentée provenant d'une source tierce.
[sn_vul_tenable_io_template	Un enregistrement de modèle est envoyé à Tenable.io , puis importé pendant la nouvelle analyse pour les éléments qui ont Tenable.io comme source.
Mettre à jour le manifeste [sn_vul_update_manifest]	Liste des tâches de rattrapage qui ont été mises à jour et qui nécessitent un recalcul par le calculateur de déploiement.
V17.1 : Utilisation par classes CI [sn_vul_licensing_usage_by_ci_classes]	Contient le nombre d'utilisations agrégé par classe CI.
Nombre d'éléments de configuration VR [sn_vul_vr_configuration_item_count]	Contient la moyenne cumulative mobile de 90 jours d'éléments de configuration importés d'intégrations tierces.
Règle d'affectation de vulnérabilité [sn_vul_assignment_rule]	Contient l'ensemble des règles évaluées pour définir le groupe d'affectation sur les VI.
Calculateur de vulnérabilité [sn_vul_calculator_group]	Contient les règles du calculateur de vulnérabilité. L'ordre de la calculatrice détermine quelle calculatrice est évaluée en premier, et dans chaque calculatrice, une règle de calculatrice, au maximum, est utilisée.
Règle du calculateur de vulnérabilité [sn_vul_calculator]	Contient les règles de tous les calculateurs. Pour chaque calculateur, les règles du calculateur sont examinées dans l'ordre. Le premier calculateur correspondant à la condition utilise les valeurs de cette règle.
CVE de vulnérabilité [sn_vul_m2m_entry_cve]	Relie les données NVD Common Vulnerability Exposures (CVE) aux entrées vulnérables.
Entrée de file d'attente d'importation de la sourc [sn_vul_ds_import_q_entry]	Mettez en file d'attente les pièces jointes avant qu'elles ne soient traitées par une source de données. Utilisé par les intégrations de vulnérabilité.
Entrée de vulnérabilité [sn_vul_entry]	Vulnérabilité documentée.
Analyse de l'entrée de vulnérabilité [sn_vul_entry_scan]	Stocke la relation entre une entrée d'analyse et une entrée de vulnérabilité.
Cadre de travail de l'exploit de vulnérabilité	Contient la relation entre les cadres de travail d'exploitation et les vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vul_m2m_framework_vul]	
V19.0 : Évaluation de l'exposition à la vulnérabilité sn_vul_analyst_sam_config	Table de configuration de l'évaluation de l'exposition pour CVE.
Configuration de la granularité des vulnérabilités [sn_vul_granularity_config]	Stocke et gère l'état du port d'inclusion ou d'exclusion pour le module Configurer la granularité VI.
Tâches de remédiation [sn_vul_vulnerability]	Collection d'éléments vulnérables organisée pour le rattrapage.
Demandes de changement de tâche de rattrapage [sn_vul_m2m_vg_change_request]	Stocke l'association des tâches de rattrapage et des demandes CHG.
Éléments de tâche de rattrapage [sn_vul_m2m_vul_group_item]	Association des tâches de rattrapage et des éléments vulnérables.
Règles de la tâche de rattrapage [sn_vul_grouping_rule]	Contient les règles qui définissent les critères avec lesquels les groupes sont automatiquement créés pour un ensemble d'éléments vulnérables.
Intégration de vulnérabilité [sn_vul_integration]	Enregistrement planifiable pour importer des données de vulnérabilité à partir d'une source externe. Prolonge l'exécution de script planifiée.
Source de données d'intégration de vulnérabilité [sn_vul_int_data_src]	Source de données à utiliser avec une intégration de vulnérabilité.
Journal d'intégration de vulnérabilité [sn_vul_integration_log]	Enregistre la sortie d'informations du journal par exécutions d'intégration de vulnérabilité.
Processus d'intégration de vulnérabilité [sn_vul_integration_process]	Occurrence unique du processus pour une intégration de vulnérabilité.
File d'attente d'intégration de vulnérabilité [sn_vul_integration_queue]	Met en file d'attente les demandes d'importation pour une exécution d'intégration lorsque toutes les sources de données sont utilisées.
Exécution de l'intégration de vulnérabilité	Invocations d'intégration de vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vul_integration_run]	**Remarque :** Si une exécution d'intégration est en cours, une seule intégration peut être à l'état Prêt dans le backlog.
Statistiques d'exécutions de l'intégration de vulnérabilité [sn_vul_integration_stats]	Stocke la répartition de chaque étape : par exemple, l'heure de l'API REST, l'heure de création du VI, etc., pour une exécution d'intégration
Tâche d'élément de vulnérabilité [sn_vul_m2m_item_task]	Éléments vulnérables associés à des problèmes, des changements et des incidents de sécurité.
Kit malware de vulnérabilité [sn_vul_m2m_malware_kit_vul]	Contient les relations entre les vulnérabilités et les kits de logiciels malveillants.
Solution prérequise de vulnérabilité [sn_vul_m2m_solution_prerequisite]	Contient les prérequis spécifiques à la source pour l'application d'une solution, lorsqu'ils sont disponibles.
Limite du taux de vulnérabilité [sn_vul_rate_limit]	Définit une limite de débit à utiliser sur un scanner.
Référence de vulnérabilité [sn_vul_reference]	Références externes pour les vulnérabilités connues.
État du rattrapage des vulnérabilités [sn_vul_m2m_ttr_status]	État de l'élément vulnérable par rapport à la règle de cible de rattrapage appliquée la plus proche.
Règle du groupe de vulnérabilité [sn_vul_calc_risk]	Règle de calculateur spécialisée utilisée avec les calculateurs de score de risque. Prend des poids indiquant les valeurs, liées à un VI, à utiliser pour calculer le score de risque.
Calculateur de déploiement de vulnérabilité [sn_vul_rollup]	Liste des calculateurs de déploiement de vulnérabilité.
Analyse des vulnérabilités [sn_vul_scan]	Analyse de vulnérabilité. Contient les éléments à numériser, avec quel scanner et un résumé des résultats de l'analyse.
Élément de configuration de l'analyse de vulnérabilité [sn_vul_m2m_scan_configuration_item]	Associe les CI CMDB qui sont en file d'attente pour être analysés.
Entrée de la file d'attente de l'analyse de vulnérabilité	Enregistrement d'analyse mis en file d'attente pour numérisation ou traitement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vul_scan_q_entry]	Facilite les demandes dans les limites de taux indiquées.
Source de l'analyse de vulnérabilité [sn_vul_m2m_scan_source]	Associe les sources à un enregistrement d'analyse et désigne tous les enregistrements qui sont mis en file d'attente pour être analysés.
Tâche d'analyse de vulnérabilité [sn_vul_m2m_scan_vulnerability]	Associe les tâches de vulnérabilité pour les sources d'un enregistrement d'analyse.
Scanner de vulnérabilité [sn_vul_scanner]	Définit les scanners tiers à utiliser dans les analyses.
Limite des taux du scanner de vulnérabilité [sn_cmn_scanner_rate_limit]	Associe un scanner à une limite de taux.
Logiciel de vulnérabilité [sn_vul_m2m_entry_software]	Contient des associations entre les vulnérabilités et les logiciels vulnérables.
Solution de vulnérabilité [sn_vul_solution]	Contient les données de relation entre la vulnérabilité et les solutions possibles.
Solution de vulnérabilité [sn_vul_m2m_vulnerability_solution]	Relie la table Entrée de vulnérabilité (sn_vul_entry) à la table Solution de vulnérabilité (sn_vul_solution).
Approbation de changement d'état de la vulnérabilité [sn_vul_change_approval]	Suit le processus d'approbation des vulnérabilités.
Solution de remplacement à la vulnérabilité [sn_vul_m2m_solution_supersedence]	Contient la relation spécifique à la source entre les solutions.
Manifeste de mise à jour de vulnérabilité [sn_vul_vuln_update]	Contient une liste de vulnérabilités dont les données de déploiement doivent être mises à jour une fois que leurs éléments vulnérables ont été mis à jour, fermés ou que leur score de risque a été modifié.
Mappage du fournisseur de vulnérabilités [sun_vul_vulnerability_vendor_mapping]	Contient une liste des vulnérabilités et de leurs fournisseurs.
Élément vulnérable [sn_vul_vulnerable_item]	Contient l'occurrence d'une vulnérabilité sur un élément de configuration.

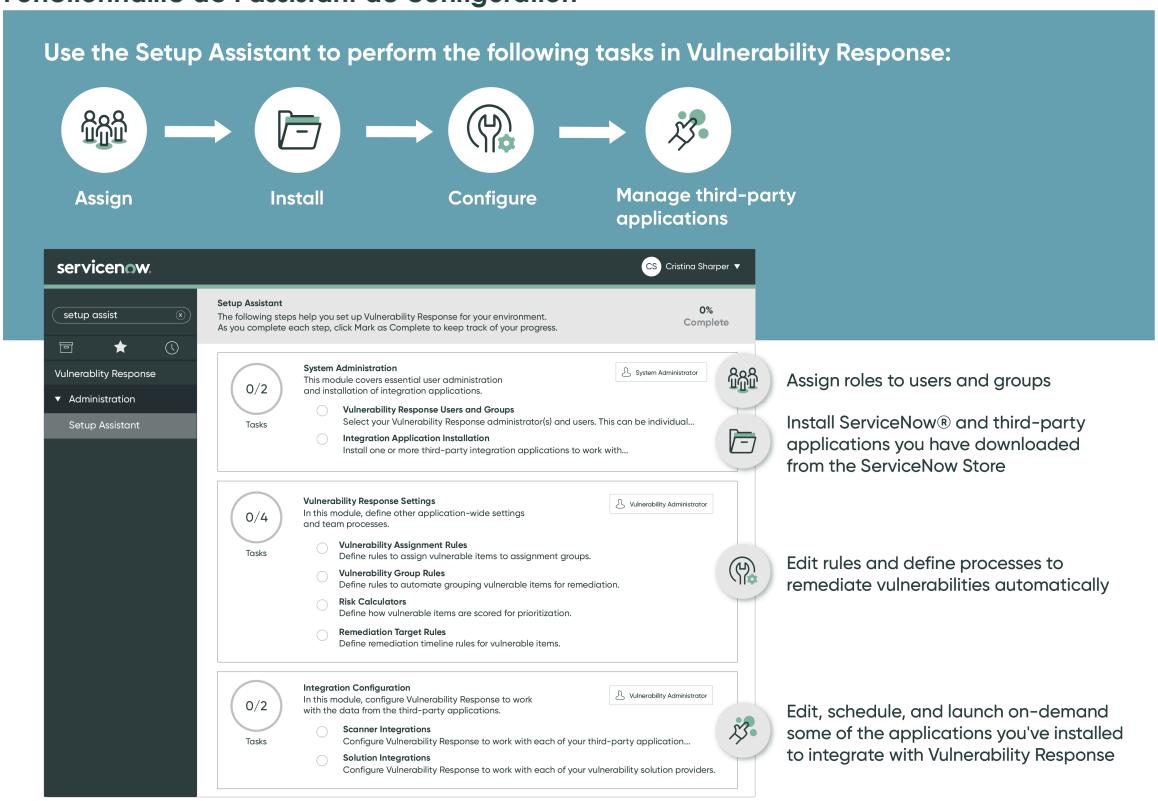
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Détection d'éléments vulnérables [sn_vul_detection]	Contient les détections d'éléments vulnérables provenant d'intégrations tierces.
Logiciel vulnérable [sn_vul_software]	Logiciel connu pour présenter certaines vulnérabilités.

Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration

L'assistant de configuration vous guide tout au long de la configuration Réponse aux vulnérabilités et de certaines intégrations tierces pour votre environnement. L'assistant de configuration fournit presque tout ce dont vous avez besoin pour installer et configurer votre environnement afin que vous puissiez utiliser Réponse aux vulnérabilités.

Fonctionnalité de l'assistant de configuration



Now Platform® roles: admin and vulnerability admin

L'utilisation de l'Assistant de configuration nécessite deux rôles différents Now Platform® : administrateur et administrateur de vulnérabilité.

Reportez-vous aux sections suivantes pour compléter les instructions et invites fournies dans l'Assistant de configuration.

Administration système : affecter des utilisateurs et des groupes et installer des applications d'intégration

Rôle requis : administrateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une liste des utilisateurs et des intégrations doit être obtenue auprès du gestionnaire des vulnérabilités avant de commencer ces tâches.

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.
2. Dans la première section, Administration système, l'administrateur affecte des rôles aux utilisateurs et aux groupes et installe les intégrations prises en charge.

   Affectez Réponse aux vulnérabilités des profils et des rôles à des utilisateurs et à des groupes dans l'Assistant de configuration.

   Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

3. Affectez des rôles dans l'Assistant de configuration.
   - Affecter le rôle de sn_vul.admin à des utilisateurs ou à des groupes.
   - Affectez le rôle sn_vul.admin pour l'administration et la configuration de Vulnerability Response, y compris les intégrations de vulnérabilité, les règles de tâche de rattrapage, les calculateurs et les règles de délai de correction.
   - Affectez le rôle sn_vul_vulnerability_write pour la création et la mise à jour des tâches de rattrapage et des éléments vulnérables.

     Remarque : Tous les autres utilisateurs reçoivent automatiquement l'accès en écriture uniquement sur les tâches de rattrapage qui leur sont affectées.

   - Affectez le rôle sn_vul_vulnerability_read pour afficher les tâches de rattrapage, les éléments vulnérables et d'autres informations sur les vulnérabilités.

     Remarque : Les utilisateurs disposant du rôle itil se voient automatiquement attribuer le rôle sn_vul.remediation_owner, ce qui leur permet d'afficher les tâches de rattrapage et les éléments vulnérables qui leur sont affectés, les entrées de vulnérabilité et les solutions dans l'application, sur Réponse aux vulnérabilités leur instance et dans l'application Agent mobile . Aucune affectation supplémentaire n'est nécessaire.

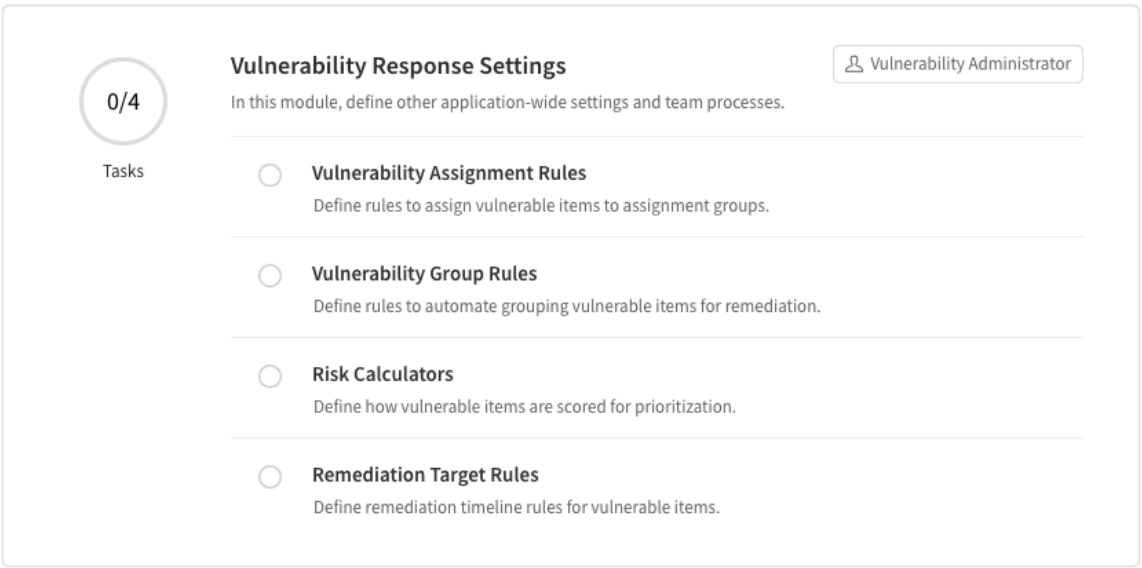
4. Installez des applications d'intégration tierces.
   - Intégrations de Réponse aux vulnérabilités Pour Installation et prise en charge des Réponse aux vulnérabilités applications plus d'informations sur les applications prises en charge par Réponse aux vulnérabilités.
   - Pour plus d'informations sur l'utilisation de l'assistant de configuration pour installer des applications prises en charge, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.

Réponse aux vulnérabilités Paramètres

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé), ou admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Dans les paramètres de Vulnerability Response, l'administrateur de vulnérabilité définit les paramètres à l'échelle de l'application et définit les règles pour Réponse aux vulnérabilités. L'administrateur peut également effectuer ces tâches.

1. Créer des règles d'affectation de vulnérabilité.

Créez des règles qui définissent l'affectation automatique des tâches de rattrapage pour la résolution. Au moins une règle est fournie avec le système de base. Consultez Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation pour plus d'informations.

Remarque :

La fonctionnalité de réapplication nécessite une application de base des règles. Une fois vos règles créées, activez la *`Reapply all vulnerability assignment rules`* tâche planifiée pour qu'elle s'exécute, à votre convenance. Dans le cas contraire, vous devrez réappliquer toutes les règles à tous les VI ouverts avant de les modifier.

Lorsque la tâche est terminée, définissez le champ **Exécuter** dans la tâche planifiée pour qu'il soit adapté à votre environnement. Selon le nombre de VI actifs dont vous disposez, leur évaluation et leur mise à jour quotidienne peuvent avoir un impact non négligeable sur les performances. Pour les environnements plus importants, envisagez une mise à jour une fois par semaine, voire une fois par mois.

La réapplication des règles d'affectation ne regroupe pas les éléments vulnérables.

2. Créez des règles de tâche de rattrapage.

Créez des règles qui définissent la création automatique de tâches de rattrapage en vue de leur résolution. Au moins une règle, **Vulnérabilité,** est fournie avec le système de base. Vous pouvez réappliquer les règles à partir de la vue de formulaire ou de liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lorsqu'une règle de groupe est supprimée, à partir du formulaire ou de la vue de liste, vous avez la possibilité de supprimer tous les groupes **ouverts** créés par cette règle. Les groupes qui ne sont pas dans l'état **Ouvert** sont exclus.
- Pour plus d'informations sur la création de règles pour votre environnement, reportez-vous à la section Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces .
- Reportez-vous à la section Exploration de l'application Réponse aux vulnérabilités pour plus d'informations sur l'utilisation Réponse aux vulnérabilités pour corriger les vulnérabilités.

3. Créez et activez des calculateurs de risque.

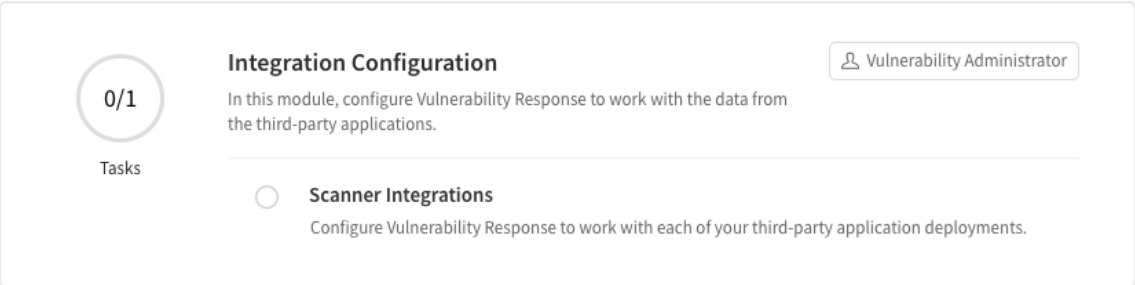
   Activez les calculateurs de risque qui définissent la notation des éléments vulnérables pour déterminer leur ordre de priorité. Plusieurs calculateurs de risque sont fournis avec le système de base. Voir les Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité informations sur la création ou la modification de calculateurs de risque pour votre environnement.

4. Créez des règles de cibles de rattrapage.

   Créez des règles de cibles de rattrapage pour les catégories de rattrapage. Au moins une règle est fournie avec le système de base. Pour plus d'informations sur la création de règles pour votre environnement, reportez-vous à la section Réponse aux vulnérabilités Règles de cibles de rattrapage .

Configuration de l'intégration

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé), ou admin.



Dans la section Configuration de l'intégration, configurez, planifiez, modifiez et lancez sur demande les intégrations de scanner de vulnérabilité tierces suivantes et, si l'application est installée, les fournisseurs de Gestion des solutions pour Réponse aux vulnérabilités solutions.

- Pour Configurer l'utilisation de l'assistant de Qualys Vulnerability Integration configuration plus d'informations sur la configuration de l'extension Qualys Vulnerability Integration.
- La configuration de l'application Intégration de Réponse aux vulnérabilités à Tenable est prise en charge. Reportez-vous à Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration.
- Une fois l'application Gestion des solutions pour vulnérabilités installée, l'option **Intégrations de solutions** s'affiche sous **Intégrations de scanners**. Cliquez sur **Intégrations de solutions** pour configurer vos fournisseurs de solutions de vulnérabilité installées dans cette section de l'Assistant de configuration. Les Intégration de solution Red Hat et Microsoft Security Response Center Solution Integration sont pris en charge.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consultez Gestion des solutions pour vulnérabilités pour plus d'informations sur les solutions installées. Reportez-vous à la section Installer l'application Gestion des solutions pour Réponse aux vulnérabilités pour plus d'informations sur l'installation.

Reportez-vous à la section Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'Assistant de configuration pour plus d'informations sur la configuration des solutions installées.

- Si une intégration est multisources, vous pouvez avoir plusieurs déploiements de la même intégration tierce.
- Les paramètres de votre intégration tierce d'origine sont utilisés comme modèle pour les paramètres de chaque nouvelle intégration.

Remarque : Si vous supprimez l'intégration de vulnérabilité d'origine, vous devez sélectionner une autre intégration à utiliser comme modèle. Envisagez de désactiver l'intégration au lieu de la supprimer. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

Les données de chaque intégration tierce sont identifiées de manière unique et disponibles dans une seule instance de Réponse aux vulnérabilités.

Remarque : Plusieurs intégrations de vulnérabilité ne Rapid7 InsightVM sont pas disponibles dans l'Assistant de configuration. Pour en savoir plus sur la configuration et la création de plusieurs Rapid7 InsightVM intégrations, consultez la rubrique Créer des importations séparées par domaine pour une intégration

Tâches supplémentaires

Pour plus d'informations sur les tâches de configuration non incluses dans l'Assistant de configuration, reportez-vous à la section Tâches d'installation et de configuration supplémentaires Réponse aux vulnérabilités .

Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration

Affectez les rôles de profil à des groupes ou à des utilisateurs à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.

Avant de commencer

Si vous avez déjà affecté des rôles de profil à Réponse aux vulnérabilités l'aide de l'Assistant de configuration et que vous souhaitez plus d'informations sur la modification et la gestion de vos rôles granulaires et de vos affectations de rôles dans le module Administration utilisateurs, reportez-vous à la section Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Si vous êtes un client de mise à niveau, vous pouvez continuer à utiliser vos rôles existants pour l'application Vulnerability Response. L'accès des utilisateurs et des groupes affectés aux autorisations sn_vul.vulnerability_read et sn_vul.vulnerability_write et aux rôles de propriétaire de rattrapage disponibles dans les versions précédentes de n'a Réponse aux vulnérabilités pas changé.

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

Si vous n'avez pas encore affecté le rôle de profil sn_vul.vulnerability_admin à l'aide de l'Assistant de configuration, procédez comme suit pour l'affecter. Une fois affecté, l'administrateur de vulnérabilité ayant ce rôle de profil a l'autorisation d'effectuer les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

tâches de l'assistant de configuration après la première section et de gérer les règles et les intégrations tierces dans l'application Réponse aux vulnérabilités .

Pour obtenir une vue d'ensemble des rôles de profil et des rôles granulaires, reportez-vous à la section Réponse aux vulnérabilités Profils et rôles granulaires.

Si vous êtes un client de mise à niveau, utilisez la table suivante comme référence.

Avant la version 10.3	À partir de la version 10.3
Si vous avez affecté sn_vul.admin	Vous préférez peut-être affecter sn_vul.vulnerability_admin : administrateur de vulnérabilité aux utilisateurs ou aux groupes. Les utilisateurs disposant de ce rôle ont un accès complet à l'application Vulnerability Response (VR) et à ses enregistrements. Les utilisateurs disposant de ce rôle configurent toutes les applications et règles de VR et installent des intégrations tierces.
Si vous avez affecté sn_vulnerability_write pour les utilisateurs et les groupes.	Vous préférez peut-être affecter sn_vul.vulnerability_analyst : analyste de vulnérabilité aux utilisateurs et aux groupes. Les utilisateurs et les groupes dotés de ce rôle affichent et mettent à jour tous les enregistrements pour le rattrapage des VI.
Si vous avez affecté sn_vul.remediation_owner	Vous préférez peut-être affecter sn_vul.remediation_owner : propriétaire du rattrapage aux utilisateurs et aux groupes. Les utilisateurs et les groupes dotés de ce rôle corrigent les vulnérabilités qui leur sont affectées ou qui sont affectées à un groupe auquel ils appartiennent. Les groupes ou utilisateurs disposant de ce rôle affichent et mettent à jour les enregistrements qui leur sont affectés ou qui sont affectés à un groupe auquel ils appartiennent.
Si vous avez affecté sn_vul.admin pour la gestion des éléments de configuration (CI) sans correspondance	Vous préférez peut-être affecter sn_vul.ci-Gestionnaire CI aux utilisateurs et aux groupes. Les utilisateurs et les groupes dotés de ce rôle gèrent les éléments de configuration (CI) sans correspondance introuvables dans la CMDB (Base de données de gestion des configurations). Les groupes ou utilisateurs ayant ce rôle mettent à jour les éléments détectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant la version 10.3	À partir de la version 10.3
Si vous avez affecté sn_vul.admin pour les reports et les approbations d'exception.	Vous préférez peut-être affecter sn_vul.exception_approver : approbateur d'exception aux utilisateurs et aux groupes. Les utilisateurs et les groupes dotés de ce rôle approuvent les exceptions, les reports et les fermetures des tâches de rattrapage et des éléments vulnérables. À partir de la version 20.0, le rôle granulaire sn_vul.read_all a été supprimé pour ce rôle afin que vous puissiez accéder aux éléments vulnérables et aux tâches de rattrapage qui vous sont affectés, à vous et à votre groupe, au lieu de tous les éléments vulnérables et tâches de rattrapage.
Si vous avez affecté sn_vul.vulnerability_read pour fournir une visibilité dans la gestion des vulnérabilités.	Vous préférez peut-être affecter l'accès en lecture à des zones spécifiques de l'application par tâche. Par exemple, affectez sn_vul.read_all afin qu'un utilisateur puisse afficher tous les enregistrements VR. Pour un accès en lecture à l'affichage des règles de tâche de rattrapage, affectez sn_vul.read_group_rules. Les utilisateurs et groupes ayant ce rôle ne mettent pas à jour les enregistrements.

Pour afficher les rôles granulaires dont un utilisateur ou un groupe ayant un rôle de profil hérite par défaut, accédez à **Tout** > **Administration utilisateurs** > **Rôles**. Localisez le rôle souhaité et cliquez dessus pour ouvrir l'enregistrement. L'onglet Contient les rôles répertorie tous les rôles granulaires du rôle de profil, ainsi que tous les rôles hérités.

Vous préférez peut-être vérifier que tous les utilisateurs et groupes requis sont créés avant d'affecter des rôles dans l'Assistant de configuration. Pour ajouter de nouveaux utilisateurs et groupes à partir de l'Assistant de configuration, vous pouvez également cliquer sur le lien du **module Administration utilisateurs** dans le formulaire illustré dans la figure suivante.

Dans l'exemple suivant, pour limiter l'accès à l'application Réponse aux vulnérabilités , cet exemple montre comment affecter à un utilisateur le profil d'administrateur de vulnérabilité. En général, vous préférez affecter des rôles de profil autres que sn_vul.vulnerability_admin aux groupes.

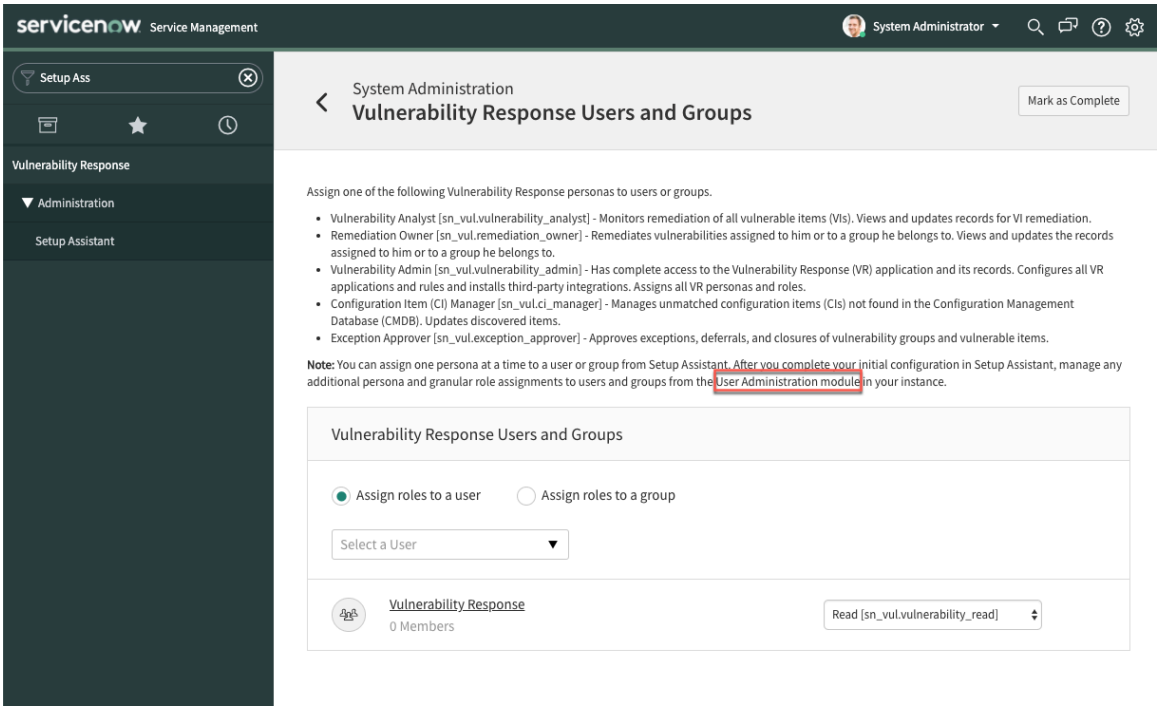
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration Assistant de configuration**. La page Setup Assistant (Assistant de configuration) s'affiche.
2. Cliquez sur Utilisateur et groupes de Vulnerability Response. La page Utilisateurs et groupes de Vulnerability Response de l'administration système s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Lorsque l'option Affecter des rôles à un utilisateur est sélectionnée, choisissez un utilisateur existant dans la liste.

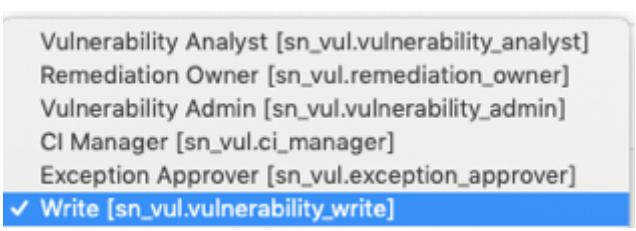
   Vous pouvez affecter un seul rôle de profil à un utilisateur ou à un groupe.

   À droite du formulaire, une fois que vous avez sélectionné un utilisateur ou un groupe, le profil par défaut, Propriétaire de rattrapage [sn_vul.remediation_owner] est affecté par défaut et reste affiché dans la liste jusqu'à ce que vous le changiez.

   Remarque : Si vous effectuez une mise à niveau vers une version Réponse aux vulnérabilités plus récente et que vous avez précédemment affecté le rôle sn_vul.vulnerability_read ou sn_vul.vulnerability_write à un utilisateur ou à un groupe avant la mise à niveau, il s'affiche avec les nouveaux rôles de profil, comme illustré dans la figure suivante.

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

   Notez que pour les utilisateurs existants ou les groupes actuellement affectés aux rôles sn_vul.vulnerability_read ou sn_vul.vulnerability_write, ces rôles sont affichés avec les rôles de profil dans la liste. Une fois que vous avez affecté un rôle de profil, l'ancien rôle n'est plus disponible à l'avenir. Par exemple, comme le montre la figure suivante, le rôle Écriture [sn_vul.vulnerability_write] n'est plus affiché en tant qu'option pour cet utilisateur ou groupe une fois que l'un des rôles de profil lui a été affecté.

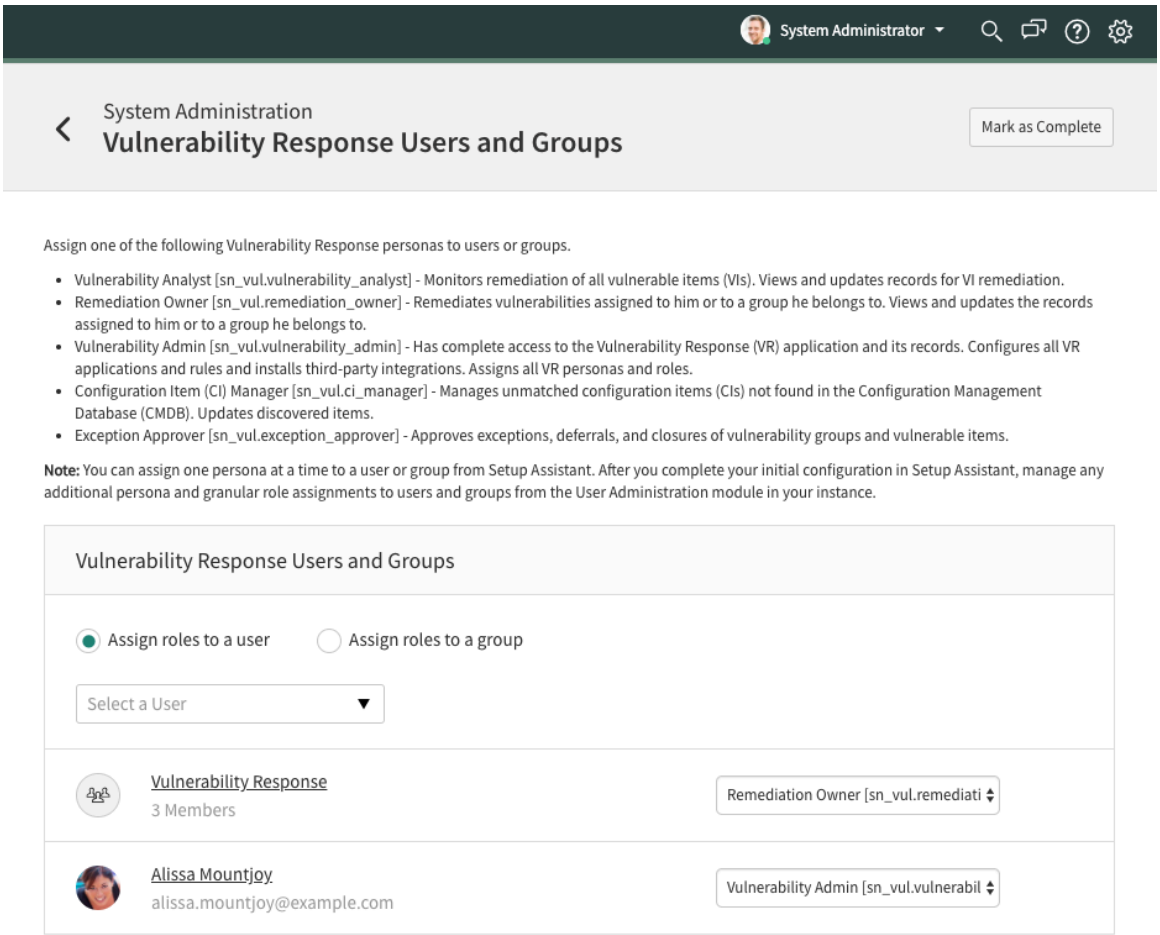


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans la liste à droite du formulaire, sélectionnez Administrateur de **vulnérabilité [sn_vul.vulnerability_admin].**
   Un message s'affiche pour indiquer que l'utilisateur ou le groupe a été affecté avec succès au profil.

Profil du propriétaire de la résolution affecté à un groupe et profil de l'administrateur de vulnérabilité affecté à un utilisateur



5. À l'aide des descriptions des rôles de profil répertoriés ci-dessus, continuez d'affecter des utilisateurs et des groupes aux rôles de profil restants : propriétaire de la correction, analyste de vulnérabilité, gestionnaire de CI et approbateur d'exception.
   Vous avez terminé avec succès l'affectation des rôles de profil aux utilisateurs et aux groupes à l'aide de l'Assistant de configuration.
6. Facultatif : Pour modifier les utilisateurs d'un groupe à partir de l'Assistant de configuration, procédez comme suit.

   a. Une fois le groupe affiché sur le formulaire, cliquez sur le nom du groupe que vous souhaitez modifier.
   L'enregistrement du groupe s'affiche.

   b. Une fois l'onglet Membres du groupe sélectionné, cliquez sur **Modifier**.
   Le formulaire Modifier les membres s'affiche

   c. Utilisez la zone de liste double pour sélectionner ou supprimer des utilisateurs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Cliquez sur **Enregistrer** pour enregistrer vos changements et revenir à l'enregistrement du groupe.

e. Cliquez sur **Mettre à jour** pour revenir à l'Assistant de configuration.

f. Sur la page Assistant de configuration, cliquez sur **Utilisateurs et groupes de Vulnerability Response** pour poursuivre votre configuration dans l'Assistant de configuration.

Que faire ensuite

En tant qu'administrateur système, poursuivez la configuration de dans l'Assistant Réponse aux vulnérabilités de configuration. Notez qu'une fois la première section terminée, vous pouvez demander à un utilisateur que vous avez affecté au rôle de profil d'administrateur de vulnérabilité d'effectuer les tâches dans l'Assistant de configuration. Pour plus d'informations sur la gestion des rôles granulaires et des exemples, reportez-vous à la section Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités

Une fois que vous avez terminé votre affectation initiale de rôles de profil à l'aide de l'Assistant de configuration, gérez les affectations de rôles granulaires supplémentaires aux utilisateurs ou aux groupes à partir du module Administration utilisateurs de votre instance.

Avant de commencer

Si vous n'avez pas déjà terminé l'installation et la configuration initiales pour Réponse aux vulnérabilités l'utilisation de l'Assistant de configuration, ou si vous n'avez pas encore affecté de rôles de profil aux utilisateurs et aux groupes, accédez à **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**. Consultez Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.

Pour connaître les termes clés et obtenir une vue d'ensemble des rôles des profils, reportez-vous à la section Réponse aux vulnérabilités Profils et rôles granulaires.

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

Si vous souhaitez que vos utilisateurs et groupes disposent de plus d'accès que ne le permet l'un des rôles, vous pouvez ajouter des rôles plus granulaires aux utilisateurs et aux groupes. À l'inverse, si vous souhaitez limiter l'accès à des utilisateurs et à des groupes spécifiques au niveau de la tâche, vous pouvez supprimer les rôles granulaires. En outre, vous pouvez créer des rôles personnalisés en fonction de vos besoins.

Rôle requis : administrateur

Procédure

1. Pour gérer les rôles granulaires pour les utilisateurs et les groupes, choisissez-en un pour continuer.

Option	Description
Modifier les rôles granulaires pour un utilisateur ou un groupe	Affectez ou supprimez des rôles granulaires pour des utilisateurs ou des groupes, ou modifiez des rôles granulaires afin que seuls

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	certains utilisateurs au sein d'un groupe disposent d'autorisations étendues ou limitées. Un exemple suit le tableau.
Créer un nouveau rôle	Créez un nouveau rôle à l'aide d'un ou de plusieurs rôles granulaires de la bibliothèque pour un intitulé de poste spécifique ou pour répondre à un besoin spécifique. Un exemple suit le tableau.

Les noms des rôles granulaires décrivent Réponse aux vulnérabilités généralement ce que les utilisateurs peuvent faire et voir. Pour afficher les descriptions des rôles granulaires spécifiques, accédez à **Tout** > **Administration utilisateurs** > **Rôles** et localisez le rôle que vous souhaitez. La description du rôle, les rôles qui sont automatiquement hérités lorsqu'un rôle est affecté et tous les rôles qui dépendent d'autres rôles sont également répertoriés.

2. Pour affecter ou supprimer un rôle granulaire pour un utilisateur ou un groupe, procédez comme suit.
   À titre d'exemple, supposons que vous souhaitiez affecter un gestionnaire informatique avec un rôle qui lui permet d'afficher les enregistrements, mais pas de les mettre à jour ou de les modifier. Pour afficher les enregistrements dans Réponse aux vulnérabilités, Analyse des performances pour Réponse aux vulnérabilitéset pour toutes les intégrations tierces, affectez à cet utilisateur le rôle granulaire sn_vul.read_all.

   a. Accédez à la **Tout** > **Administration utilisateurs** > **Utilisateurs**.

   b. Localisez l'utilisateur et, dans la colonne Nom, cliquez sur l'enregistrement pour l'ouvrir.
   L'enregistrement de l'utilisateur s'affiche.

   c. Si cette option n'est pas sélectionnée, sélectionnez l'onglet Rôles.
   Les rôles actuellement affectés à l'utilisateur s'affichent.

   d. Cliquez sur **Modifier**.
   Le formulaire Modifier les membres s'affiche.

   e. Dans le champ Collection de la zone de liste double, saisissez le nom du rôle si vous le connaissez, ou saisissez `*sn_vul` pour afficher uniquement les rôles granulaires disponibles pour Vulnerability Response.

   f. Localisez et déplacez sn_vul.read_all vers la liste des rôles.

   > **Remarque :** Utilisez le même processus pour supprimer des rôles granulaires spécifiques des utilisateurs dans la zone de sélection en déplaçant le rôle de la liste Rôles vers la liste Collection.

   g. Cliquez sur **Enregistrer**.
   L'enregistrement utilisateur s'affiche avec le nouveau rôle granulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

h. Cliquez sur **Mettre à jour** pour enregistrer vos changements et revenir à la liste d'utilisateurs.
Vous avez donné à un utilisateur l'autorisation de lire, mais pas de mettre à jour, des enregistrements dans Réponse aux vulnérabilités, Analyse des performances pour Réponse aux vulnérabilitéset pour des intégrations tierces.

3. Pour modifier un groupe afin que seuls certains membres disposent d'un accès étendu avec des rôles plus granulaires, procédez comme suit.
Par exemple, supposons que vous souhaitiez autoriser certains utilisateurs du groupe Propriétaire de rattrapage (sn_vul.remediation_owner) à créer manuellement des éléments vulnérables, mais que vous ne souhaitez pas étendre cette autorisation à tous les utilisateurs du groupe. L'autorisation de créer manuellement des éléments vulnérables est accordée par le rôle granulaire sn_vul.create_vulnerable_items. Pour accorder cette autorisation à sélectionner uniquement des utilisateurs de ce groupe, procédez comme suit.

a. Accédez à la **Tout** > **Administration utilisateurs** > **Groupes**.

b. Localisez le groupe de propriétaires de rattrapage et, dans la colonne Nom, cliquez sur le groupe pour ouvrir l'enregistrement.
L'enregistrement du groupe s'affiche.

c. Si cette option n'est pas sélectionnée, sélectionnez l'onglet Membres du groupe.
Les membres actuels du groupe s'affichent.

d. Cliquez sur un nom dans la liste à laquelle vous souhaitez affecter le rôle granulaire et ouvrez l'enregistrement.

e. Dans l'enregistrement, faites défiler jusqu'à l'onglet Rôles et sélectionnez-le.
Les rôles attribués à l'utilisateur s'affichent.

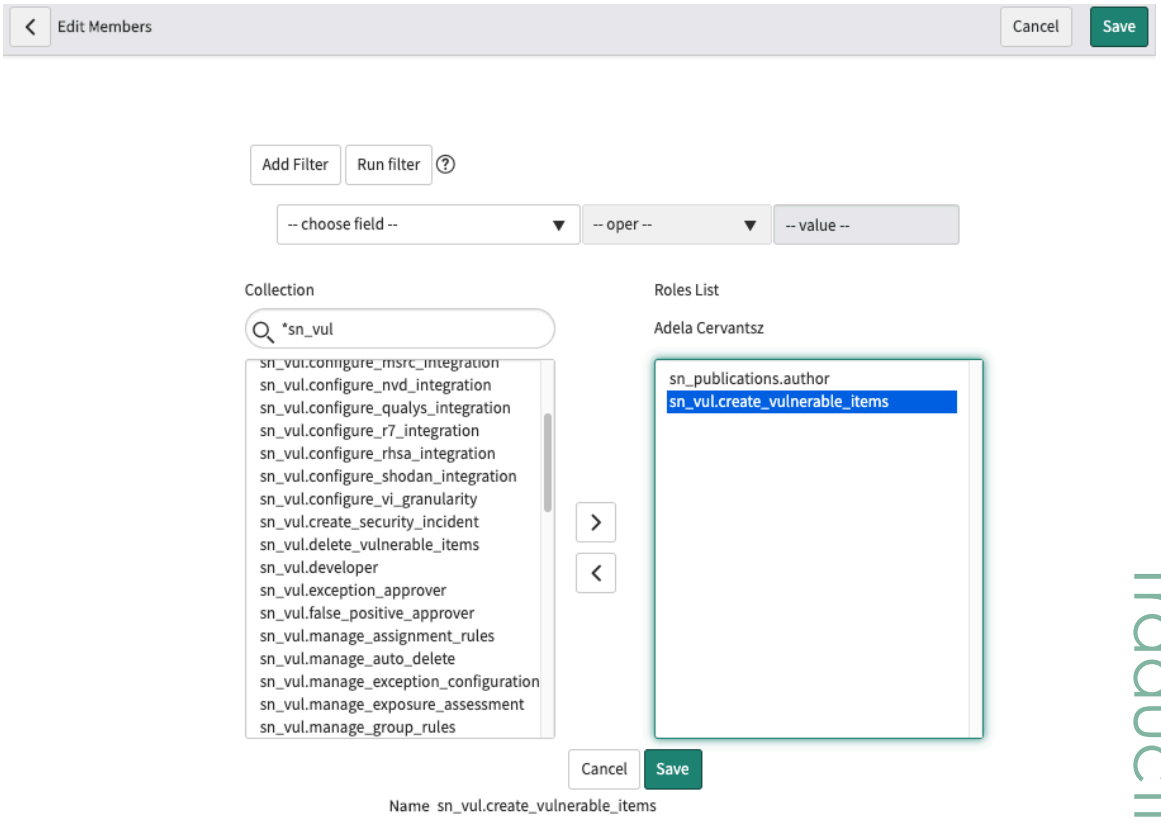
f. Cliquez sur **Modifier**.
Le formulaire Modifier les membres s'affiche.

g. Dans le champ Collection, saisissez le nom du rôle si vous le connaissez, ou saisissez `*sn_vul` pour afficher tous les rôles granulaires disponibles pour Vulnerability Response.

h. Localisez et déplacez sn_vul.create_vulnerable_items vers la liste Rôles.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



i. Cliquez sur **Enregistrer**.
L'enregistrement utilisateur s'affiche avec le nouveau rôle granulaire.

j. Cliquez sur la flèche arrière pour revenir afin d'afficher les utilisateurs dans l'enregistrement du groupe de propriétaires de rattrapage

k. Cliquez sur les noms de la liste à laquelle vous souhaitez affecter ce rôle granulaire, ouvrez leurs enregistrements et utilisez la zone de liste double pour affecter le rôle.

l. Une fois vos modifications terminées, cliquez sur **Mettre à jour** pour enregistrer vos modifications et revenir à la liste des groupes.
Vous avez autorisé certains utilisateurs du groupe Propriétaire de rattrapage (sn_vul.remediation_owner) à créer manuellement des éléments vulnérables.

4. Pour créer un nouveau rôle en utilisant uniquement les rôles granulaires que vous sélectionnez, procédez comme suit.
Pour cet exemple, supposons que vous souhaitiez créer le rôle d'un auditeur de conformité. Ce rôle travaille en étroite collaboration avec Governance, Risk, and Compliance (GRC), et la tâche nécessite les autorisations et tâches suivantes dans Réponse aux vulnérabilités:

- Gère les délais de correction pour les éléments vulnérables et les groupes de vulnérabilité
- Approuve les demandes d'exception pour prolonger les délais ou différer le rattrapage
- Gère le nettoyage des éléments vulnérables plus anciens avec suppression automatique

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Définir les scores de risque
- Lit tous les enregistrements, Réponse aux vulnérabilités mais n'est pas autorisé à les modifier.

a. Accédez à la **Tout** > **Administration utilisateurs** > **Rôles**.

b. Dans la liste Rôles, cliquez sur **Nouveau**.

c. Renseignez les champs de l'enregistrement du rôle.

Créez un nom, sélectionnez l'application qui contient cet enregistrement et entrez une brève description de votre nouveau rôle. Pour en savoir plus sur les autres champs du formulaire, consultez Créer un rôle

Remarque : Lors de la création d'un nom pour votre nouveau rôle, vous préférerez peut-être utiliser un nom facilement reconnaissable dans la liste des rôles et décrivant la fonctionnalité du rôle. Pour cet exemple, vous préférerez peut-être un titre tel que Auditeur de conformité : GRC-VR.

d. Cliquez sur **Envoyer**.
La liste des rôles s'affiche.

e. Localisez votre nouveau rôle et cliquez dessus pour ouvrir l'enregistrement.

f. Cliquez sur **Modifier**.
Le formulaire Modifier les membres s'affiche.

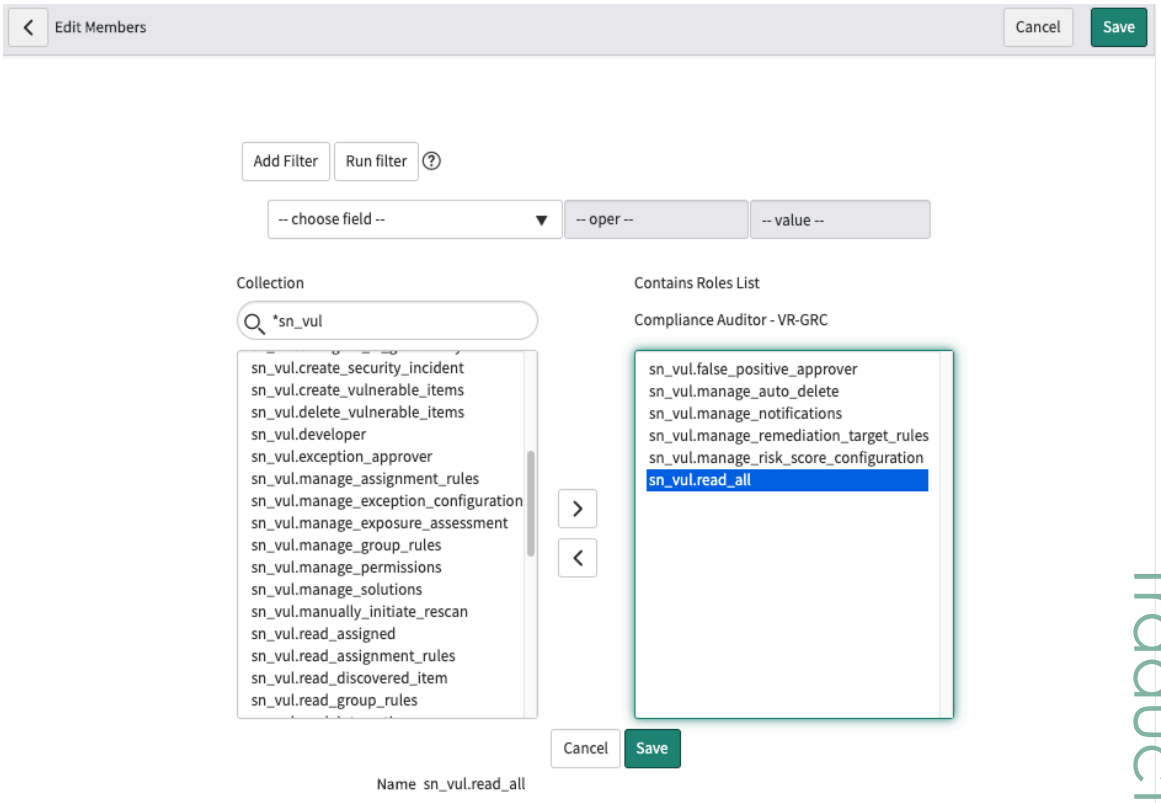
g. Utilisez la zone de liste double pour ajouter des rôles granulaires à votre nouveau rôle.

Dans cet exemple, les rôles requis pour ce nouveau rôle sont affichés dans la colonne de droite de la figure suivante.

Pour afficher uniquement les rôles granulaires pour Vulnerability Response, saisissez `*sn_vul` dans le champ Collection.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



h. Cliquez sur **Enregistrer**.
L'enregistrement de votre nouveau rôle s'affiche. À partir de l'onglet Contient les rôles, continuez à modifier le rôle selon vos besoins.

i. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.
Votre nouveau rôle s'affiche dans la liste des rôles.

Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration

Installez les applications d'intégration tierces pour lesquelles vous avez le droit d'utiliser Réponse aux vulnérabilités l'Assistant de configuration.

Avant de commencer

L'assistant de configuration prend en charge l'installation de la plupart des applications d'intégration tierces avec Réponse aux vulnérabilités, mais vous poursuivez la configuration de certaines applications que vous installez à partir de modules de configuration de votre instance. Pour Intégrations de Réponse aux vulnérabilités obtenir la liste des applications prises en charge par Réponse aux vulnérabilités.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Une fois installée, la Gestion des solutions pour vulnérabilités fonctionnalité vous permet d'accéder Réponse aux vulnérabilités au et au Microsoft Security Response Center Solution Integration dans l'Assistant Intégration de solution Red Hat de configuration.
- Gestion des solutions pour vulnérabilités est disponible par abonnement séparé. Pour plus d'informations sur la façon d'intégrer Réponse aux vulnérabilités des solutions, consultez la section Gestion des solutions pour vulnérabilités

Avant de pouvoir installer et activer des applications tierces à partir de l'Assistant de configuration, effectuez les tâches suivantes pour garantir une installation fluide :

Configurer les tâches	Description
Vérifiez que vous disposez d'autorisations valides ServiceNow pour les applications d'intégration que vous souhaitez installer.	Accédez à la **Gestion des abonnements** > **Abonnements** dans votre instance pour vérifier les autorisations. La liste affiche les abonnements que votre organisation a achetés. Pour plus d'informations sur l'obtention d'autorisations pour une Opérations de sécurité application à partir de , reportez-vous à la ServiceNow Storesection .
(Facultatif) Si elle n'est pas déjà installée et activée, il peut être préférable d'installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce.	Pour plus d'informations sur l'installation et l'activation de l'application, consultez Installer et configurer VulnerabilityRéponse aux vulnérabilités Response.
Si ce n'est pas déjà fait, vous devez activer et importer les données de vulnérabilité avec la tâche planifiée NVD Integration and CWE avant d'exécuter une application de scanner tierce pour importer les données.	Exécutez les intégrations NVD et CWE dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit de scanner tiers. Consultez Présentation des intégrations NVD pour plus d'informations.
Vérifiez que vous avez terminé toutes les tâches de configuration requises pour les intégrations tierces pour Réponse aux vulnérabilités.	Examinez toutes les tâches de configuration requises pour chaque intégration que vous souhaitez installer sur Intégrations de Réponse aux vulnérabilités.

Rôle requis : administrateur

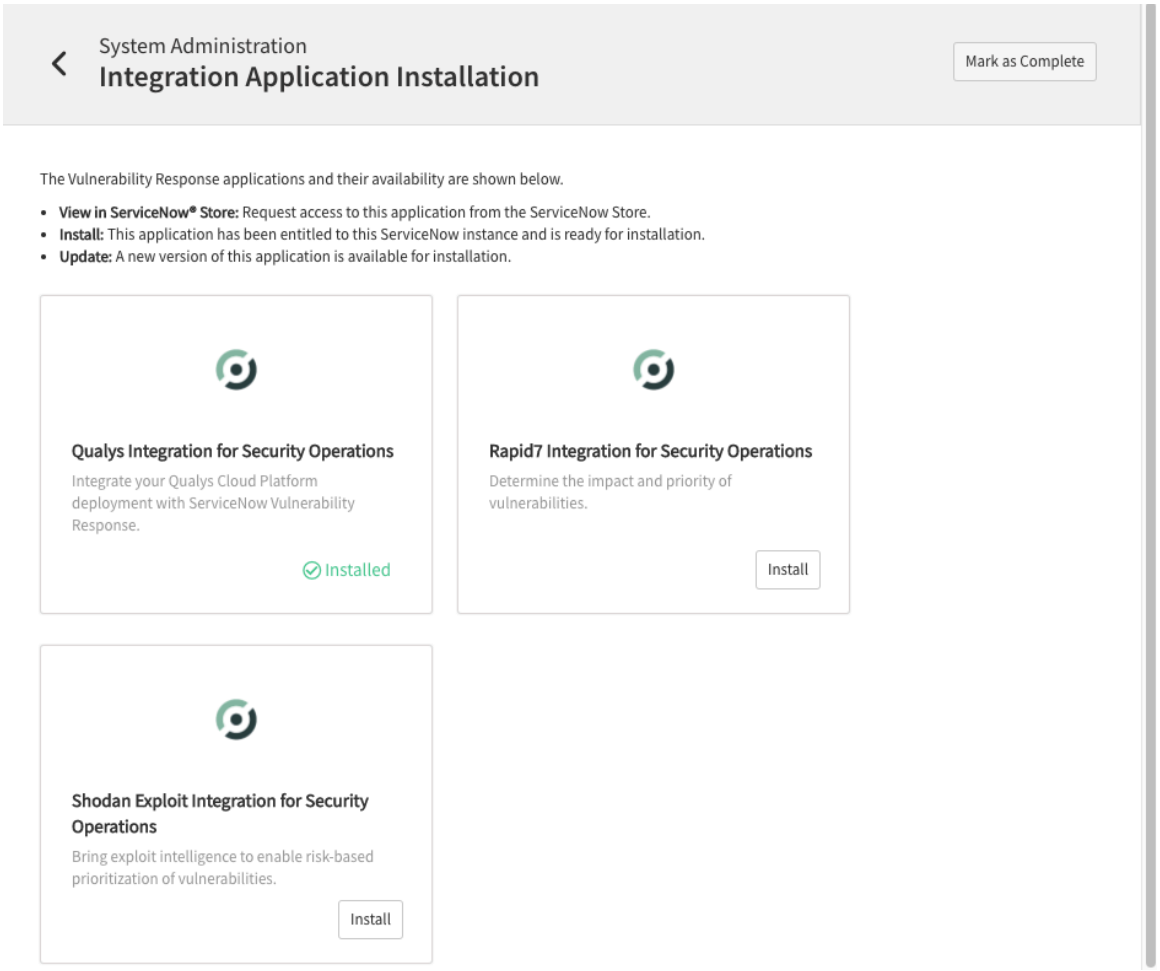
Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Administration système** > **Installation d'application d'intégration**.

   Après quelques instants, les applications pour lesquelles vous disposez des droits et qui peuvent être installées sur votre instance s'affichent.

Traduction automatique

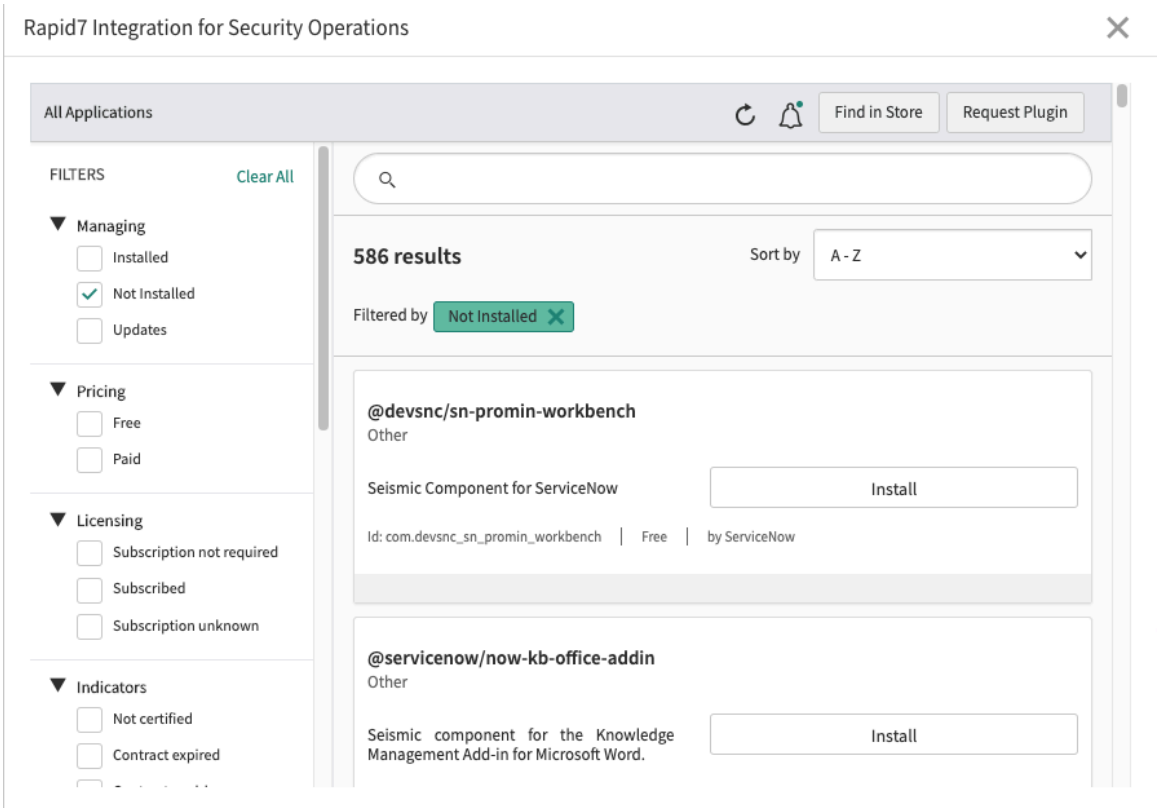
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Localisez l'application que vous souhaitez installer et cliquez sur **Installer** dans la vignette de l'application.
   La boîte de dialogue Toutes les applications s'affiche avec le nom de la vignette d'application sur laquelle vous avez cliqué, par exemple, Rapid7 Integration for Security Operations, comme illustré dans la figure suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

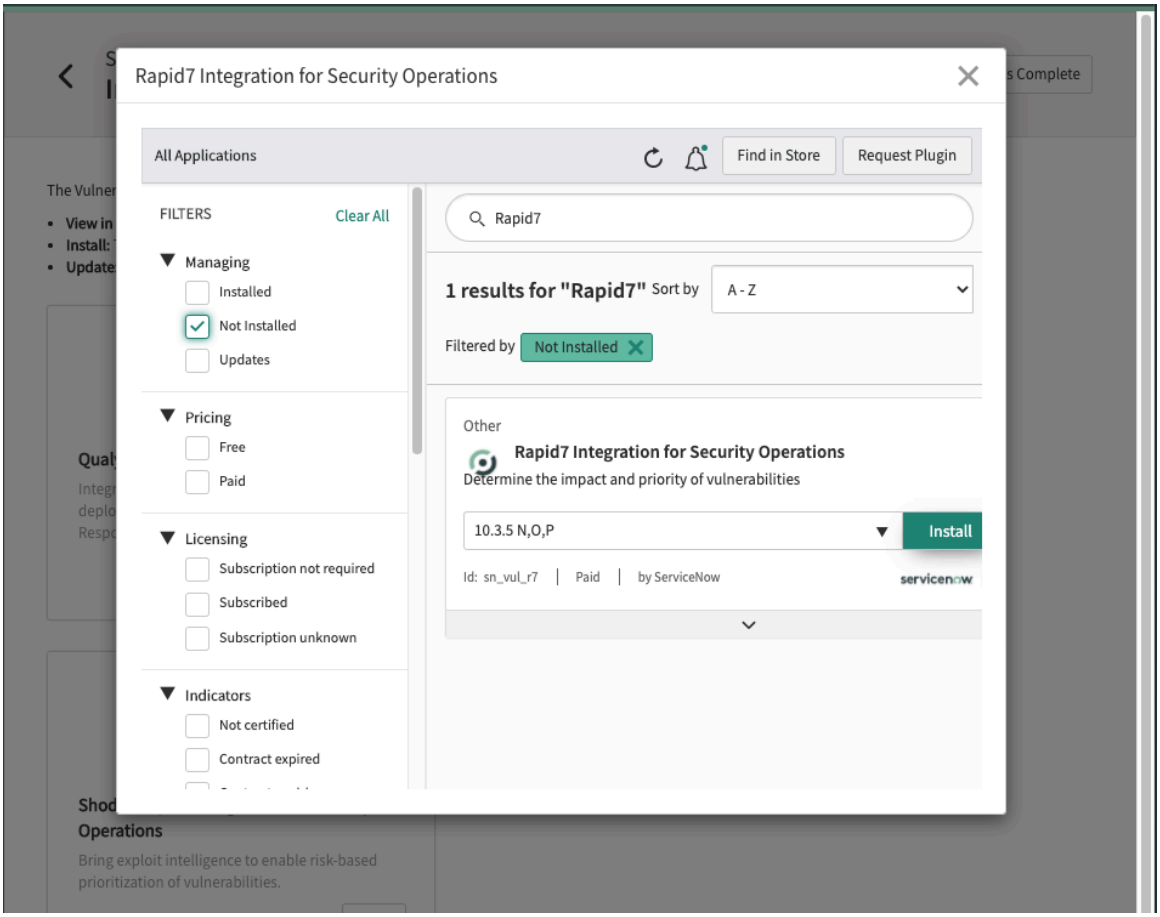


3. Localisez l'application, sélectionnez une version dans la liste de choix, puis cliquez sur **Installer**.

   Si une mise à jour est disponible pour l'application, le bouton **Mettre à jour** s'affiche.

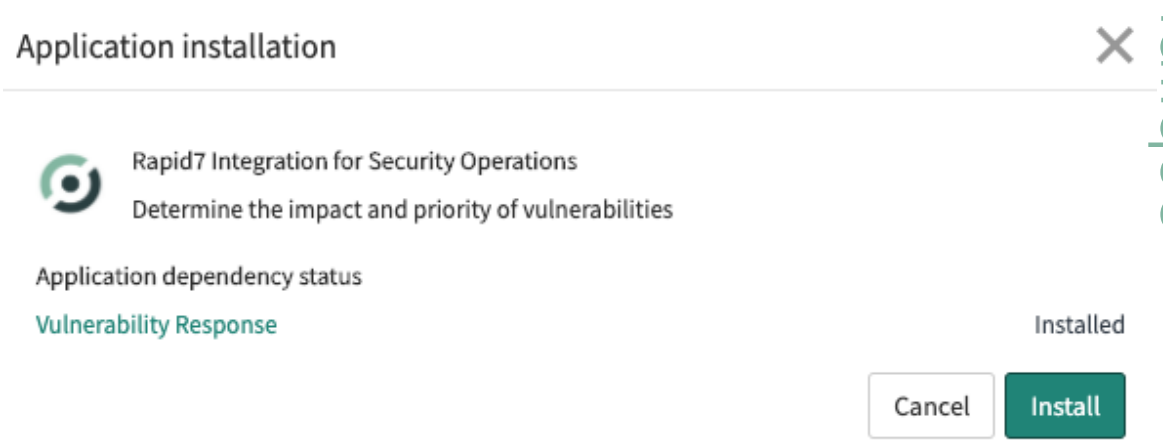
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La boîte de dialogue d'installation de l'application affiche l'état de dépendance de l'application. Toutes les dépendances requises qui ne sont pas encore installées sont automatiquement installées avec l'application.

4. Dans la boîte de dialogue Installation de l'application, cliquez sur **Installer**.



La boîte de dialogue Installer indique quand l'installation est terminée avec succès.

5. Fermez la boîte de dialogue.
La page Toutes les applications s'affiche et indique que l'application est correctement installée.

Traduction automatique

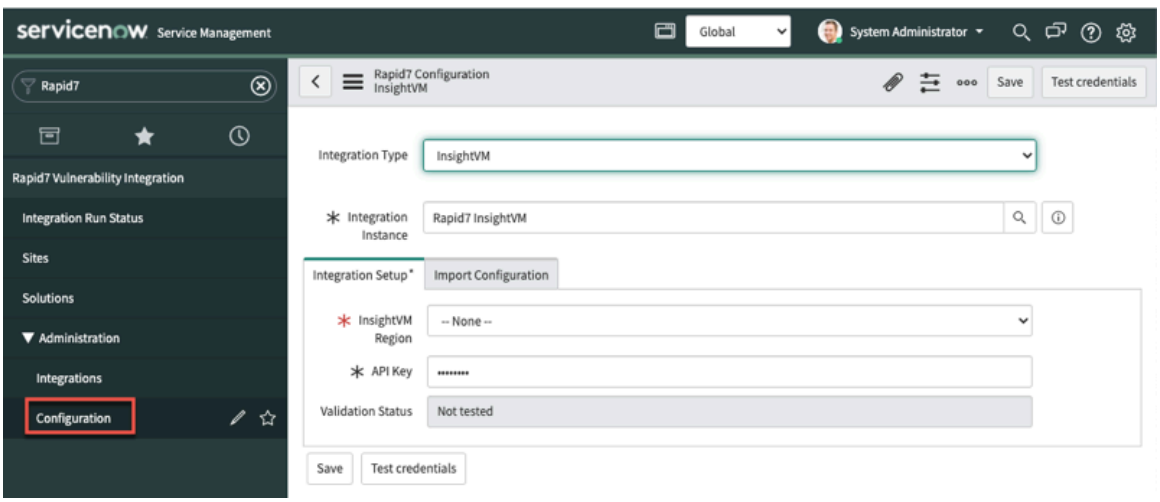
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après l'installation et l'activation, vous pouvez configurer, planifier et lancer les applications et solutions installées suivantes directement à partir de la section Configuration de l'intégration de l'Assistant de configuration :

- Le Qualys Vulnerability Integration
- Le Intégration de Réponse aux vulnérabilités à Tenablefichier .
- Le Microsoft Security Response Center Solution Integration
- Le Intégration de solution Red Hat
- Microsoft Security Response Center Solution Integration
- L'intégration Gestion des menaces et des vulnérabilités par Microsoft Defender

Pour les autres applications non répertoriées ci-dessus, accédez directement au module de configuration de l'application pour poursuivre la configuration et entrer les informations d'identification de tiers requises. Par exemple, l'image suivante montre l'emplacement de la configuration et du module de l'application Rapid7 .

Pour plus d'informations sur la configuration d'applications spécifiques, consultez la documentation produit d'installation et de configuration par nom de produit fourni pour chaque application.



Que faire ensuite

Poursuivez la configuration de votre application dans l'Assistant de configuration si votre application est prise en charge.

Si votre application n'est pas prise en charge pour la configuration dans l'Assistant de configuration, accédez directement au module de configuration de l'application pour poursuivre la configuration. Pour afficher les applications prises en charge dans l'Assistant de configuration, reportez-vous à la section Installation et prise en charge des Réponse aux vulnérabilités applications.

Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces

Si ce n'est pas déjà fait, téléchargez et exécutez l'intégration NVD et exécutez la tâche planifiée CWE dans le cadre de votre configuration initiale de Vulnerability Response et avant d'importer des données de vulnérabilité dans votre instance avec un produit de scanner tiers. L'intégration de Vulnerability Response avec NVD est disponible sur le ServiceNow Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ingestion de données CWE et NVD

Les données importées à partir des intégrations NVD et CWE sont utilisées pour enrichir les données de vulnérabilité dans votre instance et vous aider à décider s'il faut escalader le rattrapage pour une vulnérabilité, un élément vulnérable ou une tâche de rattrapage. Après une importation initiale, vous pouvez mettre à jour les notices de bibliothèque sur demande ou configurer une tâche planifiée pour mettre à jour les notices régulièrement. Réponse aux vulnérabilités les stocke sous **Bibliothèques**.

Le système de notation des vulnérabilités courantes (CVSS), inclus dans les entrées NVD et tierces, capture les principales caractéristiques d'une vulnérabilité. Réponse aux vulnérabilités utilise les données CVSS pour produire une valeur normalisée reflétant la gravité de la vulnérabilité. Lorsque la gravité est calculée, la vulnérabilité fournit une meilleure compréhension du risque posé par cette vulnérabilité pour votre organisation. La gravité vous aide à évaluer et à classer par ordre de priorité le rattrapage des vulnérabilités.

S'il s'agit de votre première installation de Réponse aux vulnérabilités, ou avant d'ingérer des données pour la première fois avec un produit de scanner tiers :

1. Effectuez une importation initiale des données CWE avec CWE Comprehensive 2000 Integration.

   Consultez Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE pour plus d'informations. Vous effectuez les mises à jour CWE **sur demande** à partir de l'enregistrement d'intégration par défaut et vous devez le configurer si vous souhaitez qu'il s'exécute en tant que tâche planifiée.

   Remarque : Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. Le jour par défaut pour la mise à jour NVD est **Hebdomadaire** , le **lundi**.

2. Vérifiez que l'intégration à l'application Réponse aux vulnérabilités NVD est installée et que les données de l'API NIST National Vulnerability Database Integration (CVE uniquement) ou de l'API NIST National Vulnerability Database Integration (CVE et CPE) sont importées.

   L'activation de ce module d'extension pour les instances de production peut nécessiter une licence distincte. Une fois installée, l'intégration NIST National Vulnerability Database Integration - API (CVE uniquement) est activée par défaut. Il fonctionne tous les jours. Voir Présentation des intégrations NVD et Installer l'intégration Réponse aux vulnérabilités dans la base de données de vulnérabilité nationale NIST pour plus d'informations.

3. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Consultez votre documentation d'intégration à l'adresse Intégrations de Réponse aux vulnérabilités pour plus d'informations sur les intégrations tierces.

Affichage des données de vulnérabilité et des éléments vulnérables importés

Les bibliothèques suivantes sont disponibles :

Bibliothèques	Description
NVD	Liste des vulnérabilités détectées par NVD et comprenant des listes de vérification de sécurité, des failles logicielles liées à la sécurité, des erreurs de configuration, des noms de produits et des mesures d'impact, y compris les exploits.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bibliothèques	Description
CWE	Liste des types de faiblesses logicielles développés par la communauté. Chaque enregistrement CWE inclut également un article de la base de connaissances associé qui décrit la faiblesse. Vous ne pouvez pas escalader une vulnérabilité à partir de l'écran Common Weakness Enumerations, c'est à titre de référence uniquement.
Tiers	Liste des vulnérabilités tierces importées dans votre instance. Contient une liste de références, d'éléments vulnérables, d'exploits et de CVE connexes.

Information associée

Afficher Réponse aux vulnérabilités les bibliothèques de vulnérabilité

Installer l'application Gestion des solutions pour Réponse aux vulnérabilités

Avant de pouvoir utiliser la Gestion des solutions pour Réponse aux vulnérabilités fonctionnalité de Réponse aux vulnérabilités dans votre instance, vous devez terminer l'installation de l'application Gestion des solutions pour vulnérabilités . Cette application est disponible sous forme d'abonnement distinct dans le ServiceNow Store.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Effectuez ces tâches de configuration pour une installation en douceur.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Les Microsoft Security Response Center Solution Integration et Intégration de solution Red Hat sont les applications de solution disponibles après Gestion des solutions pour Réponse aux vulnérabilités l'installation Gestion des solutions pour vulnérabilitésde .

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Gestion des solutions pour Réponse aux vulnérabilités nécessite l'application Réponse aux vulnérabilités . Pour la version la plus récente de Gestion des solutions pour vulnérabilités, vérifiez que vous disposez de la version la plus récente de Réponse aux vulnérabilités installée. Consultez KB0856498 la matrice de compatibilité de Vulnerability Response et les changements de schéma de mise en production . Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que vous avez les droits sur l'application.	Pour vérifier que vous disposez des droits sur l'application Gestion des solutions pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	vulnérabilités , accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Pour obtenir l'autorisation pour l'application Gestion des solutions pour vulnérabilités à ServiceNow Store partir du et la télécharger sur votre instance, reportez-vous à la Now Platform section .
Assurez-vous que vos dossiers NVD sont à jour au cours des 10 dernières années.	Consultez Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces.
Assurez-vous que vos vulnérabilités tierces sont à jour.	Pour en savoir plus sur les intégrations de vulnérabilités tierces, reportez-vous Intégrations de Réponse aux vulnérabilités à la rubrique .
Vérifiez que les rôles requis Now Platform vous ont été affectés à votre instance.	Les rôles suivants sont requis pour l'installation et la vérification des résultats attendus : Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités. • L'administrateur système [admin] installe l'application. S'il n'est pas déjà affecté, l'administrateur affecte le rôle d'administrateur de vulnérabilité [sn_vul.vulnerability_admin ou sn_vul.admin (deprecated)]. • L'administrateur de vulnérabilité supervise la configuration et vérifie les résultats attendus.

Rôles requis : admin pour installer l'application Gestion des solutions pour vulnérabilités et administrateur de vulnérabilité pour la configurer.

Procédure

1. Accédez au ServiceNow Store.

2. Cliquez sur Se connecter et saisissez vos informations **d'identification** HI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur l'onglet **Produits ServiceNow** pour afficher les produits disponibles ServiceNow .
4. Cliquez sur le signe plus (**+**) en regard **de Gestion des solutions de vulnérabilité** pour afficher toutes les applications associées auxquelles vous êtes éligible.
5. Cliquez sur **Adhérer** pour vérifier que vous avez droit à Gestion des solutions pour vulnérabilités l'application.
6. Si vous disposez déjà d'une autorisation, passez à l'étape 10 pour installer l'application sur votre Now Platform instance.
7. Cochez la case et cliquez sur **Accepter** pour accepter les termes et conditions à l'invite. Un message s'affiche qui indique que vous avez adhéré avec succès à l'application.
8. Facultatif : Cliquez sur Gérer l'autorisation si vous souhaitez gérer votre autorisation pour Gestion des solutions pour vulnérabilités d'autres Now Platform instances.

   Remarque : Si le bouton **Gérer l'autorisation** n'est pas affiché, cliquez sur l'application **Gestion des solutions en matière de vulnérabilité** dans la liste de produits pour l'afficher.

   a. Choisir une option

   b. Cliquez sur **OK** ou **Annuler** pour continuer.
   Vous êtes prêts à activer les modules d'extension et à installer l'application sur vos instances.

9. Connectez-vous à l'instance Now Platform sur laquelle vous souhaitez installer l'application Gestion des solutions pour vulnérabilités .
10. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
11. Localisez l'application Gestion des solutions pour vulnérabilités (sn_vul_solution) et cliquez sur **Installer**.
    La boîte de dialogue d'installation de l'application affiche l'état du module d'extension de dépendance d'application. Toutes les dépendances requises qui ne sont pas encore installées sont automatiquement installées avec l'application.
12. Cliquez sur **Installer**.
    Cette installation peut prendre un certain temps. Un message s'affiche dans la boîte de dialogue Installer une fois l'application et ses dépendances installées.

    L'administrateur de vulnérabilité peut désormais configurer l'application à partir de l'assistant de configuration.

13. Cliquez sur **Fermer**.

    Les Microsoft Security Response Center Solution Integration et Intégration de solution Red Hat sont les applications de solution disponibles après Gestion des solutions pour Réponse aux vulnérabilités l'installation Gestion des solutions pour vulnérabilitésde .

    Affichez les solutions en matière de vulnérabilité en naviguant vers **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions**. Consultez Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'Assistant de configuration pour plus d'informations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Après avoir configuré l'application et les solutions disponibles, vérifiez que les CVE et les solutions sont d'accord à l'aide de la table Solution de vulnérabilité [sn_vul_m2m_vulnerability_solution].

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

Avant de pouvoir utiliser l'application Analyse des performances pour Réponse aux vulnérabilités , vous devez obtenir l'autorisation et télécharger l'application à partir de , ServiceNow Storel'installer sur votre Now Platform® instance et effectuer quelques étapes d'installation et de configuration. L'application PA n'est pas installée avec elle Réponse aux vulnérabilités . Elle est disponible sous la forme d'un abonnement distinct.

Avant de commencer

Si vous avez déjà l'application sur votre instance et que vous effectuez une mise à jour vers une version plus récente de l'application, passez à l'étape 8 des étapes suivantes pour poursuivre la mise à jour et la configuration.

Pour une nouvelle installation, complétez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Pour vérifier que les modules d'extension et les applications sont installés et activés, accédez à **Tout** > **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que le module d'extension Vulnerability Response dependencies (com.snc.vul_dep) est installé et activé.	Dépendances de Vulnerability Response Ce module d'extension contient tous les modules d'extension de dépendance nécessaires à la prise en charge de l'application. Pour vérifier que le module d'extension est installé et activé, dans votre instance vers laquelle vous souhaitez que l'application navigue **Applications système** > **Toutes les applications disponibles** > **Tout**. Si vous êtes invité à mettre à jour d'autres modules d'extension de dépendance, cliquez sur les liens dans les boîtes de dialogue et suivez les invites pour continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
Vérifiez que l'application ServiceNow Réponse aux vulnérabilités (sn_vul) est installée et activée.	Réponse aux vulnérabilités Pour vérifier que le module d'extension est installé et activé, dans votre instance vers laquelle vous souhaitez que l'application navigue **Applications système** > **Toutes les applications disponibles** > **Tout**. Si vous êtes invité à mettre à jour d'autres modules d'extension de dépendance, cliquez sur les liens dans les boîtes de dialogue et suivez les invites pour continuer. L'activation de ce module d'extension pour les instances de production peut nécessiter une licence distincte. Contactez ServiceNow pour plus de détails.
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance. Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur Analyse des performances [pa_admin] ou le système [administrateur] installe l'application et vérifie les résultats attendus. • L'administrateur de vulnérabilité [sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)] supervise la configuration et vérifie les résultats attendus avec les tableaux de bord PA. • Le propriétaire du rattrapage [sn_vul.remediation_owner] supervise les tâches de gestion des changements. Il lit et met à jour les enregistrements affectés. Le rôle sn_vul.remediation_owner est également automatiquement attribué lorsqu'un utilisateur se voit attribuer le rôle itil.
Vérifiez que Performance Analytics et Réponse aux vulnérabilités les applications sont compatibles.	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

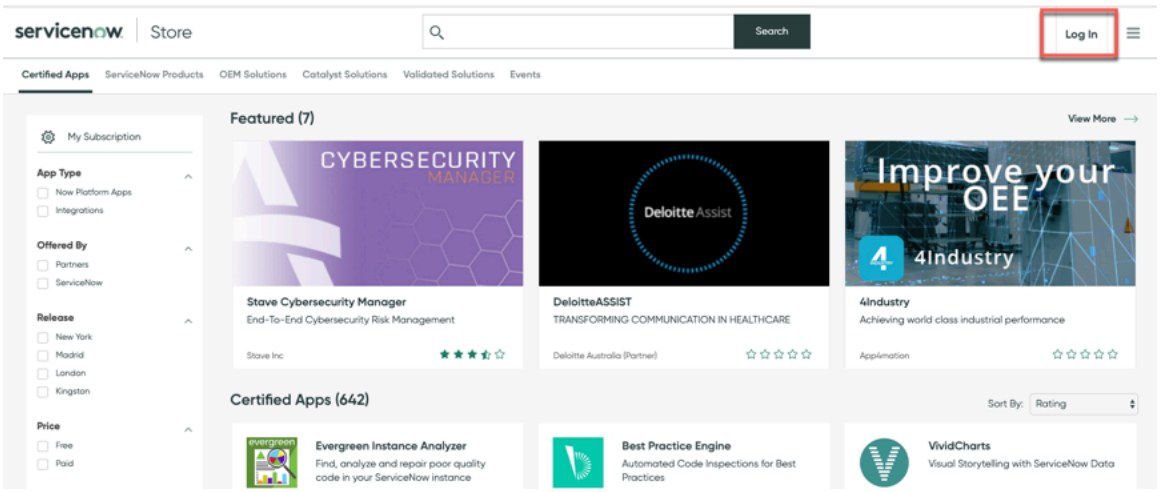
Rôle requis : admin ou pa_admin

Traduction automatique

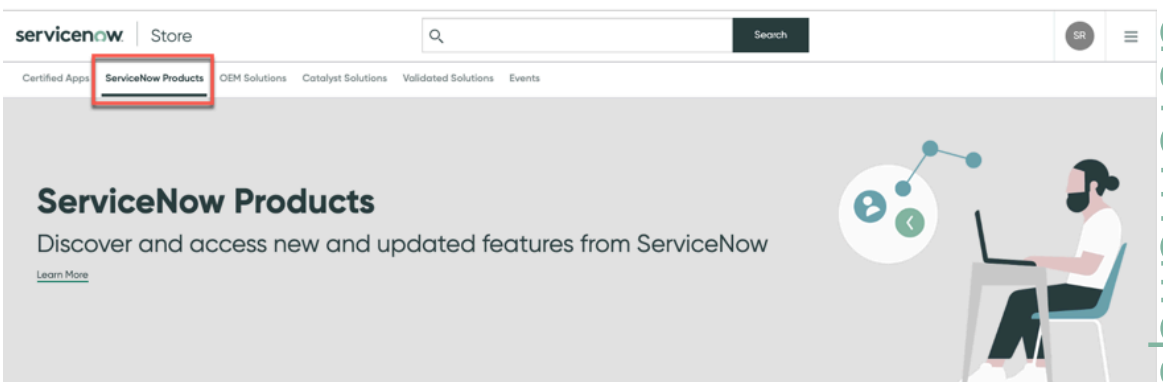
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

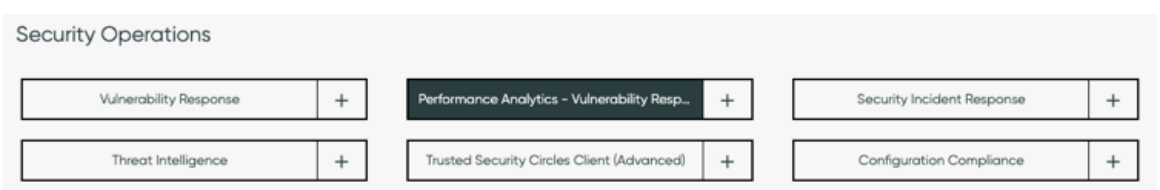
1. Pour obtenir l'autorisation et télécharger l'application sur votre Now Platform instance, accédez au ServiceNow Store.
2. En haut à droite de la page, cliquez sur **Se connecter**.



3. Dans la boîte de dialogue qui s'affiche, saisissez vos informations d'identification HI et cliquez sur **Connexion**.
4. Sur la page qui s'affiche, si elle n'est pas sélectionnée, cliquez sur l'onglet **Produits ServiceNow** .



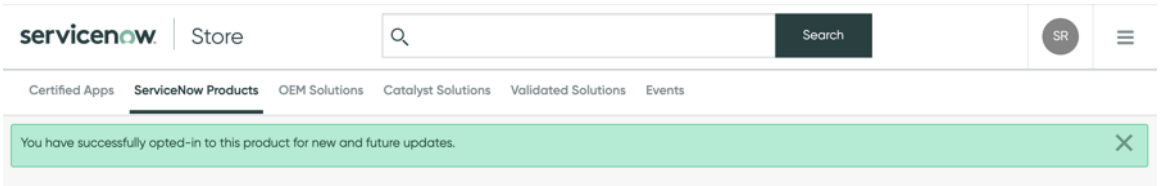
5. Sur la page de liste de produits, cliquez sur **Analyse des performances - Vulnerability Response**.



6. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**. Une page avec le bouton Opt-in s'affiche.
7. Pour obtenir l'application Analyse des performances pour Réponse aux vulnérabilités , cliquez sur **S'abonner**.
8. Pour accepter les termes et conditions, à l'invite, cochez la case et cliquez sur **Accepter**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

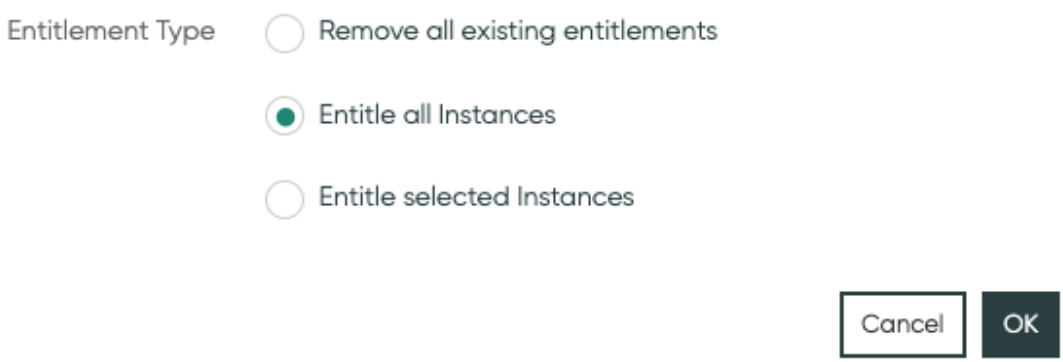


9. Facultatif : Pour gérer votre autorisation pour l'application sur d'autres Now Platform instances, suivez également les étapes suivantes.

   a. Si le bouton Gérer l'autorisation n'est pas affiché, cliquez sur l'application Analyse des performances pour Réponse aux vulnérabilités dans la liste de produits pour l'afficher.

   b. Une fois l'onglet Éligible sélectionné, cliquez sur **Gérer l'autorisation**.

   c. Dans la boîte de dialogue Gérer les autorisations pour Vulnerability Response qui s'affiche, choisissez l'une des options suivantes :

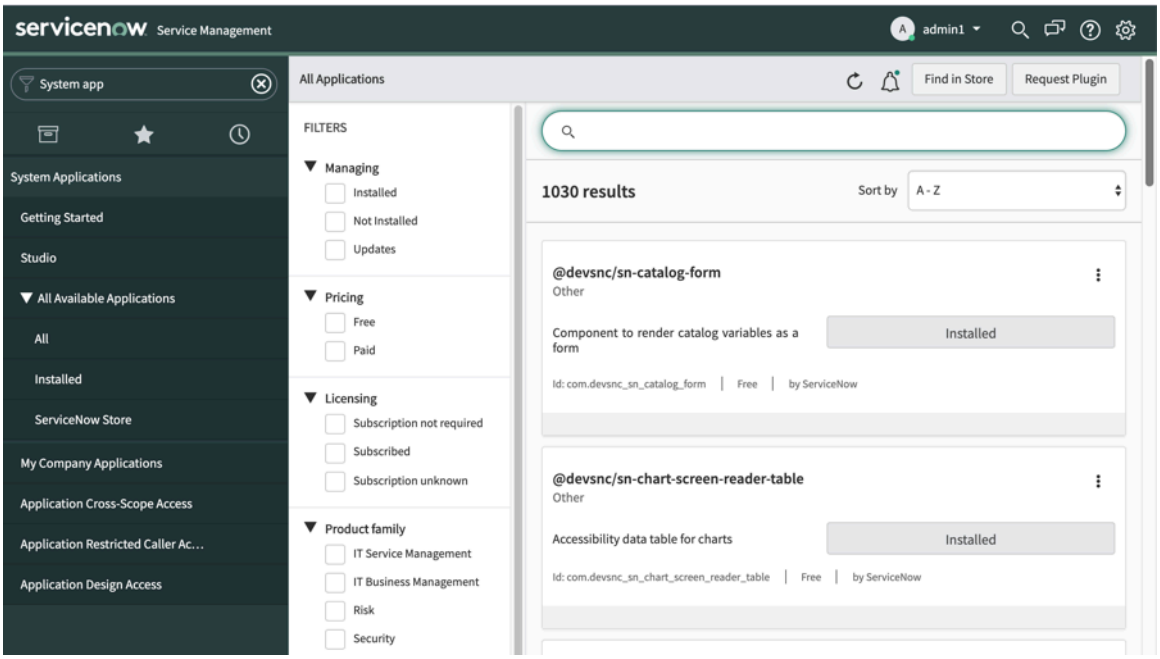


   d. Cliquez sur **OK** ou **Annuler** pour continuer.
   Vous êtes prêt à activer les modules d'extension et à installer l'application sur votre ou vos Now Platform instances.

10. Connectez-vous à l'instance Now Platform sur laquelle vous souhaitez installer l'application Réponse aux vulnérabilités .
11. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



12. Dans les applications répertoriées, localisez l'application Analyse des performances - Content Pack - Vulnerability Response (sn_vul_analytics) et cliquez sur **Installer**.

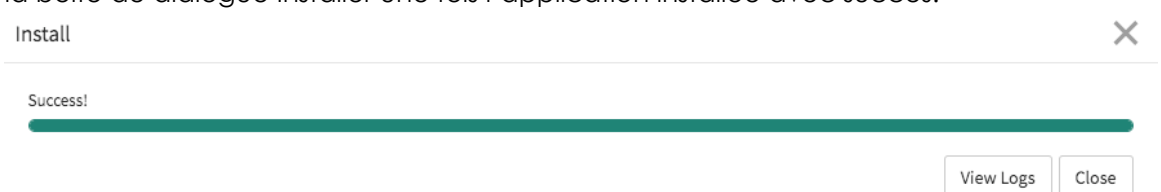
    Remarque : Si vous effectuez une mise à jour vers une nouvelle version, sélectionnez la version souhaitée dans la liste de choix.

    et cliquez sur **Mettre à jour**.
    La boîte de dialogue d'installation de l'application s'affiche. Toutes les dépendances qui seront installées automatiquement avec l'application sont également affichées.

13. Facultatif : Si vous souhaitez des données de démonstration, cochez la case Charger les données de démonstration et cliquez sur **Installer**.

    Remarque : Si vous ne cochez pas la case **Charger les données de démonstration** , les données de démonstration ne peuvent pas être installées ultérieurement à partir d'Application **Manager** . Pour plus d'informations sur l'installation ou la réinstallation de données de démonstration après l'installation initiale, consultez l'article Solution de contournement pour installer des données de démonstration si l'application est déjà installée [KB0722909] dans la base de Now Support connaissances.

    Cette installation peut prendre un certain temps. Un message s'affiche dans la boîte de dialogue Installer une fois l'application installée avec succès.



14. Cliquez sur **Fermer**.

15. Facultatif : Si vous prévoyez un grand nombre d'éléments vulnérables actifs dans votre environnement, vous préférerez peut-être modifier le paramètre par défaut pour le nombre maximal d'enregistrements collectés, activer les travaux planifiés et définir les heures de collecte pendant les heures creuses.

Traduction automatique

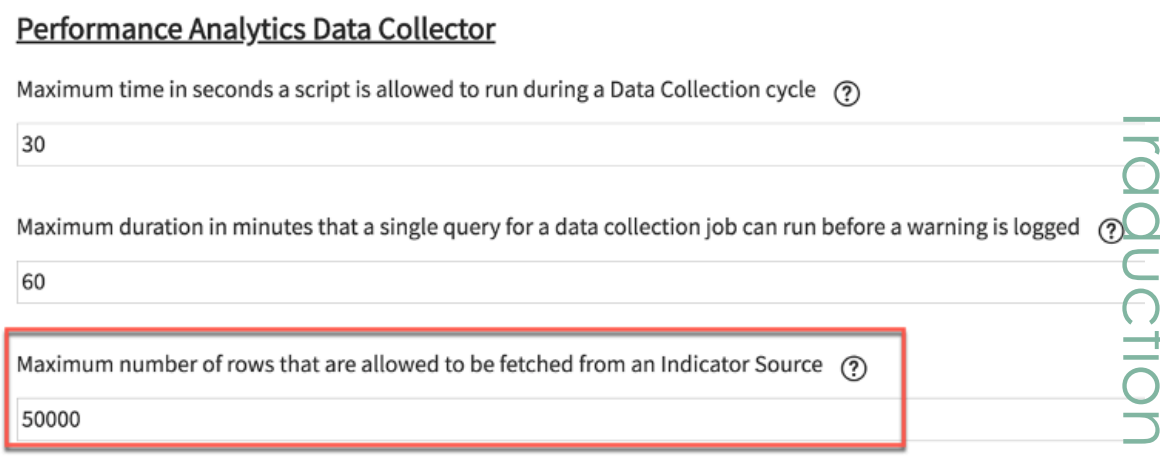
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour modifier ces paramètres et d'autres pour l'application après son installation, procédez comme suit.

a. Accédez à la **Tout** > **Analyse des performances** > **Console d'administration**.

b. Dans la vignette Configuration avancée, cliquez sur le lien **Propriétés de Performance Analytics** .

c. Sur la page [Performance Analytics] de la console d'administration, accédez à la section Collecteur de données Performance Analytics.
Le paramètre par défaut (50 000 enregistrements) s'affiche pour le Nombre maximal de lignes pouvant être extraites d'une source d'indicateur.



d. Vous préférerez peut-être augmenter ce nombre à une valeur supérieure d'environ 20 % au nombre total d'éléments vulnérables actifs (VI) que vous prévoyez dans votre environnement.

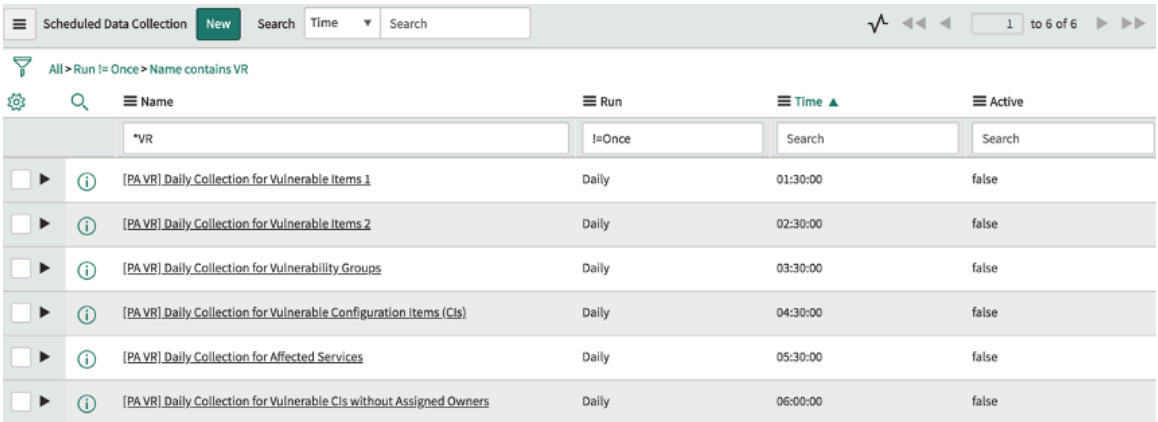
e. Cliquez sur **Enregistrer**.

f. Pour activer les travaux planifiés, accédez à **Analyse des performances** > **Collecteur de données** > **Tâches**.
La liste Collecte de données planifiée s'affiche. Dans la colonne Actif, les travaux planifiés répertoriés dans la colonne Application pour Analyse des performances - Pack de contenu - Vulnerability Response par défaut sont désactivés (`faux`).

> **Remarque :** Une tâche planifiée pour la collecte de données historiques ne s'affiche pas dans la liste des tâches. Pour les grands ensembles de données, vous pouvez commencer à collecter des données et des tendances au fil du temps en activant vos tâches quotidiennes lors de la configuration d'Analyse des performances pour Réponse aux vulnérabilités l'application.

Traduction automatique

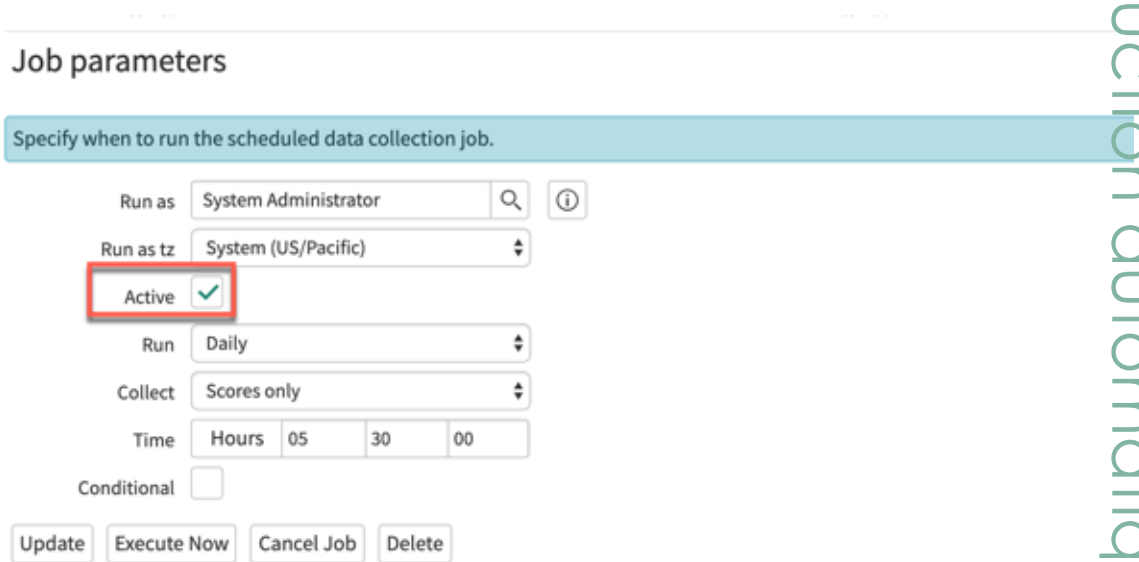
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



g. Dans la colonne Nom, cliquez sur un lien pour ouvrir un enregistrement de tâche PA_VR.

h. Si les champs ne sont pas modifiables, cliquez sur le lien **ici** pour les modifier.

i. Dans la section Paramètres de la tâche, cochez la case Actif pour planifier une tâche. Les champs Heure s'affichent.



j. Entrez l'heure de début de la tâche.
Si vous prévoyez un volume important, vous préférerez peut-être définir des heures de collecte en dehors des heures d'ouverture. Si vous prévoyez 10 millions d'éléments vulnérables actifs ou plus dans votre environnement, contactez votre ServiceNow® partenaire d'implémentation pour plus d'informations sur la configuration de votre environnement de collecte de données.

Pour plus d'informations sur les indicateurs utilisés pour la collecte des données, reportez-vous à la section Afficher les Analyse des performances indicateurs pour Réponse aux vulnérabilités [PA].

k. Une fois que vous avez activé toutes les tâches souhaitées, cliquez sur **Mettre à jour**.
La liste Collecte de données planifiée s'affiche. Pour plus d'informations, consultez Propriétés d'Analyse des performances .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Accédez à la **Réponse aux vulnérabilités** > **Vue d'ensemble** pour afficher le tableau de bord.

Créer ou modifier des Réponse aux vulnérabilités règles d'affectation

Une fois que vous avez terminé votre évaluation initiale des règles d'affectation à l'aide de l'Assistant de configuration, vous pouvez créer des règles pour affecter automatiquement les éléments vulnérables en fonction des conditions de filtre. Ces règles affectent les éléments vulnérables au fur et à mesure qu'ils sont importés ou créés manuellement.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Le système de base est livré avec une règle d'affectation de vulnérabilité, **Affecter au groupe de support CI**, qui affecte les éléments vulnérables au même groupe d'affectation que le groupe de support CI. Cette règle peut être modifiée à l'aide des conditions de filtre ou vous pouvez créer une nouvelle règle. Avec les règles d'affectation, vous définissez la ou les conditions d'affectation et l'ordre d'exécution. Une fois qu'un VI correspond à une condition de règle, la recherche d'affectation s'arrête.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'affectation**.
2. Ouvrez la règle du **groupe de support Affecter à un CI** ou cliquez sur **Nouveau**.
3. S'il s'agit **d'un nouveau**, renseignez les champs du formulaire comme il convient.

Règle d'affectation de vulnérabilité

Champ	Description
Nom	Nom de la règle de groupe.
Actif	Indique si la règle d'affectation est active.
Ordre d'exécution	Ordre dans lequel les règles sont évaluées. Les règles de priorité élevée, les éléments qui nécessitent une gestion spéciale, lorsque le risque est critique, ou un VI qui doit être traité par la conformité réglementaire, doivent être exécutés en premier. Ensuite, exécutez vos règles générales, où aucune manipulation spéciale n'est requise, et vous savez qui doit en être responsable. Enfin, créez une règle par défaut pour affecter les VI au groupe qui déterminera à quel groupe d'affectation ils doivent appartenir. Ce groupe pourrait ajouter une autre règle pour couvrir ses décisions. Cette règle par défaut s'exécute en dernier.
Description	Description de la règle d'affectation.
Condition	
Aperçu	Affiche le nombre de résultats renvoyés par cette requête.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Champs de condition	Conditions qui doivent être remplies. **Remarque :** Pour rendre Rapid7 InsightVM les balises d'actifs disponibles pour une utilisation dans le filtre de condition des règles d'affectation, vous devez exécuter l'intégration de la Rapid7 InsightVM liste des actifs avant les autres Rapid7 InsightVM intégrations. La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.
Nouveau critère	Ajoute d'autres champs de filtre de condition au choix.
Affecter à l'aide de	Pour automatiser l'affectation des groupes créés en fonction de cette règle, choisissez l'une des options disponibles. ◦ Groupe d'utilisateurs : sélectionnez un groupe d'utilisateurs dans la table de recherche. ◦ Champ de groupe d'utilisateurs : sélectionnez un champ de groupe d'utilisateurs dans le menu déroulant. ◦ Script : créer ou modifier un script. **Remarque :** La création ou la modification d'un script nécessite ServiceNow une expertise.

4. Cliquez sur **Envoyer**.
   Les règles nouvelles ou mises à jour sont évaluées lors de l'importation suivante.

Remarque :

La fonctionnalité de réapplication nécessite une application de base des règles. Une fois vos règles créées, si vous ne l'avez pas déjà fait, activez la *`Reapply all vulnerability assignment rules`* tâche planifiée à exécuter, à votre convenance. Il applique toutes les règles à tous les VI ouverts, à l'exception de ceux affectés manuellement. En fonction du nombre de VI actifs que vous avez dans votre environnement, n'oubliez pas de définir le champ **Exécuter** de manière appropriée après l'exécution initiale pour éviter tout impact sur les performances.

Si vous n'avez pas exécuté cette tâche planifiée, lorsque vous essayez d'utiliser le bouton **Appliquer les modifications** du formulaire Règles d'affectation, vous devez le faire à ce moment-là. La réapplication des règles d'affectation ne regroupe pas les éléments vulnérables.

Créer une règle d'affectation Réponse aux vulnérabilités à l'aide de ML

Utilisez le script suivant pour créer une règle d'affectation polyvalente pour les éléments vulnérables qui utilise les recommandations ML d'Intelligence prédictive pour les affecter automatiquement pour correction.

Avant de commencer

Les recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités l'application doivent être installées et activées. Cette application est disponible sur le ServiceNow Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une solution de classification doit être définie, active et formée. Vous utilisez ce modèle pour vous aider à prévoir le groupe d'affectation approprié pour les éléments vulnérables (VI) dans les cas où vos règles d'affectation n'ont pas trouvé de correspondance correcte pour les destinataires prévus.

Cette règle peut vous aider à réduire le nombre de VI non affectés une fois que d'autres règles d'affectation sont déjà terminées.

Voir Installer Recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités et Créer et former une définition de solution pour Réponse aux vulnérabilités pour plus d'informations.

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Vous préférerez peut-être effectuer cette tâche uniquement si vous avez une expérience avancée en codage ou si vous avez une connaissance approfondie de , de ses fonctionnalités d'intelligence Now Platformprédictive et du fonctionnement des règles d'affectation.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'affectation**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Consultez la rubrique Créer ou modifier des Réponse aux vulnérabilités règles d'affectation pour plus d'informations sur ces champs.
4. Dans la liste de choix Affecter à l'aide de, sélectionnez **Script**.
5. Dans l'éditeur, copiez et collez le script suivant.

```
    /*
    * Catch-all assignment rule using ML recommendation
    * NOTE: Requires Vulnerability Assignment Recommendations for
 Vulnerability Response
    * Classification Solution must be active and trained
    */
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
    var ARU = new sn_vul.AssignmentRecommendationUtils();
    ARU.initialize();

    var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
    /*
    *returns object containing array of predictions
    *payload structure:
    *
    {
        "predictions": [
            {
                "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
                "name": "Windows Server support ",
                "confidence_score": "57.54"
            },
            ...
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
        ],
        "exception": ""
    }
    */
    var viPredictionArray = viPredictionObj['predictions'];
    var topPredictionObj = viPredictionArray.shift();

    return topPredictionObj['sys_id'];
}
```

6. Sélectionnez **Soumettre**.

Que faire ensuite
Consultez Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation pour obtenir des informations plus générales sur les règles d'affectation et la *Reapply all vulnerability assignment rules* tâche planifiée.

Créer une règle d'affectation pour l'assistance Réponse aux vulnérabilités de service

Utilisez le script suivant pour créer une règle qui affecte des éléments vulnérables à des mesures correctives en fonction des services aux entreprises qu'ils impactent.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Vous préférerez peut-être effectuer cette tâche uniquement si vous avez une expérience avancée en codage ou si vous avez une connaissance approfondie du fonctionnement des règles d'affectation Now Platform .

Avec cette règle, les VI sont affectés en fonction de leur correspondance avec les services d'entreprise répertoriés dans votre CMDB. Si aucun service, département ou groupe de support connexe ne correspond, les éléments vulnérables sont affectés au groupe d'analystes de vulnérabilité.

Cette règle peut vous aider à réduire le nombre de VI qui sont affectés incorrectement ou qui ne sont pas affectés une fois que d'autres règles d'affectation sont déjà terminées.

Procédure
1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'affectation**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Consultez la rubrique Créer ou modifier des Réponse aux vulnérabilités règles d'affectation pour plus d'informations sur ces champs.
4. Dans la liste de choix Affecter à l'aide de, sélectionnez **Script**.
5. Dans l'éditeur, copiez et collez le script suivant.

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related Business
 Service
*/
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
    var ci = vitGR.getValue('cmdb_ci');
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    var defaultAssignmentGroup = 'Vulnerability Analyst';
    var defaultGR = new GlideRecord('sys_user_group');
    defaultGR.get('name', defaultAssignmentGroup);
    var defaultAssignmentGroupID = defaultGR.sys_id;

    var maxSizeValue =
 global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max
_size", 1000);
    var maxDepthValue =
 global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max
_depth", 10);
    var customValues = {
        "maxDepth": maxDepthValue,
        "maxSize": maxSizeValue
    };
    var ciu = new global.CIUtils();
    var services = ciu.servicesAffectedByCI(ci, customValues);
    var svc = new GlideRecord("cmdb_ci_service");
    var hasSvc = false;
    if (services && services.length > 0) {
        svc.addQuery("sys_id", "IN", services.join(",")); // returns
 the service with highest business criticality. Implement alternate
 logic here.
        svc.addNotNullQuery("busines_criticality"); // typo intended
        svc.orderBy("busines_criticality");
        svc.setLimit(1);
        svc.query();
        hasSvc = svc.next();
    }
    if (!hasSvc) {
        // If there are no services it should be assigned to a default
 assignent group
        return defaultAssignmentGroupID;
    } else {
        var serviceAssignmentGroup =
 hasSvc.getValue('support_group'); //Also consider managed_by_group,
 assignment_group, change_control
        return !gs.nil(serviceAssignmentGroup) ?
 serviceAssignmentGroup : defaultAssignmentGroupID; //Return the
 Service assignment group if it is not empty, return the default
 assignment group otherwise.
    }
}
```

6. Sélectionnez **Soumettre**.

Que faire ensuite

Consultez Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation pour obtenir des informations plus générales sur les règles d'affectation et la *Reapply all vulnerability assignment rules* tâche planifiée.

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

Une fois que vous avez terminé votre évaluation initiale des règles de tâche de rattrapage à l'aide de l'Assistant de configuration, vous pouvez créer des règles pour regrouper automatiquement les éléments vulnérables en fonction des conditions de filtre. Ces règles regroupent automatiquement les éléments vulnérables à mesure qu'ils sont importés ou

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

créés manuellement. Utilisez le filtre pour limiter les éléments vulnérables regroupés par cette règle, notamment en sélectionnant tous les éléments vulnérables avec des exploits.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche

Le système de base est livré avec une règle de tâche de rattrapage, **Vulnérabilité**, qui regroupe les éléments vulnérables par vulnérabilité et groupe d'affectation (à partir des **règles d'affectation**). Vous pouvez réappliquer les règles à partir de la vue de formulaire ou de liste. Pour certains exemples d'entrées, Réponse aux vulnérabilités Exemples de règles de tâche de rattrapage.

Cette règle peut être modifiée comme suit :

En utilisant des conditions de filtre et Grouper par choix.

Par défaut, les tâches de rattrapage utilisent des **règles d'affectation**, lorsqu'elles sont disponibles, dans le cadre de leurs critères de filtrage.

Remarque : Si aucune règle d'affectation n'existe, vous pouvez sélectionner un groupe à l'aide du champ **Groupe d'utilisateurs** .

À partir de la version 18.0 de , la règle de tâche de rattrapage de Réponse aux vulnérabilités**vulnérabilité** est désactivée pour Réponse aux vulnérabilités les nouvelles implémentations.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles de la tâche de rattrapage**.
2. Ouvrez la règle ou cliquez sur **Nouveau**.
3. S'il s'agit **d'un nouveau**, renseignez les champs du formulaire comme il convient.

Règle de la tâche de rattrapage

Champ	Description
Nom	Nom de la règle de tâche.
Actif	Indique si la tâche est active.
Description	Description de la règle.
Sensible à la casse	Détermine si une condition est sensible à la casse ou non. **Remarque :** La valeur par défaut n'est pas sensible à la casse.
Condition	Conditions de filtre facultatives pour la règle. **Remarque :** Pour rendre Rapid7 InsightVM les balises d'actifs disponibles pour une utilisation dans le filtre de condition pour les règles de tâche de rattrapage, vous devez exécuter l'intégration de la Rapid7 InsightVM liste des actifs avant les autres Rapid7 InsightVM intégrations. Par défaut (case à cocher **sensible à la casse** désactivée), le texte de recherche que vous saisissez dans le générateur de conditions sur les enregistrements et formulaires de règles de tâche n'est pas sensible à

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	la casse. Vous pouvez activer les recherches sensibles à la casse sur les enregistrements de tâches et les formulaires.
Grouper par (jusqu'à six ensembles de conditions sont disponibles)	
Regrouper les éléments vulnérables à partir de	Table que la règle utilise pour grouper les VI. Vous pouvez avoir jusqu'à six filtres. Les choix possibles sont les suivants : ◦ Élément vulnérable [sn_vul_vulnerable_item] ◦ Élément vulnérable → Élément de configuration [cmdb_ci] ◦ Élément vulnérable → vulnérabilité [sn_vul_third_party_entry] **Remarque :** Si vous choisissez une table étendue, le **champ Utilisation** n'est appliqué qu'aux éléments vulnérables qui utilisent cette table étendue.
Utilisation du champ	Champ de la table que la règle utilise pour regrouper les VI.
Affectation	
Affecter la tâche de rattrapage par	Lors de l'affectation automatique des tâches de rattrapage, le choix Affectation est utilisé en plus des choix **Grouper par** pour regrouper les éléments vulnérables. De nouvelles tâches sont créées, selon les besoins, pour s'assurer que chaque élément vulnérable est placé dans une tâche avec un ensemble de groupes d'affectation correspondants. Pour automatiser l'affectation des tâches créées en fonction de cette règle, choisissez l'une des options disponibles. ◦ Regrouper par champ : si vous avez sélectionné un champ de groupe d'utilisateurs à partir des valeurs du **champ Utilisation** dans la section **Grouper par**, il apparaît dans le menu déroulant. ◦ Groupe d'utilisateurs : utilisez la liste de recherche pour sélectionner un groupe d'utilisateurs statique.

Remarque : Si vous changez d'avis sur l'un des paramètres **Grouper par** , le lien connexe **Effacer les champs grouper par** réinitialise les champs **Grouper par** du formulaire.

Lorsqu'une règle de groupe est supprimée, à partir du formulaire ou de la vue de liste, vous avez la possibilité de supprimer tous les groupes **ouverts** créés par cette règle. Les groupes qui ne sont pas dans l'état **Ouvert** sont exclus.

Pour des exemples d'entrées, reportez-vous à la section Réponse aux vulnérabilités Exemples de règles de tâche de rattrapage.

Définir des champs et des poids pour la règle de risque pour les calculateurs de risque de Vulnerability Response

Personnalisez les paramètres et les pondérations de la règle de risque afin de pouvoir générer des scores de risque qui utilisent les données de vulnérabilité et d'actif propres à votre organisation. En sélectionnant les champs inclus dans la règle de risque, vous pouvez définir un cadre de travail de notation des risques efficace.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

En outre, vous pouvez utiliser des attributs dans le configuration_item [cmdb_ci] dans Base de données de gestion des configurations (CMDB) pour vous aider à créer une logique pour vos calculateurs de risque de Vulnerability Response. Si, par exemple, vous déterminez que les CI qui sont orientés vers l'extérieur dans votre organisation sont plus vulnérables et peuvent nécessiter une correction immédiate, vous pouvez affecter des attributs tels que *Internet Facing* pour ces CI. Cet attribut, ainsi que d'autres, sont répertoriés dans les notes de publication de Common Service Data Model pour la version de famille Orlando. Pour obtenir des informations et des conseils à jour sur le CMDB, consultez les rubriques suivantes :

- Modèle conceptuel de modèle de données de service commun
- Modèle de schéma CMDB

Rôle requis : sn_vul.manage_risk_score_configuration

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Calculateurs de vulnérabilités**.
2. Sur la page Calculateurs de vulnérabilité, sélectionnez **Calculateur de risque par défaut**.
3. Accédez à la **Page Calculateur de vulnérabilité** > **Onglet Règles du calculateur de vulnérabilité** > **Règle sur les risques par défaut**.
4. Facultatif : Dans la section Critères du calculateur de risque de la page Règle de risque de vulnérabilité, définissez la pondération de chaque critère en fonction de son importance dans le calcul du score de risque global.
5. Pour désactiver la règle, vous devez décocher la case **Actif** .
6. Pour ajouter des champs de règle de risque aux critères du calculateur de risque, sélectionnez **Ajouter des critères**.
7. Renseignez les champs du formulaire.

Formulaire de champ de règle de risque

Champ	Description
Choisir la table de référence	Table utilisée pour définir la pondération du score de risque. Vous pouvez sélectionner l'une des options suivantes : ◦ **Élément vulnérable** : ajoutez des champs qui sont directement accessibles par point à partir de l'élément vulnérable (VI). ◦ **Élément vulnérable : élément de configuration** : ajoutez des champs de remontée pas à pas qui font partie des extensions de table de base, comme la table Matériel. Ces champs ne font pas partie de la table de base (cmdb_ci). ◦ **Élément vulnérable : vulnérabilité** : ajoutez des champs parcourables par point qui font partie des tables qui étendent la table de base, par exemple, Entrée tierce. Ces champs ne font pas

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	partie de la table de base Entrée de vulnérabilité. ◦ **Table de référence de l'élément vulnérable** : ajoutez des champs qui font partie des tables connexes (m2m) ou des tables qui font référence à l'élément vulnérable. Ces champs ne sont pas directement accessibles par point à partir du VI. ◦ **Table de référence de l'élément de configuration** : ajoutez des champs qui font partie des tables connexes (m2m) de cmdb_ci ou des tables qui font référence à cmdb_ci. Ces champs ne sont pas directement accessibles par point à partir du VI. ◦ **Table de référence de vulnérabilité** : ajoutez des champs qui font partie des tables connexes (m2m) de sn_vul_entry ou des tables qui font référence à sn_vul_entry. Ces champs ne sont pas directement accessibles par point à partir du VI. ◦ **Conditions personnalisées** : utilisez cette option pour affecter des poids à la règle en évaluant la condition. Par exemple, le filtre accessible sur Internet détermine si un élément de configuration (CI) est externe ou interne.
Table	Champ qui n'apparaît que lorsque l'une des options suivantes est sélectionnée dans la table Choisir une référence : ◦ **Élément vulnérable -> Élément de configuration** ◦ **Élément vulnérable -> Vulnérabilité** ◦ **Table de référence de l'élément vulnérable** ◦ **Table de référence de l'élément de configuration** ◦ **Table de référence de vulnérabilité**
Champ	Champ à utiliser pour le calcul du score de risque pour cette règle.
Agrégation	Champ qui s'affiche uniquement lorsqu'une table de référence est sélectionnée à partir de l'option Choisir une table de référence. Sélectionnez la valeur minimale ou maximale à prendre en compte pour les calculs lorsque le champ

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	est sélectionné dans les tables connexes (m2m).
Poids	Pondération de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
Définir la pondération de la valeur	Composant permettant d'attribuer des poids à chaque valeur de champ. Pour les champs numériques, les valeurs de champ peuvent être définies comme une plage (par exemple, de 1 à 5). Les poids doivent être un nombre entier compris entre 0 et 100. **Remarque :** Ce champ n'apparaît pas si l'option Conditions personnalisées est sélectionnée dans la table Choisir une référence.
Table de condition	Champ qui s'affiche uniquement lorsque Conditions personnalisées est sélectionnée dans la table Choisir une référence. Sélectionnez une condition dans la liste.
Nom de champ	Champ qui s'affiche uniquement lorsque Conditions personnalisées est sélectionnée dans la table Choisir une référence. Saisissez un nom pour les critères de risque.
Condition	Champ qui s'affiche uniquement lorsque Conditions personnalisées est sélectionnée dans la table Choisir une référence. Prévisualisez les éléments de cette table qui correspondent aux conditions définies.

8. Sélectionnez **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Dans la page Règle, activez et réappliquez la règle pour réévaluer le score de risque sur les éléments vulnérables actifs.

Remarque : À partir de la version 23.0 de Réponse aux vulnérabilités, en cas de :

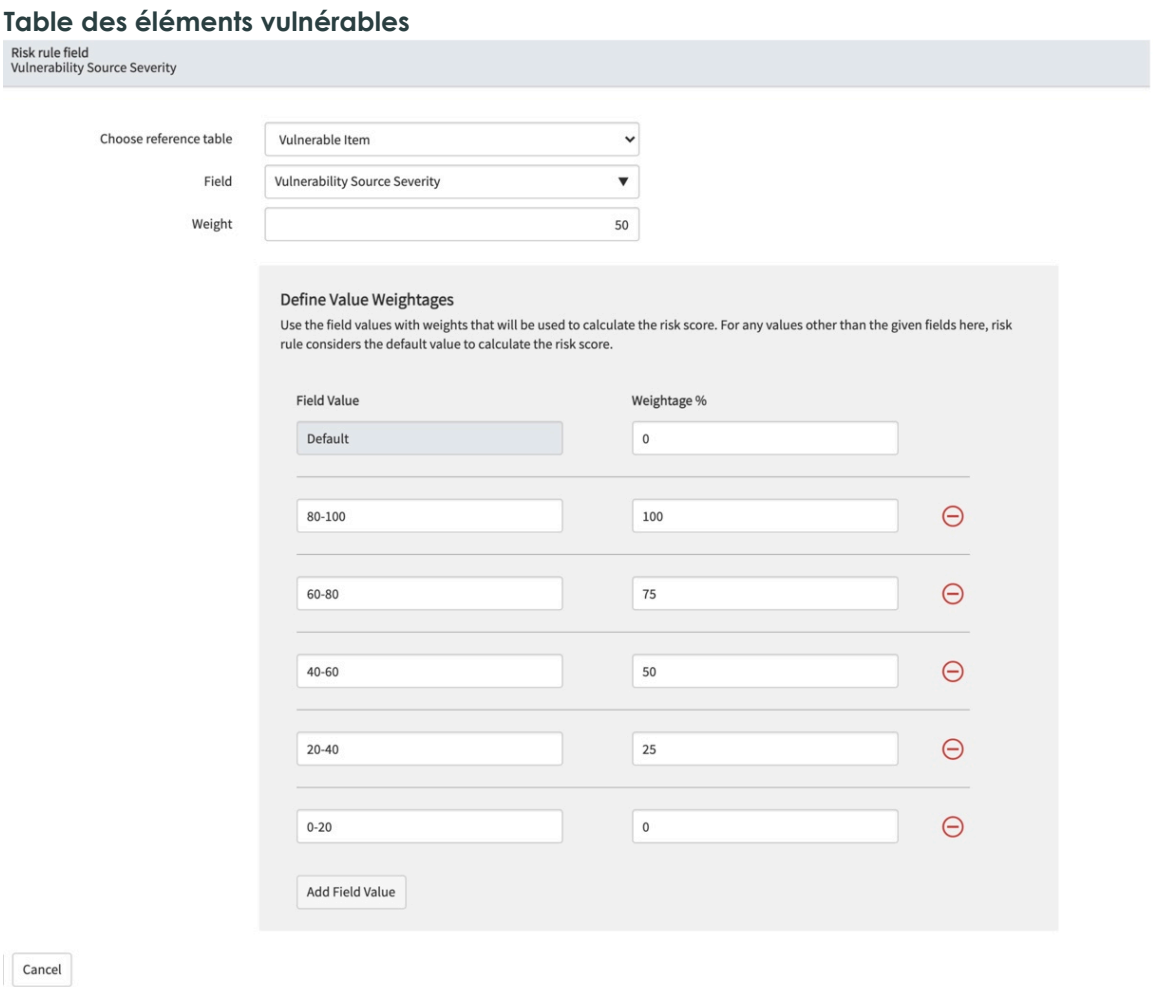
- **Règle du calculateur de risque par défaut** : chaque fois que le score de risque d'un élément vulnérable (VIT) change, les détails suivants sont documentés dans la section Notes du VIT :
  - Nom du groupe de calculateurs
  - Nom du calculateur
  - Valeurs de champ ayant une pondération supérieure à 1 et leur contribution au score de risque.
  - Score de risque final
- **Règle de risque de gravité** de la vulnérabilité : chaque fois que le score de risque est mis à jour sur un VIT, la section **Notes** est mise à jour avec les détails suivants :
  - Nom du groupe de calculateurs
  - Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre parenthèses. Pour modifier ou afficher la base de la règle du calculateur, sélectionnez n'importe quelle règle et cochez la case Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. Si le **modèle** est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si **Script** est sélectionné, vous pouvez ajouter ou mettre à jour le script existant.

Example:
Exemple 1 : ajouter une gravité de source comme critère pour une règle de risque.

Cas d'utilisation : les fournisseurs tiers, tels que Qualys et Tenable, fournissent leurs propres scores. Ces scores sont renseignés dans le champ **Gravité de la source** de la table sn_vul_entry. Utilisez ce champ pour les calculs de score de risque. Pour utiliser ce score afin de calculer le score de risque, procédez comme suit :

1. Accédez à la page Règle de risque.
2. Pour désactiver la règle, décochez la case **Actif** .
3. Pour ajouter des champs de règle de risque aux critères du calculateur de risque, sélectionnez **Ajouter des critères**.
4. Dans la liste Choisir une table de référence, sélectionnez **Élément vulnérable**.
5. Dans la liste Champ, sélectionnez **Vulnerability.Source Severity**.
6. Dans le champ **Poids** , entrez l'importance relative de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
7. Dans la section Définir la pondération des valeurs, ajoutez des valeurs de champ et attribuez-leur une pondération.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Sélectionnez **Soumettre**.

Exemple 2 : Ajouter une criticité opérationnelle comme critère pour une règle de risque.

Cas d'utilisation : supposons que votre organisation dispose de nombreux services aux entreprises. L'élément de configuration (CI) LINUX-SF-6381 est utilisé par les services suivants :

Criticité des services d'entreprise

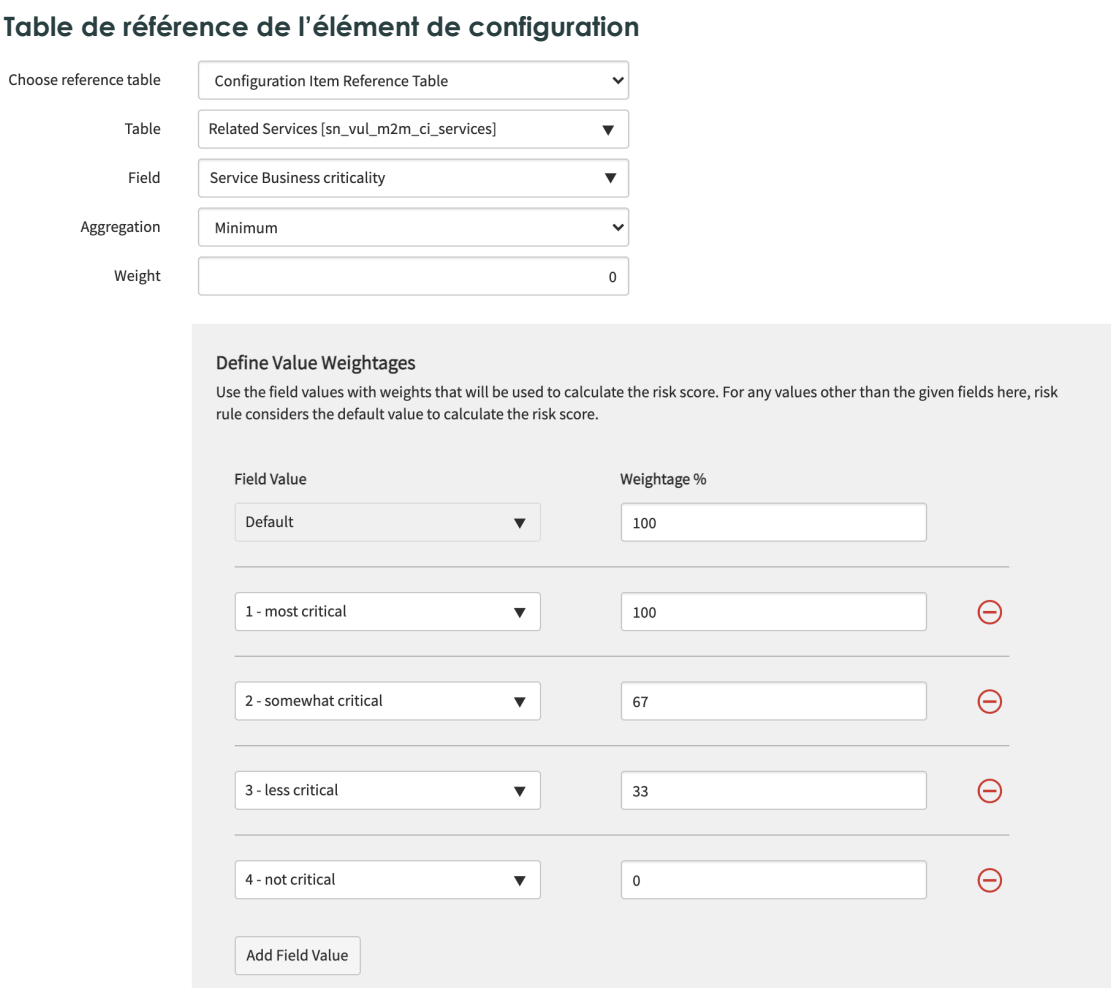
Service aux entreprises	Criticité
Gestion cloud	1 – Très critique
Commerce électronique	2 – Assez critique
Services à la clientèle	3 – Peu critique
Déplacements et dépenses	4 – Non critique

Le mappage entre le CI et les services est stocké dans la table Services associés [sn_vul_m2m_ci_services]. Lorsqu'une vulnérabilité est détectée dans l'actif LINUX-SF-6381, un élément vulnérable (VI) est créé. Vous pouvez utiliser la valeur de la criticité opérationnelle des services affectés pour calculer le score de risque de cet élément vulnérable. Pour utiliser la valeur de criticité de ces services pour calculer le score de risque, procédez comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la page Règle de risque.
2. Pour désactiver la règle, décochez la case **Actif** .
3. Pour ajouter des champs de règle de risque aux critères du calculateur de risque, sélectionnez **Ajouter des critères**.
4. Dans la liste Choisir une table de référence, sélectionnez **Table de référence de l'élément de configuration**.
5. Dans la liste Table, sélectionnez **Services associés [sn_vul_m2m_ci_services].**
6. Dans la liste **Champs, sélectionnez Criticité Service.Business**.
7. Dans le champ **Agrégation** , sélectionnez **Minimum** pour récupérer le service le plus critique pour ce cas d'utilisation (**1 : valeur la plus critique**) ou Maximum pour récupérer le service le moins critique pour ce cas d'utilisation (**4 – Valeur non critique**) pour ce cas d'utilisation.
8. Dans le champ **Poids** , entrez l'importance relative de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
9. Dans la section Définir les pondérations des valeurs, ajoutez des valeurs de champ et attribuez-leur une pondération.



10. Sélectionnez **Soumettre**.

Exemple 3 : Ajouter un critère conditionnel au calculateur de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Supposons qu'une organisation dispose de plusieurs éléments de configuration (CI), dont seuls quelques-uns peuvent être consultés par un utilisateur externe. Les utilisateurs peuvent ajouter des pondérations de score de risque pour ces CI orientés vers l'extérieur.

Remarque : Vous pouvez identifier ces CI par leur nom. Les noms commencent par « externe ».

Pour ajouter un critère conditionnel à la règle de risque, procédez comme suit :

1. Accédez à la page Règle de risque.
2. Pour désactiver la règle, décochez la case **Actif** .
3. Pour ajouter des champs de règle de risque aux critères du calculateur de risque, sélectionnez **Ajouter des critères**.
4. Dans la liste Choisir une table de référence, sélectionnez **Conditions personnalisées**.
5. Dans la liste Table de conditions, sélectionnez **Élément de configuration**.
6. Dans le champ **Nom** de champ, entrez le nom **Exposition CI**.
7. Dans le champ **Poids** , entrez l'importance relative de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
8. Dans le champ **Condition** , sélectionnez **Nom** > **commence par** et saisissez la valeur **externe**.

Conditions personnalisées pour la nouvelle règle de risque



9. Sélectionnez **Soumettre**.

Remarque : L'ajout de critères conditionnels à votre règle de risque peut dégrader les performances.

Information associée

Calculateurs Vulnerability Response et règles du calculateur de vulnérabilité

Créer un calculateur de Vulnerability Response

Filtrage dans Vulnerability Response

Réponse aux vulnérabilités Calculateurs de déploiement

Après votre évaluation initiale des calculateurs de risque dans l'Assistant de configuration, utilisez les calculateurs de déploiement de vulnérabilité pour configurer la manière dont le score de risque cumulatif est calculé pour les tâches de rattrapage et les vulnérabilités importées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez les calculateurs de déploiement de vulnérabilité pour configurer la manière dont le score de risque cumulatif est calculé pour les tâches de rattrapage et les vulnérabilités importées. Les calculateurs de cumul suivants sont fournis avec le système de base :

- *Remediation Task Rollup*: cumule les scores de risque pour tous les éléments vulnérables dans le cadre d'une tâche de correction afin de fournir un score de risque global pour l'ensemble du groupe d'éléments vulnérables.
- *Patch Update Rollup*: déploie les scores de risque pour tous les éléments vulnérables avec la même mise à jour de correctif afin de fournir un score de risque global pour la mise à jour du correctif.
- *Organization Risk Score Rollup*: cumule les scores de risque pour tous les éléments vulnérables de l'hôte, les éléments vulnérables de l'application, les éléments vulnérables du conteneur et les problèmes de configuration dans une organisation, afin de fournir un score de risque global pour l'ensemble de l'organisation dans un tableau de bord unifié.

  Remarque : À partir de la version 22.0 de , vous pouvez configurer des poids de déploiement pour le score de Réponse aux vulnérabilitésl'organisation. De plus, les calculatrices cumulatives individuelles ont été supprimées.

- *Vulnerable Item Rollup*: cumule les scores de risque pour tous les éléments vulnérables de l'hôte dans une organisation afin de contribuer au score de risque global de l'organisation entière pour le tableau de bord unifié.
- *Vulnerability Entry Rollup*: cumule les scores de risque pour tous les éléments vulnérables dans la même entrée de vulnérabilité afin de fournir un score de risque global pour l'entrée de vulnérabilité.
- *Rollup EPSS Scores from NVD to TPEs*: cumule les scores de l'EPSS pour tous les éléments vulnérables/CVE répertoriés dans la table NVD sur les TPE existants, afin de fournir une probabilité globale d'exploitation de la vulnérabilité.
- *Remediation Effort Rollup*: cumule les scores de risque pour tous les enregistrements dans le cadre d'un effort de rattrapage afin de fournir un score de risque global pour l'effort de rattrapage.

Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Calculateur de déploiement de vulnérabilité**.

Configurez le calculateur de déploiement pour spécifier le poids à donner à chacune de ces valeurs calculées dans la définition du score de risque cumulatif. Plus le poids est élevé, plus cette valeur est utilisée pour déterminer le score de risque cumulé dans les tâches de vulnérabilité ou de rattrapage.

Remarque : Lorsque **l'option Inclure les éléments différés** est sélectionnée, tous les éléments vulnérables différés sont inclus dans le calcul de déploiement pour les tâches de rattrapage. Assurez-vous de bien comprendre l'impact sur le calcul total avant de sélectionner cette option.

Les calculateurs de déploiement exécutent la tâche *Rollup vulnerable item values to vulnerability and groups*planifiée toutes les 15 minutes pour détecter les changements et déployer les détails et les scores de risque sur les tâches de rattrapage et les vulnérabilités. Ces travaux planifiés calculent également les valeurs cumulatives du nombre de VI, du score de risque maximal, de la date cible de rattrapage et de l'état des tâches de rattrapage.

Remarque : Les valeurs calculées pour les entrées de vulnérabilité n'incluent pas les données de cible de rattrapage.

Le score de risque est calculé dans les cas suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le score de risque, la cible de rattrapage, l'état du rattrapage ou les changements de vulnérabilité sur les éléments vulnérables.
- L'état de l'élément vulnérable passe à Ouvert, Différé, Fermé, ou passe de Fermé ou Différé.
- Les éléments vulnérables sont supprimés.
- Les éléments vulnérables sont ajoutés ou supprimés de la tâche de rattrapage.

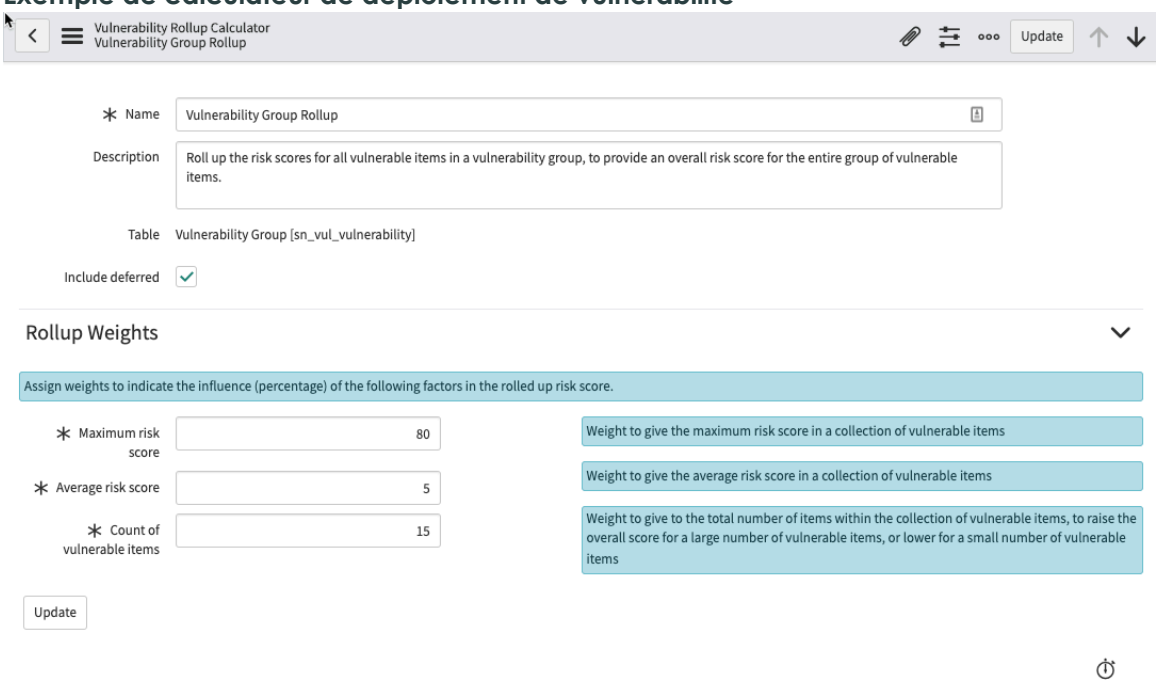
Exemple du calculateur de déploiement de vulnérabilité : prenez l'exemple d'un VUL324567 de tâche de rattrapage, qui comporte les éléments vulnérables suivants :

- VIT1001 avec un score de risque de 30
- VIT1002 avec un score de risque de 40
- VIT1003 avec un score de risque de 50

Prenez également en compte les pondérations suivantes dans le calculateur de déploiement de vulnérabilité :

- Score de risque maximal : 80
- Score de risque moyen : 5
- Nombre d'éléments vulnérables : 15

Exemple de calculateur de déploiement de vulnérabilité



Dans l'exemple du calculateur de déploiement de vulnérabilité, la formule permettant de déterminer le **score de risque** de la tâche de rattrapage est la suivante :

(**Score de risque maximal**/100) * 80 + (**Score de risque moyen** /100) * 5 + (facteur * 15)

Le facteur est déterminé comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nombre VI	Facteur
<10	0,2
10-100	0,4
101-1000	0,6
1001-10000	0,8
> 10000	1

Ainsi, pour la tâche de rattrapage, VUL324567 :

- Le score de risque moyen est de 40
- Le score de risque maximal est de 50
- 50 (score de risque maximal)
- Le facteur est de 0,2

Le **score de risque** serait de 45 [(50/100) * 80 + (40/100) * 5 + 0,2 * 15 = 40 + 2 + 3 = 45]

Cumul des scores de l'EPSS des NVD aux TPE



Calculateur de cumul de l'EPSS - Exemple

Prenons l'exemple d'une entreprise avec 100 vulnérabilités, chacune ayant 5 % de chances d'être exploitée. La question qui intéresse le plus un défenseur réseau pourrait être la suivante : quelle est la probabilité qu'au moins une de ces vulnérabilités soit exploitée, et donc quelle est ma menace globale ? La probabilité qu'au moins un événement se produise est simplement le complément (l'opposé) de l'absence d'événement, c'est-à-dire :

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are
 exploited)
```

Où : la probabilité qu'il n'y ait aucune vulnérabilité est le produit linéaire de la non-exploitation de chaque vulnérabilité. Dans cet exemple, puisque chaque vulnérabilité a 5 %

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de chances d'être exploitée, elles ont chacune 95 % de chances de ne pas être exploitées. Et puisqu'il y en a 100, on peut l'écrire comme suit :

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 -
 P(one vuln not exploited)^100 = 1 - 0.95^100 = 0.994
```

Cela signifie que la probabilité qu'au moins une des vulnérabilités soit exploitée est de 99,4 %.

Important : Pour modifier le *Rollup EPSS Scores from NVD to TPEs*, vous devez basculer la vue du menu contextuel du formulaire vers **la vue Déployer le développeur** à partir de la **vue par défaut**.

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

Après l'évaluation initiale des règles de cibles de rattrapage dans l'Assistant de configuration, les gestionnaires de vulnérabilités peuvent configurer une règle de cible de rattrapage au niveau de l'élément vulnérable pour piloter le rattrapage des vulnérabilités à haut risque en temps opportun. Lorsque la date de rattrapage d'un élément vulnérable approche, une notification est envoyée aux utilisateurs ou aux groupes spécifiés dans la règle.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles de cibles de rattrapage**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom de la règle.
Cible (jours)	Spécifiez le nombre de jours pendant lesquels les éléments vulnérables doivent être rattrapés, depuis leur dernière ouverture.
V17.1 : (date) à partir de la cible	Date à partir de laquelle les SLA cibles sont calculés. Vous pouvez spécifier uniquement les champs de date ou de type date et heure. La valeur par défaut est Date de dernière ouverture. Pour personnaliser les valeurs de ce champ, reportez-vous à KB1642413 .
Actif	Par défaut, la case **Actif** est sélectionnée, ce qui signifie que la règle de cible de rattrapage est active. Si cette case n'est pas cochée, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Notifier (jours avant l'échéance)	Nombre de jours avant l'heure de rattrapage ciblée pour l'envoi d'une notification. La date de notification calculée à l'aide de cette valeur est utilisée pour afficher l'état du rattrapage et le code

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	couleur. Si la date est antérieure à la date de notification, l'état du rattrapage est « En cours ». S'il a dépassé la date de notification et avant la date cible de rattrapage, l'état s'affiche comme approchant de la cible. **Remarque :** Si ce champ est défini sur 0, seule une notification **Cible manquée** est envoyée.
Description	Texte décrivant la règle de cible de rattrapage.
Condition	À l'aide du filtre de condition, sélectionnez les critères d'application de la règle aux éléments vulnérables. Pour éviter tout impact sur les performances, testez vos conditions à l'échelle de la production. Les tests vous permettent de déterminer la durée d'exécution de la tâche **Évaluer les cibles de rattrapage** , compte tenu des conditions et de la taille de votre Base de données de gestion des configurations (CMDB)fichier . La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.
Notifications **Remarque :** Le nombre indiqué dans l'e-mail de notification n'inclut pas les éléments vulnérables à l'état **Différé**, **Résolu** ou **Fermé** .	
Utilisateurs	Personnes à notifier quand l'élément vulnérable sélectionné approche ou dépasse son heure cible de rattrapage cible.
Groupe	Groupe à notifier quand l'élément vulnérable sélectionné approche ou dépasse son heure cible de rattrapage cible.
Historique des mises à jour	
	Non utilisé pour la création initiale d'une règle. Par la suite, les notes de travail du système sont enregistrées ici.

4. Cliquez sur **Envoyer**.
   Cette règle entre en vigueur lors de la prochaine exécution de la tâche planifiée *`Evaluate remediation targets`* ou lors de l'utilisation du bouton **Appliquer les changements** dans la vue de liste Règles de cibles de rattrapage. Il en va de même lorsqu'une règle existante est mise à jour. Pour plus d'informations sur la tâche planifiée et **l'application des modifications**, reportez-vous à la rubrique Réponse aux vulnérabilités Règles de cibles de rattrapage.

Configurer les intégrations tierces installées à l'aide de l'Assistant de configuration

Configurez Vulnerability Response pour qu'elle fonctionne avec chacun de vos déploiements d'application tierce installés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration**.
2. Sélectionnez **Intégrations de scanners pour configurer les déploiements** d'applications tierces installées.
3. Si Gestion des solutions pour Réponse aux vulnérabilités est installé, vous pouvez sélectionner **Intégrations de solutions** pour configurer vos fournisseurs de solutions de vulnérabilité.

Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'Assistant de configuration

Après avoir installé l'application Vulnerability Solution Management, vous pouvez configurer vos fournisseurs de solutions de vulnérabilité à l'aide de l'Assistant de configuration.

Avant de commencer

Rôles requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé), ou admin
Utilisez les sections suivantes pour compléter les instructions et invites fournies dans l'Assistant de configuration pour les intégrations de solutions installées pour Gestion des solutions pour Réponse aux vulnérabilités.

- Vérifiez que vous avez déjà installé Gestion des solutions pour vulnérabilités les intégrations de solutions souhaitées avant de commencer. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.
- Vérifiez que vous disposez de toutes les informations d'identification d'un compte tiers. Il est nécessaire de modifier certaines intégrations de solutions.
- Consultez Installer l'application Gestion des solutions pour Réponse aux vulnérabilités pour plus d'informations avant de configurer les solutions installées.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions**.

   Le nécessite Microsoft Security Response Center Solution Integration une clé API et une URL pour le Microsoft Security Response Center configurer.

   Remarque : La saisie de la clé API est facultative pour MSRC. Pour obtenir la MSRC clé, vous devez disposer d'un ID Microsoft provenant d'un compte de messagerie live.com, outlook.com ou Microsoft.com, d'un numéro de téléphone enregistré auprès de Microsoft ou d'une connexion Skype.

2. Entrez l'URL.
   L'URL dans l'assistant de configuration pour MSRC est `https://api.msrc.microsoft.com`.
3. Cliquez sur **Terminer**.
4. Facultatif : Vous pouvez exécuter des importations à la demande en cliquant sur **Exécuter maintenant** sur la page de configuration après avoir entré vos informations d'identification.
5. Le Intégration de solution Red Hat est également disponible.
   Il ne nécessite pas de clé API.
6. Dans l'Assistant de configuration, à droite du Intégration de solution Red Hat, cliquez sur **Modifier**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Vérifiez que l'URL dans l'Assistant de RHSI configuration est `https://access.redhat.com/hydra/rest`
8. Facultatif : Vous pouvez exécuter des importations à la demande en cliquant sur **Exécuter maintenant** sur la page de configuration.
9. Cliquez sur **Terminer** , puis **sur Marquer comme terminé** pour terminer la configuration. Une coche s'affiche dans l'assistant de configuration pour les intégrations de solutions lorsque vous avez terminé la configuration.

Configurer l'intégration de vulnérabilité MS TVM à l'aide de l'assistant de configuration

Configurez l'intégration à l'application Réponse aux vulnérabilités Microsoft Threat and Vulnerability Management (MS TVM) après l'avoir installée à l'aide de l'Assistant de configuration.

Avant de commencer

En plus des instructions et des invites fournies dans l'assistant de configuration pour l'intégration à Microsoft Réponse aux vulnérabilités Threat and Vulnerability Management, procédez comme suit :

- Vérifiez que vous avez déjà installé l'application avant de commencer. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.
- Pour plus d'informations, reportez-vous à la section Préparation à l'intégration des vulnérabilités Microsoft Threat and Vulnerability Management avant de configurer l'intégration de Gestion des menaces et des vulnérabilités de Microsoft pour Réponse aux vulnérabilités.
- Vérifiez que vous disposez des informations d'identification de votre compte MS TVM. Pour obtenir ces informations d'identification, reportez-vous à Configurer Microsoft Azure pour l'intégration MS TVM.

Rôles requis : administrateur système (admin) pour l'installation, administrateur de vulnérabilité (sn_vul.vulnerability_admin) ou sn_vul.admin (obsolète) et configurer l'intégration (sn_vul_msft_tvm.configure_integration) pour la configuration

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.

   La vignette Microsoft Threat & Vulnerability Management s'affiche.

   MS TVM est une intégration multisources, ce qui signifie que vous pouvez avoir plusieurs déploiements de la même intégration tierce. Les paramètres de votre intégration tierce d'origine sont utilisés comme modèle pour les paramètres de chaque nouvelle intégration.

   > **Remarque :** Si vous supprimez l'intégration de vulnérabilité d'origine, vous devez sélectionner une autre intégration à utiliser comme modèle. Envisagez de désactiver l'intégration au lieu de la supprimer. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

   Les données de chaque intégration tierce sont identifiées de manière unique et disponibles dans une seule instance de Réponse aux vulnérabilités.

2. Pour configurer l'intégration de Microsoft Threat and Vulnerability Management, cliquez sur **Modifier**.
3. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Informations d'identification de compte

Champ	Description
Nom	Nom de l'instance.
Région TVM	Région proche de l'emplacement de votre serveur. Utilisez le serveur le plus proche de votre emplacement pour des performances optimales de l'API.
Type d'authentification	Méthode de vérification de l'identité. L'authentification utilisateur contrôle la visibilité des actifs spécifiques pour des utilisateurs spécifiques. MS TVM exporte les groupes d'appareils autorisés pour cet utilisateur. La valeur par défaut est Application.
ID de locataire	Identité du locataire de votre organisation.
ID client	Identité du client générée après l'enregistrement de MS TVM dans Microsoft Azure.
Nom d'utilisateur	Utilisateur ayant accès au groupe d'appareils complet. Ce champ s'affiche uniquement lorsque l'utilisateur est sélectionné à partir du type d'authentification.
Mot de passe	Mot de passe du nom d'utilisateur qui a accès à l'ensemble du groupe d'appareils. Ce champ s'affiche uniquement lorsque l'utilisateur est sélectionné à partir du type d'authentification.
Secret client	Secret client généré après l'enregistrement de l'application MS TVM. Ce champ s'affiche uniquement lorsque l'Application est sélectionnée à partir du type d'authentification.

Traduction automatique

4. Pour enregistrer vos changements et passer au premier formulaire d'intégration, cliquez sur **Suivant**.
   Le formulaire Configuration de l'importation des vulnérabilités s'affiche.
5. Activez ou désactivez l'importation des vulnérabilités, déterminez la date de début initiale des vulnérabilités que vous souhaitez importer et planifiez l'exécution de l'importation des vulnérabilités MS TVM.
   Si vous souhaitez importer toutes les vulnérabilités, laissez la date de démarrage initiale vide.
   a. Pour importer des données à la demande, cliquez sur **Importer les vulnérabilités maintenant**.
   b. Pour afficher l'enregistrement d'intégration, cliquez sur **Paramètres avancés**.
6. Pour enregistrer vos changements et passer au premier formulaire d'intégration, cliquez sur **Suivant**.
   Le formulaire Configuration de l'importation des recommandations s'affiche.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Activez ou désactivez l'importation des recommandations et déterminez le calendrier d'exécution de l'importation des vulnérabilités MS TVM.
   a. Pour importer des données à la demande, cliquez sur **Importer les recommandations maintenant**.
   b. Pour afficher l'enregistrement d'intégration, cliquez sur **Paramètres avancés**.
8. Pour enregistrer vos changements et passer au premier formulaire d'intégration, cliquez sur **Suivant**.
   Le formulaire Configuration de l'importation des machines s'affiche.
9. Activez ou désactivez l'importation des machines, déterminez la date de démarrage initiale des machines que vous souhaitez importer et planifiez l'exécution de l'importation des machines MS TVM.
   Si vous souhaitez importer toutes les machines, ne renseignez pas la date de début initiale.

   Remarque : Les étiquettes des machines sont importées par défaut et utilisées pour organiser et suivre les machines répertoriées dans l'environnement MS TVM.

   a. Pour afficher les règles de recherche d'éléments de configuration (CI) par défaut, cliquez sur **Règles de recherche de CI**. Les règles de Recherche de CI définissent de quelle manière les données machine de sources tierces sont utilisées pour identifier les éléments de configuration (CI) dans le Now Platform CMDB. Vous pouvez ajouter des règles de recherche ou modifier les règles de recherche de CI par défaut sur cette page. Pour plus d'informations, consultez Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.
   b. Pour importer des données à la demande, cliquez sur **Importer des machines maintenant**.

      Remarque : Les ordinateurs dont l'état est intégré dans MS TVM sont récupérés par l'application ServiceNow.

   c. Pour afficher l'enregistrement d'intégration, cliquez sur **Paramètres avancés**.
10. Pour enregistrer vos changements et accéder au premier formulaire d'intégration, cliquez sur **Suivant**.
    Le formulaire Configuration de l'importation des vulnérabilités de la machine s'affiche.
11. Activez les intégrations suivantes et déterminez la date de début initiale des vulnérabilités que vous souhaitez importer.

Formulaire de configuration de l'importation des vulnérabilités de la machine

Intégration	Description
Importation Delta des vulnérabilités de la machine Microsoft TVM	Récupère les vulnérabilités qui ont été mises à jour pendant l'importation complète de la vulnérabilité, y compris les vulnérabilités nouvelles, corrigées et mises à jour. Vous ne pouvez importer des données delta que pour les 14 derniers jours.
Importation totale des vulnérabilités de la machine Microsoft TVM	Récupère toutes les vulnérabilités ouvertes. En raison du volume élevé d'importations de données, vous pouvez les planifier pour qu'elles s'exécutent toutes les semaines.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Exécutez l'importation des machines avant l'intégration des vulnérabilités des machines. Sinon, les VI ne sont pas créés pour les ordinateurs manquants.

12. Pour enregistrer vos modifications et terminer la configuration dans l'Assistant de configuration, cliquez sur **Terminer**.

Que faire ensuite

Si vous souhaitez activer un regroupement d'éléments vulnérables dans l'environnement classique, accédez à > **Réponse aux vulnérabilités** > **Administration** > **Règles de la tâche de rattrapage** > **Recommandation Microsoft TVM**.

Dans le formulaire qui s'affiche, sélectionnez l'option **Actif** pour l'activer. Vous pouvez également sélectionner **Nouveau** pour créer une nouvelle règle.

Pour plus d'informations, consultez Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage.

Configurer l'utilisation de l'assistant de Qualys Vulnerability Integration configuration

Une fois l'application Qualys installée, configurez-la à l'aide de l'Assistant de configuration.

Avant de commencer

Utilisez les sections suivantes pour compléter les instructions et invites fournies dans l'Assistant de configuration pour la configuration du Qualys Vulnerability Integrationfichier .

- Vérifiez que vous avez déjà installé l'application avant de commencer. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.
- Reportez-vous à la section Se préparer à la Qualys Vulnerability Integration pour plus d'informations avant de configurer le Qualys Vulnerability Integrationfichier .
- Vérifiez que vous disposez de toutes les informations d'identification d'un compte tiers. Il est nécessaire de modifier certaines applications tierces.

Rôles requis : administrateur système (admin) pour l'installation, administrateur de vulnérabilité (sn_vul.vulnerability_admin) ou sn_vul.admin (obsolète) pour la configuration.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
   Les intégrations installées s'affichent.
2. Cliquez sur **Modifier** à droite de celui Qualys Vulnerability Integration que vous souhaitez configurer.
3. Dans le formulaire Informations d'identification de compte, saisissez vos Qualys Cloud Platform informations d'identification.
   Vos informations d'identification sont requises pour le configurer.
4. Utilisez les remarques suivantes comme guide pour poursuivre la configuration.
   - Le lien **Paramètres avancés** vous dirige vers l'enregistrement d'intégration Qualys . Vous pouvez ajouter des paramètres pris en charge par le Qualys produit pour vos requêtes planifiées afin de vous aider à filtrer les données de vulnérabilité que vous importez. Voir Définir des paramètres de filtre supplémentaires pour Qualys les importations pour plus d'informations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si vous avez effectué une mise à niveau à partir d'une version antérieure ou Réponse aux vulnérabilités d'une version que vous avez déjà configurée, cette version, avec ses paramètres de Qualys Vulnerability Integration configuration conservés, est toujours disponible.

  Sous Paramètres d'importation dans la configuration de la détection d'hôte pour , Qualys Vulnerability Integrationil existe une option permettant d'afficher les enregistrements de détection de vulnérabilité fixe Qualys . Si cette option est activée, elle vous permet de créer des éléments vulnérables à partir d'enregistrements de détection à l'état fixe (état=**Fixe**). Pour en savoir plus sur la détection des éléments vulnérables, reportez-vous à la section Réponse aux vulnérabilités Détections d'éléments vulnérables à partir d'intégrations tierces.

  Vous pouvez activer la case à cocher **Rechercher par partition réseau** sur la page Configuration de la détection d'hôte pour inclure l'identificateur de partition réseau dans la recherche d'adresse IP. Consultez Mettre à jour les éléments de configuration avec l'identificateur de partition de réseau pour le Qualys Vulnerability Integration pour plus d'informations.

  Toutes les balises d'hôte sont importées dans le cadre de l'intégration de la liste d'hôtes Qualys . Les balises d'hôte sont principalement utilisées pour le filtrage dans Réponse aux vulnérabilités les règles de tâches d'affectation et de rattrapage. Ils sont affichés dans le formulaire Élément détecté.

  Remarque : L'intégration de la Qualys liste d'hôtes doit être exécutée avant la création de règles Réponse aux vulnérabilités de tâche d'affectation ou de rattrapage afin que toutes les balises puissent être présentes dans les règles et avant que les éléments vulnérables ne soient importés et regroupés.

  Qualys **Les balises d'actif** sont stockées dans le module Balises d'hôte sous .Qualys Vulnerability Integration

- Le Qualys Vulnerability Integration prend en charge multi-sources. Vous pouvez avoir plusieurs déploiements de la même intégration tierce. Pour ajouter une autre intégration, sur la page Intégrations de scanners, cliquez sur **Ajouter une intégration**.

  Les paramètres de votre intégration tierce d'origine sont utilisés comme modèle pour les paramètres de chaque nouvelle intégration.

  Remarque : Si vous supprimez l'intégration de vulnérabilité d'origine, vous devez sélectionner une autre intégration à utiliser comme modèle. Envisagez de désactiver l'intégration au lieu de la supprimer. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

  Les données de chaque intégration tierce sont identifiées de manière unique et disponibles dans une seule instance de Réponse aux vulnérabilités.

- Vous pouvez exécuter des importations à la demande en cliquant sur **Exécuter maintenant** sur une page de configuration.

5. Cliquez sur **Terminer** pour terminer la configuration dans l'Assistant de configuration.

Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration

Une fois l'application Intégration de Réponse aux vulnérabilités à Tenable installée, configurez-la à l'aide de l'Assistant de configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Utilisez les sections suivantes pour compléter les instructions et invites fournies dans l'assistant de configuration pour l'intégration Intégration de Réponse aux vulnérabilités à Tenable .

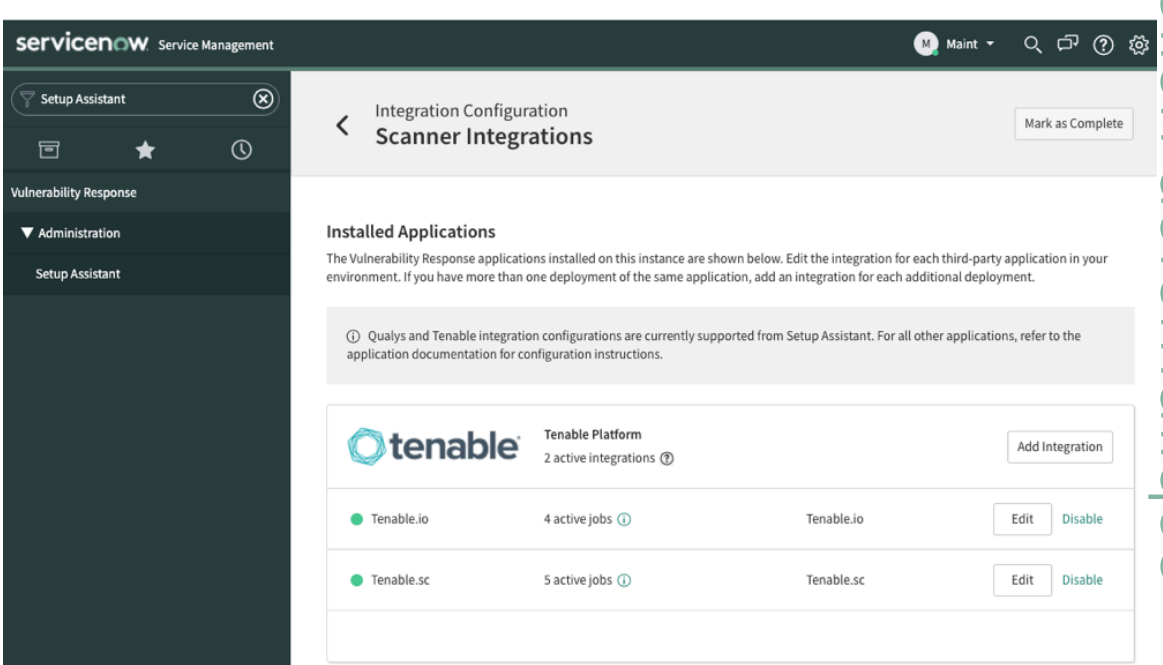
- Vérifiez que vous avez déjà installé l'application avant de commencer. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.
- Reportez-vous à la section Préparation de l'intégration Tenable Vulnerability pour plus d'informations avant de configurer le Tenable pour Réponse aux vulnérabilitésfichier .
- Vérifiez que vous disposez de toutes les informations d'identification d'un compte tiers. Il est nécessaire de modifier certaines applications tierces.

Rôles requis : administrateur système (admin) pour l'installation, administrateur de vulnérabilité (sn_vul.vulnerability_admin) ou sn_vul.admin (obsolète) et configurer l'intégration (sn_vul_tenable.configure_integrations) pour la configuration.

Procédure

1. Si ce n'est pas le cas, accédez à **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.

   Les Tenable.io intégrations et Tenable.sc s'affichent.



   Tenable est une intégration multi-sources, et vous pouvez avoir plusieurs déploiements de la même intégration tierce. Les paramètres de votre intégration tierce d'origine sont utilisés comme modèle pour les paramètres de chaque nouvelle intégration.

   Remarque : Si vous supprimez l'intégration de vulnérabilité d'origine, vous devez sélectionner une autre intégration à utiliser comme modèle. Envisagez de désactiver l'intégration au lieu de la supprimer. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

   Les données de chaque intégration tierce sont identifiées de manière unique et disponibles dans une seule instance de Réponse aux vulnérabilités.

2. À droite de l'intégration Tenable que vous souhaitez configurer, cliquez sur **Modifier**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Renseignez les champs du formulaire Informations d'identification de compte.

- Tenable.io nécessite l'accès Administrateur avec un attribut d'autorisation supérieur ou égal à 64.

  Remarque : À partir de la version 3.8 de Vulnerability Response Integration with Tenable, l'accès aux Tenable.io ne nécessite plus de privilèges d'administrateur. Un utilisateur de base avec un attribut d'autorisation égal à 16 peut également accéder au produit.

- Tenable.sc nécessite l'accès Analyste ou Gestionnaire de sécurité.

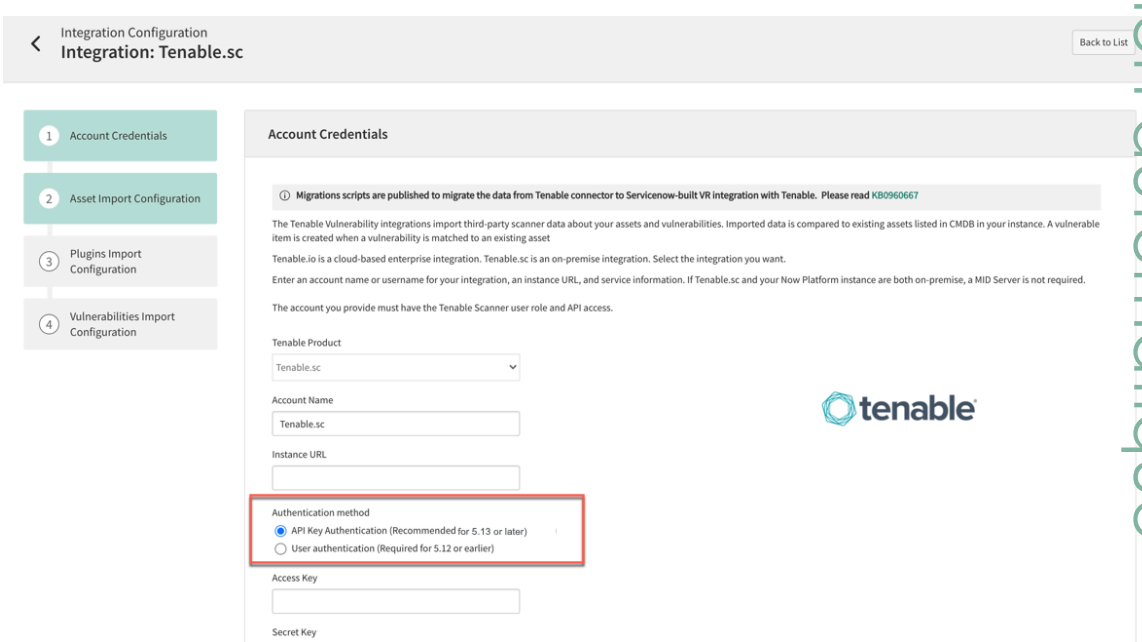
a. Sélectionnez votre produit Tenable.

b. Saisissez le nom de votre compte Tenable.

c. Dans le champ URL de l'instance, saisissez l'URL de votre plateforme Tenable.

d. Sélectionnez une méthode d'authentification.

En fonction de votre version de , vous disposez de Tenable.scdeux options d'authentification :



i. À partir de la version 5.13 de , sélectionnez Authentification de Tenable.sc**clé API**. Saisissez vos clés d'accès et secrètes Tenable.

ii. Avant la version 5.13, l'authentification utilisateur était prise en charge par votre Now Platform® instance et était requise. Entrez votre nom d'utilisateur et votre Now Platform mot de passe.

Seule l'authentification par clé API est prise en charge pour Tenable.sc. Saisissez vos clés d'accès et secrètes Tenable.

e. Facultatif : Sélectionnez un MID Server

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(Optional) Si votre Now Platform instance et votre Tenable.sc application ne se trouvent pas au même emplacement, choisissez un Serveur MID configuré dans la liste de choix. Pour plus d'informations, reportez-vous à la section Serveur MID .

- À partir des versions 15.0 et 3.0 de Réponse aux vulnérabilités , Tenable Vulnerability Integrationvous pouvez activer le *Async_request* paramètre comme décrit dans la section Paramètres de récupération de données pour Tenable Vulnerability Integration. Une certaine configuration avec Tenable est requise si vous souhaitez effectuer des appels synchrones. Contactez le produit Tenable pour obtenir de l'aide. Ce paramètre, une fois activé, est applicable pour toutes les intégrations de Tenable.sc et il y a un délai d'expiration de 30 secondes. Pour afficher les scripts correctifs, accédez à **Définition du système** > **Scripts correctifs**.

- (Optional) Pour les clients existants, un script correctif est disponible si vous utilisez des appels asynchrones.

Si votre Now Platform instance et votre Tenable.sc application sont toutes deux sur site, bien que cela ne soit pas obligatoire, vous pouvez sélectionner un serveur MID configuré dans la liste de choix.

Remarque : Que vous choisissiez d'utiliser un serveur MID ou non, les intégrations expirent au bout de cinq minutes et un message s'affiche en l'absence de réponse du serveur.

En cas d'erreur de délai d'expiration, vérifiez que vous avez saisi les informations d'identification et l'URL correctes dans l'Assistant de configuration.

4. Cliquez sur **Suivant** pour enregistrer vos changements et passer au premier formulaire d'intégration.
   Le formulaire Configuration de l'importation d'actifs s'affiche.
5. Sur ce formulaire, activez ou désactivez l'intégration de l'importation d'actifs, déterminez la date de début initiale pour les actifs que vous souhaitez importer et planifiez l'exécution de l'importation d'actifs Tenable.

   Pour Tenable.io

   - L'intégration des actifs peut être utilisée avec l'intégration des résultats de conformité et du Tenable.io remplissage des résultats de conformité pour importer des données d'évaluation de configuration sécurisée concernant vos actifs dans l'application Conformité de la configuration .
   - La version 12.2 de l'application Conformité de la configuration est requise sur votre instance si vous souhaitez importer et afficher ces données d'évaluation de configuration sécurisée.

     Consultez la rubrique Conformité de la configuration Données importées pour en savoir plus sur les données qui sont importées avec ces intégrations et où elles sont publiées.

   - Les Tenable.io intégrations Résultats de conformité et Renvoi des résultats de conformité ne sont pas activées par défaut. Si vous les activez, vous préférerez peut-être utiliser les paramètres de calendrier par défaut fournis. Consultez les étapes ci-dessous pour savoir comment localiser et activer les intégrations pour le Tenable Vulnerability Integration.
   - Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Tenable.io produit à partir de votre instance. L'intégration Tenable.io du modèle et l'intégration des informations d'identification Tenable.io de numérisation doivent être activées avant de lancer de nouvelles analyses.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, ces intégrations sont désactivées. Lorsque vous saisissez vos informations d'identification pour Tenable.io, toutes les Tenable.io intégrations sont automatiquement activées. Pour activer ou désactiver manuellement ces intégrations :

a. Accédez à la **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.

b. Dans la liste qui s'affiche, localisez les enregistrements d'intégration Tenable.io souhaités.

c. Ouvrez chaque enregistrement et cochez la case **Actif** pour activer l'intégration.

d. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

e. Revenez à l'assistant de configuration pour poursuivre la configuration avec Tenable Vulnerability IntegrationRéponse aux vulnérabilités.

- Pour l'intégration Tenable.io , vous avez également la possibilité d'activer et de désactiver l'importation des balises d'actif. Les balises d'actif sont importées par défaut et utilisées pour organiser et suivre les actifs répertoriés dans votre CMDB dans l'environnement Tenable.io .
- Pour les produits et Tenable.sc , si vous sélectionnez Activer la Tenable.io**recherche par partition réseau** sous Rechercher par partition réseau, vous pouvez créer des CI individuels à l'aide du moteur Identification et réconciliation (IRE) pour vos actifs qui ont la même adresse IP. Voir Mettre à jour les éléments de configuration avec l'identificateur de partition de réseau pour le Tenable Vulnerability Integration et Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement pour plus d'informations.
- En haut de l'écran, en regard du lien d'importation d'actifs, cliquez sur le lien **Règles de recherche de CI** pour afficher les règles de recherche d'éléments de configuration (CI) par défaut. Les règles de Recherche de CI définissent de quelle manière les données d'actif de sources tierces sont utilisées pour identifier les éléments de configuration (CI) dans la Now Platform CMDB. Vous pouvez ajouter des règles de recherche ou modifier les règles de recherche de CI par défaut sur cette page. Pour plus d'informations, consultez Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.
- Cliquez sur **Importer des actifs maintenant** pour importer des données à la demande.
- Le lien **Paramètres avancés** vous dirige vers l'enregistrement d'intégration d'actif. À partir de la version 3.3, vous pouvez ajouter des paramètres pris en charge par le Tenable.io produit pour vos requêtes planifiées afin de vous aider à filtrer les données de vulnérabilité que vous importez avec les actifs et les Tenable.io intégrations de vulnérabilités fixes et ouvertes. Voir Définir des paramètres de filtre supplémentaires pour Tenable.io les importations pour plus d'informations.

6. Cliquez sur **Suivant** pour enregistrer vos modifications et passer au formulaire suivant. Le formulaire Configuration de l'importation des modules d'extension s'affiche.

7. Dans ce formulaire, activez ou désactivez l'importation des modules d'extension (entrées de vulnérabilité tierces), déterminez la date de début initiale des modules d'extension que vous souhaitez importer et planifiez l'exécution de l'importation des modules d'extension Tenable.

Si vous souhaitez importer l'ensemble des modules d'extension, des vulnérabilités et des actifs, ne renseignez pas la date de démarrage initiale.

- Cliquez sur **Importer les modules d'extension maintenant** pour importer des données à la demande.
- Le lien **Paramètres avancés** vous dirige vers l'enregistrement d'intégration des modules d'extension.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour l'importation des vulnérabilités, vous pouvez planifier et définir les niveaux de gravité des Tenable.io vulnérabilités que vous souhaitez ingérer. Déterminez une date afin que seules les vulnérabilités créées ou mises à jour à partir d'une date spécifique soient importées.
- Pour l'intégration Tenable.sc , vous pouvez déterminer un filtre de requête et une date afin que seules les vulnérabilités créées ou mises à jour à partir d'une date spécifique soient importées.

8. Cliquez sur **Suivant** pour enregistrer vos modifications et passer au formulaire suivant. Le formulaire Configuration de l'importation des vulnérabilités s'affiche. Activez ou désactivez l'intégration et déterminez la date de début initiale des vulnérabilités que vous souhaitez importer.

   Pour le Tenable.io produit :

   - Importez uniquement les vulnérabilités et les éléments vulnérables associés qui correspondent aux conditions de votre choix avec le filtre Sévérité.
   - Pour l'intégration des Tenable.io actifs, *Last Scan Time* est importée et mise à jour uniquement pour les actifs présentant des vulnérabilités.
   - Activez l'option **Vulnérabilités corrigées** pour afficher les VI pour les enregistrements de détection fixes. Si ce marqueur est activé dans l'Assistant de configuration, de nouveaux VI sont créés pour les détections à l'état **Fixe** qui n'existent pas déjà dans votre instance. Lorsqu'elle est activée, cette fonctionnalité peut avoir un impact négatif sur vos performances d'ingestion.
   - Le lien **Paramètres avancés** en regard de Filtres d'importation vous dirige vers l'enregistrement d'intégration des vulnérabilités.
   - Cliquez sur le lien **Importer les calendriers** en haut pour configurer la fréquence à laquelle les vulnérabilités sont ingérées et activer l'intégration.

   Pour le Tenable.sc produit :

   - Importez uniquement les vulnérabilités et les VI associés qui correspondent aux filtres de condition définis par une requête Tenable dans la plateforme Tenable. Consultez la documentation Tenable pour plus d'informations sur les requêtes Tenable.

     Le filtre de requête Tenable que vous sélectionnez dans l'assistant de configuration s'applique également à l'intégration Tenable.sc des actifs. Seuls les actifs présentant les vulnérabilités qui correspondent aux conditions du filtre de requête sont importés.

   - Activez l'option **Vulnérabilités corrigées** pour afficher les VI pour les enregistrements de détection fixes. Si ce marqueur est actif dans l'Assistant de configuration, de nouveaux VI sont créés pour les détections à l'état **Fixe** qui n'existent pas déjà dans votre instance. Lorsqu'elle est active, cette fonctionnalité peut avoir un impact négatif sur vos performances d'ingestion.
   - Pour inclure l'identificateur de partition de réseau dans la recherche d'adresse IP, sélectionnez **Activer la recherche par partition de réseau** case à cocher de la **Rechercher par partition réseau** section. Pour plus d'informations, consultez Mettre à jour les éléments de configuration avec l'identificateur de partition de réseau pour le Tenable Vulnerability Integration.
   - Cliquez sur **Importer les calendriers** en haut pour configurer la fréquence à laquelle les vulnérabilités sont ingérées et activer l'intégration.
   - Le lien **Paramètres avancés** en regard de Filtres d'importation vous dirige vers l'enregistrement d'intégration des vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'intégration ServiceNow® Tenable.sc des informations d'identification de numérisation est activée (`active`) automatiquement à partir de l'assistant de configuration de votre instance lorsque vous configurez les Tenable.sc intégrations de vulnérabilités (Tenable.sc intégrations de vulnérabilités ouvertes et fixes).

  Cette intégration importe et met à jour les informations d'identification du scanner à partir Tenable.sc du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable. Accédez à la **Intégration de vulnérabilité tenable** > **Intégrations** > **Intégration des informations d'identification Tenable.sc Scan** pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation.

9. Cliquez sur **Terminer** pour enregistrer vos modifications et terminer la configuration dans l'Assistant de configuration.

Que faire ensuite

(Facultatif) Accédez à **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Calculateurs de vulnérabilités** > **Calculateur de risque par défaut** > **Règle de risque tenable** pour activer la règle de risque Tenable.

Dans le formulaire Règle du calculateur de vulnérabilité qui s'affiche, cochez la case Actif pour l'activer.

La règle de risque Tenable est installée avec l'application dans le Intégration de Réponse aux vulnérabilités à Tenable cadre du calculateur de risque par défaut dans les calculateurs de vulnérabilité à partir de Réponse aux vulnérabilités. L'évaluation de priorité de vulnérabilité (VPR) est un attribut du produit Tenable qui est importé et utilisé avec le nouveau calculateur de risque par défaut. Cette règle de risque est désactivée par défaut. En activant la règle du calculateur de risque Tenable, les valeurs VPR importées sont utilisées pour calculer le score de risque pour les éléments vulnérables. Distribution de pondération par défaut pour ce calculateur de risque : VPR = 70 %, Actif = 15 % et Criticité opérationnelle = 15 %. L'activation de cette règle du calculateur de risque Tenable peut avoir un impact sur vos performances d'ingestion de données.

Reportez-vous à la rubrique Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.

Configurer les fournisseurs de solutions de vulnérabilité

Configurez les fournisseurs de solutions de vulnérabilité en suivant la liste de vérification, puis en configurant les fournisseurs dans l'assistant de configuration.

Préparer la liste de vérification d'intégration de solution

Utilisez l'assistant de configuration pour préparer l'implémentation d'une intégration de l'intelligence des solutions pour tous les fournisseurs qui prennent en charge le format de données CVRF (Common Vulnerability Reporting Framework) ou CSAF (Common Security Advisory Framework).

Préparation de l'intégration de la solution CVRF (Common Vulnerability Reporting Framework)

Utilisez l'assistant de configuration pour préparer l'implémentation d'une intégration d'intelligence de solution pour tous les fournisseurs qui prennent en charge le format de données CVRF (Common Vulnerability Reporting Framework).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Pour une intégration avec les fournisseurs qui fournissent les solutions, assurez-vous d'effectuer les tâches de la liste de vérification suivante. Vous pouvez imprimer la liste de vérification et vérifier que les éléments répertoriés sont complétés avant d'installer l'application.

Liste de vérification de la préparation de l'intégration

Tâche	Description
Applications dépendantes ☐	Vérifiez que les applications suivantes sont installées à partir de ServiceNow Store: • Gestion des solutions de vulnérabilité : pour plus d'informations sur l'installation Gestion des solutions pour vulnérabilitésde , consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration et Installer l'application Gestion des solutions pour Réponse aux vulnérabilités. • Vulnerability Response : pour plus d'informations sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 16.1 ou Réponse aux vulnérabilités ultérieure.
Informations d'identification du compte tiers ☐	Vérifiez que vous disposez de toutes les informations d'identification d'un compte tiers. Il est nécessaire de modifier certaines intégrations de solutions.
Authentification du fournisseur ☐	Vérifiez que vous avez authentifié les fournisseurs pour l'importation de solutions à l'aide des API. Pour en savoir plus sur l'authentification des fournisseurs, reportez-vous à la section Configurer les alias de connexion et d'informations d'identification. Si vous ne souhaitez pas configurer un fournisseur basé sur une API, vous pouvez ignorer cette étape.
Personnalisation du flux et de l'action de flux ☐	Si vous souhaitez configurer un fournisseur basé sur une API autre que Cisco, vous devez personnaliser le flux et l'action de flux pour extraire une clé unique et une URL CVRF à partir de la réponse d'un conseil. **Remarque :** La publication de l'URL CVRF n'est pas standard pour tous les fournisseurs. Pour personnaliser le flux pour les fournisseurs autres que Cisco, reportez-vous à la section Configurer un fournisseur commun de Vulnerability Reporting Framework autre que Cisco.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
	Vous pouvez ignorer cette étape s'il ne souhaite pas configurer d'autres fournisseurs que Cisco. Par défaut, le flux pour Cisco a été fourni avec l'application.
Rôles ☐	Vérifiez que vous disposez d'un groupe d'administrateurs ou d'un utilisateur qui peut gérer l'intégration. Si elle n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles.

Préparation de l'intégration de la solution du Cadre consultatif de sécurité commun (CSAF)

Utilisez l'assistant de configuration pour préparer l'implémentation d'une intégration de l'intelligence des solutions pour tous les fournisseurs qui prennent en charge le format de données CSAF (Common Security Advisory Framework).

Avant de commencer

Pour une intégration avec les fournisseurs qui fournissent les solutions, assurez-vous d'effectuer les tâches de la liste de vérification suivante. Vous pouvez imprimer la liste de vérification et vérifier que les éléments répertoriés sont complétés avant d'installer l'application.

Liste de vérification de la préparation de l'intégration

Tâche	Description
Applications dépendantes ☐	Vérifiez que les applications suivantes sont installées à partir de ServiceNow Store: • Gestion des solutions de vulnérabilité : pour plus d'informations sur l'installation Gestion des solutions pour vulnérabilitésde , consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration et Installer l'application Gestion des solutions pour Réponse aux vulnérabilités. • Vulnerability Response : pour plus d'informations sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 16.1 ou Réponse aux vulnérabilités ultérieure.
Informations d'identification du compte tiers ☐	Vérifiez que vous disposez de toutes les informations d'identification d'un compte tiers. Il est nécessaire de modifier certaines intégrations de solutions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
Authentification du fournisseur ☐	Vérifiez que vous avez authentifié les fournisseurs pour l'importation de solutions à l'aide des API. Pour en savoir plus sur l'authentification des fournisseurs, reportez-vous à la section Configurer les alias de connexion et d'informations d'identification pour le Cadre de travail consultatif de sécurité commun (CSAF). Si vous ne souhaitez pas configurer un fournisseur basé sur une API, vous pouvez ignorer cette étape.
Personnalisation du flux et de l'action de flux ☐	Si vous souhaitez configurer un fournisseur basé sur une API autre que Red Hat, vous devez personnaliser le flux et l'action de flux pour l'extraction d'une clé unique et d'une URL CSAF à partir de la réponse d'un avis. **Remarque :** La publication de l'URL CSAF n'est pas la norme pour tous les fournisseurs. Pour personnaliser le flux pour les fournisseurs autres que , reportez-vous Red Hatà la section Configurer un fournisseur de cadre de travail consultatif de sécurité commun autre que Red Hat. Vous pouvez ignorer cette étape s'il ne souhaite pas configurer d'autres fournisseurs que Red Hat. Par défaut, le flux de Red Hat a été envoyé avec l'application.
Rôles ☐	Vérifiez que vous disposez d'un groupe d'administrateurs ou d'un utilisateur qui peut gérer l'intégration. Si elle n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles.

Configurer les fournisseurs de solutions en matière de vulnérabilité

Après avoir installé l'application Vulnerability Solution Management, configurez les fournisseurs de solutions de vulnérabilité à l'aide de l'Assistant de configuration.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration**.
2. Cliquez sur **Intégrations de solutions**.
3. Dans la section Solutions installées, extrayez les données à l'aide d'une URL, d'une API ou d'une importation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour extraire des données à l'aide d'une URL ou d'une API, cliquez sur **Ajouter une intégration**.
- Pour extraire des données en chargeant un fichier CVRF (Common Vulnerability Response Framework) ou CSAF (Common Security Advisory Framework), cliquez sur **Importer un fichier**.

Que faire ensuite

Selon le format dans lequel vous souhaitez importer les données, vous pouvez effectuer l'une des tâches suivantes :

- Pour CVRF :
  - Si vous souhaitez importer un fichier CVRF, reportez-vous à la section Importer des données Common Vulnerability Reporting Framework via l'importation de fichiers.
  - Si vous souhaitez importer des données CVRF à l'aide des API, reportez-vous à la section Importer des données CVRF (Common Vulnerability Reporting Framework) via l'URL CVRF.
  - Si vous souhaitez importer des données CVRF par le biais d'avis, reportez-vous à la section Importer des données Common Vulnerability Reporting Framework à partir d'avis.
- Pour le CSAF :
  - Si vous souhaitez importer un fichier CSAF, reportez-vous à la section Importer des données de Cadre de travail consultatif de Security commun via l'importation de fichiers .
  - Si vous souhaitez importer des données CSAF à l'aide des API, consultez Importer des données du Cadre de travail consultatif de sécurité commun (CSAF) par le biais de l'URL CSAF .
  - Si vous souhaitez importer des données CSAF par le biais d'avis, consultez Importer des données du Cadre consultatif de Security commun à partir d'avis.

CVRF (Common Vulnerability Reporting Framework)

Le Common Vulnerability Reporting Framework (CVRF) offre un cadre normalisé pour la création de la documentation des rapports de vulnérabilité. Il s'agit d'un langage basé sur XML qui simplifie le partage d'informations cruciales liées à la sécurité entre diverses parties prenantes au sein de plusieurs organisations. En utilisant le format CVRF, l'échange et le traitement de l'information peuvent être accélérés.

Importer des données Common Vulnerability Reporting Framework via l'importation de fichiers

Importez un fichier CVRF pour afficher les données au format CVRF. L'importation est une activité ponctuelle.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé), ou admin.

Pourquoi et quand exécuter cette tâche

Une fois importée, une entrée de file d'attente est créée avec une pièce jointe, qui est analysée lors du traitement de l'entrée. Les données sont ensuite renseignées dans les tables respectives. Avant d'analyser les données CVRF, un enregistrement de mappage d'analyse est créé en fonction de la configuration. Ensuite, les données de mappage du scanner sont transformées en données de mappage des fournisseurs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre de travail Vulnerability Response commun**.
2. Cliquez sur **Importer le fichier**.

   Remarque : Vous ne pouvez charger qu'un seul fichier XML à la fois avec une taille de fichier maximale de 1 Go.

3. Dans le champ **Nom** , saisissez un nom unique pour l'intégration.
   Le planificateur est créé avec ce nom.
4. Dans le champ **Fournisseur** , saisissez son nom.
   Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
5. Cliquez sur **Terminer**.

Résultats

Une file d'attente d'importation est créée. Cliquez sur le lien dans la barre d'informations pour afficher les entrées de file d'attente du fournisseur ainsi que la liste connexe. Vous pouvez également afficher l'état de la tâche.

Une fois les données importées au format CVRF, elles sont traitées de la manière suivante :

1. Lorsque la file d'attente est traitée, le fichier est analysé avec une source de données dédiée.
2. Une fois le traitement terminé, le journal de l'application est mis à jour.
3. Une fois le fichier XML CVRF analysé, il remplit les tables suivantes dans l'application ServiceNow® Réponse aux vulnérabilités .
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

Vous pouvez consulter les informations détaillées relatives aux erreurs ou aux exceptions dans les journaux d'application.

Configurer les alias de connexion et d'informations d'identification

Configurez les alias de connexion et d'informations d'identification pour authentifier les fournisseurs. Lors de l'analyse consultative, les fournisseurs tiers sont authentifiés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Procédure

1. Créez une authentification OAuth.
   Reportez-vous à la section Créer un point de terminaison pour que les clients accèdent à l'instance .
2. Créez un alias de connexion et d'informations d'identification.
   Reportez-vous à la section Créer un alias de connexion et d'informations d'identification .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Créez une connexion.
   a. Cliquez sur le nom de l'alias de connexion et d'informations d'identification nouvellement créé.
   b. Sous l'onglet **Connexions** , cliquez sur **Nouveau**.
   c. Si le type d'authentification est OAuth, sélectionnez le profil du registre d'application créé à l'étape 1 en tant que **profil d'entité OAuth**.
   d. Créez un enregistrement dans Connexions à partir de la liste connexe de l'enregistrement.
   e. Dans le champ **Informations d'identification** , sélectionnez l'enregistrement d'informations d'identification créé à l'étape 3D.
   f. Dans le champ **URL de connexion** , saisissez l'URL du fournisseur.
   g. Cliquez sur **Envoyer**.

Configurer un fournisseur commun de Vulnerability Reporting Framework autre que Cisco

Configurez un fournisseur CVRF (Common Vulnerability Reporting Framework) autre que Cisco avec prise en charge de l'API.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé), ou admin

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Connexion et information d'identification** > **Alias de connexion et d'informations d'identification**.
2. Créez un enregistrement avec le type d'authentification pris en charge par le fournisseur. Pour en savoir plus sur l'authentification d'un fournisseur, reportez-vous à la section Configurer les alias de connexion et d'informations d'identification.
3. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Concepteur de flux**.
4. Dupliquez le flux appelé « Analyse consultative ».

   Remarque :
   - Si l'une des actions doit être modifiée, copiez-la et utilisez-la dans le nouveau flux.
   - Mettre à jour la logique liée à la pagination selon le fournisseur

5. Si la logique de paramètre de plage de dates n'est pas la même que celle de Cisco, copiez l'action **Mettre à jour les paramètres de pagination** et apportez les modifications requises pour le fournisseur.
6. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Mappages des données d'enrichissement**.
7. Créez un enregistrement selon Cisco en modifiant la valeur de **clé de propriété** selon le fournisseur.
   Cette logique permet de mapper les champs obligatoires d'une charge utile consultative à une ServiceNow table.
8. Mappez les balises API suivantes à partir de la charge utile de l'API.
   Ces balises doivent être mappées avec des détails à renseigner dans la table de mappage des données d'enrichissement. Par défaut, le mappage spécifique à Cisco est envoyé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous devez créer un enregistrement si vous devez configurer plusieurs fournisseurs qui publient des avis.

Balise de charge utile consultative	Colonne de la table sn_vul_cvrf_solution_integration_u	Description
URL de CVRF	cvrf_url	Nom de balise qui contient l'URL de CVRF.
ID consultatif (clé unique pour la réponse)	ID	Nom de balise qui contient un identificateur unique.
Dernière date modifiée	last_modified_date	Nom de balise qui contient la date à laquelle l'enregistrement a été mis à jour pour la dernière fois.
securityAdvisoryIntegrationSysId	Intégration	Fait référence au sysId de la tâche planifiée d'intégration, qui crée les enregistrements de solution de vulnérabilité.

9. En fonction du format de la réponse, modifiez la logique d'analyse en copiant l'action **Récupérer la liste** du flux d'analyse consultatif.

Importer des données Common Vulnerability Reporting Framework à partir d'avis

Importez des données CVRF à partir d'avis en configurant l'URL du fournisseur avec le type d'importation API.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Pourquoi et quand exécuter cette tâche

Lorsque l'intégration s'exécute, les avis sont récupérés. L'URL CVRF et l'ID des avis sont extraits de la charge utile. Les appels d'API REST sont effectués pour chaque URL CVRF, et les données sont analysées et stockées dans la table sn_vul_solution.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre de travail Vulnerability Response commun**.
2. Cliquez sur **Ajouter une intégration**.
3. Renseignez les champs du formulaire.

Formulaire Avis sur les solutions d'importation

Champ	Description
Type d'importation	Option permettant de sélectionner le type d'importation. Sélectionnez **API.**
Nom	Nom unique pour l'intégration.
Fournisseur	Nom du fournisseur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
Alias de connexion	Option permettant de sélectionner des informations d'identification authentifiées. **Remarque :** La table sys_alias stocke les informations d'identification et l'URL de base pour les avis.
Calendrier	Fréquence à laquelle les données doivent être mises à jour.
Jour	Jour de la semaine où vous souhaitez que les données soient mises à jour.
Heure	Moment de la semaine où vous souhaitez que les données soient mises à jour.
Configuration de l'API	
Flux	Option permettant de sélectionner le flux. Le flux est déclenché lors de l'exécution du planificateur. Le flux se charge d'analyser les avis et extrait l'URL CVRF et stocke ces détails dans les tables de mise à jour. Vous pouvez copier le flux existant et le modifier selon vos besoins. Par exemple, vous pouvez apporter des modifications liées à la pagination.
Action de flux	Option permettant de sélectionner l'action de flux. Les actions de flux prennent en charge l'aptitude de fenêtre glissante. Vous pouvez mettre à jour les actions de flux et ajouter le paramètre de requête directement à l'action en les faisant glisser.
Table de mappage	Option permettant de sélectionner la table de mappage. L'enregistrement de la table de mappage des données d'enrichissement est utilisé pour extraire l'URL CVRF et l'ID consultatif de la charge utile des avis.
Conseils à partir de la réponse	Option permettant d'entrer le nom de la balise à partir de la charge utile des avis à partir de laquelle la liste des avis peut être extraite.
Critère de filtre	

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Paramètres de plage horaire	Option permettant de sélectionner la plage horaire pour la demande et le format de date pour les appels d'API. Date de début/date de fin Le paramètre de demande est le nom de paramètre utilisé pour la date de début et la date de fin lors des appels d'API. Par exemple, StartDate, start_date, endDate, end_date.
Format de date	Option permettant d'entrer le format de la date, par exemple, `mm/jj/aaaa`. Le format de date est le format dont l'API a besoin pour le filtrage. Les formats qui ne sont pas pris en charge par GlideDate ne fonctionnent pas.
Plage initiale en jours	Eles jours pour lesquels les données doivent être extraites lors de la première exécution du planificateur. Pour les exécutions suivantes, le mécanisme de la fenêtre coulissante est suivi. **Remarque :** Si vous ne souhaitez pas sélectionner de plage horaire, sélectionnez **Aucun paramètre**.
Mappages des analyses	
Source de l'analyse	Option permettant de sélectionner la source de l'entrée tierce (TPE).
Colonne de vulnérabilité	Option permettant de sélectionner le mot clé.
Mots clés	Option permettant d'entrer le mot clé pour rechercher la colonne de vulnérabilité sélectionnée.

4. Cliquez sur **Terminer**.

Importer des données CVRF (Common Vulnerability Reporting Framework) via l'URL CVRF

Importez des données CVRF en configurant l'URL du fournisseur dans l'Assistant de configuration.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Pourquoi et quand exécuter cette tâche

Lorsque l'intégration s'exécute, les données sont extraites de l'URL qui est analysée. Les données sont ensuite stockées dans la table sn_vul_solution avec source comme nom de fournisseur.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Oracle publie directement l'URL CVRF pour fournir des solutions. Par conséquent, si vous souhaitez configurer l'intégration pour l'importation de données Oracle, assurez-vous que vous disposez de l'URL CVRF pour Oracle et suivez les étapes suivantes.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre de travail Vulnerability Response commun**.
2. Cliquez sur **Ajouter une intégration**.
3. Renseignez les champs du formulaire.

Formulaire d'importation CVRF

Champ	Description
Type d'importation	Type d'importation. Sélectionnez **une URL.**
Nom	Nom unique pour l'intégration.
Fournisseur	Nom du fournisseur. **Remarque :** Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
URL	URL à partir de laquelle vous souhaitez extraire les données de la solution au format CVRF.
Calendrier	Fréquence à laquelle les données doivent être mises à jour. **Remarque :** Si la balise d'état de CVRF indique « FINAL », le champ est automatiquement défini sur **Sur demande** pour éviter les exécutions inutiles.
Jour	Jour de la semaine où vous souhaitez que les données soient mises à jour.
Heure	Moment de la semaine où vous souhaitez que les données soient mises à jour.

4. Cliquez sur **Terminer**.

Dépannage de l'importation de données de Common Vulnerability Reporting Framework

Les actions de dépannage peuvent aider à résoudre les problèmes courants lors de l'importation de données CVRF dans l'application Vulnerability Response.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Problème	Action
La durée d'exécution de l'intégration est longue	Si l'intégration s'exécute pendant une période plus longue que prévu, procédez comme suit : **1.** Accédez à la table sn_vul_ds_import_q_entry. **2.** **Regrouper** par le champ État. Vous pouvez voir les entrées qui sont à l'état Terminé, En cours ou En file d'attente.
Échec de l'intégration dans l'importation basée sur l'API	Si l'intégration échoue lors de l'importation basée sur l'API, procédez comme suit : **1.** Accédez à **Concepteur de flux**. **2.** Ouvrez le flux sélectionné dans la configuration. **Remarque :** Dans le cas de Cisco, ouvrez le flux d'analyse consultative. **3.** Cliquez sur **Exécutions**. **4.** Ouvrez la dernière exécution ou l'exécution qui doit être déboguée. **5.** Vérifiez le flux à chaque étape.
Échec de l'intégration dans l'importation basée sur l'API avec une erreur de délai d'expiration	Si l'intégration échoue dans une importation basée sur une API en raison d'un délai d'expiration dans le flux d'analyse consultatif, procédez comme suit : **1.** Augmentez le délai d'expiration en ouvrant `sys_properties. LISTE.` **2.** Dans la colonne Nom, recherchez `sn_vul. CVRFFlowTimeout (inMilliSeconds).` **Remarque :** Le temps est exprimé en millisecondes. **3.** Ouvrez l'enregistrement et mettez à jour la valeur avec un grand nombre. **4.** Enregistrez l'enregistrement et réexécutez l'intégration.
Échec de l'intégration avec l'erreur « Le mappage du scanner vers la transformation des données de mappage des fournisseurs est en cours »	Vérifiez si l'intégration échoue pendant l'importation basée sur l'URL ou l'API, avec l'erreur suivante : `La transformation du mappage du scanner vers les données de mappage du fournisseur est en cours. Les données ne sont renseignées qu'une fois la`

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Problème	Action
	`transformation terminée. Essayez d'exécuter après un certain temps.` Si vous rencontrez cette erreur, patientez un certain temps et exécutez à nouveau l'intégration.
La file d'attente d'importation n'est pas créée pendant l'importation du fichier	Lors de l'importation d'un fichier, il arrive que la file d'attente d'importation ne soit pas créée. Cet échec signifie que la transformation qui mappe les données de mappage de l'analyseur aux données de mappage des fournisseurs est en cours. L'entrée de file d'attente est créée une fois le processus terminé.

Cadre consultatif de sécurité commun (CSAF)

Lorsqu'il est utilisé avec Gestion des solutions pour vulnérabilités, le Cadre de travail consultatif de sécurité commun (CSAF) permet d'automatiser les notifications de sécurité via un format JSON lisible par machine.

CSAF vous permet de vous intégrer à n'importe quel fournisseur d'intelligence de solution à l'aide du cadre de travail de gestion de solution pour importer les données d'intelligence. Les notifications de sécurité de la CSAF peuvent être de l'un des types suivants.

- Avis de sécurité
- Échange d'exploitabilité des vulnérabilités (VEX)
- Réponse aux incidents de sécurité
- Avis informatif

Le CSAF ne prend en charge que les importations de fichiers, d'URL et d'API d'avis de sécurité des fournisseurs.

Importer des données de Cadre de travail consultatif de Security commun via l'importation de fichiers

Importez un fichier CSAF pour afficher les données au format CSAF. L'importation est une activité ponctuelle.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé), ou admin

Pourquoi et quand exécuter cette tâche

Une fois importée, une entrée de file d'attente est créée avec une pièce jointe, qui est analysée lors du traitement de l'entrée. Les données sont ensuite renseignées dans les tables respectives. Avant d'analyser les données CSAF, un enregistrement de mappage de scanner est créé en fonction de la configuration. Ensuite, les données de mappage du scanner sont transformées en données de mappage des fournisseurs.

Le mappage de l'analyse ne s'applique pas aux vulnérabilités basées sur la base de données de vulnérabilités nationale (NVD), qui sont des vulnérabilités avec une entrée de vulnérabilité commune (CVE) dans la base de données NVD.

Si vous n'avez qu'une seule solution de remplacement la plus élevée et qu'elle se déploie jusqu'aux éléments vulnérables, la solution privilégiée est renseignée. Lorsque plusieurs

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

solutions de fournisseur sont incluses dans une entrée NVD, la solution privilégiée n'est pas renseignée, car il y a plus d'une solution de remplacement la plus élevée. Dans ce cas, vous devez sélectionner manuellement une solution. Pour les vulnérabilités tierces, la solution privilégiée n'est renseignée que si vous ajoutez le mappage d'analyse correspondant.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre consultatif de Security commun**.
2. Sélectionnez **Importer le fichier**.

   Remarque : Vous ne pouvez charger qu'un seul fichier JSON à la fois avec une taille de fichier maximale de 15 Mo.

3. Dans le champ **Nom** , saisissez un nom unique pour l'intégration.
   Le planificateur est créé avec ce nom.
4. Dans le champ **Fournisseur** , saisissez son nom.
   Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
5. Sélectionnez **Finish** (Terminer).

Résultats

Une file d'attente d'importation est créée. Sélectionnez le lien dans la barre d'informations pour afficher les entrées de file d'attente du fournisseur ainsi que la liste connexe. Vous pouvez également afficher l'état de la tâche.

Une fois les données importées au format CSAF, elles sont traitées de la manière suivante :

1. Lorsque la file d'attente est traitée, le fichier est analysé avec une source de données dédiée.
2. Une fois le traitement terminé, le journal de l'application est mis à jour.
3. Une fois le fichier JSON CSAF analysé, il renseigne les tables suivantes dans l'application ServiceNow® Réponse aux vulnérabilités .
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

Vous pouvez consulter les informations détaillées relatives aux erreurs ou aux exceptions dans les journaux d'application.

Configurer les alias de connexion et d'informations d'identification pour le Cadre de travail consultatif de sécurité commun (CSAF)

Configurez les alias de connexion et d'informations d'identification pour authentifier les fournisseurs. Lors de l'analyse consultative, les fournisseurs tiers sont authentifiés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Créez une authentification OAuth.
   Reportez-vous à la section Créer un point de terminaison pour que les clients accèdent à l'instance .
2. Créez un alias de connexion et d'informations d'identification.
   Reportez-vous à la section Créer un alias de connexion et d'informations d'identification .
3. Créez une connexion.
   a. Sélectionnez le nom de l'alias de connexion et d'informations d'identification nouvellement créé.
   b. Sous l'onglet **Connexions** , sélectionnez **Nouveau**.
   c. Si le type d'authentification est OAuth, sélectionnez le profil du registre d'application créé à l'étape 1 en tant que **profil d'entité OAuth**.
   d. Créez un enregistrement dans Connexions à partir de la liste connexe de l'enregistrement.
   e. Dans le champ **Informations d'identification** , sélectionnez l'enregistrement d'informations d'identification créé à l'étape 3D.
   f. Dans le champ **URL de connexion** , saisissez l'URL du fournisseur.
   g. Sélectionnez **Soumettre**.

Configurer un fournisseur de cadre de travail consultatif de sécurité commun autre que Red Hat

Configurez un fournisseur CSAF (Common Security Advisory Framework) autre qu'avec le support de l'API Red Hat .

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé), ou admin

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Connexion et information d'identification** > **Alias de connexion et d'informations d'identification**.
2. Créez un enregistrement avec le type d'authentification pris en charge par le fournisseur. Pour en savoir plus sur l'authentification d'un fournisseur, reportez-vous à la section Configurer les alias de connexion et d'informations d'identification pour le Cadre de travail consultatif de sécurité commun (CSAF).
3. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Concepteur de flux**.
4. Dupliquez le flux appelé « Analyse consultative ».

   Remarque :

   - Si l'une des actions doit être modifiée, copiez-la et utilisez-la dans le nouveau flux.
   - Examinez les paramètres de page_index_key et de page_size_key selon l'API du fournisseur.
   - Mettre à jour la logique liée à la pagination selon le fournisseur

5. Si la logique du paramètre de plage de dates n'est pas la même que Red Hat, copiez l'action **Mettre à jour les paramètres de pagination** et apportez les modifications requises pour le fournisseur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Mappages des données d'enrichissement**.
7. Créez un enregistrement en Red Hat modifiant la valeur de **clé de propriété** selon le fournisseur.
   Cette logique permet de mapper les champs obligatoires d'une charge utile consultative à une ServiceNow table.
8. Mappez les balises API suivantes à partir de la charge utile de l'API.
   Ces balises doivent être mappées avec des détails à renseigner dans la table de mappage des données d'enrichissement. Par défaut, le Red Hat mappage spécifique est envoyé.

   Remarque : Vous devez créer un enregistrement si vous devez configurer plusieurs fournisseurs qui publient des avis.

Balise de charge utile consultative	Colonne de la table sn_vul_cvrf_solution_integration_u	Description
URL CSAF (URL de ressource pointant vers la charge utile CSAF)	cvrf_url	Nom de balise qui contient l'URL CSAF.
ID consultatif (clé unique pour la réponse)	ID	Nom de balise qui contient un identificateur unique.
Dernière date modifiée	last_modified_date	Nom de balise qui contient la date à laquelle l'enregistrement a été mis à jour pour la dernière fois.
csaf (valeur statique)	advisory_format	Valeur de format consultatif pour les charges utiles CSAF. Notez qu'il s'agit d'une valeur statique applicable à toutes les intégrations CSAF.
securityAdvisoryIntegrationSysId	intégration	Fait référence au sysId de la tâche planifiée d'intégration, qui crée les enregistrements de solution de vulnérabilité.

9. En fonction du format de la réponse, modifiez la logique d'analyse en copiant l'action **Récupérer la liste** du flux d'analyse consultatif.

Importer des données du Cadre consultatif de Security commun à partir d'avis

Importez les données CSAF à partir des avis en configurant l'URL du fournisseur avec le type d'importation API.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Pourquoi et quand exécuter cette tâche
Lorsque l'intégration s'exécute, les avis sont récupérés. L'URL et l'ID des avis du CSAF sont extraits de la charge utile. Les appels d'API REST sont effectués pour chaque URL CSAF, et les données sont analysées et stockées dans la table sn_vul_solution.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le mappage de l'analyse ne s'applique pas aux vulnérabilités basées sur la base de données de vulnérabilités nationale (NVD), qui sont des vulnérabilités avec une entrée de vulnérabilité commune (CVE) dans la base de données NVD.

Si vous n'avez qu'une seule solution de remplacement la plus élevée et qu'elle se déploie jusqu'aux éléments vulnérables, la solution privilégiée est renseignée. Lorsque plusieurs solutions de fournisseur sont incluses dans une entrée NVD, la solution privilégiée n'est pas renseignée, car il y a plus d'une solution de remplacement la plus élevée. Dans ce cas, vous devez sélectionner manuellement une solution. Pour les vulnérabilités tierces, la solution privilégiée n'est renseignée que si vous ajoutez le mappage d'analyse correspondant.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre consultatif de Security commun**.
2. Sélectionnez **Ajouter une intégration**.
3. Renseignez les champs du formulaire.

Formulaire Avis sur les solutions d'importation

Champ	Description
Type d'importation	Option permettant de sélectionner le type d'importation. Sélectionnez **API.**
Nom	Nom unique pour l'intégration.
Fournisseur	Nom du fournisseur. **Remarque :** Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
Alias de connexion	Option permettant de sélectionner des informations d'identification authentifiées. **Remarque :** La table sys_alias stocke les informations d'identification et l'URL de base pour les avis.
Calendrier	Fréquence à laquelle les données doivent être mises à jour.
Jour	Jour de la semaine où vous souhaitez que les données soient mises à jour.
Heure	Moment de la semaine où vous souhaitez que les données soient mises à jour.
Configuration de l'API	
Flux	Option permettant de sélectionner le flux. Le flux est déclenché lors de l'exécution du planificateur. Le flux se charge d'analyser les avis et extrait l'URL CSAF et stocke ces détails dans les tables de mise à jour. Vous pouvez copier le flux existant et le

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	modifier selon vos besoins. Par exemple, vous pouvez apporter des modifications liées à la pagination.
Action de flux	Option permettant de sélectionner l'action de flux. Les actions de flux prennent en charge l'aptitude de fenêtre glissante. Vous pouvez mettre à jour les actions de flux et ajouter le paramètre de requête directement à l'action en les faisant glisser.
Table de mappage	Option permettant de sélectionner la table de mappage. L'enregistrement de la table de mappage des données d'enrichissement est utilisé pour extraire l'URL et l'ID consultatif de la CSAF à partir de la charge utile des avis.
Conseils à partir de la réponse	Option permettant d'entrer le nom de la balise à partir de la charge utile des avis à partir de laquelle la liste des avis peut être extraite.
Critère de filtre	
Paramètres de plage horaire	Option permettant de sélectionner la plage horaire pour la demande et le format de date pour les appels d'API. Date de début/date de fin Le paramètre de demande est le nom de paramètre utilisé pour la date de début et la date de fin lors des appels d'API. Par exemple, StartDate, start_date, endDate, end_date.
Format de date	Option permettant d'entrer le format de la date, par exemple, `mm/jj/aaaa`. Le format de date est le format dont l'API a besoin pour le filtrage. Les formats qui ne sont pas pris en charge par GlideDate ne fonctionnent pas.
Plage initiale en jours	Eles jours pour lesquels les données doivent être extraites lors de la première exécution du planificateur. Pour les exécutions suivantes, le mécanisme de la fenêtre coulissante est suivi. **Remarque :** Si vous ne souhaitez pas sélectionner de plage horaire, sélectionnez **Aucun paramètre**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mappages des analyses	
Source de l'analyse	Option permettant de sélectionner la source de l'entrée tierce (TPE).
Colonne de vulnérabilité	Option permettant de sélectionner le mot clé.
Mots clés	Option permettant d'entrer le mot clé pour rechercher la colonne de vulnérabilité sélectionnée.

4. Sélectionnez **Finish** (Terminer).

Importer des données du Cadre de travail consultatif de sécurité commun (CSAF) par le biais de l'URL CSAF

Importez les données CSAF en configurant l'URL du fournisseur dans l'assistant de configuration.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Pourquoi et quand exécuter cette tâche
Lorsque l'intégration s'exécute, les données sont extraites de l'URL qui est analysée. Les données sont ensuite stockées dans la table sn_vul_solution avec source comme nom de fournisseur.

Remarque : L'URL peut être soit une charge utile CSAF directe, qui contient les détails consultatifs, soit une URL de flux ROLIE (Resource-Oriented Lightweight Information Exchange). Dans les deux cas, la charge utile est analysée en conséquence et les enregistrements de solution sont créés. Pour importer l'URL CSAF, procédez comme suit.

Vous pouvez également importer des solutions de vulnérabilité à partir d'agrégateurs CSAF ou de fournisseurs de confiance via une importation d'URL qui prend en charge le flux ROLIE. Ces solutions de vulnérabilité sont automatiquement mappées au fournisseur approprié et aux éléments vulnérables (VIT) en fonction des vulnérabilités et expositions communes (CVE).

Le mappage de l'analyse ne s'applique pas aux vulnérabilités basées sur la base de données de vulnérabilités nationale (NVD), qui sont des vulnérabilités avec une entrée de vulnérabilité commune (CVE) dans la base de données NVD.

Si vous n'avez qu'une seule solution de remplacement la plus élevée et qu'elle se déploie jusqu'aux éléments vulnérables, la solution privilégiée est renseignée. Lorsque plusieurs solutions de fournisseur sont incluses dans une entrée NVD, la solution privilégiée n'est pas renseignée, car il y a plus d'une solution de remplacement la plus élevée. Dans ce cas, vous devez sélectionner manuellement une solution. Pour les vulnérabilités tierces, la solution privilégiée n'est renseignée que si vous ajoutez le mappage d'analyse correspondant.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre consultatif de Security commun**.
2. Sélectionnez **Ajouter une intégration**.
3. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire d'importation CSAF

Champ	Description
Type d'importation	Type d'importation. Sélectionnez **une URL.**
Nom	Nom unique pour l'intégration.
Fournisseur unique	Sélectionnez cette option si vous importez CSAF d'un seul fournisseur.
Fournisseur	Nom du fournisseur. Ce champ n'est disponible que si vous sélectionnez **Fournisseur unique**. **Remarque :** Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
Multi-fournisseur	Sélectionnez cette option si vous importez CSAF à partir de plusieurs fournisseurs.
Agrégateur	Un fournisseur de confiance dont vous pouvez importer la solution.
URL	URL à partir de laquelle vous souhaitez extraire les données de la solution au format CSAF.
Calendrier	Fréquence à laquelle les données doivent être mises à jour. **Remarque :** Si la balise d'état du CSAF indique « FINAL », le champ est automatiquement défini sur **Sur demande** pour éviter les exécutions inutiles.
Jour	Jour de la semaine où vous souhaitez que les données soient mises à jour.
Heure	Moment de la semaine où vous souhaitez que les données soient mises à jour.
Mappages des analyses **Remarque :** La section Mappages des scanners est facultative pour CSAF.	
Source de l'analyse	Option permettant de sélectionner la source de l'entrée tierce (TPE).
Colonne de vulnérabilité	Option permettant de sélectionner le mot clé.
Mots clés	Option permettant d'entrer le mot clé pour rechercher la colonne de vulnérabilité sélectionnée.

4. Sélectionnez **Finish** (Terminer).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage de l'importation de données du Cadre consultatif de Security commun

Les actions de dépannage peuvent aider à résoudre les problèmes courants lors de l'importation de données CSAF dans l'application Vulnerability Response.

Problème	Action
La durée d'exécution de l'intégration est longue	Si l'intégration s'exécute pendant une période plus longue que prévu, procédez comme suit : **1.** Accédez à la table sn_vul_ds_import_q_entry. **2.** **Regrouper** par le champ État. Vous pouvez voir les entrées qui sont à l'état Terminé, En cours ou En file d'attente.
Échec de l'intégration dans l'importation basée sur l'API	Si l'intégration échoue lors de l'importation basée sur l'API, procédez comme suit : **1.** Accédez à **Concepteur de flux**. **2.** Ouvrez le flux sélectionné dans la configuration. **Remarque :** Dans le cas de Red Hat, ouvrez le flux d'analyse consultative. **3.** Sélectionnez **Exécutions**. **4.** Ouvrez la dernière exécution ou l'exécution qui doit être déboguée. **5.** Vérifiez le flux à chaque étape.
Échec de l'intégration dans l'importation basée sur l'API avec une erreur de délai d'expiration	Si l'intégration échoue dans une importation basée sur une API en raison d'un délai d'expiration dans le flux d'analyse consultatif, procédez comme suit : **1.** Augmentez le délai d'expiration en ouvrant `sys_properties. LISTE.` **2.** Dans la colonne Nom, recherchez `sn_vul. CVRFFlowTimeout (inMilliSeconds).` **Remarque :** Le temps est exprimé en millisecondes. **3.** Ouvrez l'enregistrement et mettez à jour la valeur avec un grand nombre. **4.** Enregistrez l'enregistrement et réexécutez l'intégration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Problème	Action
Échec de l'intégration avec l'erreur « Le mappage du scanner vers la transformation des données de mappage des fournisseurs est en cours »	Vérifiez si l'intégration échoue pendant l'importation basée sur l'URL ou l'API, avec l'erreur suivante : `La transformation du mappage du scanner vers les données de mappage du fournisseur est en cours. Les données ne sont renseignées qu'une fois la transformation terminée. Essayez d'exécuter après un certain temps.` Si vous rencontrez cette erreur, patientez un certain temps et exécutez à nouveau l'intégration.
La file d'attente d'importation n'est pas créée pendant l'importation du fichier	Lors de l'importation d'un fichier, il arrive que la file d'attente d'importation ne soit pas créée. Cet échec signifie que la transformation qui mappe les données de mappage de l'analyseur aux données de mappage des fournisseurs est en cours. L'entrée de file d'attente est créée une fois le processus terminé.

Tâches d'installation et de configuration supplémentaires Réponse aux vulnérabilités

Pour vous aider à y remédier, vous pouvez effectuer ces tâches de configuration administrative supplémentaires dans le cadre de votre configuration en dehors de la configuration de base. Vous effectuez ces tâches en dehors de l'Assistant de configuration.

Vous pouvez utiliser les rapports par défaut fournis pour Réponse aux vulnérabilités superviser votre posture de sécurité. Vous pouvez modifier ces rapports s'ils ne conviennent pas à votre environnement ou les utiliser comme modèles pour créer les vôtres.

Si l'application Analyse des performances pour Réponse aux vulnérabilités est installée, vous pouvez créer des rapports, des tableaux de bord réactifs, etc. Pour plus d'informations, reportez-vous à la section Mise en route des rapports .

Les notifications par e-mail augmentent la productivité et fluidifient le flux de travail.

Avec l'évaluation de l'exposition logicielle, recherchez l'éditeur, le nom du produit et le numéro de version dans Gestion des actifs logiciels (SAM Foundation) pour déterminer votre exposition aux logiciels vulnérables.

La visibilité sur les bibliothèques de vulnérabilités peut offrir une flexibilité pour les tâches de regroupement et de correction.

Configurez la gestion des exceptions pour vous aider lorsque votre organisation ne peut pas se conformer à une politique, une norme ou un guide de sécurité ou de gestion des vulnérabilités publié, vous pouvez demander une exception.

Pour d'autres tâches de configuration supplémentaires, consultez les rubriques qui suivent cette vue d'ensemble.

Tests de démarrage rapide pour Réponse aux vulnérabilités

Validez que Réponse aux vulnérabilités fonctionne toujours après avoir apporté un changement de configuration telle que l'application d'une mise à niveau ou le

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

développement d'une application. Copiez et personnalisez ces tests de démarrage rapide à effectuer lorsque vous utilisez des données spécifiques à votre instance.

La propriété d'exécution du test est désactivée par défaut pour empêcher l'exécution de tests sur un système de production. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production. Pour Exécuter la suite de tests Infrastructure de tests automatisés (ATF) pour Réponse aux vulnérabilités plus d'informations sur la configuration et l'exécution de la suite de tests pour Réponse aux vulnérabilités.

Les tests de démarrage rapide Réponse aux vulnérabilités nécessitent l'activation de l'application Réponse aux vulnérabilités (sn_vul) et le chargement des données de démonstration.

Tests Réponse aux vulnérabilités

Test	Description	Version
VR : créer une règle de cible de rattrapage	Créez une règle de cible de rattrapage.	Madrid
VR : créer une règle de groupe de vulnérabilité	Créer une règle de groupe de vulnérabilité.	Madrid
VR : créer un élément vulnérable via le formulaire	Déterminez si un utilisateur peut créer un élément vulnérable à partir du formulaire d'élément vulnérable.	Madrid
VR : cycle de vie du groupe de vulnérabilités	Déterminez si un utilisateur peut résoudre un groupe de vulnérabilités.	Madrid
VR : cycle de vie d'un élément vulnérable	Déterminez si un utilisateur peut faire évoluer un élément vulnérable tout au long de son cycle de vie, et déterminez si un élément vulnérable fermé peut être rouvert.	Madrid
VR : calculateur de déploiement	Déterminez si le calculateur de risque de déploiement peut fournir un score de risque global pour un groupe entier d'éléments vulnérables en utilisant les scores de tous les éléments vulnérables d'un groupe de vulnérabilité.	New York
VR : règles d'affectation de Réponse aux vulnérabilités	Déterminez si un exemple d'ensemble de règles d'affectation peut affecter automatiquement des éléments vulnérables à un	New York

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests Réponse aux vulnérabilités (suite)

Test	Description	Version
	groupe d'affectation pour la correction.	
VR : calculateurs de vulnérabilité	Testez les calculateurs de vulnérabilité.	New York
VR : recherche de CI - Qualys	Créez une nouvelle règle de recherche avec la méthode « field_matching » appelée « Rechercher par adaptateur réseau » pour Qualys. Déterminez si un élément de configuration est apparié avec succès dans la table Élément détecté par adaptateur réseau et adresse IP avec la nouvelle règle de recherche.	Orlando
VR : créer une demande de changement normal et urgent	Déterminez si l'utilisateur peut créer avec succès des demandes de changement normal et urgent depuis un groupe de vulnérabilité.	Orlando
VR : diviser un groupe de vulnérabilité	Déterminez si l'utilisateur peut diviser avec succès un groupe de vulnérabilité.	Orlando
VR : mettre à jour l'état d'un VG lorsqu'un CHG est annulé.	Déterminez si le champ État d'un groupe de vulnérabilité se modifie correctement lorsqu'une demande de changement associée au groupe de vulnérabilité est annulée.	Orlando
VR : mettre à jour l'état d'un VG lorsqu'un CHG passe à l'état Réviser.	Déterminez si le champ État d'un groupe de vulnérabilité se modifie correctement lorsqu'une demande de changement qui y est associée passe à l'état Réviser.	Orlando
VR : recherche de CI - Rapid7	Testez la recherche de CI à l'aide de la règle de recherche existante Intégration des vulnérabilités Rapid7, **adresse IP**.	Orlando
VR : recherche de CI - Qualys	Testez la recherche de CI en créant une règle de recherche pour Qualys Vulnerability Integration	Orlando

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests Réponse aux vulnérabilités (suite)

Test	Description	Version
VR : workflow d'approbation des exceptions pour VI	Créez une demande d'exception et vérifiez que le processus d'approbation fonctionne.	Orlando
VR : workflow d'approbation des faux positifs pour VI	Créez une demande d'exception pour les faux positifs et vérifiez que le processus d'approbation fonctionne.	Orlando
VR : Réponse aux vulnérabilités des applications (AVR)	Déterminez si vos règles et calculateurs fonctionnent correctement. Vérifiez que les mises à jour fonctionnent.	Orlando
Règles de cibles de remédiation : test d'importation VI	Teste les règles de cibles de remédiation VR pendant l'importation.	Paris
VR : règle de classification	Exemple de règle de classification qui classifie automatiquement une vulnérabilité.	Tokyo

Information associée

Tests de démarrage rapide

Exécuter la suite de tests Infrastructure de tests automatisés (ATF) pour Réponse aux vulnérabilités

Exécutez la suite de tests Infrastructure de tests automatisés (ATF) après avoir installé ou mis à niveau l'application Réponse aux vulnérabilités .

Avant de commencer

Confirmez que l'installation s'est déroulée correctement et que votre instance fonctionne comme prévu.

La propriété d'exécution du test est désactivée par défaut pour empêcher l'exécution de tests sur un système de production. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production.

- Vérifiez que vous avez installé les données de démonstration lors de l'installation de Réponse aux vulnérabilités. Des données de démonstration sont nécessaires pour exécuter la Réponse aux vulnérabilités suite de tests.
- Pour activer le test, procédez comme suit :

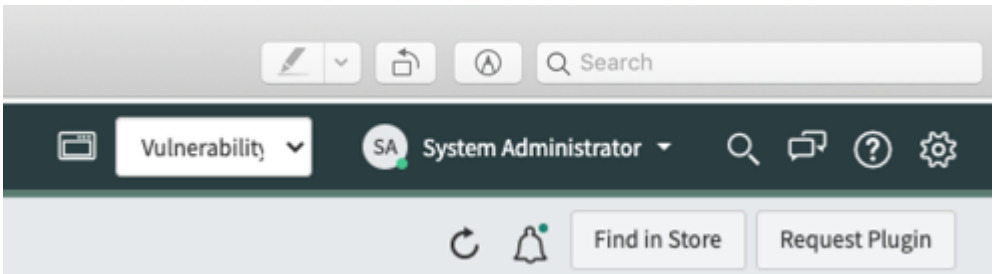
  1. Accédez à la **Tout** > **Framework de tests automatisés (ATF)** > **Administration** > **Propriétés**.
  2. Si elle n'est pas cochée, cochez la case **Activer l'exécution du test/de la suite de tests** .
  3. Cliquez sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Si le champ d'application n'est pas défini sur **Vulnerability Response** dans l'en-tête, ou s'il n'est pas affiché dans l'en-tête, cliquez sur l'icône des paramètres en haut de la page dans la fenêtre du navigateur .
5. Dans la fenêtre Paramètres système, cliquez sur **Développeur**.
6. Si cette option n'est pas sélectionnée, cliquez sur **Afficher le sélecteur d'application dans l'en-tête** et fermez la fenêtre.
7. Dans la liste qui s'affiche en regard de `Administrateur système`, cliquez sur **Vulnerability Response** pour le champ.

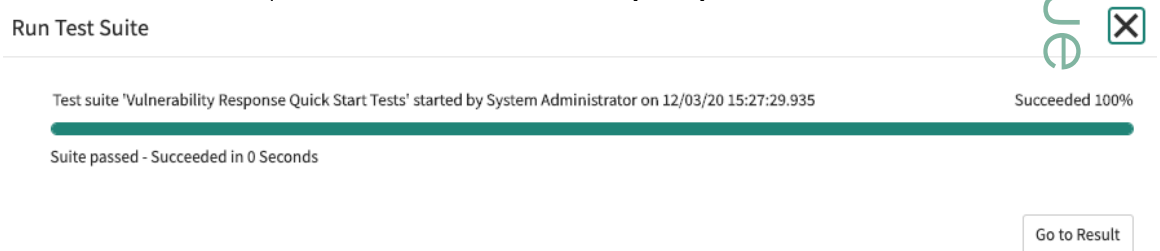
   Le champ s'affiche comme illustré dans l'image suivante.



Rôle requis : admin ou atf_test_admin

Procédure

1. Accédez à la **Tout** > **Framework de tests automatisés (ATF)** > **Suites**.
2. Dans la liste Suites de tests, localisez **les tests de démarrage rapide de Vulnerability Response**.
3. Sélectionnez-la pour ouvrir l'enregistrement.
4. Dans l'enregistrement ouvert, cochez la case **Actif** .
5. Cliquez sur **Mettre à jour**.
6. Si le bouton **Exécuter la suite de tests** n'est pas affiché, actualisez votre écran, ouvrez à nouveau l'enregistrement et cliquez sur **Exécuter la suite de tests** pour démarrer le test. Au bout de quelques instants, la boîte de dialogue Exécuter la suite de tests indique que le test a réussi. Cliquez sur **Accéder au résultat pour plus d'informations** .



Que faire ensuite

Félicitations ! Vous pouvez poursuivre la configuration de Réponse aux vulnérabilités.

Pour plus d'informations sur les tests automatisés et Réponse aux vulnérabilités les tests automatisés, les suites de tests et la création de tests automatisés, consultez Infrastructure de tests automatisés (ATF).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer Recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités

Installez Recommandations d'affectation de vulnérabilité de manière à réduire le temps que vous consacrez à l'identification des propriétaires des résultats de vulnérabilité qui ne sont pas affectés ou qui sont affectés de manière incorrecte. Cette application est disponible sous forme d'abonnement distinct dans le ServiceNow Store.

Avant de commencer

Avant d'exécuter la Recommandations d'affectation de vulnérabilité fonctionnalité dans Réponse aux vulnérabilités votre Now Platform® instance, vous devez d'abord télécharger et installer l'application Recommandations d'affectation de vulnérabilité for Réponse aux vulnérabilités . Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Pour plus d'informations, voir Activer une application ServiceNow Store.

Rôles requis : admin

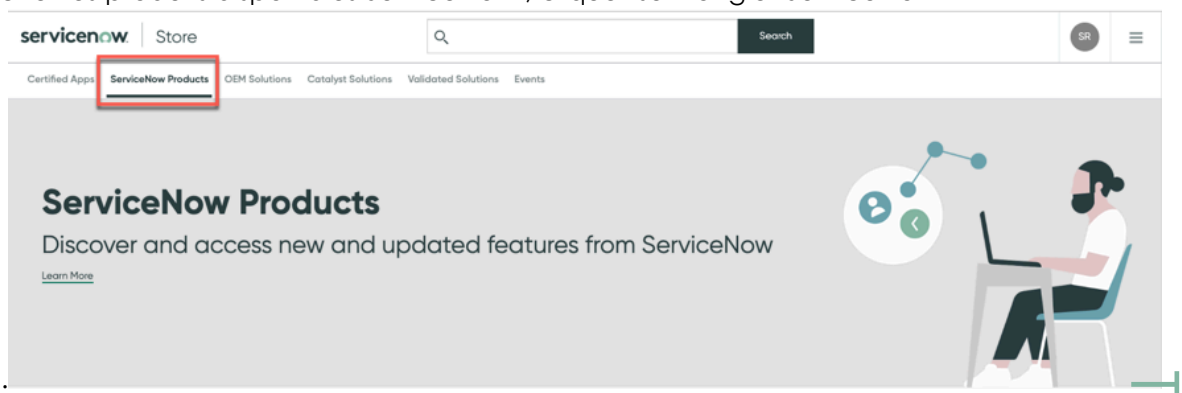
Tâches de configuration	Action
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Accédez à la **Tout** > **Applications système** > **Toutes les applications** > **Installé dans votre instance**. Réponse aux vulnérabilités s'affiche dans cette liste s'il est installé. Si l'application n'est pas installée et activée, reportez-vous à la section Installer Réponse aux vulnérabilités.
Vérifiez que l'application Intelligence prédictive est installée et activée.	Accédez à la **Applications système** > **Toutes les applications** > **Installé dans votre instance**. Intelligence prédictive s'affiche dans cette liste s'il est installé. Si l'application n'est pas installée et activée, reportez-vous à la section Installer Intelligence prédictive .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Vérifiez que vous disposez des rôles requis suivants pour l'installation et la vérification des résultats attendus : • vulnerability_admin : requise pour activer et configurer Recommandations d'affectation de vulnérabilité. Vous pouvez également l'utiliser pour afficher et sélectionner des recommandations d'affectation pour les éléments vulnérables et les tâches de rattrapage. • ServiceNow admin : requis pour installer des applications.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez au ServiceNow Store.
2. Cliquez sur **Se connecter** et saisissez vos informations d'identification HI.
3. Pour afficher les produits disponibles ServiceNow , cliquez sur l'onglet ServiceNow **Produits** .



4. Pour afficher toutes les applications associées auxquelles Recommandations d'affectation de vulnérabilitévous avez droit, cliquez sur le Réponse aux vulnérabilités produit.

   La page répertorie toutes les applications auxquelles vous êtes éligible si vous optez. Pour plus d'informations sur une application, cliquez sur le lien de la demande.

5. Pour vérifier que vous avez droit à Recommandations d'affectation de vulnérabilité, cliquez sur **Accepter**.
6. Pour accepter les termes et conditions, à l'invite, cochez la case et cliquez sur **Accepter**. Un message s'affiche qui indique que vous avez adhéré avec succès à l'application.
7. Passez à l'étape 10 pour installer l'application sur votre Now Platform instance.
8. Facultatif : Si vous souhaitez gérer votre autorisation pour l'application Recommandations d'affectation de vulnérabilité sur d'autres Now Platform instances, cliquez sur **Gérer les autorisations**.

   Remarque :

   Si le bouton **Gérer l'autorisation** n'est pas affiché, cliquez sur l'application Recommandations d'affectation de vulnérabilité dans la liste de produits pour l'afficher.

   a. Choisissez une option.

   b. Cliquez sur **OK** ou **Annuler** pour continuer.
   Vous êtes prêts à activer les modules d'extension et à installer l'application sur vos Now Platform instances.

9. Connectez-vous à l'instance Now Platform sur laquelle vous souhaitez installer l'application Recommandations d'affectation de vulnérabilité .
10. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
11. Dans les applications répertoriées, localisez l'application Recommandations d'affectation de vulnérabilité (sn_vul_recom) et cliquez sur **Installer**.
    La boîte de dialogue Installation de l'application s'affiche et toutes les dépendances installées s'affichent.
12. Facultatif : Si vous souhaitez des données de démonstration, cochez la case **Charger les données de démonstration** et cliquez sur **Installer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous ne cochez pas la case **Charger les données de démonstration** , les données de démonstration ne peuvent pas être installées ultérieurement à partir d'Application Manager. Pour plus d'informations sur l'installation ou la réinstallation de données de démonstration après l'installation initiale, consultez l'article Solution de contournement pour installer des données de démonstration si l'application est déjà installée [KB0722909] dans la base de Now Support connaissances.

Cette installation peut prendre un certain temps. Un message s'affiche dans la boîte de dialogue Installer une fois l'application et ses dépendances installées.

13. Cliquez sur **Fermer**.
14. Pour configurer Recommandations d'affectation de vulnérabilité, reportez-vous à la section Configurer les recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités.

Configurer les recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités

Activez cette option Recommandations d'affectation de vulnérabilité pour réduire le temps que vous consacrez à l'identification des propriétaires des résultats de vulnérabilité non affectés ou incorrectement affectés.

Avant de commencer
Rôle requis : sn_vul.manage_assignment_recom_config

Pourquoi et quand exécuter cette tâche
Cette application n'est pas activée par défaut.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Recommandations d'affectation**.
2. Sélectionnez **Activer les recommandations d'affectation**.
   Le **champ Définition de la solution Intelligence prédictive** s'affiche. La valeur par défaut est **Affectation d'éléments vulnérables**.
3. Cliquez sur **Enregistrer**.

Créer et former une définition de solution pour Réponse aux vulnérabilités

Créez et formez un modèle de définition de solution à Réponse aux vulnérabilités l'aide de Intelligence prédictive. Vous pouvez utiliser ce modèle pour prédire le groupe d'affectation pour un élément vulnérable (VI) ou une tâche de rattrapage (RT) en fonction des données existantes.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tout** > **Intelligence prédictive** > **Classification** > **Définitions des solutions**.
2. Sur le formulaire Classification Definitions (Définitions de classification), cliquez sur **Vulnerable Item Assignment (Affectation d'éléments vulnérables)**.
   Il s'agit de la définition de la solution par défaut.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- La fréquence de formation par défaut est de 30 jours. Cela signifie que tous les 30 jours, le modèle se reforme automatiquement à l'aide du jeu de données VI qui correspond à la condition de filtre configurée.
- Les champs de la table d'éléments vulnérables peuvent être utilisés pour la formation. La définition de la solution par défaut s'entraîne sur deux champs de VI : **Vulnerability.Summary** et **Configuration item. Nom**. Vous pouvez personnaliser les champs utilisés pour la formation en fonction des champs que vous trouvez utiles pour prédire l'appropriation des vulnérabilités dans votre organisation.

3. Pour créer et former la solution de classification, consultez Créer et former une solution de classification .

Remarque : Vous pouvez également créer et former une solution de similarité ou de clustering. Pour en savoir plus, consultez :

- Créez et formez une solution de similarité .
- Créez et formez une solution de mise en grappe .

4. Cliquez sur **Mettre à jour et reformer**.

Remarque : Pour configurer des paramètres avancés pour les solutions ML, consultez Configuration des paramètres avancés pour vos solutions ML .

Créer un Réponse aux vulnérabilités calculateur

Un calculateur de vulnérabilité est une formule prédéfinie permettant de calculer un champ cible lorsque certains critères sont remplis. Les calculateurs, qui calculent le **score de risque** de l'élément vulnérable, peuvent contenir **des règles de risque**.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Remarque : Vous remarquerez peut-être une dégradation des performances lors de l'exécution de calculateurs de vulnérabilité contenant des scripts.

Ordonnez vos règles pour exécuter d'abord les règles les plus simples et exécutez uniquement des scripts sur les éléments qui ne peuvent pas être gérés avec une condition et une valeur de modèle ou une règle de risque.

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Administration** > **Calculateurs de vulnérabilités**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire du calculateur de vulnérabilité

Champ	Description
Nom	Nom du calculateur de vulnérabilité.
Table	Rempli automatiquement avec le nom de la table d'éléments vulnérables.
Application	Rempli automatiquement avec Réponse aux vulnérabilités.
Champ cible	Champ à calculer.
Description	Description textuelle du calculateur.
Actif	Allumez ou éteignez la calculatrice.

4. Cliquez avec le bouton droit de la souris dans l'en-tête pour **enregistrer**.
   La section **Règles du calculateur de vulnérabilité** s'affiche.
5. Créez une règle pour le calculateur en cliquant sur **Nouveau**.

   Remarque : Pour le formulaire **Nouvelles règles de risque** (disponible uniquement lorsque le **champ Cible** est **Score de risque**), consultez l'étape 10.

6. Renseignez les champs comme il convient.

Formulaire Règle du calculateur de vulnérabilité

Champ	Description
Nom	Nom de la règle du calculateur.
Ordre	Ordre dans lequel exécuter le calculateur de vulnérabilité. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Renseigné automatiquement avec le parent calculateur.
Actif	Par défaut, la case **Actif** est cochée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Vue avancée	Si cette option est sélectionnée, les conditions et valeurs scriptées peuvent être sélectionnées à partir du **type de condition** et du **type de valeur**.

7. Renseignez les champs de l'onglet **Quand cette condition est remplie** , le cas échéant.

Onglet Quand cette condition est remplie

Champ	Description
Nom	Nom de la règle du calculateur.
Ordre	Ordre dans lequel exécuter le calculateur de vulnérabilité. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Renseigné automatiquement avec le parent calculateur.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Par défaut, la case **Actif** est cochée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux éléments vulnérables créés dans le système.
Vue avancée	Lorsque cette option est sélectionnée, sélectionnez les conditions et les valeurs scriptées dans **Type de condition** et **Type de valeur**.
Type de condition	Disponible lorsque vous sélectionnez la **vue avancée**. Les choix sont les suivants : ◦ Filtre : utilise des conditions de filtre. ◦ Groupe de filtres : consultez Créer un nouveau groupe de filtres pour définir les critères du calculateur. ◦ Script : condition de script utilisée pour déterminer quand appliquer ce calculateur. **Remarque :** Avant d'écrire des scripts pour déterminer quand appliquer les calculateurs, revenez à la liste **des calculateurs de vulnérabilité** . Explorez les enregistrements du calculateur de vulnérabilité expédiés avec le système de base.
Condition	Définit les conditions de filtre de base pour déterminer s'il faut utiliser le calculateur ou non. La sélection du **groupe de filtres** ou des types de conditions de **script** masque ce champ. La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.

8. Cliquez sur l'onglet **Définir ces valeurs** et renseignez les champs du formulaire comme il convient.

Définir l'onglet Définir ces champs

Champ	Description
Type de valeur	Disponible lorsque vous sélectionnez la **vue avancée**. Les choix sont les suivants : ◦ Modèle : définissez les valeurs à définir sur chaque champ. ◦ Script : utilisé pour définir les valeurs de chaque champ.
Valeurs de script	Disponible si vous avez sélectionné le type de valeur **Script** . Définit les valeurs auxquelles appliquer les calculs.
Modèle	Sélectionnez les champs et les valeurs que vous souhaitez utiliser pour le calculateur. La sélection du type **de** valeur de script masque ce champ.

9. Lorsque vous avez rempli toutes les entrées, cliquez sur **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous modifiez un calculateur existant et que vous souhaitez mettre à jour tous les scores existants, vous pouvez utiliser le bouton **Réappliquer le calculateur** . Il passe en revue tous les éléments vulnérables (VI) actifs et, si ce calculateur est utilisé pour définir leur valeur, il recalcule la valeur de ces VI. Étant donné que la réapplication d'une calculatrice peut prendre beaucoup de temps, une tâche planifiée s'en charge.

10. Pour le formulaire **Nouvelles règles de risque** , renseignez les champs comme il convient.

    Définissez chaque poids en fonction du pourcentage du résultat qui doit provenir de cette valeur. Pour toutes les données que votre scanner ne fournit pas, ou pour les données qui ne doivent pas faire partie du score de risque, définissez le poids sur zéro.

    Vous pouvez ajouter, supprimer ou mettre à jour les champs. Vous pouvez également configurer le pourcentage de pondération des valeurs de champ. Pour plus d'informations, consultez Définir des champs et des poids pour la règle de risque pour les calculateurs de risque de Vulnerability Response.

    Lorsque vous mettez à jour les pondérations, les scénarios affichent les pondérations restantes, ainsi que les résultats de **score de risque** anticipés.

Champ	Description
Nom	Nom de la règle du calculateur.
Ordre	Ordre dans lequel exécuter le calculateur de vulnérabilité. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Renseigné automatiquement avec le parent calculateur.
Actif	Par défaut, la case **Actif** est cochée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Condition	Définit les conditions de filtre de base pour déterminer s'il faut utiliser le calculateur. La sélection du **groupe de filtres** ou des types de conditions de **script** masque ce champ.
Pondérations	
Gravité de la vulnérabilité	Pourcentage du résultat qui provient de la gravité.
Score EPSS de vulnérabilité	Probabilité d'exploitation de la vulnérabilité. Par défaut, le poids de ce critère est zéro. Si vous souhaitez l'utiliser pour le calcul de votre score de risque, définissez une pondération appropriée par rapport à ce critère.
Existence de l'exploit	Pourcentage du résultat qui provient de l'existence d'un exploit. Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.
Niveau de compétence de l'exploit	Pourcentage du résultat qui provient du niveau de compétence requis par l'exploit. Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.

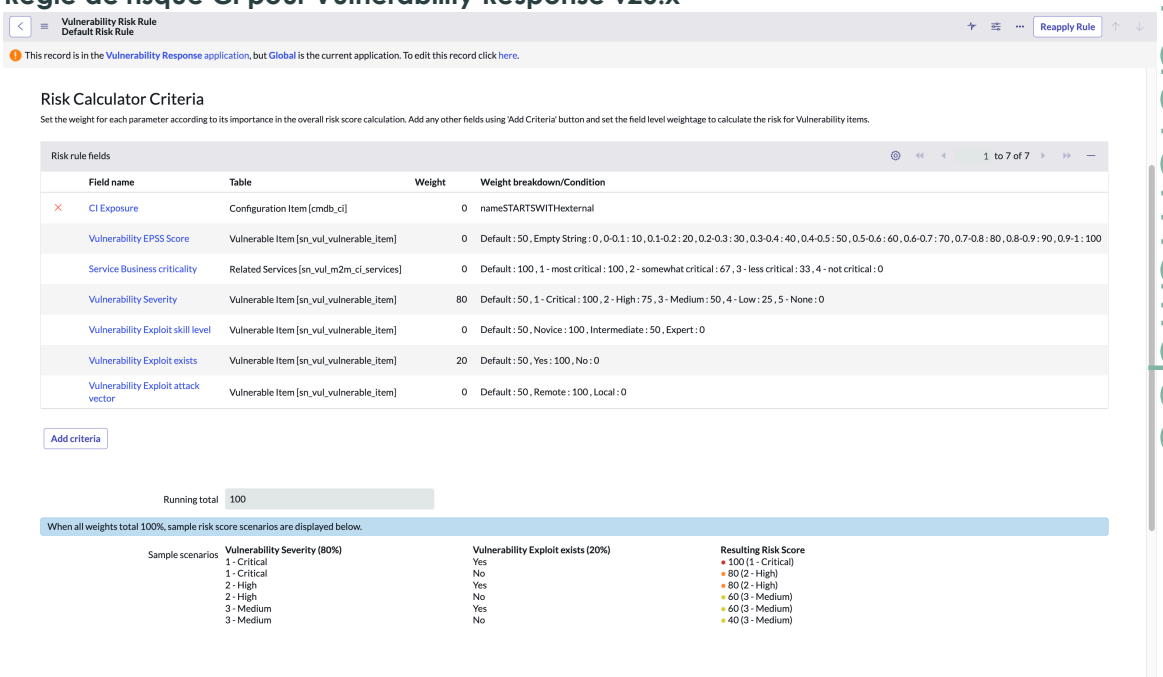
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Vecteur d'attaque de l'exploit	Pourcentage du résultat qui provient de l'endroit où l'attaque est ciblée. Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.
Criticité opérationnelle de service	Pourcentage du résultat qui provient de la criticité opérationnelle. Si vous n'avez pas lié vos CI aux services d'entreprise, définissez le poids sur zéro.
Exposition CI	Pourcentage du résultat qui provient du fait que le CI soit orienté vers Internet. Si le poids n'est pas nul, un filtre de condition apparaît pour définir les CI accessibles sur Internet. Définissez le filtre pour sélectionner vos éléments de configuration orientés vers Internet. Vous pouvez prévisualiser les enregistrements qui correspondent à la condition.
Exécution totale	Totaux des pourcentages calculés automatiquement. Lorsque cette valeur atteint 100, l'aperçu du scénario vous montre des échantillons de scores de risque dans différents scénarios.
Scénarios de score du risque	Lorsque tous les poids totalisent 100 %, les scénarios de score de risque s'affichent, fournissant un aperçu du score de risque dans certains des scénarios possibles.

Vous pouvez ajouter ou supprimer des critères et ajuster le poids de chaque critère à l'aide de la liste incorporée.

Règle de risque CI pour Vulnerability Response v20.x



11. Cliquez sur **Envoyer**.

Désactiver le calculateur de vulnérabilité par défaut s'il n'est pas utilisé

Si vous n'utilisez pas de calculateurs de vulnérabilité, désactivez le calculateur par défaut, en plus de tous les autres que vous avez définis. Les calculateurs de vulnérabilité s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est créé ou mis à jour, ce qui peut avoir un impact sur les performances d'importation initiales.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Procédure
1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Calculateurs de vulnérabilités**.
2. Ouvrez le calculateur correspondant.
3. Décochez la case **Actif** pour désactiver le calculateur.
4. Cliquez sur **Mettre à jour**.

Créer, activer ou modifier Réponse aux vulnérabilités des règles de suppression automatique

Vous pouvez créer, activer ou modifier les règles de suppression de l'élément de vulnérabilité (VI) et de la tâche de rattrapage (RT). Utilisez la suppression automatique pour supprimer les enregistrements plus anciens des tables VI et RT.

Avant de commencer
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôles requis :

- Administrateur : modifier les règles de suppression automatique
- sn_vul.vulnerability_admin ou sn_vul.admin (obsolète) : afficher le module de suppression automatique

Pourquoi et quand exécuter cette tâche
Au fil du temps, une grande quantité d'enregistrements fermés est susceptible de s'accumuler dans les tables VI et VUL de votre instance. Bon nombre de ces documents peuvent avoir été fermés pendant plus de 365 jours, mais n'ont pas été supprimés. Utilisez des règles de suppression automatique pour supprimer un grand nombre de ces enregistrements anciens et fermés. La suppression de ces enregistrements permet non seulement de réduire considérablement le nombre d'enregistrements dans les tables VI et VUL, mais aussi de maintenir des performances élevées.

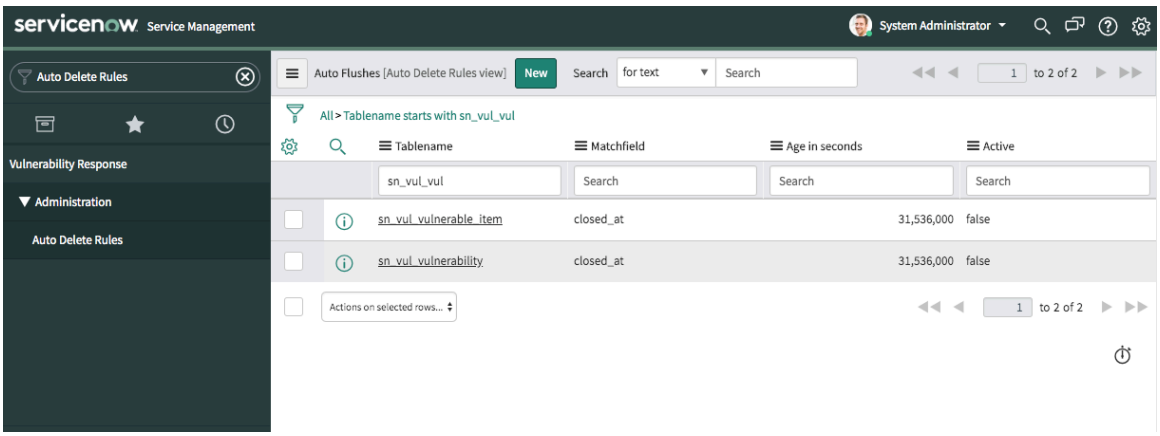
Bien que la suppression automatique cible par défaut les enregistrements qui ont été fermés pendant 365 jours, la toute première exécution peut tenter de purger trop d'enregistrements dans une seule transaction. En fonction de la taille de votre environnement, vous pouvez échelonner le processus de suppression pour limiter la portée de la requête. Par exemple, vous pouvez démarrer votre première exécution pour les enregistrements fermés de plus de 450 jours. Une fois cette exécution terminée, vous pouvez descendre par incréments plus petits (425, 400, 375) jusqu'à ce que vous ayez réduit le nombre d'enregistrements antérieurs à 365 jours.

Deux règles sont fournies avec votre Now Platform® et suppriment automatiquement les enregistrements fermés qui remplissent les conditions spécifiées, ainsi que tous les enregistrements qui s'y rapportent. Une règle supprime les éléments vulnérables et l'autre règle supprime les tâches de rattrapage. Par défaut, ces règles de suppression automatique sont désactivées, de sorte que vous devez les activer manuellement avant de supprimer des enregistrements. Vous pouvez choisir les deux règles préconfigurées fournies avec votre instance ou créer les vôtres.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles de suppression automatique**.
   La vue de liste s'affiche.

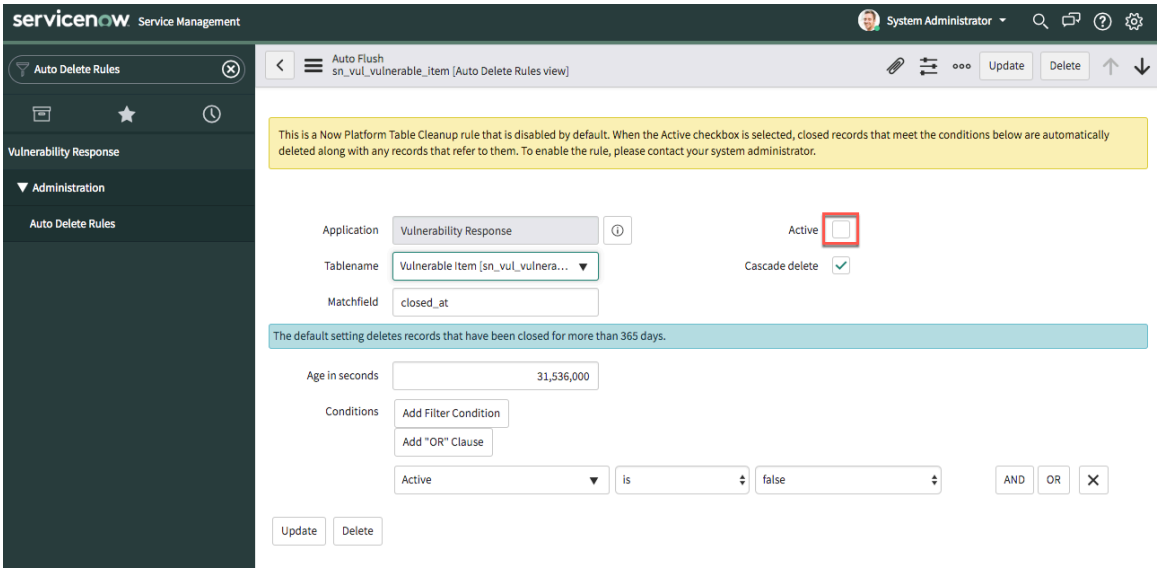


2. Pour effectuer une modification, sélectionnez la règle de suppression des éléments vulnérables (sn_vul_vulnerable_item) ou celle des tâches de rattrapage (sn_vul_vulnerability).
3. Pour créer une règle, cliquez sur **Nouveau**.
4. Renseignez ou modifiez les champs du formulaire, selon vos besoins.

Champ	Description
Application	Nom de l'application dans laquelle les enregistrements sont supprimés. La valeur par défaut est Vulnerability Response.
Nom de table	Nom de la table à laquelle la règle est appliquée.
Champ de correspondance	Champ dont le système surveille la durée.
Actif	Option permettant d'activer la règle. Une fois activé, l'enregistrement peut être supprimé.
Suppression en cascade	Option permettant de supprimer tous les enregistrements correspondants, ainsi que tous les enregistrements qui s'y rapportent. Si cette option n'est pas sélectionnée, seuls les enregistrements correspondants sont supprimés, mais pas les enregistrements qui y font référence.
Âge en secondes	Âge de l'enregistrement de vulnérabilité à supprimer. Pour les règles VI et RT, l'âge est de 365 jours. Cet âge s'affiche en secondes.
Conditions	Conditions de filtre définissant les enregistrements dans les tables VI et RT (VUL) auxquelles les règles s'appliquent.

5. Cochez la case **Actif** pour activer une règle.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois la règle activée, la fonction horaire de la plateforme, **Purge automatique**, supprime ces enregistrements de la table pour laquelle la règle est activée.

Si votre environnement compte des millions, voire des dizaines de millions, d'enregistrements qui correspondent à vos critères de suppression, il est recommandé de contacter ServiceNow l'assistance clientèle avant d'activer les règles de suppression automatique pour vous aider à supprimer des enregistrements à l'aide d'un processus par étapes.

Ajouter des graphiques d'importance de la vulnérabilité à la page d'accueil de Vulnerability Response

Vous pouvez ajouter des graphiques de définition de l'importance de la vulnérabilité et d'autres visualisations à la vue d'ensemble.

Avant de commencer

- Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.
- Le module d'extension Analyse de vulnérabilité doit être activé.

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Vue d'ensemble**.
   Certains rapports sont ajoutés au tableau de bord par défaut. Pour en savoir plus sur ces rapports, reportez-vous à Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.
2. Près de l'en-tête du tableau de bord, cliquez sur l'icône de vue de carte + **Ajouter du contenu** pour ouvrir la boîte de dialogue afin d'ajouter d'autres widgets.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans les listes de la boîte de dialogue **Ajouter des widgets** , sélectionnez **Rapports** pour afficher d'autres Réponse aux vulnérabilités rapports.

Contenu	Options
Détails de la tâche de rattrapage	**Arborescence** > **Importance de la vulnérabilité** > **Importance de la vulnérabilité**
Rapport sur le score d'importance de la vulnérabilité	**Analyse des performances** > **Score** > **Services avec une vulnérabilité importante**
Entrée vulnérable	**Rapports** > **Entrée vulnérable** > **Vulnérabilités par impact, score, semaine**
Tâche de rattrapage	**Rapports** > **Tâche de rattrapage** > **Tâche de remédiation par délai de rattrapage de l'état**
Élément de tâche de rattrapage	**Rapports** > **Élément de tâche de rattrapage** > **Nouveaux éléments vulnérables**
Exécution de l'intégration de vulnérabilité	**Rapports** > **Exécution de l'intégration de vulnérabilité** > **Doublons Qualys, nouveaux VI, résultats, VI mis à jour, exécutions d'intégration Qualys au cours des 30 derniers jours**
Élément vulnérable	**Rapports** > **Élément vulnérable** > **Une liste exhaustive de filtres d'éléments vulnérables, y compris les VI Qualys ouverts.**.

4. Cliquez sur l'emplacement de l'écran où vous souhaitez ajouter la jauge.
5. Fermez la zone **Ajouter du contenu** .

Définir les Réponse aux vulnérabilités notifications par e-mail

Configurez des notifications par e-mail pour partager des informations utiles sur les mises à jour et les activités importantes, telles que l'approbation et le rejet des demandes de faux positifs. La création d'une notification par e-mail implique de spécifier quand l'envoyer, qui la reçoit et ce qu'elle contient.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Modèles d'e-mail**.
2. Sélectionnez **Nouveau**.

   Pour obtenir des instructions détaillées sur la création de notifications par e-mail, reportez-vous à la section Créer une notification par e-mail .

Résultats

À partir de la version 21.0 de , lorsqu'un destinataire clique sur les liens d'une notification par e-mail, les liens s'ouvrent dans ou Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT en fonction de Réponse aux vulnérabilitésson rôle.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les liens s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs disposant des rôles sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.
- Les liens s'ouvrent dans le Espace de travail de remédiation IT pour les utilisateurs disposant du rôle sn_vul.remediation_owner.

Si le destinataire n'a aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Définir des modèles d'e-mail Réponse aux vulnérabilités

La création d'une notification par e-mail implique de spécifier quand l'envoyer, qui la reçoit et ce qu'elle contient.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Administration** > **Modèles d'e-mail**.
2. Sélectionnez **Nouveau**.

   Pour obtenir des instructions détaillées sur la création de modèles d'e-mail, reportez-vous à la section Construire un e-mail avec un modèle .

Créer ou modifier des notifications de cibles de rattrapage

Les administrateurs de vulnérabilité peuvent modifier les notifications de cible de rattrapage ou en ajouter de nouvelles, en spécifiant le moment d'envoi de la notification, qui reçoit la notification et quel contenu contient la notification.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Notifications**.
2. Sélectionnez l'enregistrement de notification de cible de rattrapage ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Pour plus d'informations sur les champs de formulaire, consultez Créer une notification par e-mail .
4. Sélectionnez **Prévisualiser la notification** pour afficher le message.

Résultats

À partir de la version 21.0 de , lorsqu'un destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans ou Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT en fonction de Réponse aux vulnérabilitésson rôle.

- Les liens s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs disposant des rôles sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.
- Les liens s'ouvrent dans le Espace de travail de remédiation IT pour les utilisateurs disposant de rôles, sn_vul.remediation_owner.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si le destinataire n'a aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Configurer l'évaluation de l'exposition à la vulnérabilité

Évaluez l'exposition zero-day (jour actuel) de vos actifs aux logiciels vulnérables avec l'application Vulnerability Exposure Assessment.

Important : Vous pouvez effectuer l'évaluation de l'exposition par logiciel et par vulnérabilités et expositions courantes (CVE) pour tirer parti des options supplémentaires de l'espace de travail d'évaluation de la vulnérabilité. Pour plus d'informations, consultez Explorer l'espace de travail de l'évaluation de la vulnérabilité.

Rôle requis : administrateur

Compatibilité et configuration requise

L'application Réponse aux vulnérabilités est disponible sur le ServiceNow Store. L'application Gestion des actifs logiciels (SAM) Foundation [com.snc.asset_management] est installée avec l'application Réponse aux vulnérabilités . Pour vérifier que l'application SAM Foundation est installée sur votre instance, accédez à **Applications système** > **Toutes les applications disponibles** > **Tout** et recherchez `com.snc.asset_management`. Si l'application n'est pas installée, sélectionnez **Installer**. Pour plus d'informations sur les SAM Foundation, voir Module d'extension Software Asset Management Foundation .

Étant donné que l'application Évaluation de l'exposition à la vulnérabilité nécessite l'accès aux données d'actif sur votre Now Platform® instance, les applications de gestion des actifs doivent avoir des données à référencer. La table des modèles de détection de logiciels [cmdb_sam_sw_discovery_model] et la table des installations de logiciels [cmdb_sam_sw_install] nécessitent des données.

L'application d'évaluation de l'exposition à la vulnérabilité fonctionne également avec les SAM Foundation applications SAM Pro ou SAM ProNow Platform®. L'application SAM Pro ne fait pas partie du produit principal Réponse aux vulnérabilités et ServiceNow Store nécessite un abonnement distinct.

Remarque : L'application SAM Pro n'est requise que pour la bibliothèque de contenu, car elle peut donner de meilleurs résultats.

À partir de la version 23.0 de Réponse aux vulnérabilités, si vous disposez de l'abonnement Pro ou Enterprise, vous serez redirigé vers la page **Évaluation de l'exposition** dans les espaces de travail en fonction de votre rôle lorsque vous cliquerez sur le lien **Évaluation de l'exposition** dans le menu **Tout** :

Accès à la page d'évaluation de l'exposition dans les espaces de travail

Rôle	Espace de travail
Responsable des vulnérabilités	Espace de travail du gestionnaire de vulnérabilité
Gestionnaire d'événements [sn_vul_analyst.vul_event_manager] ou Réponse d'urgence [sn_vul_analyst.emergency_response]	Espace de travail de l'évaluation de la vulnérabilité

Pour éviter d'être redirigé vers les espaces de travail et rester sur la page Évaluation de l'exposition classique, définissez le **type de lien** sur *Liste des enregistrements* dans l'onglet Type de lien de la page Module - Évaluation de l'exposition. Vous pouvez accéder à la

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

page Module - Évaluation de l'exposition en sélectionnant l'icône **Modifier le module** à côté du lien Évaluation de **l'exposition** dans le menu **Tout** .

Avec le rôle d'écriture de vulnérabilité [sn_vulnerability_write], vous pouvez afficher le module d'évaluation de l'exposition et créer et modifier des enregistrements d'évaluation de l'exposition sur demande pour les logiciels vulnérables de votre instance avec l'application Réponse aux vulnérabilités .

Information associée

Évaluer votre exposition aux logiciels vulnérables

Configurer la gestion des exceptions pour Réponse aux vulnérabilités

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive de sécurité ou de gestion des vulnérabilités publiée, vous pouvez demander une exception. La gestion des exceptions implique de demander, examiner, approuver ou rejeter des exceptions à un élément vulnérable (VI) ou à une tâche de rattrapage (RT) qui ne peuvent pas être corrigés conformément à la politique.

Avant de commencer

Limitez la durée d'une demande d'exception et ajoutez un questionnaire à la demande d'exception ou de faux positif à l'aide du Réponse aux vulnérabilités module. Par défaut, une exception est demandée à l'aide du ServiceNow® Réponse aux vulnérabilités module. Vous pouvez également demander une exception à l'aide de l'intégration GRC : gestion de la politique et de la conformité .

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.manage_exception_configuration

Pourquoi et quand exécuter cette tâche

Si Réponse aux vulnérabilités cette option est activée, vous pouvez limiter la durée pendant laquelle une exception peut être demandée. De même, si le GRC : gestion de la politique et de la conformité module est installé, vous pouvez le sélectionner GRC : gestion de la politique et de la conformité sur l'écran de configuration. L'activation de cette option vous permet de demander une exception qui spécifie l'objectif de politique et de contrôle à partir de GRC.

Si vous ajoutez un questionnaire, il est envoyé à la personne qui émet la demande d'exception ou de faux positif. Vous pouvez utiliser le questionnaire par défaut ou en créer un en fonction de vos besoins.

Il est utile que l'approbateur de l'exception comprenne le motif de la demande d'exception.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire Configuration de la gestion des exceptions, sélectionnez la façon dont vous souhaitez gérer une exception en sélectionnant une option dans la liste **Gérer les exceptions à l'aide** de.
   Vous pouvez sélectionner ou Réponse aux vulnérabilitésGRC : gestion de la politique et de la conformité. Vous devez activer le GRC module d'extension à utiliser GRC : gestion

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de la politique et de la conformité pour demander une exception. La modification de la configuration n'a pas d'impact sur les données existantes.

3. Si vous avez sélectionné l'option Réponse aux vulnérabilités , entrez les informations suivantes :

Formulaire Paramètres pour VR Exception Management

Champ	Description
Durée	Période pour laquelle une exception peut être demandée.
Unité	Unité de temps pour la période spécifiée.
Activer le questionnaire pour demander une exception	Option permettant d'ajouter un questionnaire à la demande d'exception émise.
Questionnaire pour demander une exception	Affiche le questionnaire que vous avez sélectionné pour demander une exception. Le **questionnaire d'exceptions** est affiché par défaut. **Remarque :** Ce champ s'affiche uniquement lorsque vous cochez la case **Activer le questionnaire pour demander une exception** .
Questionnaire pour le contrôle de compensation	Affiche le questionnaire auquel un propriétaire de rattrapage doit répondre pour les demandes de réduction des risques. À partir de la version 20.0 de , vous pouvez définir un questionnaire pour les demandes de réduction des Réponse aux vulnérabilitésrisques. Le **questionnaire de contrôle de compensation** est sélectionné par défaut. **Remarque :** Ce champ s'affiche uniquement lorsque vous cochez la case **Activer le questionnaire pour demander une exception** .
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Questionnaire pour marquer comme faux positif	Affiche le questionnaire que vous avez sélectionné pour le marquer comme faux positif. Le questionnaire des demandes de faux positif est affiché par défaut. **Remarque :** Ce champ s'affiche uniquement lorsque la case **Activer le questionnaire pour marquer comme faux positif** est cochée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous avez personnalisé le questionnaire existant et mis à niveau vers la version 20.0, ce questionnaire personnalisé s'affiche pour la demande de réduction des risques au lieu du **questionnaire de contrôle de compensation** par défaut.

4. Si vous avez sélectionné l'option GRC : gestion de la politique et de la conformité , entrez les informations suivantes :

Formulaire Paramètres pour VR Exception Management

Champ	Description
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Questionnaire pour marquer comme faux positif	Affiche le questionnaire que vous avez sélectionné pour le marquer comme faux positif. Le questionnaire des demandes de faux positif est affiché par défaut.

5. Pour configurer des questionnaires basés sur des conditions pour les demandes d'exception et les faux positifs :

   a. Dans la section Configuration du questionnaire VR, sélectionnez **Nouveau**.

   b. Dans le formulaire Configuration du questionnaire - nouvel enregistrement, renseignez les champs et sélectionnez **Soumettre**.
   Pour en savoir plus sur les champs du formulaire Configuration du questionnaire, reportez-vous à Champs de formulaire de configuration du questionnaire.
   Le questionnaire créé apparaît dans la section Configuration du questionnaire VR du formulaire Paramètres pour la gestion des exceptions VR.

   Par exemple, si vous souhaitez configurer un questionnaire pour les demandes de faux positif pour les éléments vulnérables critiques, puis sélectionnez la règle d'approbation **Faux positif pour les éléments vulnérables** , fournissez la condition `Cote de risque 1 - Critique` et sélectionnez le questionnaire souhaité dans le formulaire Configuration du questionnaire .

6. Sélectionnez **Enregistrer**.

Ajouter un approbateur d'exception

Ajoutez des utilisateurs aux groupes d'approbation afin de pouvoir demander une exception.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche

Jusqu'à la Réponse aux vulnérabilités version 14.0, une demande d'exceptionpour un élément vulnérable ou une tâche de rattrapage est approuvée à l'aide du workflow

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'approbation à deux niveaux par défaut. La demande doit être approuvée par deux niveaux d'approbateurs.

Remarque : Jusqu'à Réponse aux vulnérabilités la version 14.0, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Toutefois, à partir de la Réponse aux vulnérabilités version 15.0, si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas le repasser en workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et des faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Groupes**.
2. Dans la colonne Nom, recherchez **Exception**, puis cliquez sur **Approbateur d'exception - Niveau 1**.

   Remarque : À partir de la Réponse aux vulnérabilités version 12.8.1, vous pouvez utiliser les propriétés système fournies dans le système de base pour les approbations d'exceptions via le workflow de la table Propriétés système [sys_properties]. Ainsi, lorsqu'une demande d'exception ou de faux positif est émise via le workflow, elle est envoyée pour approbation aux ID de groupe définis dans la propriété système. Accédez à la **Tout** > **Propriétés système** et sélectionnez *sn_vul.exception_approver_L1*, *sn_vul.exception_approver_L2* ou *sn_vul.false_positive_approver_group* pour modifier la valeur de la propriété.

3. Dans le formulaire Approbateur d'exception de groupe - niveau 1, cliquez sur la liste connexe Membres du groupe.
4. Cliquez sur **Nouveau** pour créer une liste.
5. Renseignez les champs du formulaire.

Formulaire d'utilisateur

Champ	Description
ID d'utilisateur	Identificateur unique pour l'utilisateur.
Prénom	Prénom de l'utilisateur.
Nom de famille	Nom de famille de l'utilisateur.
Titre	Fonction de l'utilisateur. Saisissez un titre ou une description de poste, ou sélectionnez-en un dans la liste.
Département	Département de l'utilisateur.
Mot de passe	Mot de passe affecté à l'utilisateur. Ce mot de passe peut être permanent ou temporaire.
Mot de passe à réinitialiser	Option permettant à l'utilisateur de réinitialiser le mot de passe pour garantir la sécurité.
Verrouillé	Option permettant de verrouiller l'utilisateur hors de l'instance et de mettre fin à toutes

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	les sessions actives de l'utilisateur. Le système empêche les utilisateurs disposant du rôle administrateur de se verrouiller eux-mêmes.
Actif	Option pour rendre cet utilisateur actif. Vous seul pouvez voir un utilisateur inactif dans ces zones : ◦ Listes d'utilisateurs ◦ Liste de sélection sur les champs de référence (icône de loupe) ◦ Liste de saisie semi-automatique qui s'affiche lorsque vous entrez du texte dans un champ de référence
Accès au service Web uniquement	Option permettant de désigner cet utilisateur comme utilisateur non interactif.
Utilisateur d'intégration interne	Option permettant de désigner cet utilisateur en tant qu'utilisateur d'intégration interne.
E-mail	Adresse e-mail de l'utilisateur.
Langue	Langue préférée de l'utilisateur.
Intégration du calendrier	Calendrier utilisé pour gérer le calendrier de travail. Par exemple, Outlook.
Fuseau horaire	Fuseau horaire de l'emplacement de cet utilisateur.
Format de date	Format préféré de l'utilisateur pour les dates.
Tél. professionnel	Téléphone professionnel de l'utilisateur.
Tél. mobile	Téléphone portable de l'utilisateur.
Photo	Photo que vous pouvez télécharger en cliquant sur **Cliquer pour ajouter...**.

Traduction automatique

6. Cliquez sur **Envoyer**.
7. Répétez les étapes 1 à 5 pour créer un approbateur d'exception de niveau 2. L'approbateur doit accéder à **Vulnerability Response** > **Mes approbations** et approuver les demandes.

> **Remarque :** Pour approuver une exception pour GRC : gestion de la politique et de la conformité, consultez la configuration facultative de Policy and Compliance Management .

Configurer les règles d'approbation pour la gestion des exceptions

À partir de la Réponse aux vulnérabilités version 15.0, utilisez le concepteur de flux pour approuver les demandes d'exception pour la gestion des exceptions, les règles d'exception et la gestion des faux positifs. Si vous déployez Réponse aux vulnérabilités (VR) pour la première fois, Flow Designer est activé par défaut.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Si vous êtes un utilisateur VR existant, l'option par défaut est workflow.
Si vous avez déployé Réponse aux vulnérabilités la version 15.0 ou ultérieure, la valeur de la propriété *sn_vul.flow_designer_activation* système est définie sur true. Cela signifie que Flow Designer est activé par défaut.

Si vous utilisez Réponse aux vulnérabilités déjà une version antérieure à la version 15.0, la valeur de cette propriété système est définie sur false. Vous pouvez activer le concepteur de flux en changeant la valeur sur vrai.

Remarque : Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer. Pour une comparaison détaillée entre le workflow et Flow Designer, reportez-vous à la section Comparaison du workflow de gestion des exceptions et de Flow Designer.

Pour utiliser le concepteur de flux, créez des règles à l'aide du module Règles d'approbation. À l'aide de ce module, vous pouvez configurer des règles d'approbation pour chacun des workflows de gestion des exceptions suivants.

- Demande d'exception pour les tâches de rattrapage
- Demande d'exception pour les éléments vulnérables
- Règle d'exception
- Faux positif pour les tâches de remédiation
- Faux positif pour les éléments vulnérables

Remarque : Vous pouvez également définir des conditions contenant plusieurs niveaux d'approbation au sein d'une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant. Pour plus d'informations sur la configuration des niveaux d'approbation, reportez-vous à la section Créer des niveaux d'approbation pour la gestion des exceptions.

Procédure
1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.
2. Sur la page Règles d'approbation, sélectionnez le groupe pour lequel vous souhaitez définir la règle d'approbation.
3. Renseignez les champs du formulaire.

Formulaire Règle d'approbation

Champ	Description
Nom	Nom de configuration de l'approbation.
Table	Table sur laquelle la règle est appliquée.
Application	La valeur par défaut est Vulnerability Response.
Type de règle	Spécifie le type de règle. Par exemple, gestion des exceptions, faux positif ou règle d'exception.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Activé par défaut, ce qui signifie que la règle d'approbation est utilisée.
Description	Brève description des règles d'approbation.
Expiration de l'approbation (jours) À partir de la v21.0 de Réponse aux vulnérabilités	Date jusqu'à laquelle l'approbateur peut approuver la demande.
Notification de l'approbateur (jours) À partir de la v21.0 de Réponse aux vulnérabilités	Date après laquelle l'approbateur est invité à prendre des mesures.

4. Sélectionnez **Mettre à jour**.
   Dans l'onglet Configurations d'approbation, deux niveaux d'approbateurs sont configurés par défaut. Vous pouvez sélectionner une règle pour définir les conditions en fonction de différents cas d'utilisation au sein d'une règle. Pour plus d'informations, consultez Créer des configurations pour une règle d'approbation.

   Remarque : Dans chaque page de configuration, vous pouvez créer plusieurs niveaux d'approbation. Pour plus d'informations, consultez Créer des niveaux d'approbation pour la gestion des exceptions.

Example:
En fonction des différents cas d'utilisation, vous pouvez définir différents processus d'approbation pour les mêmes vulnérabilités trouvées sur différents éléments de configuration.

Créer des configurations pour une règle d'approbation

Définissez les conditions pour filtrer les éléments vulnérables, les tâches de rattrapage ou les règles d'exception correspondants pour un niveau d'approbation.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Dans le module Configurations d'approbation, vous pouvez configurer plusieurs niveaux d'approbation pour différentes configurations. Définissez des règles basées sur des conditions, chaque règle contenant plusieurs niveaux d'approbation.

Remarque : Utilisez le module Règles d'approbation pour configurer des règles d'approbation pour les workflows de gestion des exceptions. Pour en savoir plus sur la configuration des règles d'approbation, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.
2. Sélectionnez une règle d'approbation et accédez à l'onglet **Configurations d'approbation** .
3. Sélectionnez une configuration.
4. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de configuration de l'approbation

Champ	Description
Nom	Nom de configuration de l'approbation.
Règle d'approbation	Contient les détails de table et de type pour la règle d'approbation.
Ordre	Ordre d'exécution des différentes configurations au sein d'une règle. Par exemple, une configuration avec une entrée d'ordre de 100 est exécutée avant une configuration avec une entrée d'ordre de 200.
Actif	Activé par défaut, ce qui signifie que la configuration d'approbation est en cours d'utilisation.
Description	Brève description des niveaux de configuration de l'approbation.

5. Définissez une condition pour les éléments vulnérables ou les tâches de rattrapage de l'une des façons suivantes :

Champ	Description
Condition	Identifie les éléments vulnérables ou les tâches de rattrapage correspondants.
Condition avancée	Script qui définit la condition des éléments vulnérables ou des tâches de rattrapage. **Remarque :** Ce champ s'affiche lorsque vous cochez la case **Avancé** .

6. Sélectionnez **Mettre à jour**.
   Vous pouvez définir des conditions contenant plusieurs niveaux d'approbation au sein d'une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant. Pour plus d'informations sur la configuration des niveaux d'approbation, reportez-vous à la section Créer des niveaux d'approbation pour la gestion des exceptions.

Example:
Vous pouvez définir différents chemins d'approbation pour :

- Exemple 1 : Différents types de vulnérabilités ou d'éléments de configuration (accessibles sur Internet ou internes).
- Exemple 2 : Demandes de report et de réduction du risque lorsqu'un propriétaire de rattrapage émet ces demandes simultanément pour des éléments vulnérables de l'hôte (VIT) ou des tâches de rattrapage (VUL).

  La colonne Approbation de changement contient les enregistrements d'approbation de changement d'état de report. Lorsque vous définissez une condition sur la colonne Approbation de changement à l'aide du Créateur de conditions, l'enregistrement

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'approbation de report est pris en compte, mais pas l'enregistrement d'approbation de réduction de risque. Ainsi, pour définir la condition sur l'enregistrement d'approbation de changement d'état de réduction du risque, utilisez le champ **Condition avancée** .

Pour la règle d'approbation **Demande d'exception pour les éléments vulnérables** , la **configuration Demande d'évaluation du risque de moyen à faible** est fournie avec le système de base. Par défaut, cette configuration est définie sur faux. Vous pouvez utiliser cette configuration pour définir un chemin d'approbation pour les demandes de réduction des risques de moyen à faible. Vous pouvez également mettre à jour le script dans cette configuration afin qu'il soit applicable pour divers changements de cote de risque dans les demandes de réduction des risques.

Demande d'évaluation des risques de configuration de moyen à faible :

```
function evaluate() {
    var gr = new GlideRecord("sn_vul_change_approval");
    gr.addQuery("sys_id", approval);
    gr.addQuery("current_value", "3 - Medium");
    gr.addQuery("desired_value", "4 - Low");
    gr.query();
    if (gr.next()) {
        return true;
    }
    return false;
}
evaluate();
```

Définissez la configuration précédente sur vrai avec l'ordre le plus bas et définissez la **configuration par défaut - Demande d'exception pour** la configuration des VI sur vrai.

Résultat : lorsqu'un propriétaire de rattrapage soumet simultanément des demandes de report et de réduction du risque à partir de l'espace de travail de remédiation informatique, les demandes d'approbation de report sont redirigées vers les approbateurs définis dans la **configuration par défaut - demande d'exception pour** VI et les demandes d'approbation de réduction du risque sont redirigées vers les approbateurs définis dans la **demande d'évaluation des risques de la configuration Moyen à Faible** .

Créer des niveaux d'approbation pour la gestion des exceptions

Définissez les niveaux d'utilisateurs et de groupes d'utilisateurs qui vont approuver les demandes d'exception.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.
2. Sélectionnez une règle d'approbation et accédez à l'onglet **Configurations d'approbation** .
3. Sélectionnez une configuration.
4. Dans la section Niveaux d'approbateur, sélectionnez un niveau d'approbateur.
5. Renseignez les champs du formulaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire du niveau de l'approbateur

Champ	Description
Nom	Nom du niveau d'approbation.
Approbation requise	Sélectionnez le nombre d'approbations requises pour le niveau sélectionné : ◦ Un approbateur requis ◦ Approbation de tous les utilisateurs requise
Actif	Activé par défaut, ce qui signifie que le niveau d'approbation est utilisé.
Ordre	Ordre d'exécution des différentes configurations au sein d'une règle. Par exemple, une configuration avec une entrée d'ordre de 100 s'exécute avant une configuration avec une entrée d'ordre de 200.
Règle d'approbation	Contient les détails de table et de type pour la règle d'approbation.
Configuration de l'approbation	Contient les configurations d'approbation.
Affecter à l'aide de	Sélectionnez une option parmi : ◦ Utilisateur et groupe d'utilisateurs ◦ Champ de la table des approbations ◦ Script
Groupes	Groupe de niveau de l'approbateur composé de plusieurs utilisateurs. L'utilisateur doit avoir l'un des rôles suivants : ◦ sn_vul.exception_approver : pour la gestion des exceptions et les règles d'exception ◦ sn_vul.false_positive_approver : pour les faux positifs
Utilisateurs	Modifier les utilisateurs répertoriés dans les groupes.

6. Pour enregistrer les changements, sélectionnez **Mettre à jour**.

Remarque : Avant la version 15.0, le processus de workflow était fonctionnel s'il n'y avait que des utilisateurs au niveau d'exception 1. Cependant, à partir de la version 15.0, il doit y avoir au moins un utilisateur dans chaque niveau.

Avant la version 15.0, dans le workflow, s'il n'y avait pas d'utilisateur au deuxième niveau, l'élément de vulnérabilité ou le groupe vulnérable était différé. Toutefois, à partir de la version 15.0, s'il n'y a pas d'utilisateur au deuxième niveau, la demande d'approbation est automatiquement rejetée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example:
Il peut y avoir différents niveaux d'approbation des vulnérabilités pour les serveurs Linux et Windows.

Comparaison du workflow de gestion des exceptions et de Flow Designer

À partir de la Réponse aux vulnérabilités version 15.0, si vous déployez (VR) pour la première fois, le concepteur de Réponse aux vulnérabilités flux pour l'approbation des demandes d'exception dans la gestion des exceptions est activé par défaut. Si vous êtes un utilisateur VR existant, l'option par défaut est workflow.

Remarque : À partir de la Réponse aux vulnérabilités version 19.0, seul Flow Designer est pris en charge pour les nouveaux clients. Si vous êtes un utilisateur existant et que vous effectuez une mise à niveau vers Réponse aux vulnérabilités la version 19.0, Flow Designer et le workflow de gestion des exceptions sont pris en charge.

Workflow et Flow Designer

Considérations	Workflow	Flow Designer
Version	Avant la version 15.0 de Réponse aux vulnérabilités.	À partir de la v15.0 de Réponse aux vulnérabilités.
Option par défaut	Option par défaut si vous êtes un utilisateur VR existant.	Option par défaut pour les nouveaux utilisateurs VR à partir de la version 15.0.
Définition du processus d'approbation	La gestion des exceptions inclut les demandes d'exception et de faux positif, ainsi que les règles d'exception.	Inclut la définition de différents niveaux et l'ajout de différents approbateurs pour différents cas d'utilisation. Plus facile à mettre en œuvre que le workflow. La gestion des exceptions inclut les demandes d'exception et de faux positif, ainsi que les règles d'exception.
Mise à niveau vers Flow Designer	Vous pouvez effectuer une mise à niveau vers Flow Designer depuis le workflow. Toutefois, les demandes existantes ne peuvent être approuvées qu'à l'aide du workflow.	Flow Designer est activé par défaut.
Propriété système *sn_vul.flow_designer_activation*	Si vous avez utilisé le workflow pour la gestion des exceptions avant la version 15.0, la propriété système est définie sur false. Pour activer le concepteur de flux, définissez cette propriété sur vrai.	Si vous utilisez VR pour la première fois pour la version 15.0 ou ultérieure, la valeur de propriété système est définie sur true par défaut.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow et Flow Designer (suite)

Considérations	Workflow	Flow Designer
	Remarque : Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer.	
Module de règles d'approbation	Une fois la propriété système définie sur vrai, la tâche planifiée **Activer les règles d'approbation du module** s'exécute dans les 24 heures. Cette tâche planifiée active le module **Règles d'approbation** . Pour activer ce module instantanément, exécutez cette tâche manuellement.	Si vous avez déployé VR pour la première fois à partir de VR v15.0, ce module est disponible par défaut.
Niveaux d'approbation	Permet de définir uniquement deux niveaux d'approbateurs.	Fournit plusieurs options, telles que la définition d'un nombre illimité de configurations, de niveaux d'approbateurs et l'ajout dynamique d'approbateurs pour chaque règle.

Ajouter un approbateur faux positif

Seuls les utilisateurs ajoutés au groupe d'approbateurs de faux positifs peuvent approuver les faux positifs pour les éléments vulnérables (VI) et les tâches de rattrapage (VUL). L'octroi d'un faux positif est un processus d'approbation à un seul niveau.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Remarque :

À partir de Vulnerability Response v15.0, si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas le repasser en workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et des faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Rôle requis : sn_vul.vulnerability_admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > > **Administration utilisateurs** > **Groupes**.
2. Dans la colonne **Nom** , recherchez **Faux positif** et cliquez sur l'option.
3. Dans le formulaire Groupe, accédez à **Membres du groupe** > **Nouveau** (ou **Modifier**).
4. Dans le formulaire Utilisateur, créez un enregistrement en saisissant les détails de l'utilisateur, puis cliquez sur **Soumettre**.
   Tous les rôles sont accordés à l'utilisateur. Les utilisateurs sélectionnés sont ajoutés à la liste des membres du groupe. Ces membres peuvent approuver les demandes de marquage des VI ou des tâches de rattrapage comme faux positifs. Une fois approuvé, l'état de l'enregistrement est mis à jour sur Fermé et il n'est rouvert qu'à la date spécifiée.

Configurer le questionnaire pour la réduction du risque

À partir de la Réponse aux vulnérabilités version 20.0, vous pouvez personnaliser le questionnaire de la demande de réduction des risques pour un ensemble d'éléments vulnérables filtrés ou de tâches de rattrapage.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Le **Questionnaire pour les contrôles de compensation des éléments vulnérables** et le **Questionnaire pour les contrôles de compensation des** règles d'approbation des groupes vulnérables sont fournis avec le système de base.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire Paramètres de VR Exception Management, cochez la case Activer le questionnaire pour demander une exception.
3. Pour configurer des questionnaires basés sur des conditions pour les demandes de réduction des risques :

   a. Dans la section Configuration du questionnaire VR, sélectionnez **Nouveau**.

   b. Dans le formulaire Configuration du questionnaire - Nouvel enregistrement, sélectionnez la règle d'approbation **Questionnaire pour la compensation des contrôles pour les groupes vulnérables** ou **Questionnaire pour la compensation des contrôles pour les éléments vulnérables** et fournissez la condition.

   c. Sélectionnez le questionnaire souhaité et sélectionnez **Soumettre**.
   Pour en savoir plus sur les champs du formulaire Configuration du questionnaire, reportez-vous à Champs de formulaire de configuration du questionnaire.
   Le questionnaire créé apparaît dans la section Configuration du questionnaire VR du formulaire Paramètres pour la gestion des exceptions VR.

4. Sélectionnez **Enregistrer** dans le formulaire Paramètres pour la gestion des exceptions VR.

Afficher les SLA de Vulnerability Response pour les tâches de remédiation

Pour vous assurer que les éléments vulnérables sont traités correctement, vous pouvez définir un accord sur les niveaux de service (SLA) pour Réponse aux vulnérabilités les tâches de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche
Les définitions de SLA de cette liste sont un sous-ensemble de la liste des SLA de la plateforme, spécifique à Réponse aux vulnérabilités.

Pour obtenir des instructions, consultez Créer une définition de SLA .

Si vous suivez le temps nécessaire pour corriger les VI, vous préférerez peut-être utiliser Réponse aux vulnérabilités Règles de cibles de rattrapage. Les règles de cibles de rattrapage définissent les délais prévus pour la correction des éléments vulnérables (VI) spécifiquement dans le contexte de Vulnerability Response, tandis que les SLA peuvent fournir un délai pour la correction de la vulnérabilité elle-même.

Procédure
1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Définitions de SLA**.
2. Cliquez sur une définition.
   Les SLA de tâche sont affichés dans les listes connexes des **tâches de rattrapage**.

Configurer WatchDog

Utilisez la page de configuration de chien de garde pour créer de nouveaux chiens de garde ou mettre à jour des chiens de garde existants avec les conditions que vous souhaitez spécifier. Vous pouvez activer la notification pour chaque chien de garde et recevoir une notification lorsque les conditions sont remplies.

Avant de commencer
Rôle requis : sn_sec_cmn.admin

Procédure
1. Accédez à la **Tout** > **Security Operations** > **WatchDog** > **Configuration**.
2. Sélectionnez le chien de garde que vous souhaitez implémenter.
3. Renseignez les champs du formulaire.

Formulaire d'intégration WatchDog

Champ	Description
Nom	Nom du chien de garde.
Actif	Cochez la case *true* pour activer le chien de garde.
Type de condition	Choisissez entre Filtre ou Script.
Condition avancée	Ce champ s'affiche uniquement lorsqu'un script est sélectionné dans Type de condition.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Table	Sélectionnez une table pour exécuter la condition de surveillance.
Condition	Condition pour évaluer le chien de garde.
Notification	Case à cocher permettant de notifier les groupes ou les utilisateurs si la condition de surveillance est remplie.
Utilisateurs	Liste des utilisateurs à informer si la condition de chien de garde est remplie.
Groupes	Groupe à informer si la condition de chien de garde est remplie.
Journal de surveillance	
Chien de garde	Référence à la table de surveillance.
Nombre	Nombre d'enregistrements qui répondent aux critères de surveillance.
Notes	Remarques supplémentaires pour les journaux de surveillance.

4. Sélectionnez **Mettre à jour**.

Tâches de configuration avancées Réponse aux vulnérabilités

Les tâches de configuration suivantes nécessitent un codage ou une expertise avancée ServiceNow et ne sont pas considérées comme faisant partie de la configuration de base.

Vous préférerez peut-être effectuer ces tâches uniquement si vous avez une expérience avancée en codage ou si vous avez une connaissance approfondie du Now Platform.

Créer des importations séparées par domaine pour une intégration

Si vous avez besoin que les données importées se trouvent dans un domaine spécifique, l'utilisateur affecté à l'exécution des intégrations doit appartenir à ce domaine.

Avant de commencer

Rôle requis :
import_admin et configurez le rôle d'intégration de votre intégration spécifique, par exemple, sn_vul.configure_r7_integration ou sn_vul_tenable.configure_integration.

Pourquoi et quand exécuter cette tâche

Cet ensemble de tâches nécessite un codage ou une expertise avancée ServiceNow .

Les files d'attente d'importation contiennent des pièces jointes de données traitées par les travaux planifiés (intégrations). Dans un environnement séparé par domaine, vous devez faire correspondre la tâche planifiée avec la file d'attente d'importation appropriée.

Procédure

1. Créez un domaine.
2. Pour chaque domaine que vous créez, créez un utilisateur et affectez-le à ce domaine.

   Considérez cet utilisateur comme un espace réservé **run_as** pour le domaine dans votre intégration de vulnérabilité. C'est l'équivalent de la **VR. Utilisateur système** dans

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le domaine global. Cet utilisateur doit accéder aux sources de données, aux cartes de transformation et aux données de vulnérabilité.

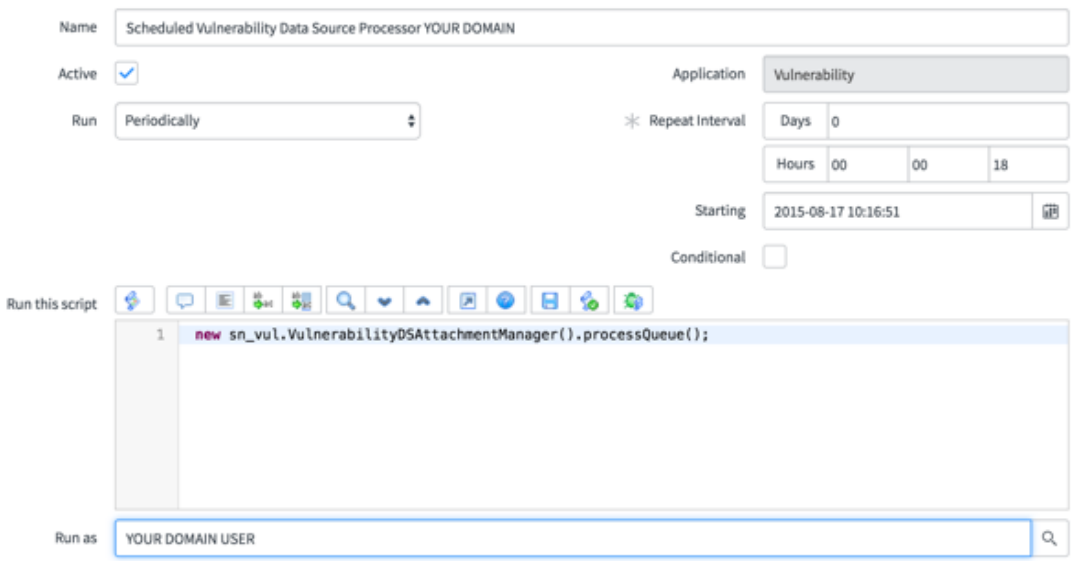
Remarque : N'utilisez pas cet utilisateur à d'autres fins.

3. Créez une tâche planifiée dans chaque domaine.
   Pour en savoir plus sur les précautions et les réglages supplémentaires, reportez-vous à la section Paramètres supplémentaires pour Séparation de domaine.

   a. Accédez à la **Tout** > **Définition du système** > **Travaux planifiés**.

   b. **Copier le processeur de source de données de vulnérabilité planifiée** dans le domaine.

   c. Pour identifier la tâche planifiée, ajoutez le domaine au nom.



   d. Dans le champ **Exécuter en tant que** , remplacez l'utilisateur **run_as** par l'utilisateur que vous avez créé à l'étape 2.

À partir de la version 20.1 du , les changements de Réponse aux vulnérabilitésscript suivants sont fournis avec le système de base.

4. **Remarque :** Modifiez l'action d'interface utilisateur suivante afin que l'intégration s'exécute dans le **domaine utilisateur run_as** .

   Modifiez l'action d'interface utilisateur **Exécuter maintenant** dans la tâche d'intégration de **l'intégration de la détection d'hôte Qualys** pour ajouter ce bloc de code en haut du fichier.

   Example

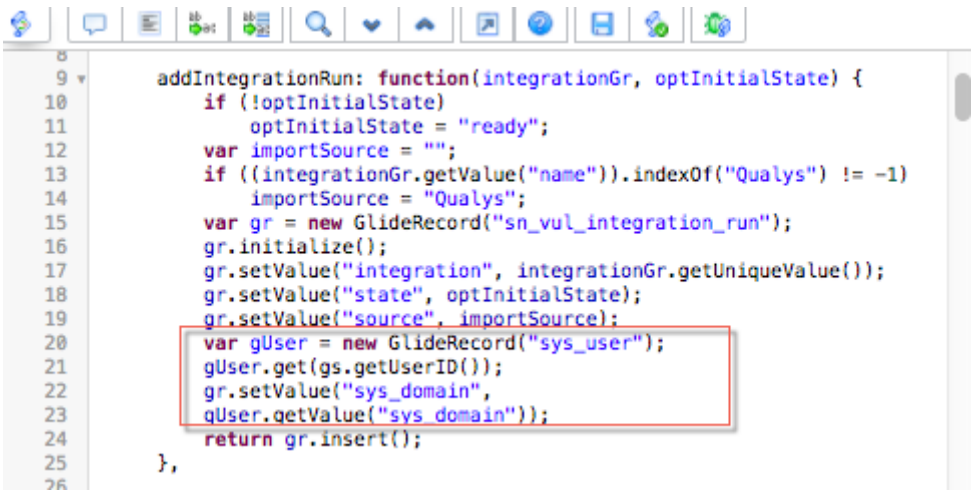
```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

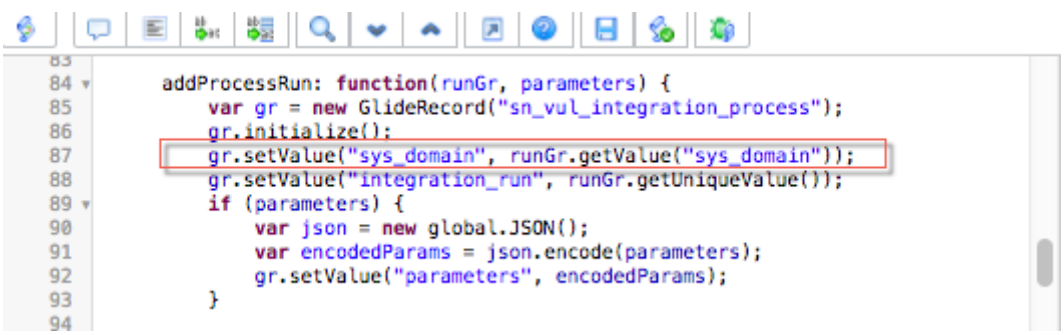
5. **Remarque :** Modifiez les includes de script suivants afin que l'intégration s'exécute dans le domaine de l'utilisateur **run_as** .

   Modifier la méthode d'include de script **VulnerabilityIntegrationUtilsaddIntegrationRun** pour ajouter le code en surbrillance



```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. Modifiez la méthode d'include de script **VulnerabilityIntegrationUtils** , **addProcessRun** pour ajouter le code en surbrillance dans l'image suivante.
   Code addProcessRun



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

7. Modifiez la méthode d'include de script **VulnerabilityIntegrationUtils** , **copyProcess** pour ajouter le code en surbrillance dans l'image suivante.
   code copyProcess

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Script

```
325
326     _copyProcess: function(intProcGr, isProcessErrored) {
327         var copy = new GlideRecord('sn_vul_integration_process');
328         copy.initialize();
329         copy.setValue('integration_run', intProcGr.getValue('integration_run'));
330         copy.setValue('parameters', intProcGr.getValue('parameters'));
331         copy.setValue('state', 'new');
332         copy.setValue('notes', '');
333         copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
334         if (isProcessErrored) {
335             copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
336             var nextRetryDueOn;
337             if (intProcGr.getValue('next_retry_due_on') != '')
338                 nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
339             else
340                 nextRetryDueOn = new GlideDateTime();
341
342             var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
343             var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
344             nextRetryDueOn.addSeconds(nextRetryDelay * 60);
345             if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
346                 copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
347         } else
348             copy.setValue('retries', intProcGr.retries + 1);
349
350         copy.insert();
351         return copy;
352     },
```

8. Modifier la méthode d'include de script **DataSourceVulnReportRefreshProcessor_processFromDataSourceGroups** pour modifier ce code d'origine :
Code _processFromDataSourcesGroups d'origine

```
23
24     _processFromDataSourceGroups: function(payload, fileName) {
25         var gr = new GlideRecord("sn_vul_int_data_src");
26         gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27         gr.orderBy("ds_group_number");
28         gr.orderBy("last_used");
29         gr.query();
30         var lastGroup;
31         if (gr.getRowCount() == 0) {
32             throw new Error("There are no data sources to provide data to.");
33         }
34         while (gr.next()) {
35             var thisGroup = gr.getValue("ds_group_number");
36             if (lastGroup == thisGroup && lastGroup !== undefined) {
37                 continue;
38             } else {
39                 var ds = new GlideRecord("sys_data_source");
40                 if (!ds.get(gr.sys_data_source + ""))
41                     continue;
42
43                 var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                 mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue());
45                 gr.setValue("last_used", new GlideDateTime().getValue());
46                 gr.update();
47                 lastGroup = thisGroup;
48             }
```

À :

Code _processFromDataSourcesGroups modifié

```
43                 var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                 mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                 gr.setValue("last_used", new GlideDateTime().getValue());
46                 gr.update();
47                 lastGroup = thisGroup;
```

9. Modifiez la méthode d'include de script **VulnerabilityDSAttachmentManager** , **queueItem** pour ajouter les blocs de code en surbrillance suivants
Élément en file d'attente

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.initialize();
    gr.setValue("status", "NEW");
    gr.setValue("data_source", dataSource);
    if (optIntegrationProcess)
        gr.setValue("integration_process", optIntegrationProcess);
    if(optDomain){
            gr.setValue("sys_domain", optDomain);
    }
    var sysId = gr.insert();
```

_getNext

```
_getNext: function() {
    // First go through the retries, if any
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    var sysDomainUser = gUser.getValue("sys_domain");
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "RETRY");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.orderBy("queued_on");
    gr.query();
    if (gr.next()) {
        return gr;
    }

    // Then handle the regular queued items
    gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "QUEUED");
    gr.orderBy("queued_on");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.query();
    if (gr.next()) {
        return gr;
    }
```

_processQueueEntry fonction

```
_processQueueEntry: function(entry) {
    var schedGrId = this._getScheduledImportSet(entry.data_source);
    if (gs.nil(schedGrId)) {
        return;
    }

    var dataSourceGr = new GlideRecord("sys_data_source");
    if (!dataSourceGr.get(entry.data_source)) {
        gs.warn("Non existent data source - marking as complete");
        entry.setValue("status", "COMPLETE");
        entry.setValue("processing_notes", "Data source does not exist, could not process.");
        entry.update();
        return;
    }

    try {
        this._deleteDataSourceAttachments(entry.data_source);
        if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
            gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue
entry " + entry.sys_id);
            throw "Attachments not deleted";
        }
        var attachmentApi = new GlideSysAttachment();
        attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
        var schedGr = new GlideRecord("scheduled_import_set");
        schedGr.get(schedGrId);
        schedGr.setValue("data_source", entry.data_source);
        schedGr.setValue("run_as", gs.getUserID());
        schedGr.update();
```

À ce stade, vous êtes prêt pour les importations séparées par domaine.

Remarque : Si vous avez plusieurs déploiements d'une Réponse aux vulnérabilités intégration ou Réponse aux vulnérabilités des applications , répétez ce processus pour chaque déploiement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer et prendre en charge plusieurs domaines dans le cadre de travail des tâches en arrière-plan

Les tâches en arrière-plan dans les produits Vulnerability Response sont conçues pour s'exécuter pendant de longues périodes afin d'effectuer plusieurs processus sur vos enregistrements. Les processeurs de tâches en arrière-plan sont fournis avec le système de base qui s'exécute via l'utilisateur système et crée des enregistrements dans le domaine global.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Administrateur de domaine** > **Domaines**.
2. Créez un domaine.

   Pour en savoir plus sur la création d'un domaine, reportez-vous à la section Créer un domaine .

   Pour chaque domaine créé, créez un utilisateur et affectez-lui l'utilisateur au domaine. Supposons cet utilisateur en tant qu'espace réservé run_as pour le domaine. C'est l'équivalent de la réalité virtuelle. Utilisateur système dans le domaine global. Cet utilisateur doit accéder aux données de vulnérabilité.
3. Modifiez la run_as des travaux planifiés *`Scheduled Background Job Manager`*, et *`Close the parent background job`*.

   Si vous avez créé plusieurs domaines, dupliquez cette tâche et modifiez run_as utilisateur en conséquence. Vous pouvez également conserver une copie des tâches précédentes avec l'utilisateur run_as du domaine global en mode inactif.

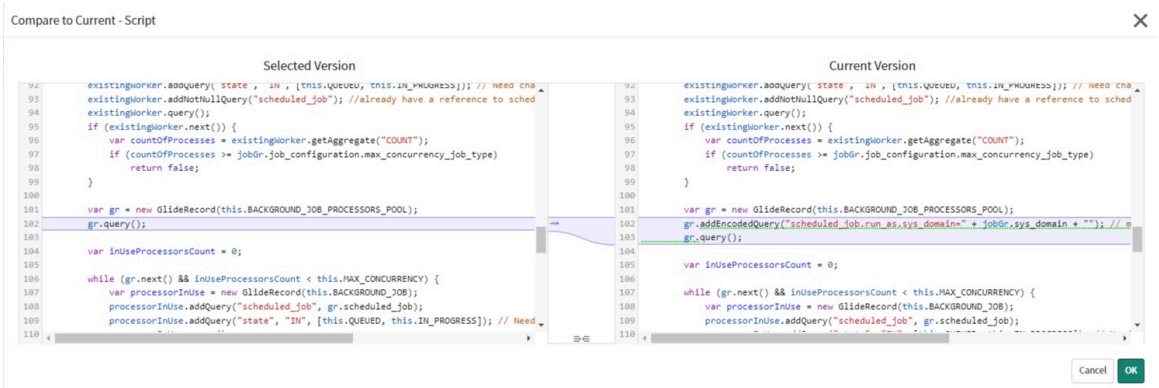
   Dix tâches de processeur (par exemple, *`Background job processor 10`*) sont fournies avec le système de base. Modifiez l'exécution à partir de ces tâches pour l'utilisateur séparé par domaine. Si plusieurs domaines sont présents, deux tâches par domaine suffisent, mais ces tâches peuvent également être dupliquées si nécessaire. Conservez deux tâches de processeur avec run_as utilisateur dans le domaine global.

   À partir de la version 20.0 du , les changements de Réponse aux vulnérabilitésscript suivants sont fournis avec le système de base.
4. Modifiez l'include *`BackgroundJobManager`*de script et ajoutez la ligne suivante, comme illustré dans l'image suivante.

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" +
 jobGr.sys_domain + "");
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Déclenchez la réapplication sur demande de toutes les règles du domaine approprié.

Créer une règle de recherche de CI de Vulnerability Response

Le module **Règles de recherche de CI** contient des règles qui sont utilisées pour trouver l'enregistrement correspondant aux informations sur l'hôte reçues lors des importations d'intégration de vulnérabilité tierces. Les informations sur l'hôte sont mises en correspondance avec les éléments détectés, les classes d'éléments de configuration sans correspondance et le Base de données de gestion des configurations (CMDB)fichier .

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

La création de règles de recherche de CI nécessite un niveau avancé ServiceNow et Réponse aux vulnérabilités une expertise. Plutôt que de modifier l'une des règles de recherche existantes, envisagez de la copier et de modifier la copie. Lorsque vous êtes convaincu que la nouvelle règle fait ce que vous voulez, désactivez l'originale.

Remarque : Les règles, une fois supprimées, ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **CMDB** > **Règles de recherche de CI**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Règle de recherche de CI

Champ	Description
Nom	Nom de la règle.
Méthode de recherche	Méthode utilisée pour la correspondance. Les choix possibles sont les suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ **Script** : Script prédéfini (adresse IP, nom DNS, etc.) ou personnalisé. ◦ **Correspondance de champ** : recherche sur une table ou un champ dans la CMDB.
Type	Type utilisé avec la **méthode Recherche de** script.
Ordre	Ordre de priorité de la règle. Les règles dont l'ordre est le plus bas sont évaluées en premier.
Actif	Cochez la case pour indiquer si la règle est active ou désactivée.
Source	Source utilisée comme entrée dans cette règle.
Champ source	Champ source utilisé comme entrée à cette règle. Sélectionnez n'importe quel champ, mais il est traité comme une valeur de chaîne.
Condition	Condition d'application de la règle de recherche de CI. Cette condition dépend de l'attribut de l'analyseur tiers. **Remarque :** L'attribut d'actif fait partie de la charge utile. Elle provient de l'analyseur tiers. Consultez la table Éléments détectés pour des exemples de charge utile.
Script	Un exemple de script modifiable, basé sur le **type**, est affiché. Implémentez le script personnalisé en fonction des commentaires inclus dans le modèle de la fonction par défaut. **Remarque :** La fonction process comporte trois paramètres : *rule*, *sourceValue*et *sourcePayload*
Rechercher sur la table	Table à rechercher dans la CMDB. Utilisé avec la **méthode de recherche** de correspondance de champ.
Rechercher sur le champ	Champ qui contient des informations pouvant être utilisées pour localiser un CI. Utilisé avec la **méthode de recherche** de correspondance de champ. Ce champ peut se trouver sur l'enregistrement CI ou sur un enregistrement connexe, tel qu'une carte réseau.

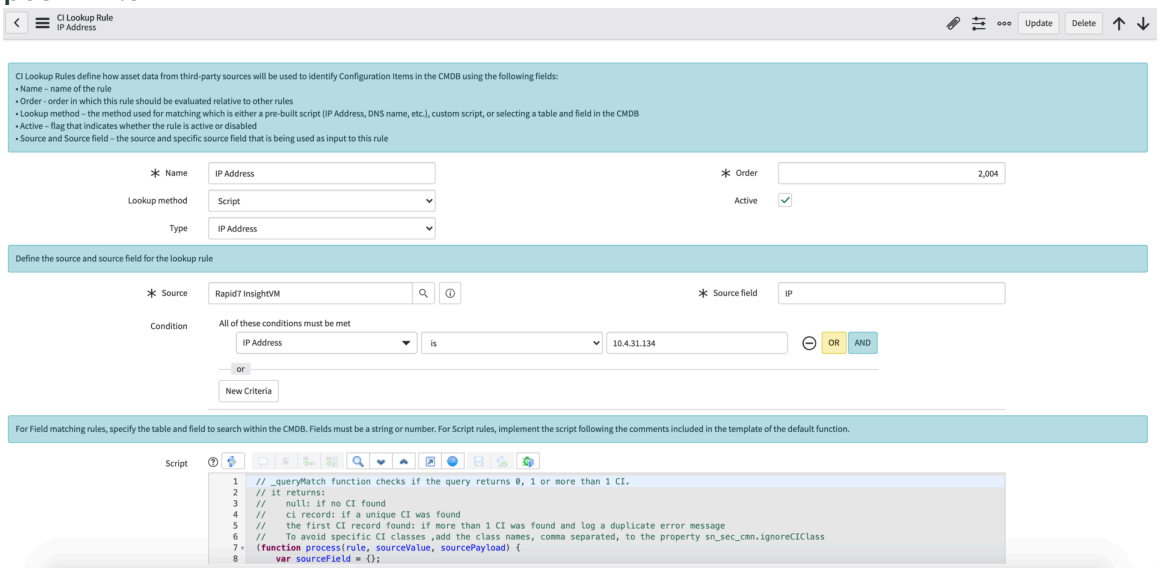
4. Cliquez sur **Envoyer**.

Pour plus d'informations sur l'implémentation des règles de recherche de CI, reportez-vous à la section Étapes pour empêcher les enregistrements en double ou orphelins après l'exécution de Réponse aux vulnérabilités règles de recherche de CI.

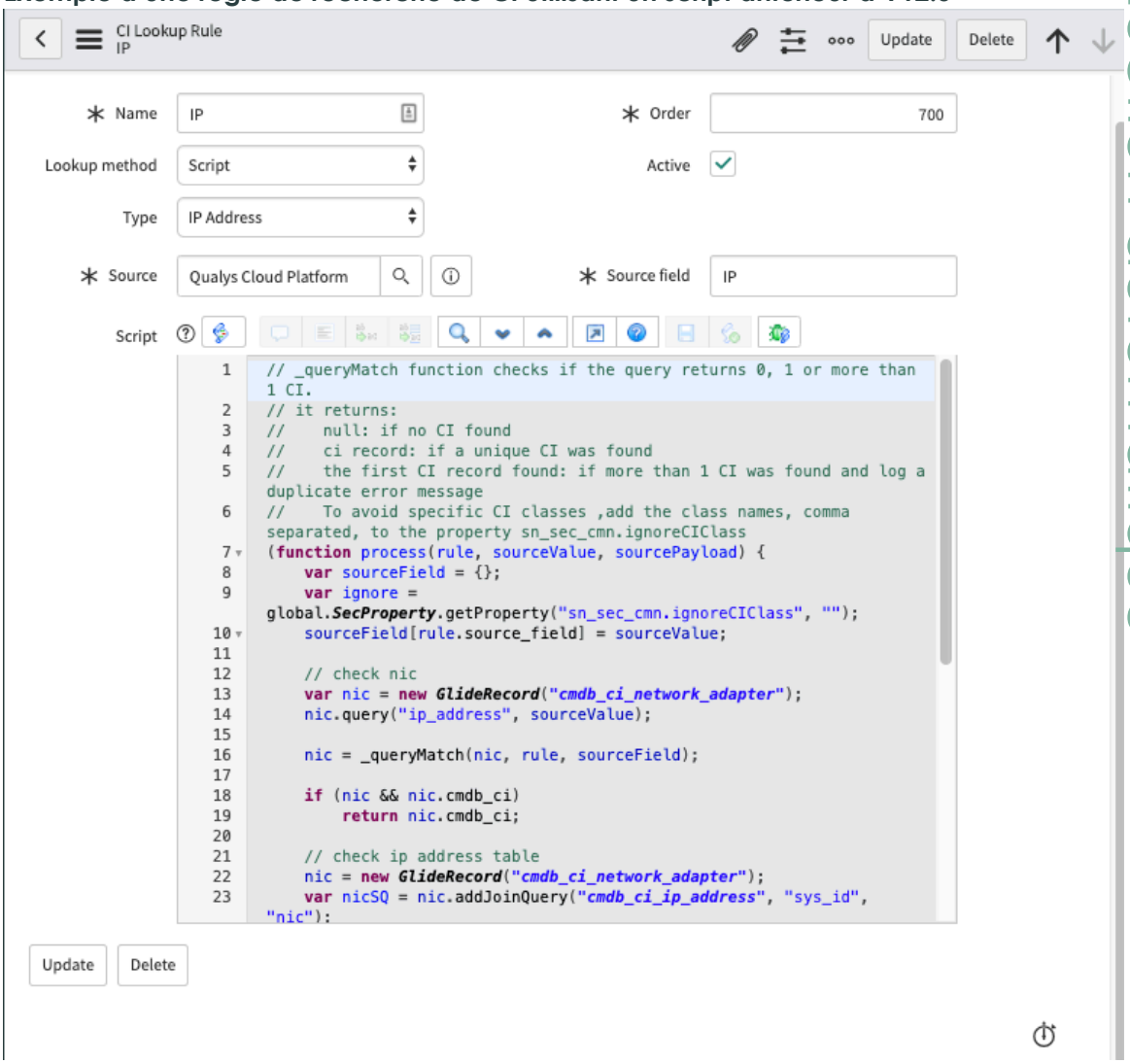
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple d'une règle de recherche de CI utilisant un générateur de conditions pour V12.0



Exemple d'une règle de recherche de CI utilisant un script antérieur à V12.0



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Réponse aux vulnérabilités Champs du formulaire d'élément vulnérable

Ignorer les classes CI

Pour ignorer certaines classes d'éléments de configuration (CI), par exemple Équilibreur de charge [cmdb_ci_lb), lors de l'exécution de règles de recherche de CI, définissez la propriété système **ignoreCIClass** [*sn_sec_cmn.ignoreCIClass*].

Avant de commencer

Rôle requis : administrateur

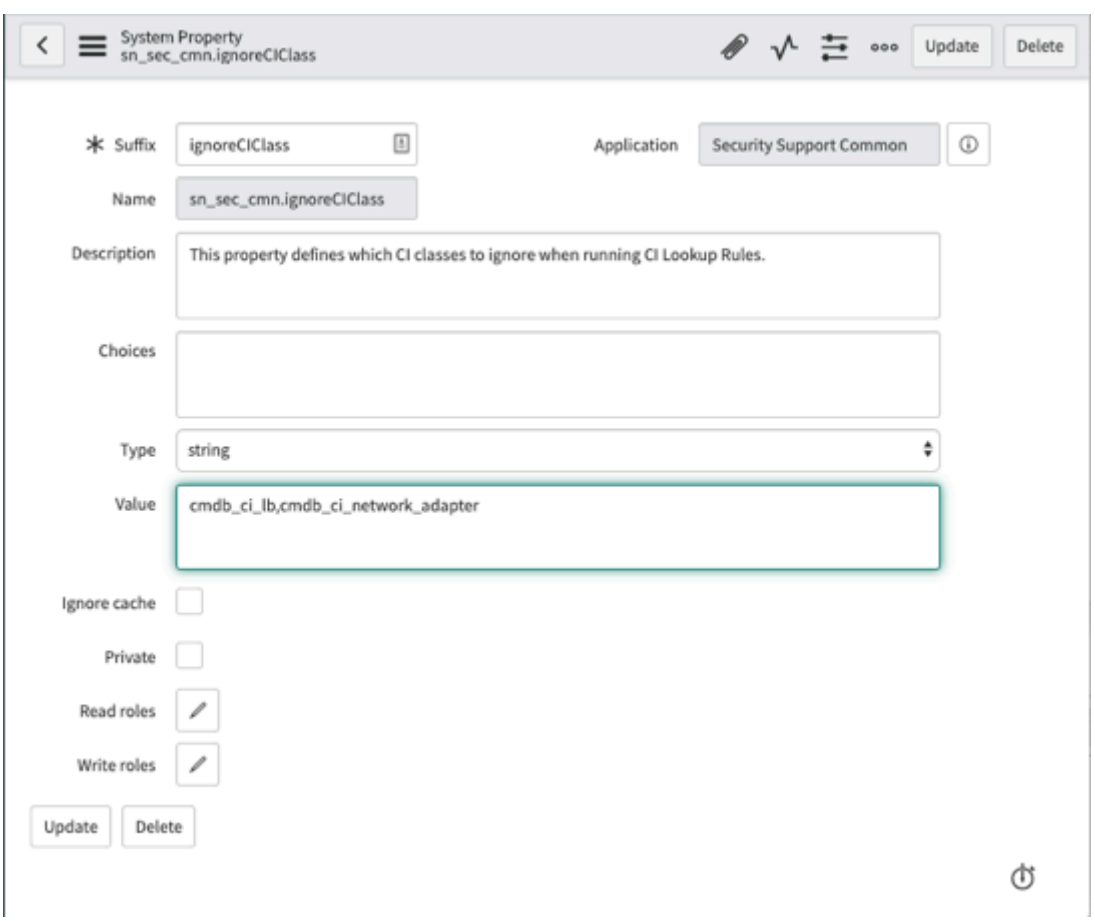
Remarque :

La propriété système **ignoreCIClass** est disponible à partir de la Réponse aux vulnérabilités version 9.0, mais la fonctionnalité de la propriété n'est pas disponible lors de la mise à niveau à partir d'une version antérieure.

Si vous avez effectué une mise à niveau à partir d'une Opérations de sécurité application antérieure à la version 9.0, consultez KB0788209 pour obtenir des instructions sur la façon d'activer cette fonctionnalité.

Procédure

1. Saisissez `sys_properties.list` dans la barre de navigation de gauche.
2. Cliquez sur **Entrée**.
3. Dans le menu **Rechercher** , sous **Nom** , saisissez `sn_sec_cmn.ignoreCIClass`.
4. Dans la zone de texte **Valeur** , entrez les classes CI à exclure dans une liste séparée par des virgules.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Mettre à jour**.
   Cette liste est utilisée par les règles de recherche de CI lors de l'importation suivante. Les éléments vulnérables créés lors de l'importation ne sont associés à aucun CI d'un type répertorié dans le champ **Valeur** de la propriété système `sn_sec_cmn.ignoreCIClass` .

Filtrer les CI désactivés

Filtrez les éléments de configuration (CI) mis hors service lors de l'exécution des règles de recherche de CI. Pour filtrer les CI mis hors service lors de l'exécution des règles de recherche de CI Security Operations CMDB, définissez la propriété système **filterOutDecommissionedCI** [**sn_sec_cmn.filterOutDecommissionedCI**] sur vrai.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
La valeur par défaut de la propriété système est true. Cette propriété ne s'applique qu'aux règles de recherche de CI dans Réponse aux vulnérabilités et n'a aucun impact sur la logique de recherche IRE.

Procédure

1. Saisissez `sys_properties.list` dans la barre de navigation de gauche.
2. Sélectionnez **Entrée**.
3. Dans le menu **Rechercher** , sous **Nom** , saisissez `sn_sec_cmn.filterOutDecommissionedCI` pour filtrer les CI désactivés.
4. Dans la zone de texte **Valeur** , entrez la valeur true ou false.
   La valeur par défaut est vrai.
5. Sélectionnez **Mettre à jour**.
   Cette valeur est utilisée par les règles de recherche de CI lors de la prochaine importation. La propriété système `sn_sec_cmn.filterOutDecommissionedCI` filtre les CI mis hors service lors de l'exécution de ces règles de recherche.

Promouvoir automatiquement les CI

Modifiez la chaîne JSON dans la propriété système **autoPromoteFields** [**sn_sec_cmn.autoPromoteFields**] afin que vos règles de recherche d'éléments de configuration (CI) promeuvent automatiquement tous les CI CMDB Security Operations en entrées correspondantes dans la table [cmdb_ci].

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Le type de propriété système est « chaîne » et nécessite l'entrée d'une chaîne JSON. Cette propriété est activée par défaut et favorise la correspondance des CI lors de l'exécution des règles de recherche de CI.

Les scripts de recherche écrits sur mesure peuvent renvoyer des enregistrements de table enfant à partir du script. Pour cette propriété, la *_autoPromoteCI* fonction de la *CIIdentify Script Include* prend le CI renvoyé par le script de recherche et parcourt automatiquement les relations pour arriver à l'entrée *cmdb_ci* et la renvoyer.

Pour remplacer la logique d'auto-promotion, c'est-à-dire pour ajouter ou mettre à jour de nouvelles classes CI, ajoutez l'objet JSON dans le champ Valeur de la propriété système [**sn_sec_cmn.autoPromoteFields**].

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Saisissez `sys_properties.list` dans la barre de navigation de gauche.
2. Sélectionnez **Entrée**.
3. Localisez la propriété système `[sn_sec_cmn.autoPromoteFields]` et sélectionnez l'enregistrement pour l'ouvrir.

   Chaîne par défaut :

```
{
 "dscy_switchport":"cmdb_ci",
 "cmdb_ci_network_adapter":"cmdb_ci",
 "cmdb_ci_nic":"cmdb_ci",
 "cmdb_ci_ip_address":"nic"
}
```

4. Dans la zone de texte **Valeur** , modifiez la chaîne à l'aide du format d'appariement par défaut.
5. Sélectionnez **Mettre à jour**.
   Cette valeur est utilisée par les règles de recherche de CI lors de la prochaine importation.

Configurer la clé de l'élément vulnérable

Configurez la granularité de la clé d'élément vulnérable (VI) dans l'application Réponse aux vulnérabilités pour définir ce qui constitue un élément vulnérable (EV) dans votre organisation.

Avant de commencer

Rôle requis : administrateur
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Termes clés :

Élément de configuration (CI)

Un actif existant répertorié sur votre CMDB.

Vulnérabilité

Un enregistrement d'une vulnérabilité connue importé du National Institute of Standards and Technology (NIST), de la National Vulnerability Database (NVD), de Common Vulnerabilities and Exposures (CWE) ou d'intégrations tierces avec Réponse aux vulnérabilités.

Élément vulnérable

Un élément vulnérable est créé lorsqu'une vulnérabilité importée correspond à un élément de configuration dans votre CMDB.

Détection

Une occurrence unique et distincte d'une vulnérabilité signalée par les scanners de vos intégrations tierces. Les détections sont importées et affichées à la fois sur les enregistrements de détection et les enregistrements d'éléments vulnérables de votre instance. Également appelée détection d'éléments vulnérables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, un élément vulnérable est la combinaison unique d'un élément de configuration (CI), d'une vulnérabilité et d'une instance d'intégration. Pour créer des éléments vulnérables avec plus de granularité, ajoutez des ports uniques à partir des détections d'éléments vulnérables pour vous aider à gérer le rattrapage des vulnérabilités au niveau que vous estimez le plus efficace pour votre organisation.

Si vous souhaitez créer des éléments vulnérables avec plus de granularité, configurez la clé de l'élément vulnérable afin qu'elle inclue le port. Lorsque l'option Inclure le port est activée, les éléments vulnérables sont créés par des ports uniques à partir des détections d'éléments vulnérables.

À partir de Vulnerability Response V17.1, vous pouvez identifier et corriger les vulnérabilités Rapid7 en ajoutant la preuve comme clé de VI. Pour plus d'informations, consultez Ajout d'une preuve aux clés d'éléments vulnérables Rapid7.

Choisissez une option dans le tableau suivant pour activer l'option Inclure le port.

Trois scénarios pour activer l'option Inclure le port avec la clé VI pour la première fois

Si...	Description
Une ou plusieurs des conditions suivantes sont vraies : • Vous effectuez une mise à niveau à partir d'une version antérieure à v10.0 qui ne prenait pas en charge les détections d'éléments Réponse aux vulnérabilités vulnérables. • Vous êtes un nouveau client et vous n'avez pas de données Vulnerability Response (éléments vulnérables ou détections d'éléments vulnérables) dans votre Now Platform® instance. • Vous avez déjà supprimé tous vos enregistrements d'éléments vulnérables et les données connexes dans votre instance et vous êtes prêt à créer toutes vos données Vulnerability Response en commençant par une nouvelle importation pour inclure les VI se distinguant par un port unique.	Activez Inclure le port. Une fois que l'option Inclure le port est activée, les détections importées créent des éléments vulnérables qui incluent des éléments vulnérables qui se distinguent par un port unique, en commençant par l'importation suivante.
Les deux conditions sont vraies : • Vous disposez de la version 10.0 ou ultérieure de Réponse aux vulnérabilités et vous souhaitez conserver des données Vulnerability Response (éléments vulnérables ou détections d'éléments vulnérables) dans votre instance. • Vous voulez commencer à créer de nouveaux éléments vulnérables pour inclure des VI se distinguant par un port unique.	Activez Include port. Vos détections existantes et leurs éléments vulnérables associés seront conservés. Une fois que l'option Inclure le port est activée, les nouvelles détections créent de nouveaux éléments vulnérables qui incluent des éléments vulnérables se distinguant par un port unique, en commençant par l'importation suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Trois scénarios pour activer l'option Inclure le port avec la clé VI pour la première fois (suite)

Si...	Description
Les deux conditions sont vraies : • Vous disposez de la version 10.0 ou ultérieure de Réponse aux vulnérabilités. • Vous disposez de données Vulnerability Response existantes (éléments vulnérables ou détections d'éléments vulnérables), mais vous ne souhaitez pas conserver vos données existantes, car vous préférez créer vos données de vulnérabilité à partir d'une nouvelle importation et vous souhaitez inclure des VI se distinguant par un port unique.	1. Supprimez tous vos enregistrements d'éléments vulnérables et les données connexes de votre instance. 2. Activez Include port. Une fois que l'option Inclure le port est activée, les nouvelles détections créent de nouveaux éléments vulnérables qui incluent des éléments vulnérables se distinguant par un port unique, en commençant par l'importation suivante.

Remarque :

Si l'option Inclure le port est activée, plus d'un élément vulnérable peut être créé pour un élément de configuration. Par exemple, s'il existe une vulnérabilité pour deux ports d'un élément de configuration, les ports 80 et 443, deux VI uniques sont créés, un pour chaque port commençant par l'importation suivante.

Remarque : Avant d'activer cette fonctionnalité, assurez-vous de vouloir créer des VI pour inclure des VI par ports uniques. Une fois que vous avez activé la clé de VI pour inclure le port, vous devez d'abord supprimer vos données Vulnerability Response avant de pouvoir désactiver Inclure le port et revenir à l'importation des données de vulnérabilité à l'aide de la granularité de clé de VI par défaut, c'est-à-dire lorsque les VI sont créés pour le port, mais ne se distinguent pas par un port unique. Pour en savoir plus sur la suppression de vos données de vulnérabilité, reportez-vous à la section Supprimer tous vos enregistrements d'éléments vulnérables et les données connexes dans Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Configurer la granularité VI**.

   Le champ Dernière mise à jour affiche la date à laquelle la clé VI a été configurée pour la dernière fois.

2. Cochez la case Inclure le port pour l'activer.
3. Cliquez sur **Enregistrer**.
   La boîte de dialogue de confirmation s'affiche.

   Si vous n'avez aucun enregistrement de détection d'élément vulnérable dans votre instance, les détections d'éléments vulnérables et les éléments vulnérables sont créés par un port unique en commençant par votre importation suivante.

   Si vous avez des détections d'éléments vulnérables et des éléments vulnérables existants dans votre instance, les détections existantes et les éléments vulnérables associés seront conservés. Les nouvelles détections créent de nouveaux éléments vulnérables qui incluent des VI qui se distinguent par un port unique, à partir de l'importation suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Vérifiez que les éléments vulnérables par port sont affichés dans les enregistrements de détection d'éléments vulnérables et d'éléments vulnérables. Pour plus d'informations, consultez Afficher les Réponse aux vulnérabilités données de détection des éléments vulnérables.

Ajout d'une preuve aux clés d'éléments vulnérables Rapid7

Ajoutez la preuve en tant que clé d'élément vulnérable (VI) pour les Rapid7 VI. L'inclusion de la preuve pour des vulnérabilités spécifiques permet à l'intégration du Rapid7 scanner de créer des VI pour chaque preuve reçue de .Rapid7

Une clé de VI est la combinaison de la vulnérabilité, de l'élément de configuration (CI) et de l'instance d'intégration. La division des détections en différents éléments vulnérables en fonction de la preuve crée plusieurs éléments vulnérables. Vous pouvez affecter les vulnérabilités aux propriétaires de rattrapage appropriés.

Par exemple, il peut y avoir deux détections avec la même vulnérabilité et le même CI, mais avec des preuves différentes, conduisant à la création d'un VI. À partir de la Réponse aux vulnérabilités version 17.1, vous pouvez identifier et corriger les vulnérabilités en ajoutant la preuve comme clé de VI.

Vous pouvez ajouter la preuve en tant que clé de VI de la manière suivante :

Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Configurer la granularité VI** et sélectionnez l'option permettant d'inclure une preuve.

Cas d'utilisation : inclure une preuve dans la clé de VI pour les VI existants ou diviser les VI existants en fonction de la preuve de détection

Pour créer des VI basés sur des preuves, vous pouvez utiliser les vulnérabilités R7 log4j. Par exemple, vous pouvez utiliser l'une des multiples vulnérabilités R7 log4j telles que `R7-apache-log4j-core-cve-2021-44228`, `R7-amazon_linux-cve-2021-44228` ou `R7-amazon-linux-ami-2-cve-2021-44228`.

Si toutes les détections dans un VI ont la même preuve, alors le VI existant est mis à jour pour inclure « Preuve dans la clé de VI (external_id) ». S'il existe plusieurs détections avec différentes preuves, le VI existant est fermé. Les détections sont réparties sur les nouveaux VI avec « Preuve dans la clé de VI (external_id) ».

Remarque :

Si vous fournissez l'ID de vulnérabilité, les VI existants sont divisés en fonction de la preuve. Les nouvelles vulnérabilités pour cet ID de vulnérabilité ont également la preuve comme l'une des clés de VI.

Supprimer tous vos enregistrements d'éléments vulnérables et les données connexes dans Réponse aux vulnérabilités

Supprimez définitivement toutes les données Vulnerability Response (éléments vulnérables ou détections d'éléments vulnérables) ainsi que les données et enregistrements connexes de l'application Réponse aux vulnérabilités dans votre Now Platform® instance.

Avant de commencer

Supprimez de votre instance les enregistrements de détection d'éléments vulnérables, les éléments vulnérables, les groupes de vulnérabilité et tous les enregistrements connexes dans l'application Réponse aux vulnérabilités . Utilisez ce processus pour nettoyer votre instance afin d'importer des données avec un nouveau départ à partir de vos intégrations tierces, ou comme condition préalable au retour de la configuration de clé d'élément vulnérable (VI) à

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

son paramètre par défaut. Pour plus d'informations sur la configuration de la clé VI, reportez-vous à la section Configurer la clé de l'élément vulnérable.

Remarque : Cette action supprime tous les enregistrements d'éléments vulnérables et toutes les données connexes de votre instance. Ces données, une fois supprimées, ne peuvent pas être récupérées. Vous devez également suspendre l'importation de données et désactiver vos intégrations tierces actives avec Réponse aux vulnérabilités.

La suppression de vos données d'éléments vulnérables avec ce processus avant de modifier la configuration de la clé de VI est requise. La suppression de toutes les données garantit que tous vos éléments vulnérables et détections d'éléments vulnérables sont mappés et mis à jour avec les données les plus récentes à partir de la prochaine importation.

Vérifiez que les conditions suivantes s'appliquent avant de supprimer vos données :

- Vous avez la version 10.0 ou ultérieure de Réponse aux vulnérabilités installée. Pour plus d'informations, consultez Réponse aux vulnérabilités Détections d'éléments vulnérables à partir d'intégrations tierces.
- Vous souhaitez désactiver Inclure le port et rétablir le paramètre par défaut de la configuration de la clé VI.
- Vous avez des éléments vulnérables et des détections d'éléments vulnérables existants, mais vous ne voulez pas ou n'avez pas besoin de les mettre à jour et de les conserver.
- Vous avez déterminé que vous souhaitez supprimer toutes les données Vulnerability Response existantes et les enregistrements connexes pour nettoyer votre instance.

Rôle requis : sn_vul.vulnerability_admin

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Intégrations de vulnérabilité**.
2. Enregistrez toutes les intégrations actives qui sont affichées.

   Toutes les intégrations actives répertoriées avec les travaux planifiés sont désactivées avant la suppression de tous vos éléments vulnérables et données connexes, de sorte qu'aucune nouvelle donnée ne soit importée pendant la suppression des données. L'enregistrement de cette liste vous permet d'activer vos intégrations une fois la suppression terminée.

3. Passez en revue l'article Comment supprimer les données existantes de Vulnerability Response pour réimporter dans la base de connaissances HI.
4. Si un message d'avertissement vous empêche d'écrire dans la colonne Active s'affiche pour désactiver les intégrations actives, procédez comme suit.

   a. Dans la colonne Nom, cliquez sur un élément pour ouvrir l'enregistrement.

   b. Si vous ne pouvez pas modifier la case à cocher Actif, cliquez sur le lien **ici** pour modifier l'enregistrement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Cochez la case **Actif** pour désactiver l'intégration et annuler la tâche planifiée suivante.

d. Cliquez sur **Mettre à jour** pour enregistrer vos changements et revenir à la liste.

e. Vérifiez que vous avez désactivé toutes les intégrations actives de la liste Intégrations. Une fois que vous avez désactivé une intégration, elle n'apparaît plus dans la liste des intégrations actives. Pour afficher une liste d'intégrations inactives et localiser toutes les intégrations que vous avez désactivées après avoir supprimé toutes vos données de vulnérabilité, dans la colonne Actif en haut, saisissez `=faux`.

5. Poursuivez avec les étapes décrites dans l'article de la base de connaissances pour supprimer vos données de vulnérabilité existantes.
6. Une fois que vous avez confirmé que toutes les données sont correctement supprimées, accédez à **Réponse aux vulnérabilités** > **Administration** > **Configurer la granularité VI**.
7. Sur le formulaire :
   - Si vous avez supprimé des données parce que vous préférez créer vos données de vulnérabilité pour inclure le port à partir d'une nouvelle importation, activez Inclure le port et cliquez sur **Enregistrer**.
   - Si vous avez supprimé des données parce que vous souhaitez rétablir les paramètres par défaut de la clé VI, désactivez l'option Inclure le port et cliquez sur **Enregistrer**.

   Pour plus d'informations, consultez Configurer la clé de l'élément vulnérable.

Filtrage au sein de Réponse aux vulnérabilités

Les règles de tâche de rattrapage, les calculateurs et les règles d'affectation utilisent des conditions pendant l'importation, créées à l'aide du **Créateur de conditions**. Les changements apportés à leurs critères peuvent affecter les performances, car chaque enregistrement est évalué à l'aide de ces filtres.

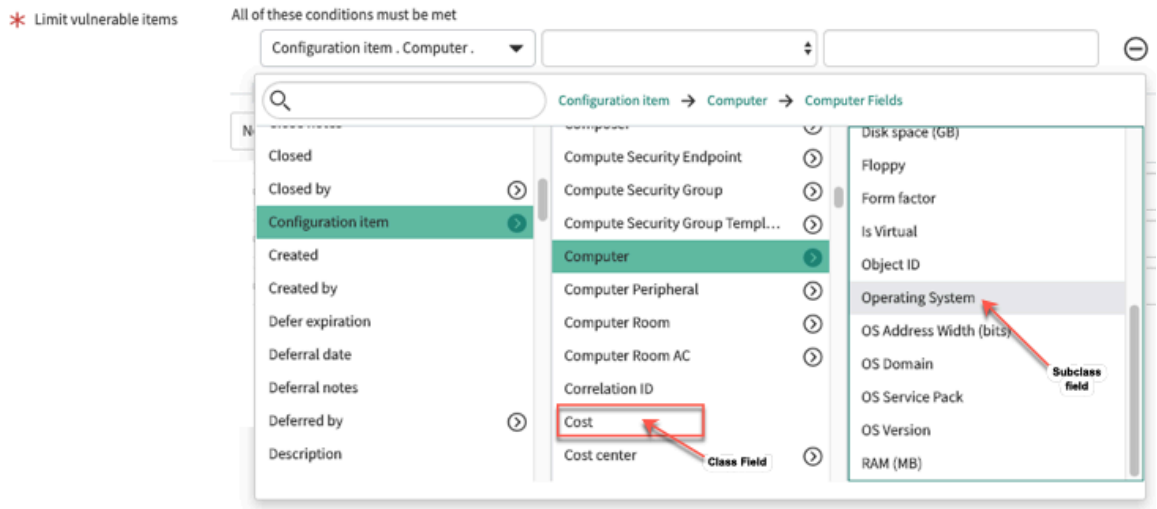
Les règles et les calculateurs fournis avec le système de base sont optimisés en termes de performances. L'édition ou la création de règles ou de calculatrices prend soin et peut nécessiter à la fois ServiceNow une Réponse aux vulnérabilités expertise.

Éviter le filtrage basé sur les champs de sous-classe

Certaines tables prennent en charge l'extension. La table CI [cmdb_ci] CMDB en est un exemple. Les tables telles que cmdb_ci_hardware et cmdb_ci_computer étendent cette table. Si vous filtrez en fonction d'un champ qui n'est pas sur la table parente, ce filtre peut être coûteux à construire et à évaluer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Par exemple, filtrer **ID d'élément de configuration** > **Coût** n'affecterait pas négativement les performances, car **Coût** est un champ de classe et non un champ de sous-classe de **l'élément de configuration**.



ID d'élément de configuration > **Ordinateur**, cependant, est une sous-classe nécessitant une remontée pas à pas vers un autre champ, en l'occurrence **Operating System**. Ce processus peut prendre plusieurs millisecondes, ce qui s'accumule rapidement, lorsque des millions d'éléments vulnérables sont importés, et affecte les performances.



Remarque : L'utilisation de la condition [contains] s'apparente à une recherche par caractères génériques et peut avoir un impact sur les performances. L'utilisation [est], dans la mesure du possible, est plus efficace.

Mappage de gravité pour Vulnerability Response

Vulnerability Response est livré avec la base de données de vulnérabilité nationale (NVD) vers le mappage de gravité ServiceNow normalisé. Les intégrations tierces ServiceNow fournissent des mappages de gravité lors de l'installation. Ces cartes peuvent être ajustées en modifiant les champs des cartes existantes.

Mappage de gravité de l'intégration de vulnérabilité Rapid7

Normalised_Severity

Calculez normalised_severity sur l'entrée tierce à l'aide de la gravité provenant de **sn_vul_nvd_entry** table. Elle est définie à l'aide des Règles métier pour rechercher la gravité normalisée **sur sn_vul_entry** table.

Source_severity

Les données de la table **severity_score** sont mappées à **source_severity** table pendant l'exécution de **l'API d'intégration de vulnérabilité Rapid7** .

Priorité

Ce champ est vide.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de gravité de l'intégration de vulnérabilité Qualys

Normalised_Severity

Calculez normalised_severity sur l'entrée tierce à l'aide de la gravité provenant de **sn_vul_nvd_entry** table. Elle est définie à l'aide des Règles métier pour rechercher la gravité normalisée **sur sn_vul_entry** table.

Source_severity

Les données du **SEVERITY_LEVEL** sont mappées à la table **source_severity** pendant l'exécution de l'intégration de la **base de connaissances Qualys** .

Priorité

Les données du champ Priorité sont obtenues à partir de la **table SEVERITY** et mappées à la table de **priorité** pendant que **l'intégration de la détection d'hôte Qualys** est en cours d'exécution à l'aide de la règle métier mappée aux données Qualys.

Remarque : Les règles métier s'exécutent en arrière-plan et vérifient la priorité pour Qualys et la mappent en conséquence. Ainsi, pour cartographier les données Qualys, BR est responsable.

Mappage de gravité de l'intégration de vulnérabilité Tenable.io

Normalised_Severity

Calculez normalised_severity sur l'entrée tierce à l'aide de la gravité provenant de **sn_vul_nvd_entry** table. Elle est définie à l'aide des Règles métier pour rechercher la gravité normalisée **sur sn_vul_entry** table.

Source_severity

Les données de **risk_factor** table sont mappées à **source_severity** table pendant que **l'intégration du module d'extension Tenable.io** est en cours d'exécution.

Priorité

Les données provenant de **severity_id** sont mappées à **source_severity** pendant l'exécution **de l'intégration des vulnérabilités Tenable.io ouvertes** .

VPR (en anglais seulement)

Les données du **score** sont mappées à **Source_risk_score** lorsque **Tenable.io intégration du module d'extension est en cours d'exécution** .

Les données de **Calculé à partir du score** sont mappées à **Source_risk_rating** lorsque Tenable.io intégration du **module d'extension est en cours d'exécution** .

Mappage de gravité de l'intégration de vulnérabilité Tenable.sc

Normalised_Severity

Calculez **normalised_severity** sur l'entrée tierce à l'aide de la gravité provenant de sn_vul_nvd_entry table. Elle est définie à l'aide des Règles métier pour rechercher la gravité normalisée **sur sn_vul_entry** table.

Source_severity

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les données de la table **riskFactor** sont mappées à **source_severity** lorsque **l'intégration du module d'extension Tenable.io** est en cours d'exécution.

Priorité

Les données de **gravité** reçues en tant que **« sévérité » : { « id » : « 0 », « name » : « Info »,** **« description » : « Informatif » }** sont mappées à **source_severity** pendant que **l'intégration des vulnérabilités ouvertes Tenable.io** est en cours d'exécution.

VPR (en anglais seulement)

Les données de **vprScore** sont mappées à **Source_risk_score** pendant **que Tenable.io intégration du module d'extension est en cours d'exécution** .

Les données de **Calculé à partir du vprScore** sont mappées à **Source_risk_rating** lorsque **Tenable.io intégration du module d'extension est en cours d'exécution** .

Mappage de gravité TVM

Normalised_Severity

Calculez normalised_severity sur l'entrée tierce à l'aide de la valeur distincte provenant de **sn_vul_nvd_entry** table. Elle est définie à l'aide des Règles métier pour rechercher la gravité normalisée **sur sn_vul_entry** table.

Source_severity

Les données de **la** table de gravité sont mappées aux **source_severity** lorsque **l'intégration de la vulnérabilité Microsoft TVM (CVE)** est en cours d'exécution.

Priorité

Ce champ est vide.

Créer une carte de Réponse aux vulnérabilités gravité

Réponse aux vulnérabilités Le mappage de gravité transforme les champs de gravité sources tierces en champs reconnaissables au format Réponse aux vulnérabilités.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Réponse aux vulnérabilités Livré avec la base de données de vulnérabilité nationale (NVD) au mappage de gravité normalisé ServiceNow . ServiceNow Intégrations tierces telles que le Qualys Vulnerability Integration Fournissez des mappages de gravité lors de l'installation. Ces cartes peuvent être ajustées en modifiant les champs des cartes existantes.

La création ou la modification d'une carte de gravité est uniquement destinée aux mappages tiers personnalisés ou non standard dans votre environnement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Mappage de gravité normalisée**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Mappage de champs

Champ	Description
Source	Nom de la source pour le mappage de gravité.
Valeur de la source	Valeur de gravité de la source.
Valeur cible	La valeur de gravité cible. Les choix possibles sont les suivants : ◦ 1 - Critique ◦ 2 : élevé ◦ 3 : moyen ◦ 4 : faible ◦ 5 : aucun

4. Répétez l'étape 3 pour chaque niveau de gravité de la source.
5. Cliquez sur **Envoyer**.

Définir les classifications de service pour Réponse aux vulnérabilités la génération de rapports et les listes connexes

Mettez davantage l'accent sur la génération de rapports et les listes connexes en Réponse aux vulnérabilités définissant des classifications de services. En outre, la réduction du nombre de classifications de service demandées peut améliorer les performances de la collecte de Réponse aux vulnérabilités données.

Avant de commencer

Rôle requis : administrateur

Remarque :

La modification des propriétés système nécessite à la fois ServiceNow une expertise et Réponse aux vulnérabilités une expertise.

Procédure

1. Entrez `sys_properties_list.do` dans la barre de navigation de gauche.
2. Cliquez sur **Entrée**.
3. Dans le menu **Rechercher** , sous **Nom** , saisissez `sn_vul.service_classifications`.
4. Ouvrez la *`sn_vul.service_classifications`* propriété système.
5. Dans la zone de texte **Valeur** , saisissez la liste des classifications de service de votre choix, séparées par des virgules.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque ce paramètre est vide, tous les services sont répertoriés.

Exemples :

Pour afficher les services d'entreprise, les services techniques et les services d'application et exclure les offres de service, les services partagés et les services non classifiés, définissez la valeur sur : **Service d'entreprise, Service technique, Service d'application**.

Pour afficher les services d'application, définissez la valeur sur : **Service d'application**.

6. Cliquez sur **Mettre à jour**.
   Les données de chaque rapport et liste connexe des éléments vulnérables sont filtrées par classification de service lors de la prochaine exécution de la tâche d'analyse des performances nocturne.

Vérifier les champs sélectionnés dans la table des éléments vulnérables

Activez l'audit pour les champs que vous spécifiez dans la table Élément vulnérable [sn_vul_vulnerable_item]. Cette méthode d'audit est utile lorsque vous souhaitez auditer des champs que vous ne pouvez pas auditer par défaut.

Avant de commencer

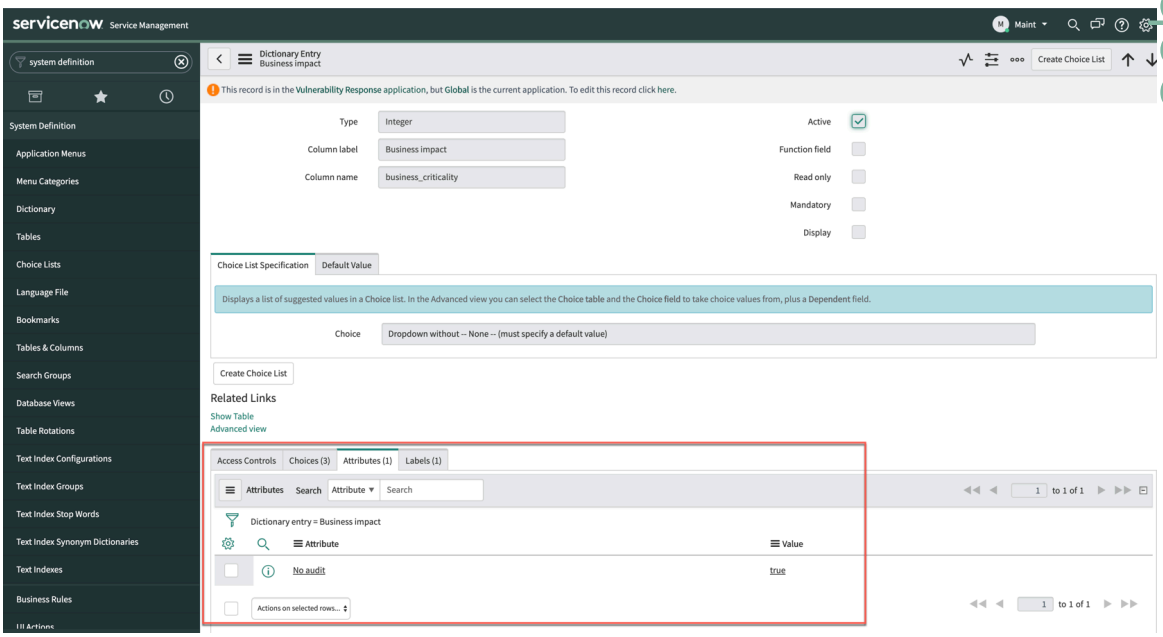
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

La table sn_vul_vulnerable_item est auditable par défaut. Les champs dont l'attribut no_audit est défini sur vrai ne sont pas auditables. Pour plus d'informations sur l'audit des tables, consultez Activer l'audit pour une table .

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Définition du système** > **Tables** et recherchez la table sn_vul_vulnerable_item.
   La liste des entrées de dictionnaire de la table s'affiche.
2. Pour activer l'audit pour un champ, cliquez sur le nom de l'entrée.
   La page d'entrée du dictionnaire correspondant à cette entrée s'affiche.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Accédez à la **Attributs** > **Pas d'audit**.
   La page Attribut de dictionnaire s'affiche.
4. Pour supprimer l'attribut no audit=true, cliquez sur **Supprimer**.
   L'audit de ce champ est activé.

Réponse aux vulnérabilités Configuration du cadre de travail de la tâche en arrière-plan

Définissez le cadre de travail de la tâche en arrière-plan dans votre Now Platform® instance. Ces changements de configuration peuvent vous aider à améliorer les performances en réduisant la quantité de ressources système utilisées pour exécuter vos tâches en arrière-plan.

Que pouvez-vous modifier dans le cadre de travail de la tâche en arrière-plan ?

Avec le module de configuration de la tâche en arrière-plan, vous disposez des options de réglage suivantes dans le cadre de travail :

- Vous pouvez définir le nombre de tâches en arrière-plan qui s'exécutent simultanément pour Réponse aux vulnérabilités les processus.
- Pour les tâches longues qui s'exécutent en arrière-plan et traitent de grandes quantités de données, vous pouvez créer des partitions pour traiter les données en blocs plus petits.
- Vous pouvez annuler une tâche.

Pourquoi configurer le cadre de travail des tâches en arrière-plan ?

Les tâches en arrière-plan dans votre Now Platform® sont conçues pour s'exécuter pendant de longues périodes afin d'exécuter plusieurs processus sur vos enregistrements dans Réponse aux vulnérabilités. Ces tâches étaient auparavant basées sur des règles métier qui s'exécutent de manière asynchrone. Il n'existe aucune limite au nombre de ces travaux qui peuvent s'exécuter en arrière-plan dans votre instance afin que les grandes quantités d'enregistrements impactés par ces travaux puissent être traitées. Lorsque plusieurs tâches dont l'exécution prend beaucoup de temps s'exécutent simultanément en arrière-plan, les ressources système utilisées pour exécuter vos travaux planifiés sont impactées, ce qui peut à son tour avoir un impact négatif sur vos performances.

La configuration du cadre de travail des tâches en arrière-plan peut vous aider à améliorer vos performances en réduisant la quantité de ressources système utilisées pour exécuter vos tâches en arrière-plan.

Termes clés

Aptitude de la tâche

Décrit les emplois particuliers. Par exemple, une tâche particulière peut inclure les options suivantes :

- La tâche peut être exécutée en parallèle avec une autre tâche du même type.
- La tâche peut être partitionnée.
- La tâche peut être annulée en cours d'exécution.

Concurrence

Désigne des tâches ou des éléments de tâches qui s'exécutent en parallèle.

Partition

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les partitions sont des éléments de travail qui peuvent être divisés afin qu'ils puissent être traités en parallèle pour obtenir de meilleures performances. Désigne généralement les tâches avec de longs temps d'exécution.

Configuration de la tâche

Désigne les paramètres d'une tâche planifiée particulière.

Tâche planifiée

Les tâches planifiées sont des tâches automatisées qui peuvent être effectuées à une heure spécifique ou selon un calendrier récurrent.

Ressources système

Fait référence à la quantité de ressources système dont vous avez besoin pour prendre en charge un nombre donné de tâches en arrière-plan et de tâches planifiées dans votre environnement.

Propriété système

Les propriétés système stockent des informations de configuration qui ne changent que rarement, voire jamais. Chaque fois que vous modifiez ou ajoutez une propriété système, le système vide le cache pour maintenir la synchronisation de tous les nœuds de la grappe. Cette purge du cache a un impact sur les performances.

Règle métier

Une règle métier est un script de serveur qui s'exécute lorsqu'un enregistrement est affiché, inséré, mis à jour ou supprimé, ou lorsqu'une table est interrogée. Les règles métier accomplissent des tâches telles que le changement automatique des valeurs dans les champs de formulaire lorsque certaines conditions sont satisfaites, ou la création d'événements pour les notifications par e-mail et les actions des scripts.

Cas d'utilisation pour définir le cadre de travail de la tâche en arrière-plan

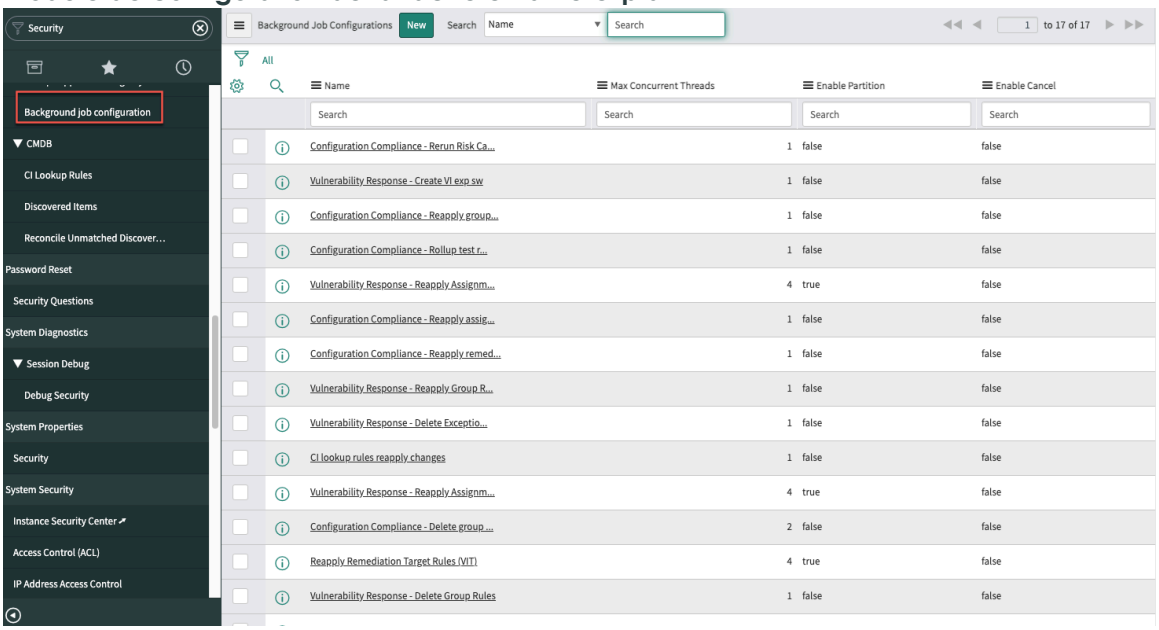
Par exemple, la tâche en arrière-plan qui applique des règles de cible de rattrapage pour les enregistrements d'éléments vulnérables (VIT) et les enregistrements d'éléments vulnérables (AVIT) d'Application Vulnerability Response traite simultanément de grandes quantités d'enregistrements avec plusieurs tâches.

Selon la taille de l'importation et le nombre d'enregistrements dont vous disposez dans votre environnement, cette tâche peut utiliser une grande quantité de vos ressources système disponibles et prendre beaucoup de temps. Les tâches de maintenance du système ou d'autres travaux planifiés peuvent s'exécuter plus lentement.

Dans le module de configuration des tâches en arrière-plan, les tâches sont répertoriées par nom et un ID de configuration unique. Sur ces enregistrements, vous pouvez définir le nombre de tâches que vous souhaitez exécuter simultanément pour une tâche d'arrière-plan donnée. Vous pouvez également configurer la tâche pour traiter des partitions de données afin que les tâches s'effectuent plus rapidement et plus facilement et utilisent moins de ressources système. Vous pouvez également annuler une tâche si vous déterminez qu'elle est en cours d'exécution trop longtemps.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Module de configuration de la tâche en arrière-plan



Pour plus d'informations sur les étapes requises pour définir les configurations des tâches en arrière-plan, reportez-vous à la section Définir des configurations de tâche en arrière-plan dans Réponse aux vulnérabilités.

Définir des configurations de tâche en arrière-plan dans Réponse aux vulnérabilités

Définissez le nombre de tâches que vous souhaitez exécuter simultanément pour une tâche en arrière-plan donnée. Vous pouvez également configurer la tâche pour importer des partitions de données afin que les tâches s'effectuent plus rapidement et plus facilement et utilisent moins de ressources système. Vous pouvez également annuler une tâche si vous déterminez qu'elle est en cours d'exécution trop longtemps.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou Gestionnaires des vulnérabilités avec le rôle granulaire sn_sec_cmn.manage_background_job

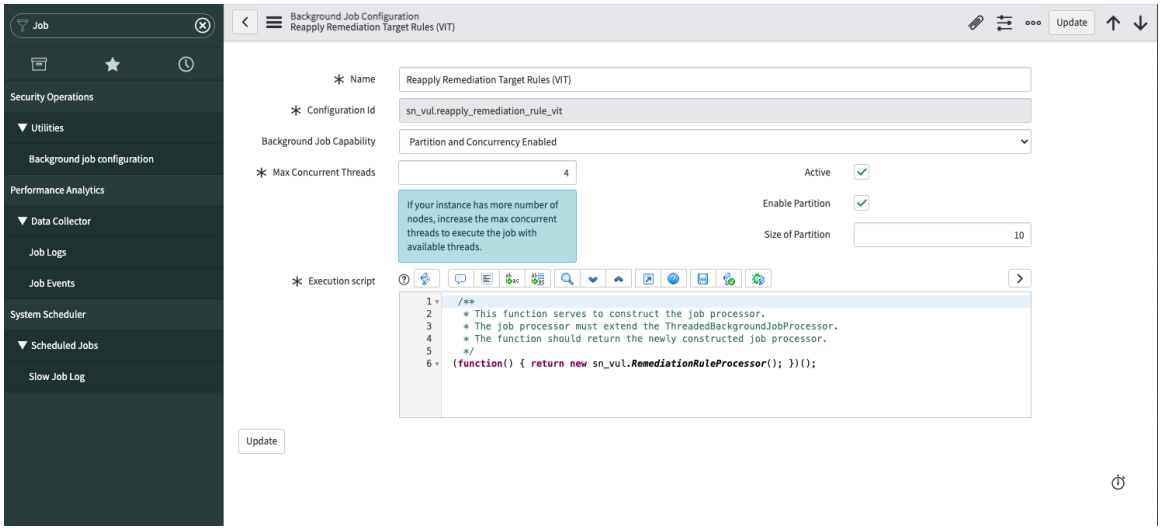
Reportez-vous à la section ci-dessous pour obtenir un exemple.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Configurations des tâches en arrière-plan**.
2. Dans la colonne Nom, cliquez sur un enregistrement pour l'ouvrir.
3. Modifiez les champs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Champ	Description
Nom	Nom de la tâche.
ID de configuration	Lecture seule. ID unique utilisé pour identifier la tâche.
Aptitude de la tâche en arrière-plan	Choisissez-en un. ◦ Partition et concurrence activées : une tâche avec une longue durée d'exécution peut être divisée et la tâche peut être exécutée en parallèle avec une autre tâche du même type. ◦ Concurrence activée : la tâche peut être exécutée en parallèle avec une autre tâche du même type. ◦ Annulation activée : la tâche peut être annulée. ◦ Concurrence et annulation activées : la tâche peut être exécutée en parallèle d'une autre tâche et être annulée. ◦ Partition, concurrence et annulation activées : une tâche avec une longue durée d'exécution peut être divisée, la tâche peut être exécutée en parallèle avec une autre tâche du même type et la tâche peut être annulée. ◦ Aucun La valeur affichée indique si une tâche prend en charge le partitionnement, la concurrence et l'annulation.
Nombre maximal de threads simultanés	ce champ n'est affiché que si la concurrence est prise en charge. Entrez le nombre maximal de tâches que vous souhaitez que cette configuration exécute en parallèle. Le nombre de travaux

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	planifiés pris en charge par votre instance est par défaut de 10. Vous pouvez réduire cette valeur si vous pensez pouvoir utiliser ou disposer de ressources système inférieures pour exécuter vos tâches en arrière-plan.
Actif	Activer ou désactiver la tâche Si une tâche est désactivée, vous ne pouvez pas créer de tâches de ce type. Les tâches existantes dans la file d'attente ne seront pas traitées.
Activer la partition	ce champ n'est affiché que si le partitionnement est pris en charge. Cette option vous permet de limiter et de définir le nombre d'éléments que cette tâche peut traiter à la fois. Le champ Taille de la partition est également affiché. Si vous laissez ce champ désactivé, les tâches en arrière-plan qui prennent en charge le partitionnement traitent tous les éléments de votre instance avec cette tâche.
Taille de la partition	ce champ n'est affiché que si le partitionnement est pris en charge. La valeur par défaut est de 10 000 éléments. Entrez une valeur pour le nombre d'éléments par bloc de données que vous souhaitez que cette tâche traite. Cette option est disponible pour les tâches qui traitent un grand nombre d'enregistrements tels que les éléments vulnérables, les tâches de rattrapage, les résultats des tests et les groupes de résultats des tests.
Script d'exécution	Affiche le processeur de tâche utilisé pour exécuter cette tâche. Une méthode par défaut est fournie pour les tâches qui prennent en charge le partitionnement.
Activer l'annulation	ce champ s'affiche uniquement si l'annulation de tâche est prise en charge. Cette option est prise en charge pour les tâches qui traitent les éléments détectés et réappliquent les règles de CI.

4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

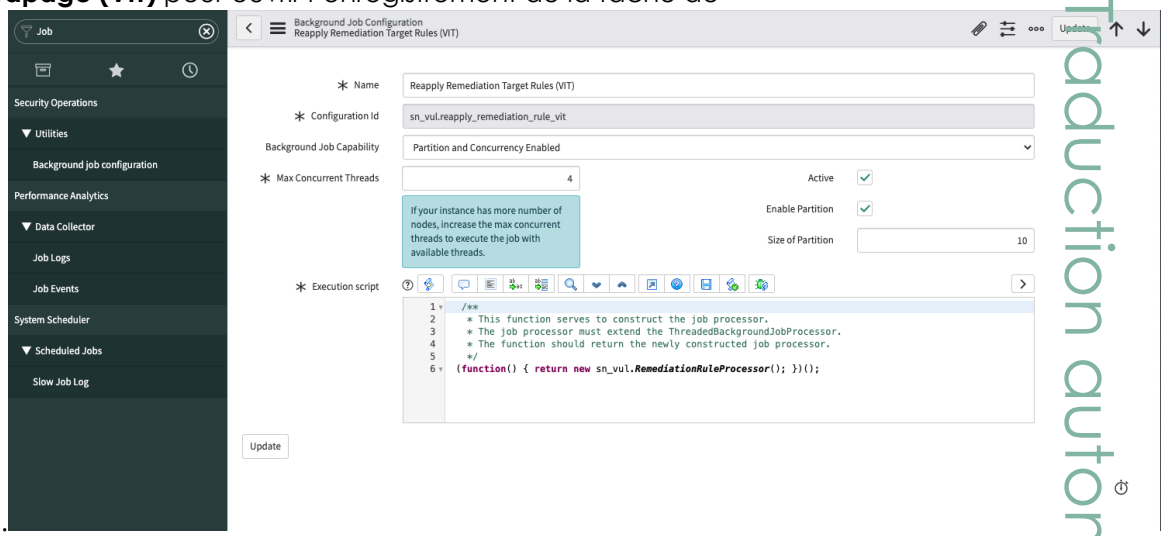
Consultez l'exemple suivant pour savoir comment vérifier les résultats de vos changements de configuration.

Deux configurations de tâches de règles de cibles de rattrapage sont incluses dans l'application, une pour les éléments vulnérables et l'autre pour les éléments vulnérables de l'application :

- Réappliquer les règles de cibles de rattrapage (VIT)
- Réappliquer les règles de cibles de rattrapage (AVIT)

Supposons que vous apportiez un changement à vos règles de cible de rattrapage et que vous souhaitiez les réappliquer sans utiliser la plupart de vos ressources de traitement système disponibles. Pour vous aider à limiter les ressources de traitement, vous pouvez contrôler le nombre de tâches en arrière-plan que vous exécutez et le nombre d'éléments que vous traitez par tâche dans le module Configurations des tâches en arrière-plan.

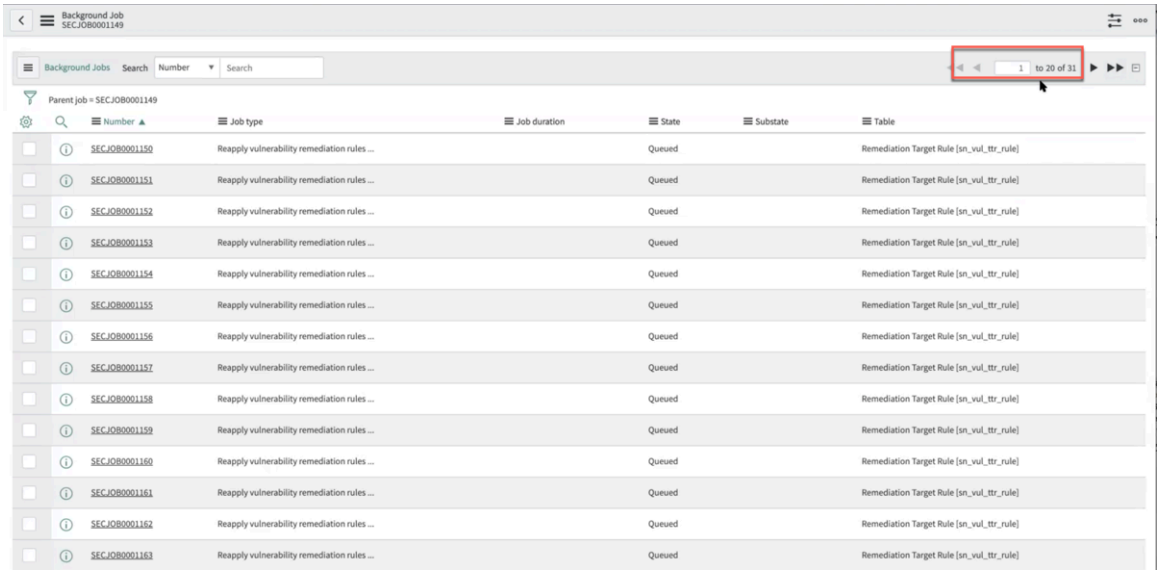
5. Pour définir ces paramètres, accédez à **Security Operations** > **Configurations des tâches en arrière-plan** et cliquez sur **Réappliquer les règles de cibles de rattrapage (VIT)** pour ouvrir l'enregistrement de la tâche de configuration.



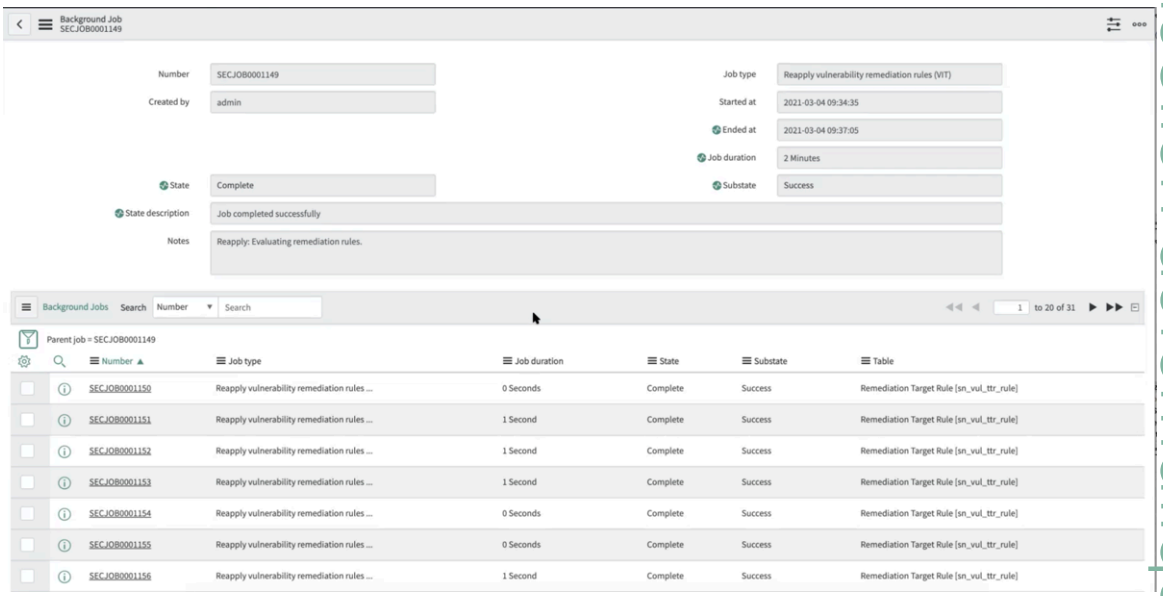
Pour les besoins de l'exemple, disons que vous savez que vous avez un peu plus de 300 VI.

6. Sur l'enregistrement de tâche de configuration ouvert, modifiez la valeur Taille de la partition de **4** à **10**.
7. Accédez à la **Réponse aux vulnérabilités** > **Règles de cibles de rattrapage**, localisez la règle de rattrapage Réappliquer la vulnérabilité que vous avez modifiée, sélectionnez l'enregistrement dans la liste et cliquez sur **Appliquer les changements** pour réévaluer vos règles cibles pour vos VI existants.
   La tâche Réappliquer les règles de rattrapage de vulnérabilité (VIT) est en file d'attente.
8. Cliquez sur le lien **Afficher l'état** pour afficher l'enregistrement de tâche en arrière-plan et vérifier que les tâches sont en file d'attente, comme illustré dans l'image suivante.
   Pour cet exemple, 31 tâches sont créées pour traiter les règles cibles pour 307 VI (maximum de 10 éléments par tâche). Ces tâches sont des tâches enfants de la tâche d'arrière-plan principale. Les tâches enfants traitent les enregistrements de façon séquentielle.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Lorsque toutes les tâches sont terminées avec succès, les champs sont mis à jour sur l'enregistrement de la tâche en arrière-plan.



Traduction automatique

9. Accédez à vos éléments vulnérables et vérifiez qu'ils reflètent votre nouveau changement de règle.

Traitement parallèle avancé pour les tâches en arrière-plan dans Réponse aux vulnérabilités

Ce paramètre avancé permet de contrôler le nombre total de tâches en arrière-plan traitées en parallèle, quel que soit le type de tâche.

Avant de commencer

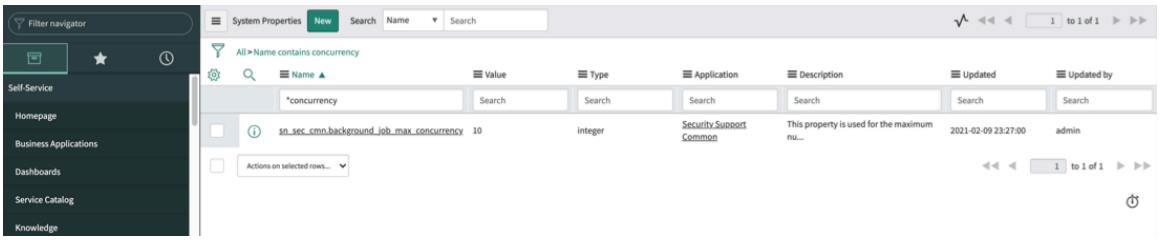
Rôle requis : sn_vul.vulnerability_admin ou gestionnaires des vulnérabilités avec le rôle granulaire sn_sec_cmn.manage_background_job

Remarque : Cette procédure nécessite des connaissances avancées en programmation.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans le navigateur de filtre, saisissez **sys_properties.list** et localisez la *sn_sec_cmn.background_job_max_concurrency* propriété système.



2. Cliquez dessus pour ouvrir l'enregistrement.

   Par défaut, la *sn_sec_cmn.background_job_max_concurrency* propriété système exécute un maximum de 10 tâches en arrière-plan en parallèle.

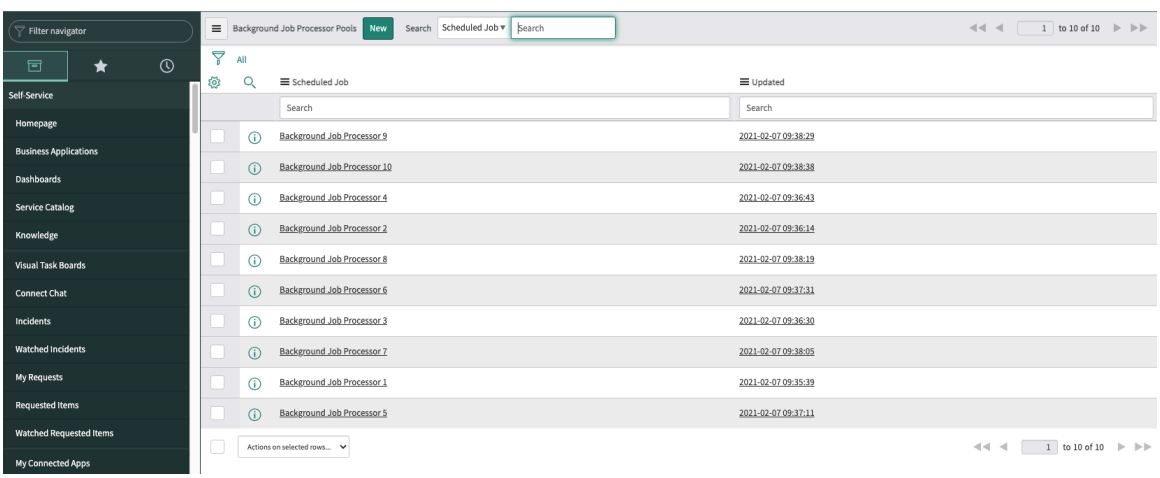
   Si votre instance comporte un faible nombre de nœuds, vous pouvez réduire cette valeur dans la propriété système. Par exemple, supposons que vous ayez sept règles d'affectation sur votre liste Règles de groupe. Sur l'enregistrement de configuration de la tâche Réappliquer les règles d'affectation, trois tâches sont définies pour le nombre maximal de threads simultanés. Votre valeur de concurrence pour votre infrastructure est de 10, mais votre système est une instance à nœud unique, de sorte que vous pouvez traiter simultanément deux tâches partitionnées à partir de votre tâche Réappliquer les règles d'affectation. Si vous définissez le nombre maximal de threads simultanés sur un enregistrement de tâche Règles d'affectation, tous les types de tâches Réappliquer les règles d'affectation sont traités séquentiellement.

   Inversement, si votre instance dispose de plusieurs nœuds, vous pouvez augmenter cette valeur, mais vous devez également ajouter plus de travaux planifiés pour effectuer ce changement.

   Pour augmenter le nombre de travaux planifiés, dupliquez un travail planifié autant de fois que nécessaire pour correspondre à la valeur selon laquelle vous avez augmenté votre propriété système. Par exemple, par défaut, il y a 10 travaux planifiés. Donc, si vous voulez 20 tâches, vous devez dupliquer une tâche 10 fois.

   Les dix travaux planifiés inclus avec le Now Platform® pour traitement sont affichés dans la table sn_sec_cmn_background_job_processor_pool.

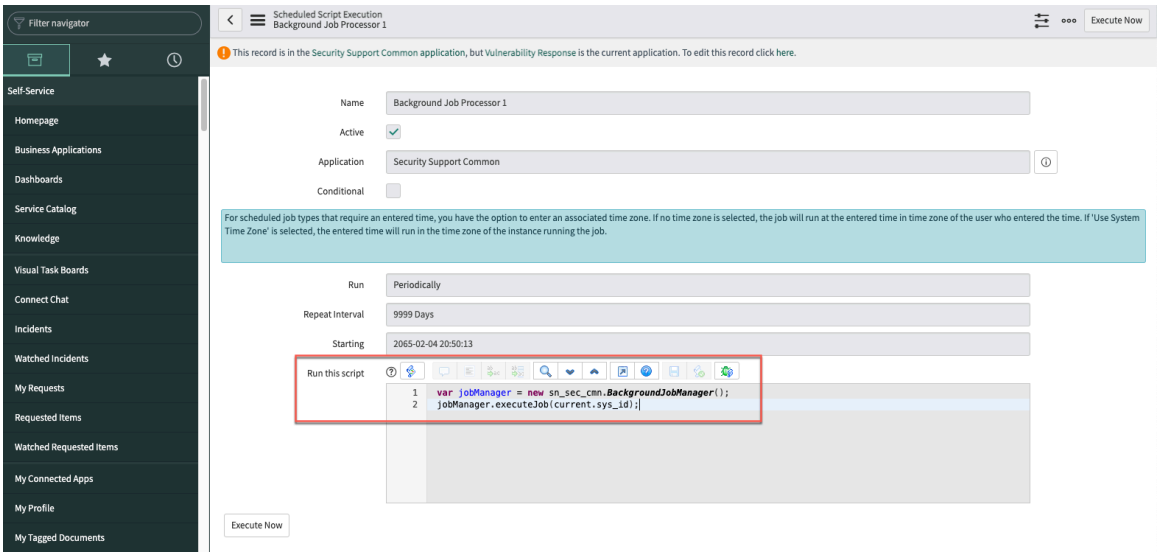
3. Dans le navigateur de filtre, saisissez **sn_sec_cmn_background_job_processor_pool.list**



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur une tâche pour la copier et la dupliquer autant de fois que nécessaire afin que le nombre de tâches corresponde à la valeur selon laquelle vous avez augmenté votre propriété système.



5. Une fois la tâche planifiée définie, ajoutez une référence en cliquant sur **Nouveau** dans la liste sn_sec_cmn_background_job_processor_pool de la tâche que vous avez copiée.

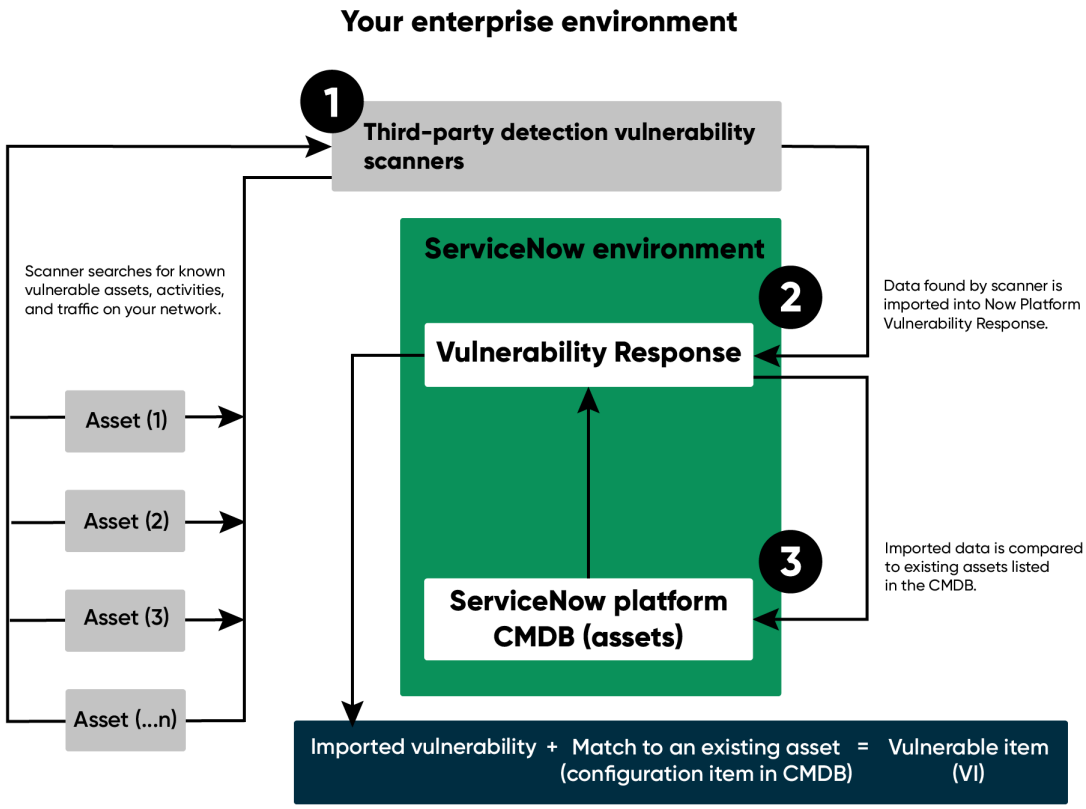
Intégrations de Réponse aux vulnérabilités

Réponse aux vulnérabilités inclut la prise en charge des intégrations tierces. Vous trouverez dans cette section des directives de base pour le développement de vos propres intégrations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations tierces



Les vulnérabilités importées à partir de la base de données de vulnérabilité nationale (NVD) et les données de détection provenant d'analyseurs tiers sont rapprochées avec les actifs de votre CMDB. Lorsqu'une vulnérabilité importée correspond à un actif existant, un élément vulnérable est créé. Les éléments vulnérables sont automatiquement regroupés en tâches de correction, évalués en fonction du risque et du contexte business, classés par ordre de priorité et affectés aux équipes appropriées pour le rattrapage.

Remarque :

Les intégrations tierces sont traitées séparément. Si plusieurs applications d'intégration tierces sont utilisées dans votre environnement, il n'y a pas de déduplication des éléments vulnérables (VI) entre les intégrations. Par exemple, déduplication VI entre Rapid7 et Qualys n'est pas disponible.

Toutefois, des incohérences dans le nombre de détections entre un scanner tiers (par exemple, Qualys) et des VI dans votre ServiceNow instance sont attendues, car nous dédupliquons les adresses IP, les ports, etc.

Pour en savoir plus sur les intégrations tierces prises en charge par Réponse aux vulnérabilités des applicationsIntégrer Réponse aux vulnérabilités des applications avec d'autres applications

- Intégration de CISA Known Exploit Vulnerability (KEV)
- Présentation de l'intégration des vulnérabilités de Microsoft Threat and Vulnerability Management
- Présentation de l'intégration de l'orchestration des correctifs HCL BigFix avec Réponse aux vulnérabilités

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Présentation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités
- Présentation des intégrations NVD
- Qualys Vulnerability Integration
- Présentation de Intégration des vulnérabilités Rapid7
- Shodan Exploit Integration
- Présentation de l'intégration Tenable Vulnerability
- Microsoft Security Response Center Solution Integration

  Le Microsoft Security Response Center Solution Integration est disponible avec Gestion des solutions pour vulnérabilités. Pour plus d'informations sur l'installation et la configuration du Microsoft Security Response Center Solution Integration et du Intégration de solution Red Hat, reportez-vous à la section Installer l'application Gestion des solutions pour Réponse aux vulnérabilités. Vous pouvez configurer, modifier, planifier et lancer les et les Microsoft Security Response Center Solution IntegrationIntégration de solution Red Hat à la demande à partir de l'assistant de configuration.

Notes supplémentaires pour les intégrations

Si plusieurs déploiements sont pris en charge pour une intégration, reportez-vous Créer des importations séparées par domaine pour une intégrationà .

- Vous pouvez installer, configurer, planifier et lancer à la demande un grand nombre d'applications d'intégration à partir de l'Assistant de configuration.
- Vous pouvez installer l'application à partir de l'Assistant Intégration des vulnérabilités Rapid7 de configuration, mais la configuration n'est pas prise en charge pour cette intégration à partir de l'Assistant de configuration. Consultez Installer Intégration des vulnérabilités Rapid7 pour plus d'informations.
- L'application Tenable pour Réponse aux vulnérabilités de Tenable est créée et gérée par Tenable. Consultez leur documentation à l'adresse suivante : Tenable pour Réponse aux vulnérabilités.

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

À partir de VR v17.1, les noms d'état des processus d'intégration suivants ont été mis à jour :

Nom de l'état antérieur à la version 17.1	Nom de l'état à partir de la version 17.1
En cours de traitement	En cours de récupération
WaitComplete (en anglais seulement)	En attente/en cours de traitement

Remarque : Vous pouvez afficher les pièces jointes qui sont téléchargées et traitées. Lorsque l'état de l'exécution de l'intégration est `En attente`, le pourcentage d'achèvement de l'intégration s'affiche.

Intégrations créées manuellement

Vous pouvez ajouter d'autres intégrations qui ne sont pas disponibles en tant qu'applications ServiceNow Store , selon les besoins. Consultez Créer manuellement une intégration de vulnérabilité pour plus d'informations.

Présentation des intégrations NVD

Les intégrations NVD utilisent des données importées du produit National Vulnerability Database (NVD) du National Institute of Standards and Technology (NIST) pour vous aider à déterminer l'impact et la priorité des failles dans votre code. Exécutez cette intégration dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit de scanner tiers.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Le NVD NIST collecte à la fois des données CVE (Common Vulnerabilities and Exposures) et CPE (Common Platform Enumeration) et met ces données à la disposition du Now Platform®. Il s'intègre Réponse aux vulnérabilités facilement pour mapper les vulnérabilités CVE et CPE, enrichissant ainsi les données dans votre instance.

Important : Un utilisateur d'exécution en tant que configuré est défini pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Une fois installée, l'intégration de l'API NIST National Vulnerability Database Integration (CVE uniquement) est appelée automatiquement en tant que tâche planifiée et s'exécute quotidiennement. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conseil : L'activation de ce module d'extension pour les instances de production peut nécessiter une licence distincte.

Versions disponibles

Version	Notes de publication
Réponse aux vulnérabilités Intégration avec NVD v1.2	

Importation initiale des données de vulnérabilité avec les intégrations NVD et CWE

1. Effectuez une importation initiale des données CWE avec CWE Comprehensive 2000 Integration.

   Consultez Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE. Vous effectuez les mises à jour CWE **sur demande** à partir de l'enregistrement d'intégration par défaut, et vous devez le configurer.

   Remarque : Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. Le jour par défaut pour la mise à jour NVD est **Hebdomadaire** , le **lundi**.

2. Vérifiez que l'application Réponse aux vulnérabilités Integration with NVD est installée et qu'une importation de données initiale à partir de l'API NIST National Vulnerability Database Integration (CVE uniquement) ou de l'API NIST National Vulnerability Database Integration (CVE et CPE) réussit.

   Pour les CPE, vérifiez qu'une importation de données initiale à partir de l'API - NIST National Vulnerability Database Integration (CPE uniquement) réussit.

   L'activation de ce module d'extension pour les instances de production peut nécessiter une licence distincte. Une fois le module d'extension installé, l'API NIST National Vulnerability Database Integration (CVE uniquement) est activée par défaut. Il fonctionne tous les jours. Consultez Installer l'intégration Réponse aux vulnérabilités dans la base de données de vulnérabilité nationale NIST pour plus d'informations.

3. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Consultez votre documentation d'intégration à l'adresse Intégrations de Réponse aux vulnérabilités pour plus d'informations sur les intégrations tierces.

Présentation des données de vulnérabilité et des éléments vulnérables importés

Dans votre Now Platform instance, chaque vulnérabilité importée est représentée par une entrée de vulnérabilité dans les bibliothèques sources des produits de scanner tiers comme Qualys, par exemple. Les éléments vulnérables (VI) qui sont importés et mis à jour dans votre instance sont des références à des bibliothèques tierces, telles que la Qualys bibliothèque. Une bibliothèque tierce peut, à son tour, faire référence au NVD.

Par exemple, lorsque vous ingérez des données de vulnérabilité tierces à partir d'un produit comme Qualys, vous ingérez des VI qui font référence à un QID (Qualys identificateur). Dans le cas de Qualys, ce QID fait à son tour référence à un CVE de la bibliothèque NVD. Lorsque vous cliquez sur ce QID dans une tâche de rattrapage ou un enregistrement d'élément vulnérable dans l'application Réponse aux vulnérabilités , et que vous avez exécuté les intégrations NVD et CWE pour ingérer des données, vous affichez des données

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de vulnérabilité actuelles et enrichies qui vous permettent de voir les relations qui existent entre vos VI et CVE, CWE et CPE.

Avant d'exécuter un scanner tiers qui Qualys possède sa propre bibliothèque, vous devez d'abord installer et exécuter, au minimum, l'intégration NIST National Vulnerability Database Integration - API (CVE uniquement) (comprend également les détails liés à CISA), l'intégration CWE pour ingérer les données de vulnérabilité. Ces importations de données NVD et CWE enrichissent vos Réponse aux vulnérabilités données OR Réponse aux vulnérabilités des applications avant d'importer des données avec un produit tiers.

Pour plus d'informations sur la gestion et l'affichage des bibliothèques NVD, CWE et tierces, consultez Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces et Afficher Réponse aux vulnérabilités les bibliothèques de vulnérabilité.

Après avoir vérifié l'importation réussie de NVD, pour enrichir davantage vos données de vulnérabilité, Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE.

Effectuez les importations NVD et CWE avant d'importer les données de vulnérabilité avec un produit tiers. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Consultez votre documentation d'intégration à l'adresse Intégrations de Réponse aux vulnérabilités pour plus d'informations sur les intégrations tierces.

Localisation des intégrations NVD

Pour afficher les intégrations NVD, accédez à **Vulnerability Response ou Application Vulnerability Response** > **Administration** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base.

Remarque : Par défaut, seule l'intégration NIST National Vulnerability Database Integration - API (CVE uniquement) est active.

Intégrations NVD

Intégration	Description
NIST National Vulnerability Database Integration - API (CVE uniquement)	Récupère uniquement les données de vulnérabilité NIST NVD (CVE). Par défaut, cette intégration est automatiquement définie pour s'exécuter quotidiennement.
NIST National Vulnerability Database Integration-API (CPE uniquement)	Récupère les données CPE à partir de NIST NVD. Cette intégration est désactivée par défaut. Activez cette intégration si vous souhaitez capturer des données CPE qui incluent un format de nom formel, une méthode de vérification des noms par rapport à un système et un format de description pour lier le texte et les tests à un nom. Ces informations sont stockées dans un logiciel vulnérable. Cette intégration est définie pour s'exécuter quotidiennement et est inactive par défaut. Pour activer cette intégration, reportez-vous à la section Activer l'API NIST National Vulnerability Database (CPE uniquement).
NIST National	Récupère les données CPE associées aux CVE extraits à partir de NIST NVD. Cette intégration est désactivée par défaut.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations NVD (suite)

Intégration	Description
Vulnerability Database Integration-API (CPE non mappé)	Activez cette intégration si vous souhaitez capturer des données CPE qui incluent un format de nom formel, une méthode de vérification des noms par rapport à un système et un format de description pour lier le texte et les tests à un nom. Ces informations sont stockées dans une liste connexe d'enregistrement d'entrée de vulnérabilité NVD. Cette intégration est définie pour s'exécuter sur demande et est inactive par défaut. Pour activer cette intégration, reportez-vous à la section Activer la base de données des vulnérabilités nationale NIST : API (CPE non mappé).

Important : L'intégration « NIST National Vulnerability Database Integration-API (CVE and CPE) » est déconseillée.

Pour les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation de l'intégration NVD (Base de données nationale des vulnérabilités).

Préparation des intégrations NVD

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Préparez l'intégration en effectuant ces tâches. Les intégrations NVD supposent que vous connaissez la base de données de vulnérabilité nationale (NVD) du NIST.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter les intégrations NVD, apportez les changements de configuration nécessaires en fonction de vos besoins.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE

Les importations DATAà partir de CWE enrichissent davantage les données de vulnérabilité dans votre instance. Utilisez les enregistrements CWE (Common Weakness Enumeration) téléchargés à partir de la base de données CWE pour référence lorsque vous décidez si une vulnérabilité doit être remontée. Exécutez cette intégration dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit de scanner tiers.

Avant de commencer

Rôles requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. Le jour par défaut pour la mise à jour NVD est **Hebdomadaire** , le **lundi**.

Mettez à jour régulièrement les enregistrements de faiblesses courantes à partir de la base de données Common Weakness Enumeration. Vous pouvez également mettre à jour le script par défaut ou écrire vos propres scripts, selon vos besoins.

Chaque enregistrement CWE inclut également un article de la base de connaissances associé qui décrit la faiblesse. Vous ne pouvez pas escalader une vulnérabilité à partir de la page Common Weakness Enumerations.

- Si vous disposez du rôle administrateur, vous pouvez ajouter des référentiels à la tâche planifiée.
- Si vous disposez de sn_vul.vulnerability_read, vous pouvez exécuter la tâche planifiée.
- Si vous disposez de sn_vul.vulnerability_write, vous pouvez modifier les détails de la tâche planifiée.

Pourquoi et quand exécuter cette tâche

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.
2. Sélectionnez la tâche planifiée **CWE Comprehensive 2000 Integration** .
3. Modifiez les champs selon vos besoins.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire d'intégration de vulnérabilité

Champ	Description
Nom	Nom de la tâche planifiée.
Actif	Indique si la tâche planifiée est active. Si vous ne souhaitez pas que la tâche s'exécute pendant une période spécifique, vous pouvez configurer les paramètres que vous souhaitez utiliser et désactiver la tâche.
Exécuter	Fréquence à laquelle vous souhaitez que la tâche s'exécute. Les champs suivants sont affichés ou masqués en fonction des paramètres que vous avez définis dans ce champ. **Remarque :** La mise à jour CWE est **Sur demande** par défaut. Définissez une période planifiée antérieure à vos mises à jour NVD. Les choix sont les suivants : ◦ Tous les jours : choisissez une **heure** ◦ Hebdomadaire : (choix le plus courant) Choisissez un **jour** et une**heure** ◦ Mensuel : choisissez **le jour** et **l'heure** ◦ Périodiquement : choisissez un **intervalle de répétition**, la date et l'heure **de début** ◦ Une fois : choisissez une date et une heure **de démarrage**
Jour	Jour où vous souhaitez que la tâche planifiée s'exécute. Si vous avez sélectionné **Hebdomadaire** dans le champ **Exécuter** , ce champ affiche les jours de la semaine. Si vous avez sélectionné **Mensuel** dans le champ **Exécuter** , ce champ affiche les jours du mois. **Remarque :** Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. Le jour par défaut pour la mise à jour NVD est **Hebdomadaire** , le **lundi**.
Heure	Heure à laquelle vous souhaitez que la tâche planifiée commence.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. L'heure par défaut pour la mise à jour NVD est 01:00:00
Script d'intégration	Script permettant d'extraire les données des sources de données spécifiées dans la liste connexe **Sources de données** .
Intégration source	[Lecture seule]
Instance source	[Lecture seule]
Application	[Lecture seule] Nom de l'application pour laquelle vous exécutez la tâche planifiée.
Intervalle de répétition	Nombre de jours et d'heures avant que la tâche planifiée ne s'exécute à nouveau. Ce champ s'affiche lorsque **l'option Périodiquement** est sélectionnée dans la liste **Exécuter** .
En cours de démarrage	Date et heure de début des mises à jour périodiques. Ce champ s'affiche lorsque **l'option Périodiquement** est sélectionnée dans la liste **Exécuter** .
Conditionnel	Case à cocher permettant d'ajouter des paramètres conditionnels.
Condition	Conditions d'exécution de la tâche planifiée. Ce champ s'affiche lorsque la case **Conditionnel** est cochée.
Stratégie de processeur de rapport	Stratégie d'extraction des données et de traitement de la tâche planifiée. ◦ Pour extraire des données des sources de données de la liste connexe **Sources de données** à l'aide du script dans le champ **Script d'intégration** , sélectionnez **Pièce jointe de source de données**. ◦ Pour sélectionner un processeur personnalisé dans le champ de **script Processeur de rapport** , sélectionnez le **processeur de rapport personnalisé**.
Script de processeur de rapport	Script à exécuter lors de l'exécution de la tâche planifiée. Ce champ s'affiche lorsque **l'option Processeur de rapport personnalisé** est sélectionnée dans la liste **Stratégie de processeur de rapport** .
Script de l'instanciateur de processeur	Script permettant de créer le processeur de rapports. Ce champ s'affiche lorsque **l'option Processeur de rapport personnalisé**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	est sélectionnée dans la liste **Stratégie de processeur de rapport** .

4. Cliquez avec le bouton droit de la souris dans l'en-tête pour **enregistrer** vos modifications.
5. Pour exécuter immédiatement la tâche planifiée, cliquez **sur Exécuter maintenant**. Vous êtes renvoyé à la vue Intégrations de vulnérabilité.
6. Pour observer la progression de l'importation, sélectionnez à nouveau la tâche planifiée **CWE Comprehensive 2000 Integration** et sélectionnez l'onglet **Exécutions de l'intégration de vulnérabilité** .

   Consultez Afficher Réponse aux vulnérabilités les bibliothèques de vulnérabilité pour afficher les entrées importées.

Installer l'intégration Réponse aux vulnérabilités dans la base de données de vulnérabilité nationale NIST

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit NIST National Vulnerability Database (NVD) s'intègre correctement à Réponse aux vulnérabilités. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au gestionnaire de vulnérabilité dans Réponse aux vulnérabilités ou au groupe de gestionnaires App-Sec dans Réponse aux vulnérabilités des applications. Pour plus d'informations sur les rôles de groupe dans Réponse aux vulnérabilités la section

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités. Pour en savoir plus sur les rôles de groupe dans Réponse aux vulnérabilités des applications la section Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs. • Le gestionnaire de vulnérabilité ou le gestionnaire de sécurité des applications supervise la configuration et vérifie les résultats attendus.

Rôle requis : admin

Remarque : Avant d'exécuter les intégrations NVD, apportez les changements de configuration nécessaires en fonction de vos besoins.

Un utilisateur d'exécution en tant que configuré est défini pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne changez pas cette valeur.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer les intégrations NVD.
2. Accédez au ServiceNow Store.
3. Dans le ServiceNow Store, recherchez l'application Vulnerability Response Integration with NVD.
4. Sélectionnez la vignette de l'application.
   Des informations détaillées sur l'application que vous installez s'affichent.

   Remarque : Envisagez de lire les sections **Autres exigences** et **Dépendances** , le cas échéant.

5. Sélectionnez **Demande d'application** et entrez vos Now Support informations d'identification de connexion.
6. Sélectionnez **Obtenir**.
7. Entrez le **nom** et le **motif de l'instance**, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demander**.
   Vous recevrez un e-mail avec des instructions d'installation détaillées.
9. Accédez à la **Tout** > **Applications système** > **Applications** > **Tout**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Après l'installation initiale, pour les modifications, reportez-vous à la section Modification et activités de l'intégration NVD en option.

Activer la base de données des vulnérabilités nationale NIST : API (CPE non mappé)

Pour ingérer des données CPE (Common Platform Enumeration) pour les données CVE (Common Vulnerabilities and Exposures) extraites, vous pouvez effectuer une importation complète de données avec une tâche planifiée à la demande.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

L'intégration National Vulnerability Database Integration (NVD) – API (Unmapped CPE) du National Institute of Standards and Technology (NIST) capture des données (CPE) qui incluent un format de nom formel, une méthode de vérification des noms par rapport à un système et un format de description pour lier le texte et les tests à un nom. Ces informations sont stockées dans une liste connexe d'enregistrement d'entrée de vulnérabilité NVD.

Rôle requis : sn_vul.vulnerability_admin ou App-Sec Manager

Procédure

1. Accédez à la **Tout** > **Vulnerability Response ou Application Vulnerability Response** > **NVD** > **Intégrations**.
2. Sélectionnez l'intégration NIST National Vulnerability Database Integration-API (Unmaped CPE).
3. Sélectionnez la case à cocher **Activé**.

   Remarque : L'intégration est préconfigurée pour s'exécuter sur demande. En activant l'intégration, elle s'exécutera automatiquement après l'intégration de l'API d'intégration NIST NVD (CVE uniquement). La modification de tout autre paramètre d'intégration nécessite à la fois ServiceNow une expertise et et Réponse aux vulnérabilités et peut entraîner des données incomplètes.

   a. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.

   b. Sélectionnez NIST National Vulnerability Database Integration–API (Unmaped CPE) Integration.

   c. Sélectionnez l'onglet **Détails de l'intégration** .
   Quelle que soit la valeur du champ **Importer depuis** , les CVE de tous les CVE récupérés sont récupérés.
4. Sélectionnez **Exécuter maintenant** pour effectuer une première exécution d'intégration de prise en charge complète.
   Une fois l'importation initiale terminée, les importations planifiées de données delta reprennent. Pour connaître les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation de l'intégration NVD (Base de données nationale des vulnérabilités).

Activer l'API NIST National Vulnerability Database (CPE uniquement)

Pour ingérer des données CPE (Common Platform Enumeration), vous pouvez effectuer une importation de données complète avec une tâche planifiée quotidienne.

Avant de commencer

L'intégration National Vulnerability Database Integration (NVD) – API (CPE uniquement) du National Institute of Standards and Technology (NIST) capture des données (CPE uniquement) qui incluent un format de nom formel, une méthode de vérification des noms par rapport à un système et un format de description pour lier le texte et les tests à un nom. Ces informations sont stockées dans une table de logiciels vulnérables.

Rôle requis : sn_vul.vulnerability_admin ou App-Sec Manager

Procédure

1. Accédez à la **Tout** > **Vulnerability Response ou Application Vulnerability Response** > **NVD** > **Intégrations**.
2. Sélectionnez l'intégration NIST National Vulnerability Database Integration-API (CPE uniquement).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez la case à cocher **Activé**.

   - L'intégration est préconfigurée pour s'exécuter quotidiennement. La modification de tout autre paramètre d'intégration nécessite à la fois ServiceNow de l'expertise et peut entraîner des données incomplètes.
   - L'activation de cette intégration activera automatiquement les intégrations NIST National Vulnerability Database Integration-API (CVE uniquement) et NIST National Vulnerability Database Integration-API (CPE non mappé) et définira son champ Exécuter sur demande.
   - En outre, une exécution réussie de l'intégration de la base de données des vulnérabilités nationale du NIST - API (CPE uniquement) déclenchera automatiquement l'API de l'intégration de la base de données des vulnérabilités nationale du NIST (CVE uniquement). De plus, l'achèvement réussi de l'API NIST National Vulnerability Database Integration (CVE uniquement) déclenchera automatiquement l'API NIST National Vulnerability Database Integration (CVE non mappé).

   Remarque : Le champ Importer depuis la date de l'intégration de l'API (CPE uniquement) est vide par défaut. Conservez-le vide pour récupérer les données des 357 derniers jours.

   Pour récupérer des données historiques lors de votre importation initiale à partir de l'analyse NVD, définissez une date de début dans l'enregistrement d'intégration NIST National Vulnerability Database Integration- API (CPE uniquement).

   a. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.

   b. Sélectionnez NIST National Vulnerability Database Integration–API Integration (CPE uniquement).

   c. Sélectionnez l'onglet **Détails de l'intégration** .

   d. Définissez la valeur du champ **Importer depuis** sur la date la plus ancienne que vous souhaitez récupérer.

   Chaque importation réussie réinitialise cette date à la date et à l'heure du jour sélectionné.

4. Sélectionnez **Exécuter maintenant** pour effectuer une première exécution d'intégration de prise en charge complète.
   Une fois l'importation initiale terminée, les importations planifiées de données delta reprennent. Pour connaître les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation de l'intégration NVD (Base de données nationale des vulnérabilités).

Modification et activités de l'intégration NVD en option

Configurez des modifications facultatives spécifiquement pour les intégrations NVD.

Remarque : La modification d'autres paramètres d'intégration NVD, autres que ceux répertoriés ici, nécessite un niveau avancé ServiceNow et Réponse aux vulnérabilités une expertise et dépasse le cadre de la documentation du produit.

Effectuer une importation manuelle de NVD Integration

Si votre importation initiale a échoué, ou si vous ne souhaitez pas attendre l'importation initiale planifiée, vous pouvez effectuer une importation complète de données indépendamment de la tâche planifiée quotidienne ou hebdomadaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Remarque : Les intégrations NIST National Vulnerability Database Integration-API (CPE uniquement) et NIST National Vulnerability Database Integration-API (CPE non mappée) sont inactives par défaut. Voir Activer l'API NIST National Vulnerability Database (CPE uniquement) et Activer la base de données des vulnérabilités nationale NIST : API (CPE non mappé) pour plus d'informations.

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tout** > **Vulnerability Response ou Application Vulnerability Response** > **Administration** > **Intégrations**.
2. Choisissez et intégration, par exemple, l'intégration NIST National Vulnerability Database Integration - API (CVE uniquement).
3. Sélectionnez **Exécuter maintenant**.

   Remarque : Si l'intégration NIST National Vulnerability Database Integration-API (Unmapped CPE) est activée, les données CPE associées sont stockées dans la liste connexe Logiciel vulnérable de l'entrée de vulnérabilité NVD. Consultez Réponse aux vulnérabilités Champs du formulaire de vulnérabilité.

4. Pour les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation de l'intégration NVD (Base de données nationale des vulnérabilités).

Afficher l'état de l'exécution de l'importation de l'intégration NVD (Base de données nationale des vulnérabilités)

Utilisez la liste connexe **Exécutions de l'intégration de vulnérabilité** pour vérifier la réussite de vos exécutions d'intégration, localiser les problèmes et prendre des décisions de rattrapage.

Avant de commencer

Pour afficher l'état de l'exécution de l'importation de l'intégration NVD :

- Réponse aux vulnérabilités et l'application Vulnerability Response integration avec NVD integration doit être installée et configurée.
- Les importations de l'intégration NVD doivent être en cours d'exécution. L'intégration NIST National Vulnerability Database Integration-API (CVE uniquement) s'exécute par défaut.

  Remarque : Les intégrations NIST National Vulnerability Database Integration-API (CPE uniquement) et NIST National Vulnerability Database Integration-API (CPE non mappée) sont inactives par défaut. Voir Activer l'API NIST National Vulnerability Database (CPE uniquement) et Activer la base de données des vulnérabilités nationale NIST : API (CPE non mappé) pour plus d'informations.

Rôle requis : sn_vul.vulnerability_admin ou App-Sec Manager

Pourquoi et quand exécuter cette tâche

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Le fait que le dernier enregistrement traité date de plus d'une heure indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Si vous n'utilisez pas le graphique d'état d'exécution de l'intégration NVD, Accédez à la **Tout** > **Vulnerability Response ou Application Vulnerability Response** > **Administration** > **Intégrations**.
2. Sélectionnez un **lien** pour une intégration.
3. Sélectionnez la liste connexe **Exécutions de l'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.

Trouble?

Les causes les plus courantes d'un échec d'exécution sont les suivantes :

- Interruption du réseau.
- Un problème dans le transfert de données entraînant la corruption des données pendant la transformation.

Si vous rencontrez l'une de ces conditions, sélectionnez **Exécuter maintenant**, puis réexécutez l'intégration.

Information associée

Réponse aux vulnérabilités Champs du formulaire de vulnérabilité

Ajouter des CVE à des entrées tierces

Les informations sur les vulnérabilités et les expositions courantes (CVE) peuvent être liées à une seule vulnérabilité tierce. Il est généralement ajouté lors d'une importation d'intégration tierce. Cependant, vous pouvez ajouter plusieurs CVE (vulnérabilités) manuellement.

Avant de commencer

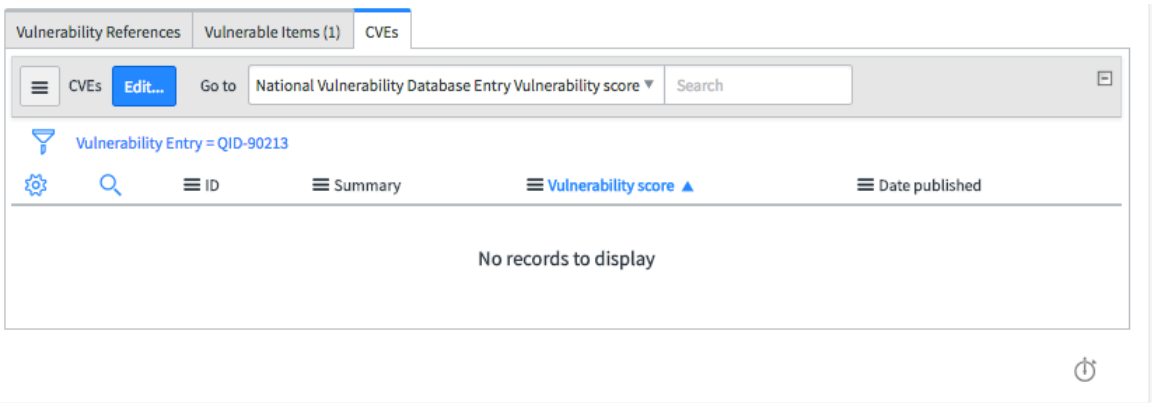
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers**.
2. Ouvrez un enregistrement.
3. Cliquez sur l'onglet de liste connexe **CVE.**



4. Cliquez sur **Modifier**.
5. Choisissez les CVE à ajouter.

> **Remarque :** Vous pouvez utiliser des filtres de condition pour affiner la collection CVE.

6. Cliquez sur **Enregistrer**.

Information associée

Réponse aux vulnérabilités Champs du formulaire de vulnérabilité

Afficher Réponse aux vulnérabilités les bibliothèques de vulnérabilité

Vous pouvez consulter les données de vulnérabilité importées à partir de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou de tiers pour décider d'escalader ou non une tâche de correction.

Avant de commencer

Rôle requis : sn_vul.remediation_owner

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Bibliothèques**.

   Pour en savoir plus sur des champs spécifiques, reportez-vous à la section Réponse aux vulnérabilités Champs du formulaire de vulnérabilité.

   Les bibliothèques suivantes sont disponibles :

Bibliothèques	Description
NVD	Liste des vulnérabilités détectées par NVD et comprenant des listes de vérification de sécurité, des failles logicielles liées à la sécurité, des erreurs de configuration, des noms de produits et des mesures d'impact, y compris les exploits.

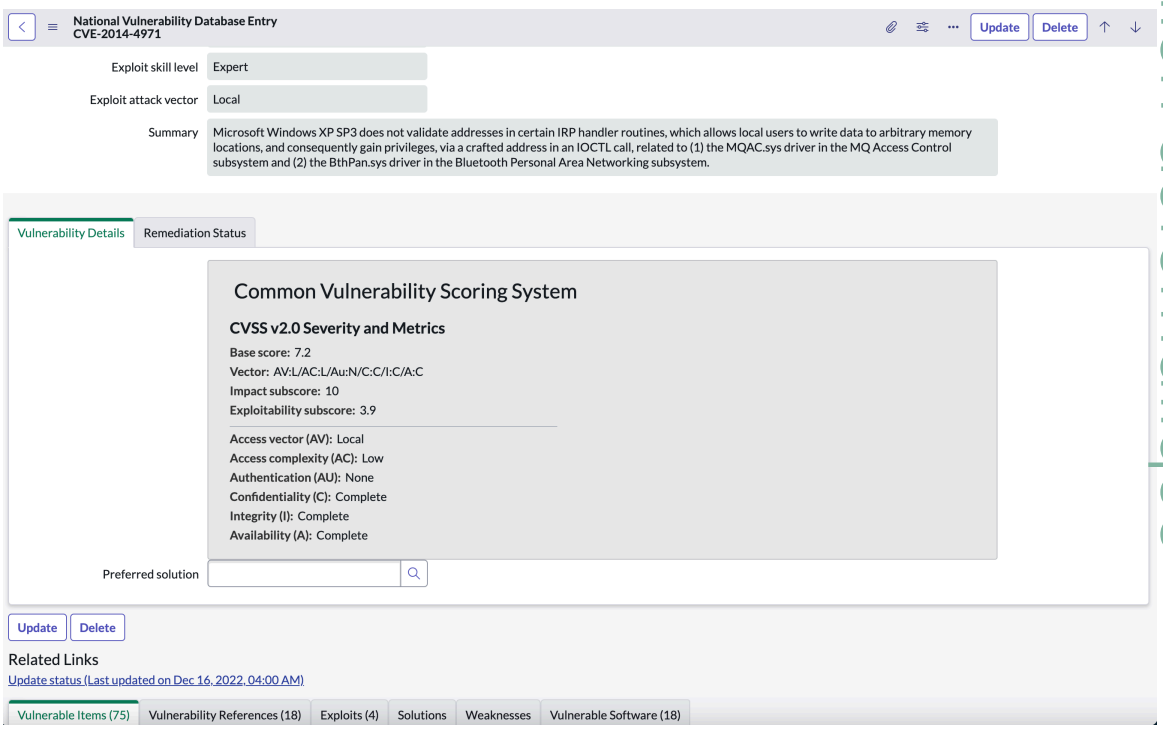
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bibliothèques	Description
CWE	Liste des types de faiblesses logicielles développés par la communauté. Chaque enregistrement CWE inclut également un article de la base de connaissances associé qui décrit la faiblesse. Vous ne pouvez pas escalader une vulnérabilité à partir de l'écran Common Weakness Enumerations, c'est à titre de référence uniquement.
Tiers	Liste des vulnérabilités tierces importées dans votre instance. Contient une liste de références, d'éléments vulnérables, d'exploits et de CVE connexes.

2. Choisissez une bibliothèque pour afficher les vulnérabilités.
3. Cliquez sur un lien dans la liste pour ouvrir un enregistrement.

   Un enregistrement CVE dans la bibliothèque d'entrées de la base de données nationale des vulnérabilités. Plus d'informations sont disponibles dans les **liens connexes**. Après une importation de données, vous pouvez sélectionner une vulnérabilité et explorer ses relations avec les éléments vulnérables, les exploits, les solutions possibles, les correctifs potentiels et toutes les références aux articles de la base de connaissances dans la base de connaissances HI. Si Gestion des solutions pour vulnérabilités elle est installée, vous pouvez afficher une solution préférée sur les enregistrements NVD si elle est disponible.



Intégration de CISA Known Exploit Vulnerability (KEV)

L'intégration Réponse aux vulnérabilités avec le catalogue des vulnérabilités exploitées connues (KEV) de CISA ingère les données pour vous aider à hiérarchiser et à corriger efficacement ces vulnérabilités.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

CISA permet de remédier de manière urgente et prioritaire aux vulnérabilités activement exploitées pour les agences gouvernementales et les entreprises.

À propos de CISA

La Cybersecurity & Infrastructure Security Agency (CISA) est une agence américaine de cybersécurité et de sécurité des infrastructures qui publie un rapport sur les vulnérabilités les plus exploitées. Il s'intègre Réponse aux vulnérabilités facilement pour mapper les vulnérabilités courantes et les expositions (CVE), enrichissant ainsi les données dans votre instance. Ces informations sont ensuite déployées dans la table Entrées de vulnérabilité tierces. La date d'échéance la plus proche est prise en compte pour le déploiement des éléments vulnérables.

Remarque : La case à cocher **CISA existe** pour les CVE récupérés par CISA.

Valeurs récupérées à partir de l'intégration CISA :

- ID des CVE
- Date d'échéance
- Date d'ajout
- Fournisseur/Projet
- Produit
- Rançongiciel connu (à partir de la version 21.0 de , un nouveau champ **connu pour être utilisé dans les campagnes de**Réponse aux vulnérabilitésrançongiciel est ingéré à partir du catalogue des vulnérabilités exploitées connues (KEV) de CISA. Il est indiqué par le marquage du champ **Rançongiciel connu** dans la table de base de données Entrée de vulnérabilité nationale. Le marqueur est défini au niveau des vulnérabilités et expositions communes (CVE) et déployé jusqu'à l'entrée tierce (TPE).

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Travaux planifiés

L'intégration CISA est invoquée automatiquement en tant que tâche planifiée quotidienne. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Versions disponibles

Version	Notes de publication
Réponse aux vulnérabilités v16.5, v18.0 Réponse aux vulnérabilités Intégration avec CISA v1.0, v1.2	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage de l'intégration CISA

Pour afficher l'intégration de CISA, accédez à **Réponse aux vulnérabilités** > **Administration** > **Intégrations** > **Intégration de vulnérabilité d'exploit connu CISA**.

Les intégrations suivantes sont incluses dans le système de base.

Remarque : Par défaut, seule l'intégration CISA est active.

Intégration de la CISA

Intégration	Description
Intégration de la cybersécurité et de la sécurité des infrastructures (CISA)	Récupère les données de vulnérabilité CISA (CVE) et enrichit les données de vulnérabilité existantes. Cette intégration est définie automatiquement pour s'exécuter quotidiennement.

Pour afficher les données dans les vulnérabilités tierces, reportez-vous à la section Afficher Réponse aux vulnérabilités les bibliothèques de vulnérabilité.

Préparation à l'intégration de CISA

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Préparez l'intégration en effectuant ces tâches. L'intégration CISA Known Exploited Vulnerability suppose que vous connaissez la Cybersecurity & Infrastructure Security Agency (CISA).

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter l'intégration CISA, apportez tout changement de configuration nécessaire en fonction de vos besoins.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Installer l'intégration de Vulnerability Response avec l'application ServiceNow® CISA

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le conseiller en vulnérabilités exploitées connues de la CISA (Cybersecurity & Infrastructure Security Agency) s'intègre à Réponse aux vulnérabilités. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que l'intégration à l'application Réponse aux vulnérabilités NVD est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer l'intégration Réponse aux vulnérabilités dans la base de données de vulnérabilité nationale NISTreportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au gestionnaire de vulnérabilité dans Réponse aux

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	vulnérabilités. Pour plus d'informations sur les rôles de groupe dans Réponse aux vulnérabilités la section Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités. • Le gestionnaire de vulnérabilité supervise la configuration et vérifie les résultats attendus.

Rôle requis : administrateur

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez l'installer Intégration de Réponse aux vulnérabilités à CISA .
2. Accédez au ServiceNow Store.
3. Dans le ServiceNow Store, recherchez l'application Intégration de Réponse aux vulnérabilités à CISA .
4. Sélectionnez la vignette de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **Dépendances** , le cas échéant.

5. Sélectionnez **Demande d'application** et entrez vos Now Support informations d'identification de connexion.
6. Sélectionnez **Obtenir**.
7. Entrez le **nom** et le **motif de l'instance**, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Remarque : Aucune configuration n'est requise pour l'intégration CISA .

Présentation de l'intégration de l'Exploit Prediction Scoring System (EPSS)

Vue d'ensemble de l'intégration de l'EPSS avec Réponse aux vulnérabilités.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble

L'intégration EPSS (Exploit Prediction Scoring System) importe les données EPSS relatives aux vulnérabilités et expositions courantes (CVE) à partir des First.org afin de hiérarchiser et corriger les vulnérabilités. Pour plus d'informations, reportez-vous à la section https://www.first.org . L'Exploit Prediction Scoring System (EPSS) est un effort basé sur les données pour estimer la probabilité qu'une vulnérabilité logicielle soit exploitée dans la nature. Le modèle EPSS produit un score de probabilité compris entre 0 et 1 (0 et 100 %). Plus le score est élevé, plus la probabilité qu'une vulnérabilité soit exploitée est grande.

Les importations de données issues de l'intégration EPSS enrichissent davantage les données NVD dans votre instance. Si les enregistrements NVD ne sont pas présents, un espace réservé est créé dans la table CVE et les détails de l'EPSS sont ajoutés dans la même table. Exécutez cette intégration dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit de scanner tiers.

Important : Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est VR. Système. Ne modifiez en aucun cas cette valeur.

Importation initiale des données avec l'intégration de l'EPSS

1. Effectuez une importation initiale des données de l'EPSS avec l'intégration de l'EPSS First.org. Pour plus d'informations, consultez Configurer et exécuter une tâche planifiée pour mettre à jour les enregistrements CVE avec des données EPSS.

   Important : Vous effectuez des mises à jour EPSS **quotidiennes** à partir de l'enregistrement d'intégration par défaut, et vous devez le configurer si vous souhaitez qu'il s'exécute en tant que tâche planifiée.

2. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Pour plus d'informations, consultez Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces.

   Important : Il est recommandé d'effectuer des intégrations NIST National Vulnerability Database Integration : API (CVE uniquement) avant EPSS.

Effectuez les importations EPSS avant d'importer les données de vulnérabilité avec un produit tiers. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Consultez votre documentation d'intégration dans Intégrations de la réponse aux vulnérabilités pour plus d'informations sur les intégrations tierces.

Important : L'intégration suivante est incluse dans le système de base. L'intégration est active par défaut.

Après l'exécution initiale, les travaux planifiés du système de base exécutent automatiquement les intégrations dans l'ordre. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Lors de l'activation de l'intégration de l'EPSS, les champs Score de l'EPSS, Centile de l'EPSS et Dernière modification de l'EPSS sont ajoutés à la table Entrées de vulnérabilité. Pour les CVE existants, ces champs sont mis à jour automatiquement à l'issue de la tâche d'importation initiale. Si de nouveaux CVE sont ajoutés à la table Entrées de vulnérabilité après l'achèvement de la tâche planifiée EPSS, les CVE nouvellement ajoutés indiqueront

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

leur source en tant qu'EPSS. Les scores sont déployés sur les TPE existants à partir des CVE de la table NVD, à l'aide du système *Rollup EPSS score from NVD to TPEs calculator*de base . Vous pouvez également modifier le calculateur. Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs de déploiement.

Information associée

Créer un Réponse aux vulnérabilités calculateur

Configurer et exécuter une tâche planifiée pour mettre à jour les enregistrements CVE avec des données EPSS

Personnalisez la tâche planifiée du système de base pour mettre à jour les enregistrements CVE avec les données EPSS.

Avant de commencer

Important : Vous devez télécharger et activer le module d'extension Intégration de Réponse aux vulnérabilités à CISA (com.snc.vulnerability.cisa) pour activer l'intégration EPSS.

Voici la liste des nouveaux champs ajoutés dans la table NVD pour stocker les données EPSS.

- Score de l'EPSS
- Centile de l'EPSS
- Dernière modification de l'EPSS

Remarque : Configurez la vue de liste ou la vue de formulaire selon les besoins pour afficher les champs nouvellement ajoutés.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Les importations de données à partir de l'intégration EPSS enrichissent davantage les données NVD dans votre instance. Si les enregistrements NVD ne sont pas présents, un espace réservé est créé dans la table CVE et les détails de l'EPSS sont ajoutés dans la même table. Exécutez cette intégration dans le cadre de votre configuration initiale de Vulnerability Response et publiez-la dans l'importation des données de vulnérabilité dans votre instance.

Remarque : Par défaut, l'intégration First.org EPSS est à l'état **Actif** . La tâche planifiée du système de base est configurée par défaut pour s'exécuter quotidiennement.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.
2. Recherchez et sélectionnez First.org intégration EPSS.
3. Modifiez les champs selon vos besoins.
4. Cliquez avec le bouton droit de la souris sur l'en-tête pour **enregistrer** vos modifications.
5. Sélectionnez **Exécuter maintenant** pour exécuter la tâche planifiée immédiatement.
   Vous êtes renvoyé à la vue Intégrations de vulnérabilité.
6. Sélectionner **First.org EPSS** > **Onglet Exécutions de l'intégration de vulnérabilité** pour afficher la progression de l'importation.
   Une fois la tâche planifiée terminée avec succès, les scores EPSS, le centile et les horodatages des scores EPSS derniers changements sont mis à jour sur les CVE.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

- Consultez Ajouter une condition de score de l'EPSS dans la règle métier du calculateur de risques.
- Consultez Afficher Réponse aux vulnérabilités les bibliothèques de vulnérabilité pour afficher les entrées importées.

Ajouter une condition de score de l'EPSS dans la règle métier du calculateur de risques

Modifier la règle métier pour ajouter une condition de score EPSS au calculateur de risque.

Avant de commencer

Remarque : La procédure suivante est requise pour que les mises à jour de l'EPSS sur les vulnérabilités soient déployées vers les éléments vulnérables.

Rôle requis : sn_vul.manage_risk_score_configuration

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Règle métier**.
2. Rechercher **Définir le marqueur de recalcul**.

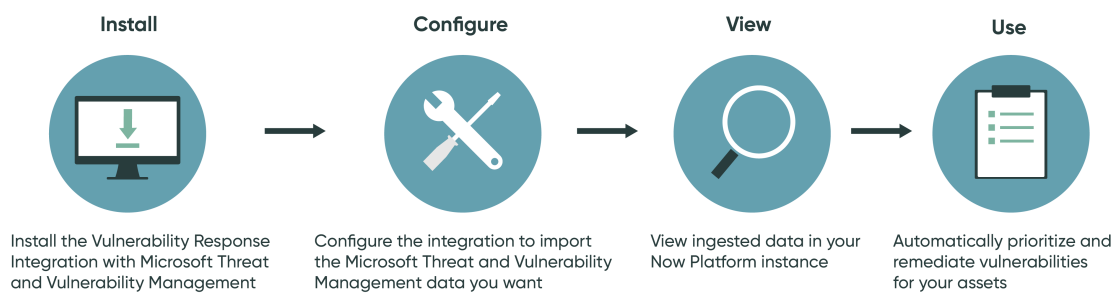
   Remarque : Il y a deux *`Set recalculate flag`*règles métier. Vous pouvez utiliser l'un ou l'autre.

3. Accédez à l'onglet **Quand exécuter** .
4. Sélectionnez **Ajouter une clause « OU »** et sélectionnez `Score EPSS` dans **Choisir un champ** et `Changements` dans **le champ Choisir un opérateur** .
5. Sélectionnez **Mettre à jour**.

Présentation de l'intégration des vulnérabilités de Microsoft Threat and Vulnerability Management

L'intégration Réponse aux vulnérabilités à l'application Microsoft Threat and Vulnerability Management (MS TVM) utilise des données importées de MS TVM pour vous aider à hiérarchiser et à corriger les vulnérabilités de vos actifs. L'application est disponible avec un abonnement distinct à partir du ServiceNow Storefichier .

Vous pouvez utiliser l'intégration des vulnérabilités MS TVM pour importer des données d'analyseurs tiers concernant vos actifs et vos vulnérabilités. Vous pouvez ensuite afficher des rapports sur les vulnérabilités et les éléments vulnérables sur les Réponse aux vulnérabilités tableaux de bord.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions disponibles

Version	Notes de publication
Réponse aux vulnérabilités Intégration avec MS TVM v2.2	Pour plus d'informations sur les versions publiées de l'application Vulnerability Response, la compatibilité et les changements de schéma, consultez l'article Matrice de compatibilité de Vulnerability Response et Changements de schéma de mise en production [KB0856498] dans la base de connaissances HI .

Séparation de domaine et MS TVM

Importez les données d'intégration de vulnérabilité dans un domaine spécifié en affectant un utilisateur de ce domaine pour exécuter les intégrations. Pour créer des importations séparées par domaine pour l'intégration des vulnérabilités MS TVM, reportez-vous à la section Créer des importations séparées par domaine pour une intégration.

Termes et fonctionnalités clés des intégrations

Éléments vulnérables et vulnérabilités

Un élément vulnérable est créé dans votre instance lorsque :Now Platform

- Une vulnérabilité importée à partir d'un scanner tiers est mise en correspondance avec un actif existant (élément de configuration) dans votre CMDB). Le produit MS TVM qualifie ces correspondances de vulnérabilités.
- Une vulnérabilité importée à partir d'un scanner tiers ne correspond pas à un actif existant dans votre CMDB. Dans ce cas, un élément de configuration (CI) sans correspondance est également créé avec un élément vulnérable.

  Utilisez le moteur Identification et rapprochement (IRE) pour créer des CI dans deux nouvelles classes lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte. Dans le cas contraire, des CI sans correspondance sont créés dans les classes de CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement.

Entrées de vulnérabilité tierces

Les entrées de vulnérabilité tierces sont importées à partir d'analyseurs tiers tels que MS TVM et sont répertoriées dans la table Entrées de vulnérabilité tierces de votre Now Platform instance. De plus, les entrées de la base de données de vulnérabilité nationale (CVE) sont importées à partir de MS TVM. Les informations sur l'exploit associées à ces deux types d'entrées proviennent de MS TVM. Ces informations sur l'exploit peuvent être utilisées pour le calcul du risque.

Remarque : Une vulnérabilité tierce n'est récupérée que pour les vulnérabilités auxquelles aucun CVE n'est affecté. MS TVM peut ajouter un nom temporaire pour la vulnérabilité, par exemple, `TVM-XXXX-XXXX`. Ce nom est mis à jour après l'affectation d'un ID CVE.

Élément de configuration (CI)

Les CI sont les actifs existants répertoriés dans votre CMDBfichier .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément détecté

Les éléments détectés sont les actifs ingérés à partir de l'importation de l'ordinateur MS TVM qui correspondent aux CI existants dans votre CMDB.

Si aucune correspondance n'est trouvée, un CI est créé dans la classe CI sans correspondance du CMDB. Activez le module d'extension Modèles de classe CI CMDB. Le moteur Identification et rapprochement (IRE) crée des CI à l'aide de nouvelles classes. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement. Si le CI d'origine, sans correspondance, est reclassé, les enregistrements de l'élément détecté sont mis à jour pour refléter cet état. Les éléments détectés vous donnent une visibilité sur la façon dont les actifs sont identifiés et mappés aux CI dans le CMDB.

Règles de recherche de CI

Lorsque des données sont importées à partir de MS TVM, Réponse aux vulnérabilités utilise automatiquement les données de l'ordinateur (actif) pour rechercher des correspondances dans le CMDBfichier . Les règles de recherche de CI sont utilisées pour identifier les CI et les ajouter aux enregistrements de VI lors de la création de VI.

Instance

Une instance fait référence à plusieurs comptes de MS TVM. Chaque compte peut être une instance de l'application MS TVM.

Intégration

Une intégration est une tâche planifiée qui récupère des informations à partir d'une source tierce, comme l'intégration des machines MS TVM.

Déploiement

Lorsqu'une intégration prend en charge plusieurs sources, une existence d'intégration unique est appelée déploiement de votre intégration. Un déploiement fait référence aux intégrations et aux produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de MS TVM dans votre environnement.

L'intégration MS TVM comprend également les fonctionnalités clés suivantes :

- Vous pouvez identifier les actifs dans votre environnement et mettre à jour les CI de vos éléments détectés, éléments vulnérables et enregistrements de détection existants pour vous donner plus de détails sur vos vulnérabilités.
- Vous pouvez planifier le moment où vous souhaitez que les tâches s'exécutent pour toutes les intégrations MS TVM. Vous pouvez également exécuter des travaux planifiés sur demande.
- Vous pouvez regrouper des éléments vulnérables.
- Vous pouvez configurer des règles de recherche de CI pour définir la manière dont les données d'actif de sources tierces sont utilisées pour identifier les CI dans votre CMDB.

Rôles Now Platform requis

Les tâches d'intégration nécessitent les rôles suivants dans votre Now Platform instance.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

administrateur

L'administrateur système utilise l'Assistant de configuration pour installer l'application MS TVM. Si elle n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'Assistant de configuration.

sn_vul.vulnerability_admin

Une fois affecté, l'administrateur de vulnérabilité termine la configuration des intégrations MS TVM dans l'Assistant de configuration. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités et à ses enregistrements. L'administrateur de vulnérabilité configure toutes les applications et toutes les règles pour les Réponse aux vulnérabilités intégrations tierces installées.

sn_vul_msft_tvm.configure_integration

Ce rôle contient le rôle granulaire `sn_vul_msft_tvm.read_integration`. Les utilisateurs disposant de ce rôle peuvent configurer Vulnerability Response Integration avec l'application Microsoft Threat and Vulnerability Management.

sn_vul_msft_tvm.read_integration

Les utilisateurs disposant de ce rôle peuvent uniquement afficher l'intégration de Vulnerability Response avec les enregistrements de l'application Microsoft Threat and Vulnerability Management.

Groupe Vulnerability Response

Par défaut, le groupe Vulnerability Response est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Vulnerability Response héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner.

Intégrations MS TVM

La fonction multisource est prise en charge pour toutes les intégrations MS TVM. Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'Assistant de configuration dans Réponse aux vulnérabilités. Vous pouvez également installer et configurer l'intégration Réponse aux vulnérabilités à l'application MS TVM à partir de l'Assistant de configuration.

Pour afficher les intégrations MS TVM, accédez à **Intégration de vulnérabilité Microsoft TVM** > **Administration** > **Intégrations**. Réponse aux vulnérabilités fournit des intégrations avec les points de terminaison MS TVM pour importer les données en fonction des intervalles de temps planifiés. Les intégrations suivantes sont incluses dans le système de base.

Intégrations MS TVM

Séquence d'exécution	Calendrier	Intégration	Description
1	Quotidien	Intégration des recommandations Microsoft TVM	Récupère une liste de toutes les recommandations de sécurité activables pour corriger les vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations MS TVM (suite)

Séquence d'exécution	Calendrier	Intégration	Description
2	Quotidien	Intégration de Microsoft TVM Vulnerability (CVE)	Récupère une liste des entrées de la base de données de vulnérabilité nationale et des entrées de vulnérabilité tierces, ainsi que leurs informations sur l'exploitation.
3	Quotidien	Intégration des machines Microsoft TVM	Récupère toutes les données d'actif (machine), y compris les balises d'ordinateur, à partir de Microsoft TVM et les traite dans votre instance.
4	Hebdomadaire **Remarque :** Après l'installation, cette intégration est exécutée automatiquement après l'importation des machines.	Intégration des vulnérabilités des machines Microsoft TVM (importation complète)	Récupère toutes les vulnérabilités ouvertes sur tous les actifs.
5	Quotidien	Intégration des vulnérabilités des machines Microsoft TVM (importation Delta)	Récupère toutes les informations qui ont changé dans l'importation complète de vulnérabilité de l'organisation, y compris les vulnérabilités nouvelles, corrigées et mises à jour.

Les éléments vulnérables sont regroupés en tâches de rattrapage en fonction des règles de groupe que vous définissez et sont affectés au rattrapage en fonction de vos règles d'affectation. Pour plus d'informations, consultez Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage et Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles de recherche de CI

Lorsque des données sont importées à partir de MS TVM, Réponse aux vulnérabilités utilise automatiquement les données de l'ordinateur (actif) pour rechercher des correspondances dans le Base de données de gestion des configurations (CMDB)fichier . Les règles de recherche de CI sont utilisées pour identifier les CI et les ajouter aux enregistrements de VI lors de la création de VI. Pour plus d'informations sur le fonctionnement des règles de recherche de CI, reportez-vous à Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Remarque : Une fois que vous avez supprimé une règle, vous ne pouvez pas la récupérer. Au lieu de supprimer une règle existante, vous devez la désactiver.

Les règles de recherche MS TVM suivantes sont fournies avec le système de base :

- MAC_ADDRESS
- FQDN
- IP

Remarque : Vous pouvez utiliser plusieurs valeurs pour le IP_ADDRESS et le MAC_ADDRESS d'un actif. Une règle de recherche de CI tient compte de toutes les valeurs pour établir une correspondance.

Éléments détectés

Vous pouvez afficher les CI qui ont été détectés lors d'une importation à partir de l'intégration des machines MS TVM.

Remarque : Le filtre par défaut de cette liste est défini sur `Sans correspondance`. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour plus d'informations, consultez Éléments détectés.

Balises d'ordinateur

Les balises d'ordinateur, également appelées balises d'hôte, sont utilisées pour organiser et suivre les actifs de votre organisation. Vous attribuez des balises à vos machines.

Toutes les balises de machine sont importées dans le cadre de l'intégration des machines MS TVM. Les balises d'ordinateur sont généralement utilisées pour le filtrage dans Réponse aux vulnérabilités les règles d'affectation et les règles de groupe de vulnérabilité. Les balises sont affichées dans le formulaire Élément détecté.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Exécutez l'intégration de l'ordinateur MS TVM avant de créer des Réponse aux vulnérabilités règles de tâche d'affectation ou de rattrapage dans l'application afin que toutes les balises soient disponibles pour ces règles avant que Réponse aux vulnérabilités les éléments vulnérables ne soient importés et regroupés. Notez également les points suivants concernant les balises :

- Le stockage des balises n'est pas sensible à la casse. Si une balise Paris est créée, elle ne peut pas être stockée dans la table des balises Machine. `Paris` et `PARIS` sont considérés comme étant la même étiquette machine par le système. La balise importée en premier est celle qui est stockée et reconnue.
- L'utilisation de balises machine en tant que clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les clés de groupe sont des colonnes dans la table des tâches de rattrapage, tandis que les balises machine sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises d'ordinateur sont contrôlées par la propriété système globale sn_vul.import_host_tags. Cette propriété est définie sur `vrai` par défaut. La désactivation des balises les désactive dans toutes les Now Platform® instances.

Étapes suivantes

Une fois que vous avez téléchargé l'intégration avec Microsoft Threat and Vulnerability Management à partir de , l'installation et la ServiceNow® Storeconfiguration sont prises en charge par l'assistant Réponse aux vulnérabilités de configuration dans Réponse aux vulnérabilités. Pour plus d'informations, consultez Installez et configurez Vulnerability Response Integration avec l'application MS TVM à l'aide de l'Assistant de configuration.

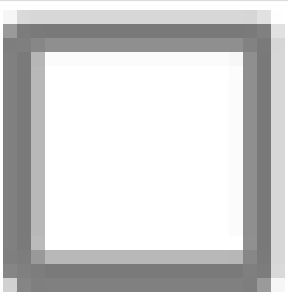
Préparation à l'intégration des vulnérabilités Microsoft Threat and Vulnerability Management

Vous pouvez préparer l'intégration des ServiceNow® vulnérabilités de Microsoft Threat and Vulnerability Management (MS TVM) en effectuant des tâches de configuration.

Avant de commencer à utiliser une liste de vérification

Pour installer et configurer l'intégration Réponse aux vulnérabilités à l'application MS TVM, vous pouvez imprimer la liste de vérification suivante et vérifier que les éléments répertoriés sont terminés avant d'installer l'application et d'importer les données de vulnérabilité dans votre Now Platform® instance.

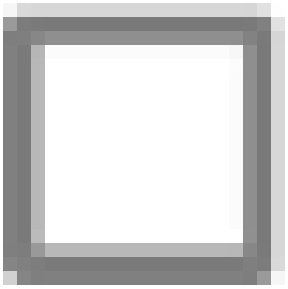
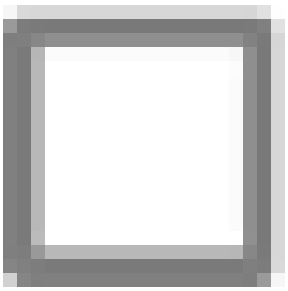
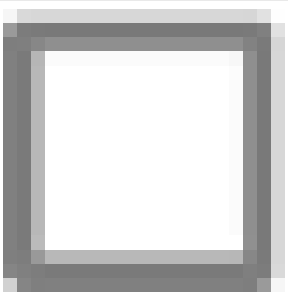
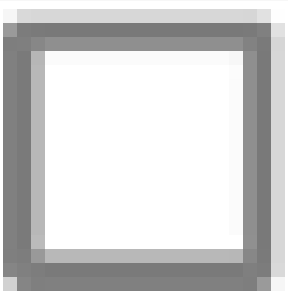
Liste de vérification de la préparation de l'intégration

Tâche	Description
	Vérifiez que vous disposez de l'un des ensembles d'informations suivants : • ClientSecret, ClientId et TenantId pour votre compte MS TVM • Nom d'utilisateur, mot de passe, ClientId et TenantId de votre compte MS TVM. Pour obtenir ces informations, reportez-vous à la section Configurer Microsoft Azure pour l'intégration MS TVM.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

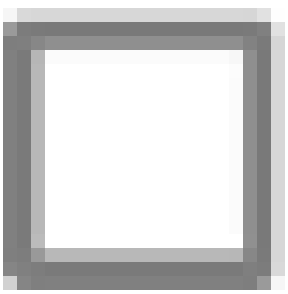
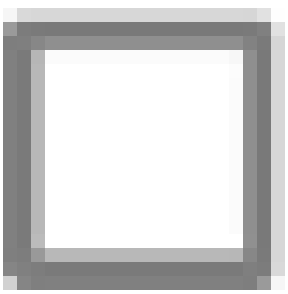
Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
	Si elle n'est pas déjà installée et activée, installez l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour en savoir plus sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 14.0 ou Réponse aux vulnérabilités ultérieure.
	Si vous n'avez pas déjà l'application sur votre instance, obtenez les autorisations et téléchargez l'intégration à l'application Réponse aux vulnérabilités MS TVM sur votre Now Platform® instance. Consultez .
	Estimez le nombre d'éléments vulnérables que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance ou si vous avez besoin d'aide, contactez ServiceNow® le support technique.
	Vérifiez que vous disposez des groupes ou utilisateurs suivants pour gérer les intégrations et corriger les éléments vulnérables : administrateur Utilise l'assistant de configuration pour installer l'intégration de Vulnerability Response avec l'application MS TVM. Si elle n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'Assistant de configuration. sn_vul.vulnerability_admin Termine la configuration de l'intégration MS TVM. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Cet administrateur configure toutes les applications et règles de VR et configure les intégrations tierces. sn_vul_msft_tvm.configure_integration Configure l'intégration des vulnérabilités MS TVM. Ce rôle contient le rôle granulaire sn_vul_msft_tvm.read_integration. sn_vul_msft_tvm.read_integration

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
	Affiche (lit) les enregistrements de l'intégration de vulnérabilité MS TVM. Groupe Vulnerability Response Par défaut, le groupe Vulnerability Response est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Vulnerability Response héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires et ajouter des utilisateurs avec le module d'administration des utilisateurs dans votre instance avant d'utiliser l'Assistant de configuration. Pour plus d'informations, consultez Créer un groupe d'utilisateurs . Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Réponse aux vulnérabilités . Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.
	Installez l'intégration Réponse aux vulnérabilités à NVD et exécutez l'API NIST National Vulnerability Database Integration (CVE uniquement).
	Pour améliorer les performances de votre première importation, vous pouvez désactiver certaines fonctionnalités, règles ou tâches dans votre instance. • Désactivez les calculateurs de vulnérabilité si vous ne les utilisez pas. Ces calculateurs, ainsi que ceux que vous avez définis, s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est créé ou mis à jour. Pour plus d'informations, consultez Désactiver le calculateur de vulnérabilité par défaut s'il n'est pas utilisé. • Lors de l'importation initiale des enregistrements, certaines règles métier liées aux notifications peuvent entraîner la génération de nombreuses notifications, ce qui peut avoir un impact sur les performances de l'ingestion.

Vous êtes prêt à Installez et configurez Vulnerability Response Integration avec l'application MS TVM à l'aide de l'Assistant de configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Microsoft Azure pour l'intégration MS TVM

Configurez votre compte dans le Microsoft portail Azure pour accéder à distance à l'API Microsoft Threat and Vulnerability Management (MS TVM). Vous avez besoin de ce compte pour pouvoir accéder au locataire MS TVM afin de recueillir des informations sur les machines, les vulnérabilités et les recommandations de sécurité.

Avant de commencer

Rôle requis : Microsoft administrateur du portail Azure.

Pourquoi et quand exécuter cette tâche

Effectuez les tâches de configuration suivantes dans votre Microsoft portail Azure avant d'installer l'application ServiceNow® pour cette intégration.

Pour vérifier que vous avez accès au contenu le plus récent, consultez le site Web de la documentation Microsoft . Si vous n'avez pas créé d'ID d'application pour l'authentification OAuth 2.0 dans le Microsoft portail Azure, suivez les étapes de cette procédure.

Procédure

1. Connectez-vous au Microsoft portail Azure à l'aide de vos informations d'identification d'administrateur du portail Azure.
2. Dans le panneau de navigation de gauche du volet Accueil, cliquez sur **Azure Active Directory**.
3. Dans le volet Vue d'ensemble, cliquez sur **Inscriptions d'applications (aperçu).**
4. Dans le volet Inscriptions d'applications (aperçu), cliquez sur **Nouvelle inscription**.
   Le formulaire Enregistrer une demande s'affiche.
5. Renseignez les champs du formulaire.

Enregistrer un formulaire d'application

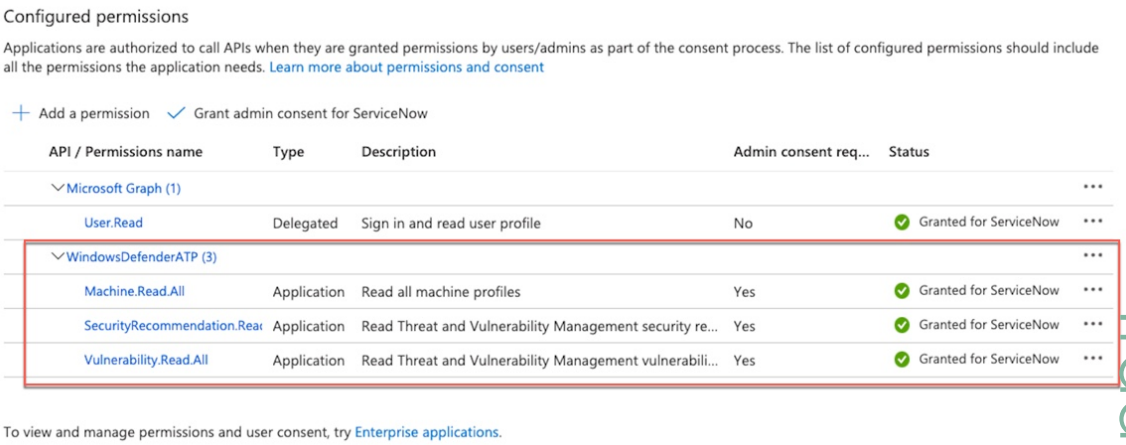
Champ	Description
Nom	Nom de l'application. Dans cet exemple, `l'intégration ServiceNow MS TVM` est saisie.
Types de compte pris en charge	Pour ce compte, dans Types de comptes pris en charge, cliquez sur **Comptes dans ce répertoire d'organisation uniquement (ServiceNow uniquement - locataire unique).**
URL de redirection (facultatif)	Si vous saisissez une valeur pour ce champ, elle n'est pas utilisée par l'intégration.

6. Cliquez sur **Inscrire**.
   L'ID (client) de l'application et l'ID (locataire) du répertoire sont créés. Saisissez ces valeurs sur la page de configuration dans les champs **ID client** et **ID locataire** lors de l'étape de configuration dans l'assistant de configuration de l'intégration ServiceNow VR-TVM. Cette étape a été décrite dans Installez et configurez Vulnerability Response Integration avec l'application MS TVM à l'aide de l'Assistant de configurationla section .
7. Lorsque l'ID d'application (client) s'affiche dans le volet Intégration MS TVM, cliquez sur **Afficher les autorisations d'API**ServiceNow.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Accédez à la **Demander des autorisations API** > **API utilisées par mon organisation**, puis cliquez sur **Windows Defender ATP**.
9. Dans le volet Intégration ServiceNow MS TVM - Autorisations de l'API, cliquez sur **Ajouter une autorisation**.
10. Fournissez un accès en lecture aux machines, aux vulnérabilités et aux recommandations de



sécurité.
11. Cliquez sur **Accorder le consentement de l'administrateur pour <nom de votre organisation>**.

> **Remarque :** Pour vous authentifier en tant qu'application à partir d'une ServiceNow instance, effectuez les actions suivantes :

a. Accédez à la **Intégration ServiceNow MS TVM** > **Certificats et secrets**, puis cliquez sur **Nouvelle clé secrète du client**.
b. Renseignez les champs du formulaire.

Formulaire de secrets clients

Champ	Description
Description	Nom de l'application.
Date d'expiration	Date d'expiration.

c. Cliquez sur **Ajouter**.

Le champ **Valeur** contient le nouveau secret client, qui est votre nouveau mot de passe.

> **Remarque :** Vous aurez besoin de ce mot de passe lorsque vous configurerez l'intégration dans votre Now Platform instance. Pour plus d'informations, consultez Installez et configurez Vulnerability Response Integration avec l'application MS TVM à l'aide de l'Assistant de configuration.

d. Conservez ce mot de passe en lieu sûr. Une fois que vous avez quitté cette page, ce mot de passe n'est plus disponible.

Vous avez créé avec succès un ID d'application pour l'authentification dans le Microsoft portail Azure.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Vous êtes prêt à configurer votre Now Platform® instance pour l'intégration.

Installez et configurez Vulnerability Response Integration avec l'application MS TVM à l'aide de l'Assistant de configuration

Installez et configurez l'intégration Réponse aux vulnérabilités à l'application Microsoft Threat and Vulnerability Management (MS TVM) afin de pouvoir utiliser les données importées de MS TVM pour prioriser et corriger les vulnérabilités de vos actifs.

Avant de commencer
Avant d'exécuter Microsoft ServiceNow® Threat and Vulnerability Management Vulnerability Integration, vous devez télécharger l'application Vulnerability Response Integration with Microsoft Threat and Vulnerability Management à partir de et ServiceNow Store l'installer et la configurer à l'aide de l'assistant de configuration de l'application Réponse aux vulnérabilités .

Avant d'installer l'application MS TVM, vérifiez que vous avez rempli tous les éléments de la Préparation à l'intégration des vulnérabilités Microsoft Threat and Vulnerability Management liste de vérification. Pour en savoir plus sur la configuration de votre Microsoft compte Azure, consultez Configurer Microsoft Azure pour l'intégration MS TVM.

Rôles requis : admin pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application Microsoft Threat and Vulnerability Management dans l'Assistant de configuration. Administrateur de vulnérabilité (sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) pour configurer l'application dans l'Assistant de configuration après son installation.

Pourquoi et quand exécuter cette tâche
Procédez comme suit avant d'installer et de configurer l'intégration MS TVM.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation de l'application d'intégration**.

   Après quelques instants, les applications disponibles pour installation sur votre instance s'affichent.

2. Localisez la vignette **Microsoft Threat and Vulnerability Management** et cliquez sur **Installer**.

   L'application Réponse aux vulnérabilités Intégration avec Microsoft Gestion des menaces et des vulnérabilités que vous avez téléchargée à partir du ServiceNow Store est installée.

3. Suivez les instructions de l'assistant de configuration pour poursuivre l'installation.
   Pour en savoir plus sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.

Que faire ensuite
Une fois l'installation terminée dans l'Assistant de configuration, accédez à **Configuration de l'intégration** > **Intégrations de scanners** dans l'Assistant de configuration pour poursuivre la configuration. Pour plus d'informations sur les invites fournies dans l'Assistant de configuration, reportez-vous à la section Configurer l'intégration de vulnérabilité MS TVM à l'aide de l'assistant de configuration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Paramètres de récupération de données pour Microsoft Threat and Vulnerability Management Integration

Vous pouvez utiliser des paramètres de récupération de données pour vous aider à déterminer le type et le champ d'application des données que vous souhaitez importer de l'intégration de vulnérabilité ServiceNow® de Microsoft Threat and Vulnerability Management (MS TVM) vers votre Now Platform® instance.

Les paramètres de récupération de données vous aident à contrôler les données que vous souhaitez importer. Vous pouvez définir les valeurs de ces filtres dans les instances d'intégration. Pour afficher les instances d'intégration, accédez à **Intégration de vulnérabilité de Microsoft Threat and Vulnerability Management** > **Instances d'intégration** et cliquez sur votre intégration MS TVM.

Sur la page Instance d'intégration, cliquez sur **Paramètres d'instance d'intégration** pour afficher une liste des paramètres, ou cliquez sur l'onglet **Intégrations de vulnérabilité** pour obtenir un calendrier, des détails REST, des détails d'intégration, des sources de données et des informations sur l'exécution de l'intégration.

Paramètres et filtres de récupération de données pour les intégrations MS TVM dans votre Now Platform instance

Les paramètres suivants sont disponibles pour les intégrations MS TVM dans votre Now Platform instance. Ces paramètres de configuration, ainsi que d'autres, sont affichés sur la page Instance d'intégration de votre Now Platform instance. Vous préférez peut-être conserver ces paramètres par défaut pour les premières exécutions d'intégration.

MS TVM.

vi_size_limit

Définit le nombre d'enregistrements d'éléments vulnérables à inclure dans le jeu de résultats à partir de l'intégration des vulnérabilités des ordinateurs MS TVM. Ce paramètre doit être au format int32. La valeur par défaut est 2 000.

vulnerabilities_size_limit

Définit le nombre d'enregistrements de vulnérabilité à inclure dans l'ensemble de résultats à partir de l'intégration de vulnérabilité MS TVM (CVE). Ce paramètre doit être au format int32. La valeur par défaut est 2 000.

recommendations_size_limit

Définit le nombre d'enregistrements de vulnérabilité à inclure dans le jeu de résultats à partir de l'intégration des recommandations MS TVM. Ce paramètre doit être au format int32. La valeur par défaut est 2 000.

asset_size_limit

Définit le nombre d'enregistrements de vulnérabilité à inclure dans le jeu de résultats à partir de l'intégration des machines MS TVM. Ce paramètre doit être au format int32. La valeur par défaut est 2 000.

machine_filter

Filtre les machines qui proviennent de MS TVM. Ce filtre est appliqué à l'intégration des machines MS TVM. La valeur par défaut est d'apporter des machines dans lesquelles onBoardingStatus est activé.

Messages REST pour Microsoft Threat and Vulnerability Management Vulnerability Integration

Vous pouvez utiliser les messages REST pour l'intégration ServiceNow® de vulnérabilité Microsoft Threat and Vulnerability Management (MS TVM) afin d'effectuer des appels à l'API MS TVM.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Jeton d'accès MS TVM

Vous pouvez également utiliser les messages REST pour le jeton d'accès MS TVM afin de récupérer le jeton d'accès de l'API MS TVM afin de pouvoir authentifier les demandes d'API REST. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes d'authentification adressées à MS TVM.

Intégration MS TVM

Vous pouvez utiliser le message REST pour l'intégration MS TVM afin de récupérer des informations de MS TVM. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes adressées à MS TVM pour récupérer des informations. Les messages REST contiennent les méthodes REST suivantes.

Méthodes REST

Méthode REST	Description de la méthode
Obtenir des vulnérabilités	Récupère les informations de vulnérabilité et d'exploitation à partir de MS TVM.
Vulnérabilités logicielles GET par ordinateur	Récupère toutes les vulnérabilités ouvertes.
Recommandations GET	Récupère la liste de toutes les recommandations de sécurité activables qui affectent l'organisation.
Obtenir des machines	Récupère la collection d'actifs.
GET Changements de vulnérabilités logicielles par ordinateur	Récupère toutes les informations qui ont changé dans l'importation complète de vulnérabilité de l'organisation, y compris les vulnérabilités nouvelles, corrigées et mises à jour.

Transformation des données pour Microsoft Threat and Vulnerability Management Vulnerability Integration

Une fois que vous avez identifié les données que vous souhaitez importer, celles-ci sont récupérées à partir de l'application ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM), traitées via un ensemble de sources de données et transformées dans votre instance.

Lors de l'installation, les cartes de gravité normalisées sont installées dans le module Mappage de gravité normalisée. Ces cartes transforment les niveaux de gravité de vulnérabilité tiers importés Microsoft en niveaux de gravité standard pour le traitement dans votre instance. Pour en savoir plus sur la création de cartes de gravité, reportez-vous à la section Créer une carte de Réponse aux vulnérabilités gravité.

Importation des machines MS TVM

Les données des machines importées sont d'abord chargées dans la table d'importation des machines MS TVM [sn_vul_msft_tvm_machines_import].

La transformation des machines MS TVM est utilisée pour transformer les informations sur les machines importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données provenant de l'importation des machines MS TVM sont traitées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez **Microsoft TVM Machines Transform**.

La table suivante répertorie les champs de carte de transformation par intégration.

Champs de carte de transformation des machines MS TVM

Champ source	Champ cible	Description
u_id	source_id	ID unique des actifs. Cet ID correspond au source_id de l'enregistrement de l'élément détecté.
u_ipaddresses.macAddress	mac_address	Adresse MAC mappée depuis l'API vers le champ d'adresse MAC hôte de l'enregistrement cmdb_ci.
u_ipaddresses.ipAddress	ip_address	Champ Adresse IP mappé sur le champ Adresse IP de l'enregistrement cmdb_ci.
u_lastseen	last_scan_date	Champ mappé au champ last_scan_date sur l'enregistrement de l'élément détecté.
u_machinetags		Balises enregistrées dans sn_sec_cmn_host_tag. Le mappage des balises aux ressources est enregistré dans sn_sec_cmn_m2m_src_ci_tag.
u_osplatform	système d'exploitation	Champ mappé au champ OS de l'enregistrement cmdb_ci.
u_computerdnsname	fqdn	Champ qui mappe le champ dnsname de l'API au champ fqdn sur l'enregistrement cmdb_ci.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Machines MS TVM Délai et objectif du script de carte de transformation

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application (sn_vul_msft_tvm) pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour mettre à jour les valeurs dans l'hôte et vérifier si l'hôte existe. En

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque le script est exécuté	Objectif
	fonction des résultats, ce script modifie les valeurs de la variable de champ d'application (sn_vul_msft_tvm). Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre de CI créés, mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

L'include de script MicrosoftTVMMachinesProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de l'intégration des machines Microsoft TVM et la transforme en CI. Toute modification apportée à cet include de script peut altérer la transformation des données des ordinateurs Microsoft TVM dans la table CI et Élément détecté.

Intégration des vulnérabilités MS TVM

Les données de vulnérabilités importées sont d'abord chargées dans la table d'importation [sn_vul_msft_tvm_vulnerabilities_import] CVE (vulnérabilités) Microsoft TVM.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données provenant de l'importation des vulnérabilités MS TVM sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez la **transformation des vulnérabilités Microsoft TVM**.

La table suivante répertorie les champs de carte de transformation par intégration.

Champs de carte de transformation des vulnérabilités Microsoft TVM

Champ source	Champ cible	Description
u_id	id	Mappe à la colonne ID de l'enregistrement sn_vul_entry.
u_severity	source_severity	Mappe le champ Gravité à la gravité. La valeur par défaut est de 5.
u_publishedon	date_published	Mappe le champ de u_publishedon à la date de publication.
u_publicexploit	public_exploit	Mappe les u_publicexploit fournies par le scanner à la colonne Exploitation publique dans la table d'entrée de vulnérabilité.
u_cvssv3	v3_base_score	Mappe le score cvssv3 au score de base v3 dans l'enregistrement d'entrée de vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation des vulnérabilités Microsoft TVM (suite)

Champ source	Champ cible	Description
u_description	résumé	Mappe la description au champ Résumé dans l'enregistrement de l'entrée de vulnérabilité.
u_exploitinkit	malware_kit	Mappe le champ u_exploitinkit au kit malware dans la table Exploit.
u_exploittypes	type	Mappe le type d'exploit au type de la table Exploit.
u_exploitverified	is_exploit_verified	Mappe le champ u_exploitverified à l'exploit vérifié dans la table Exploit.
u_exploituris	exploit_links	Mappe le champ u_exploituris aux liens d'exploitation dans la table Exploit.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application (sn_vul_msft_tvm) pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour créer ou mettre à jour les valeurs dans la table NVD ou la table d'entrée tierce. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir les valeurs des nouveaux éléments qui ont été créés et des éléments qui ont été mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Importation des recommandations MS TVM

Les données de recommandation importées sont d'abord chargées dans la table Importation des recommandations MS TVM [sn_vul_msft_tvm_recom_import].

Remarque : Les modifications apportées à cette carte de transformation modifient le traitement des données issues de l'importation des recommandations MS TVM.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez **MS TVM Recommendation Transform**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La table suivante répertorie les champs de carte de transformation par intégration.

Recommandation MS TVM Champs de carte de transformation

Champ source	Champ cible	Description
u_recommendedvendor	recommended_vendor	Mappe le champ u_recommendedvendor à la colonne Fournisseur.
u_weaknesses	Faiblesses	Mappe le champ u_weaknesses à la colonne Faiblesses.
u_exposedmachinescount	src_exposed_machines_cnt	Mappe le champ u_exposedmachinescount à la colonne Nombre d'ordinateurs exposés.
u_status	statut	Mappe l'état au champ État dans l'enregistrement de recommandation.
u_productname	product_name	Mappe le champ u_productname au nom du produit dans l'enregistrement de recommandation.
u_nonproductiv_impactedassets	non_prod_impacted_assets	Mappe le champ u_nonproductiv_impactedassets à la colonne Actifs impactés dans l'enregistrement de recommandation.
u_activealert	active_alert	Mappe le champ u_activealert à la colonne Alerte active dans l'enregistrement de recommandation.
u_recommendedversion	recommended_version	Mappe le champ u_recommendedversion à la colonne Version recommandée dans l'enregistrement de recommandation.
u_totalmachinecount	total_machine_count	Mappe le champ u_totalmachinecount à la colonne Nombre total d'ordinateurs dans l'enregistrement de recommandation.
u_exposureimpact	exposure_impact	Mappe le champ u_exposureimpact à la colonne Impact de l'exposition dans l'enregistrement de recommandation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recommandation MS TVM Champs de carte de transformation (suite)

Champ source	Champ cible	Description
u_recommendationname	recommendation_name	Mappe le champ u_recommendationname à la colonne Nom de la recommandation dans l'enregistrement de recommandation.
u_subcategory	sous-catégorie	Mappe le champ u_subcategory à la colonne Sous-catégorie dans l'enregistrement de recommandation.
u_id	source_id	Mappe l'ID de recommandation de MS TVM à la colonne ID de la source.
u_remediationtype	remediation_type	Mappe le champ u_remediationtype à la colonne Type de rattrapage dans l'enregistrement de recommandation.
u_relatedcomponent	related_component	Mappe le champ u_relatedcomponent à la colonne Composant connexe dans l'enregistrement de recommandation.
u_recommendedprogram	recommended_program	Mappe le champ u_recommendedprogram à la colonne Programme recommandé dans l'enregistrement de recommandation.
u_recommendationcategory	recommendation_category	Mappe le champ u_recommendationcategory à la colonne Catégorie de recommandation dans l'enregistrement de recommandation.
u_publicexploit	public_exploit	Mappe le champ u_publicexploit à la colonne Exploitation publique dans l'enregistrement de recommandation.
u_vendor	vendor	Mappe le champ u_vendor à la colonne Fournisseur dans l'enregistrement de recommandation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recommandation MS TVM Champs de carte de transformation (suite)

Champ source	Champ cible	Description
[Script]	integration_instance	Nom de l'instance à partir de laquelle la recommandation est importée.
[Script]	sys_domain	Domaine dans lequel cet enregistrement est importé.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Recommandation MS TVM Script de carte de transformation

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application (sn_vul_msft_tvm) pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour mettre à jour les valeurs dans les recommandations et vérifier si les recommandations existent. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir les valeurs des éléments créés, mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Importation des vulnérabilités de la machine MS TVM

La carte de transformation des vulnérabilités des machines MS TVM est utilisée pour transformer les informations ouvertes et corrigées sur les vulnérabilités importées à partir de MS TVM.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données provenant de l'importation des vulnérabilités des machines MS TVM sont traitées.

Pour accéder aux cartes de transformation des vulnérabilités ouvertes et corrigées de MS TVM, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez la **transformation des vulnérabilités de la machine MS TVM**.

La table suivante répertorie les champs de carte de transformation par intégration.

Champs de carte de transformation des vulnérabilités de la machine MS TVM

Champ source	Champ cible	Description
u_id	detection_key	Mappe le champ u_id à la colonne Clé

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation des vulnérabilités de la machine MS TVM (suite)

Champ source	Champ cible	Description
		de détection dans la table de détection.
u_diskpaths	proof	Mappe le champ u_diskpaths à la colonne Preuve dans la table de détection.
u_registrypaths	proof	Mappe le champ u_registrypaths à la colonne Preuve dans la table de détection.
u_recommendedsecurityupdateid	preferred_solution	Mappe le champ u_recommendedsecurityupdateid à la colonne Solution préférée dans la table des éléments vulnérables, si la solution existe avec le même ID dans la table sn_vul_solution.
u_recommendationreference	recommandation	Mappe le champ u_recommendationreference à la colonne Recommandation de la table des éléments vulnérables.
u_cveid	vulnerability	Mappe le champ u_cveid à la colonne Vulnérabilité dans la table des éléments vulnérables.
u_status	source_status	Mappe le champ u_status à la colonne État de la source dans la table de détection.
u_eventtimestamp	temporal_score	Mappe le champ u_eventtimestamp à la colonne Dernier résultat dans la table des éléments vulnérables.
u_lastseentimestamp	last_seen	Mappe le champ u_lastseentimestamp à la colonne Dernier observé dans la table des éléments vulnérables.
u_firstseentimestamp	first_seen	Mappe le champ u_firstseentimestamp

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation des vulnérabilités de la machine MS TVM (suite)

Champ source	Champ cible	Description
		à la colonne Premier observé dans la table des éléments vulnérables.
u_recommendedsecurityupdate	solution_summary	Mappe le champ u_recommendedsecurityupdate à la colonne Résumé de la solution dans la table des éléments vulnérables.
u_recommendedsecurityupdateurl	solution_summary	Mappe le champ u_recommendedsecurityupdateurl à la colonne Résumé de la solution dans la table des éléments vulnérables.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application (sn_vul_msft_tvm) pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour vérifier si l'entrée de vulnérabilité et les détections existent. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour mettre à jour le nombre de VI et de détections tel qu'importé de MS TVM. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Graphique d'état de l'exécution de l'intégration pour Microsoft Threat and Vulnerability Management Vulnerability Integration

Vous pouvez utiliser le module État de l'exécution de l'intégration de Microsoft Threat and Vulnerability Management (MS TVM) pour vous fournir une vue graphique de l'état des exécutions de l'intégration MS TVM.

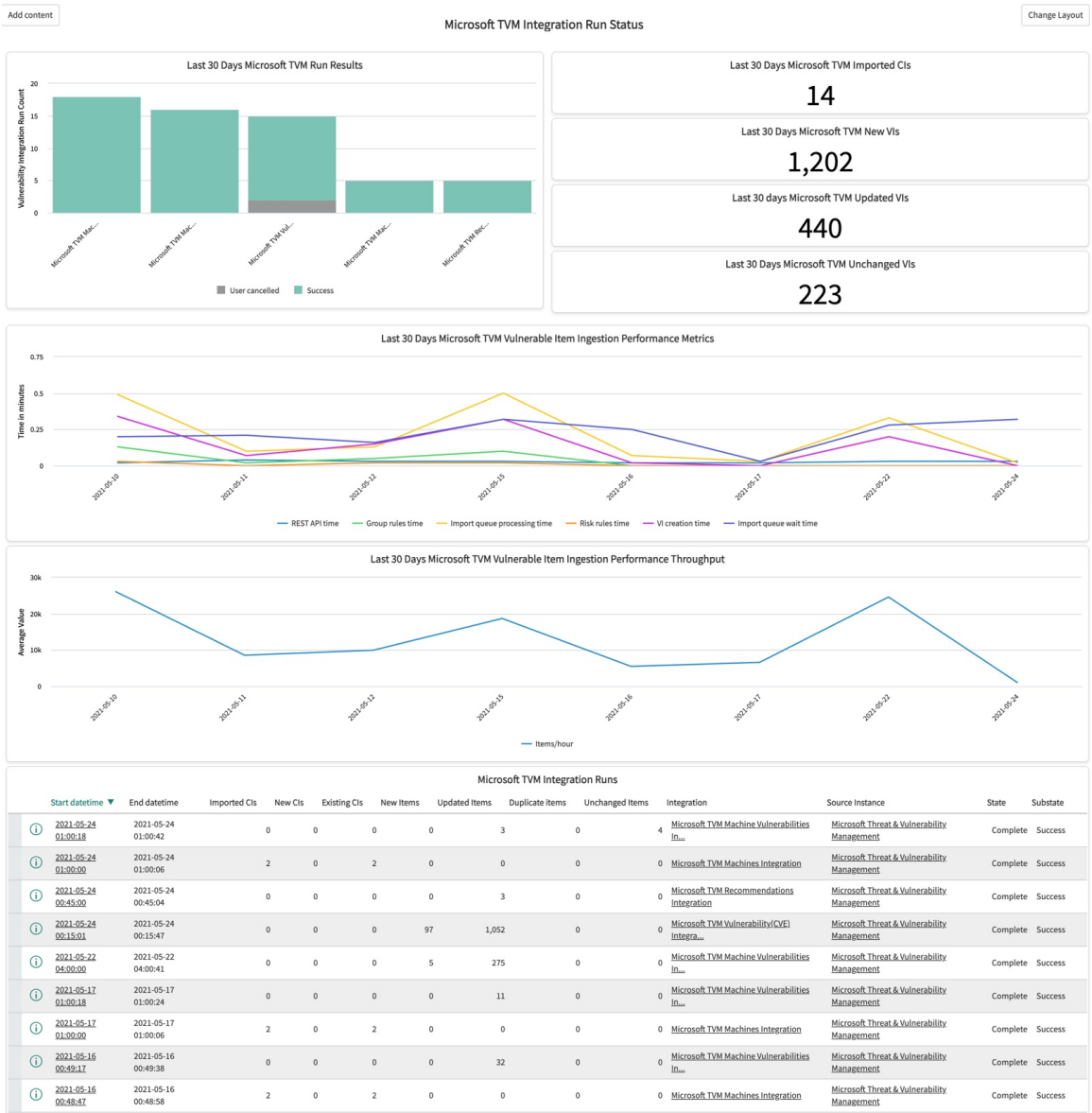
À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans le diagramme, vous pouvez pointer sur n'importe quelle partie du graphique pour afficher un résumé des données spécifiques à cette partie. Si vous cliquez sur une partie du graphique à barres, une liste s'ouvre pour fournir des informations plus détaillées.



Rapports de graphiques d'état de l'exécution de l'exécution de l'intégration MS TVM

Nom	Description
Résultats Microsoft TVM des 30 derniers jours	Nombre d'exécutions d'intégration terminées pour chaque intégration. Ce rapport affiche à la fois les exécutions réussies et échouées. Chaque exécution est affichée sous forme de barre dans le graphique.
Nouveaux VI Microsoft TVM au cours des 30 derniers jours	Nombre de nouveaux éléments vulnérables qui ont été importés au cours des 30 derniers jours.
VI mis à jour Microsoft TVM au cours des 30 derniers jours	Nombre d'éléments vulnérables mis à jour qui ont été importés au cours des 30 derniers jours.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
VI inchangés Microsoft TVM au cours des 30 derniers jours	Nombre d'éléments vulnérables en double qui ont été importés au cours des 30 derniers jours.
Exécutions de l'intégration MS TVM	Enregistrements d'exécution de l'intégration dans une liste. **Remarque : V16.1 :** Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection de la *sn_vul_detection* table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, après la fin de l'exécution de l'intégration.
Mesures de performance d'ingestion d'élément vulnérables Microsoft TVM au cours des 30 derniers jours	Mesures de performances quotidiennes pour les éléments vulnérables comparées au cours des 30 derniers jours.
Rendement de performance d'ingestion d'élément vulnérable Microsoft TVM au cours des 30 derniers jours	Débit quotidien d'ingestion d'éléments vulnérables qui a été mesuré pour l'intégration de détection d'hôte Microsoft TVM au cours des 30 derniers jours.
CI importés Microsoft TVM au cours des 30 derniers jours	Nombre de nouveaux éléments de configuration importés au cours des 30 derniers jours.

Vérifier l'état de l'exécution de l'importation de l'intégration de Microsoft Threat and Vulnerability Management

Utilisez l'état de l'exécution de l'importation de Microsoft Threat and Vulnerability Management (MS TVM) pour vérifier la réussite de vos exécutions d'intégration et localiser d'éventuels problèmes.

Avant de commencer

Cette procédure repose sur les hypothèses suivantes :

- Vous avez Réponse aux vulnérabilités installé et configuré l'intégration de vulnérabilité MS TVM.
- Les importations d'intégration de vulnérabilité MS TVM sont planifiées et en cours d'exécution.

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à la **Tout** > **Gestion des menaces et des vulnérabilités Microsoft** > **Intégrations**.
   a. Choisissez une intégration.
   b. Cliquez sur la liste connexe Exécutions de l'intégration de vulnérabilité.
2. Vérifiez que l'état des importations est Terminé et que le Sous-état est Réussite.
   Les causes les plus courantes d'un échec d'exécution sont les suivantes :
   - Interruption du réseau.
   - Désintégration du bit dans le transfert de données, ce qui entraîne la corruption des données pendant la transformation.
3. Facultatif : Si l'une de ces conditions entraîne un échec d'exécution, cliquez sur **Exécuter maintenant** et réexécutez l'intégration.

Présentation de l'intégration de l'orchestration des correctifs HCL BigFix avec Réponse aux vulnérabilités

Vous pouvez gérer les correctifs et les déploiements de correctifs pour les vulnérabilités critiques de grands groupes d'actifs avec l'intégration Réponse aux vulnérabilités d'orchestration de correctifs au produit HCL BigFix.

Orchestration des correctifs avec Réponse aux vulnérabilités

L'orchestration des correctifs utilise Réponse aux vulnérabilités des importations planifiées à partir d'intégrations de solutions tierces, de fournisseurs de correctifs et d'analyseurs de vulnérabilité. Les données de détection des scanners associent les actifs de votre environnement aux vulnérabilités et aux mises à jour de correctifs susceptibles de les corriger. Soumettez des demandes de correctifs pour approbation, planifiez des mises à jour de correctifs pour résoudre les éléments vulnérables et surveillez la progression du rattrapage, le tout à partir d'enregistrements enregistrés dans l'application Réponse aux vulnérabilités dans votre Now Platform®.

Orchestration des correctifs Vulnerability Response avec HCL BigFix

Lorsque l'application Vulnerability Response Patch Orchestration with HCL BigFix integration est utilisée avec le , Patch ServiceNow® Gestion des solutions pour vulnérabilitésOrchestration et Réponse aux vulnérabilités les applications, les gestionnaires et analystes de vulnérabilités peuvent effectuer les tâches suivantes :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour plus d'informations sur les types de correctifs et les solutions des fournisseurs (correctifs), consultez le contexte et les informations sur les types de correctifs et les solutions des fournisseurs (correctifs).
- Affichez et surveillez les données de vulnérabilité et de solution, ainsi que la progression du rattrapage des vulnérabilités à partir des enregistrements dans les Réponse aux vulnérabilités espaces de travail.

Les spécialistes informatiques et les responsables du rattrapage peuvent effectuer les tâches suivantes :

- Déployez les correctifs pris en charge par le produit BigFix pour leurs Windowsactifs, CentOS, MAC, Oracle et autres à intervalles réguliers et planifiés en dehors des heures de travail afin d'éviter les conflits de travail.
- Identifiez les actifs non corrigés présentant des vulnérabilités ou ceux qui n'ont pas été mis à jour correctement par les correctifs planifiés à partir de données de détection importées d'analyseurs tiers.
- Planifiez les correctifs disponibles à partir de l'espace de travail de remédiation informatique ou de l'environnement classique pour les actifs vulnérables non corrigés à partir de la mise à jour des correctifs, de la tâche de rattrapage et des enregistrements d'éléments détectés.

Termes clés dans les Réponse aux vulnérabilités applications et BigFix

Élément de configuration (CI)

Les CI sont les actifs existants répertoriés dans votre Base de données de gestion des configurations (CMDB)fichier . BigFix appelle les CI, les ordinateurs.

Groupes d'ordinateurs

Terminologie utilisée dans le produit BigFix qui fait référence à un groupe d'actifs.

Élément vulnérable

Une vulnérabilité importée qui correspond à un actif existant dans votre CMDB.

Instance

Un compte distinct de l'application BigFix. Chaque compte d'utilisateur peut être une instance de l'application BigFix. Ce terme désigne également une adresse Web unique et sécurisée pour une Now Platform instance.

Intégration

Une intégration est une tâche planifiée dans le Now Platform qui récupère des informations à partir d'une source tierce, telle que l'intégration avec les machines BigFix.

Solution

Il existe deux types de solutions dans le cadre de cette intégration, potentielles et préférées. Une solution potentielle est une solution qui pourrait remédier à une vulnérabilité. Les vulnérabilités ont souvent de nombreuses solutions potentielles. #Une solution privilégiée correspond à la solution la plus efficace pour une vulnérabilité spécifique détectée.

Correctif

Mises à jour logicielles qui corrigent les vulnérabilités. Dans l'application BigFix, les correctifs sont appelés Fixlets. Par exemple, BigFix propose des fixlets pour Windows, CentOS, Oracle MAC et d'autres produits.

Correctif préféré

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les correctifs préférés sont les mises à jour logicielles destinées à corriger des vulnérabilités spécifiques. Les correctifs, une fois déployés, sont mappés aux éléments vulnérables liés à des vulnérabilités spécifiques et corrigent-les.

Tâche de rattrapage

Listes des éléments vulnérables dans l'application Réponse aux vulnérabilités des actions requises pour corriger les vulnérabilités.

Déploiement

Aux fins de cette intégration, le déploiement désigne le moment où vous appliquez, lancez ou planifiez un correctif sur un ordinateur. BigFix appelle ces déploiements des actions. Vous pouvez déployer (créer des actions) pour les correctifs que vous avez téléchargés à partir de BigFix dans votre Now Platformfichier . Accédez aux éléments, correctifs ou tâches de remédiation détectés à partir d'enregistrements individuels dans Réponse aux vulnérabilités. Vous pouvez déployer des correctifs avec des travaux planifiés sur des machines individuelles ou sur des groupes d'ordinateurs.

Le déploiement dans le Now Platform peut également faire référence à une intégration qui prend en charge plusieurs sources. Une existence d'intégration unique est appelée un déploiement de votre intégration. Un déploiement fait référence aux intégrations et aux produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de l'intégration BigFix Vulnerability dans votre environnement.

Vulnerability Solution Management et Vulnerability Response Patch Orchestration with HCL BigFix Integration

La gestion de la solution est assurée par l'application Gestion des solutions pour vulnérabilités , une Now Platform application qui met en corrélation vos résultats de vulnérabilité avec la répartition des solutions (correctifs) qui les corrige. Identifiez les correctifs logiciels de tiers pour les produits et services, les mises à jour de configuration et les autres contrôles ayant le plus d'impact pour votre organisation. Outre les informations des scanners tiers, les applications Orchestration des Gestion des solutions pour Réponse aux vulnérabilitésRéponse aux vulnérabilitéscorrectifs de réponse aux vulnérabilités avec HCL BigFix fonctionnent ensemble pour déployer les correctifs préférés de la solution à la vulnérabilité et à l'élément vulnérable pour vous aider à corriger et à fermer les vulnérabilités de votre environnement.

Le Gestion des solutions pour Réponse aux vulnérabilités, Réponse aux vulnérabilitéset Vulnerability Response Patch Orchestration with HCL BigFix Integration sont tous disponibles dans le ServiceNow® Store.

Rôles Now Platform requis

Les tâches d'intégration, d'installation, de configuration et de rattrapage nécessitent les rôles suivants dans votre Now Platform instance.

administrateur

Les utilisateurs dotés de ce rôle obtiennent des autorisations pour les applications dans le ServiceNow Store et les télécharge dans Now Platform les instances.

sn_vul.vulnerability_admin

Les utilisateurs ayant ce rôle activent les applications dans l'instance Now Platform et terminent la configuration de l'application Réponse aux vulnérabilités . Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Cet utilisateur administrateur configure toutes les applications, règles et intégrations tierces VR.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sn_vul_bigfix.configure_integration

Les utilisateurs ayant ce rôle configurent l'application BigFix Patch Orchestration Integration. Ce rôle contient le rôle granulaire sn_vul_bigfix.read_integration.

sn_vul_bigfix.read_integration

Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les enregistrements de l'application Réponse aux vulnérabilités BigFix Patch Orchestration Integration et les données d'orchestration des correctifs.

sn_vul_patch_orch.configure_patch

Les utilisateurs disposant de ce rôle peuvent configurer et appliquer des correctifs.

sn_vul_patch_orch.read_patch

Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les informations sur les correctifs.

Approbateurs

Affectez des utilisations aux groupes d'approbateurs de niveau 1 et d'approbateurs de niveau 2 si vous souhaitez que les demandes de correctifs soumises soient approuvées avant le déploiement.

Pour en savoir plus sur l'affectation de ces rôles à l'aide de l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur les rôles dans votre Réponse aux vulnérabilitésNow Platform, reportez-vous à la section Réponse aux vulnérabilités Profils et rôles granulaires.

Règles de recherche de CI

Lorsque les données sont importées à partir de l'application BigFix, l'application Réponse aux vulnérabilités recherche automatiquement des correspondances dans les données de l'ordinateur Base de données de gestion des configurations (CMDB) utilisateur (actif). Les règles de recherche de CI sont utilisées pour identifier les CI (actifs) et les ajouter automatiquement aux enregistrements d'éléments vulnérables (VI) lorsque des VI sont créés.

Les règles de recherche de CI suivantes sont fournies avec le système de base et sont utilisées pour identifier les CI (actifs) et les ajouter à l'application Réponse aux vulnérabilités :

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

Vous pouvez utiliser plusieurs valeurs pour le IP_ADDRESS d'un actif. Une règle de recherche de CI tient compte de toutes les valeurs pour établir une correspondance. Pour plus d'informations sur le fonctionnement et le fonctionnement des règles de recherche de CI, reportez-vous à Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Serveur MID

L'intégration Réponse aux vulnérabilités de Patch Orchestration avec HCL BigFix est une intégration sur site. Il nécessite un serveur MID autonome qui ne fait pas partie d'une grappe de serveurs MID. Le MID Server doit exécuter des scripts sur des machines distantes à partir de votre instance afin d'importer des données à partir du serveur BigFix. Les API pour cette intégration sont appelées à l'aide des MID Servers que vous configurez dans votre

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Now Platform instance. Consultez Préparez-vous à l'intégration de Patch Réponse aux vulnérabilités Orchestration avec HCL BigFix pour plus d'informations.

Intégrations et dépendances de l'intégration Réponse aux vulnérabilités Patch Orchestration avec HCL BigFix

Les applications de produits et de dépendances suivantes sont requises pour Vulnerability Response Patch Orchestration with HCL BigFix Integration. Ces applications sont disponibles dans le ServiceNow® Storefichier .

Versions disponibles des applications et dépendances requises pour l'intégration d'orchestration de correctifs

Pour afficher les données d'orchestration des correctifs et les mises à jour (correctifs) disponibles dans les espaces de travail de Réponse aux vulnérabilités, les applications suivantes sont requises. Toutes les applications répertoriées sont disponibles dans le ServiceNow® Storefichier . Certaines applications nécessitent des abonnements distincts.

Pour plus d'informations sur la compatibilité des versions avec les applications requises et les versions de famille, consultez l'article Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production dans la base de connaissances HI.

Application et version de mise en production
Réponse aux vulnérabilités
Gestion des solutions pour vulnérabilités
Application Orchestration de correctif pour Vulnerability Response
Réponse aux vulnérabilités Orchestration des correctifs avec l'application HCL BigFix
Security Support Common
Orchestration de support de sécurité
Une application de scanner de vulnérabilité tierce prise en charge

Réponse aux vulnérabilités Tables de l'application Orchestration de correctifs

L'application Réponse aux vulnérabilités Patch Orchestration contient les tables suivantes :

Table	Description
Mise à jour de correctif [sn_vul_patch_orch_update]	Stocke des informations sur les correctifs disponibles sur des instances distinctes.
Mise à jour de l'appareil [sn_vul_patch_orch_m2m_src_ci_update]	Stocke les données relatives aux correctifs déployés, ainsi que l'état de déploiement, qui sont affichés sur les enregistrements d'éléments détectés.
Collecte [sn_vul_patch_orch_collection]	Stocke les données de collection provenant d'instances distinctes.
Collection d'appareils [sn_vul_patch_orch_m2m_src_ci_collection]	Stocke les données de collection sur les éléments détectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Déploiement de correctif [sn_vul_patch_orch_deployment]	Stocke des informations sur les correctifs déployés, sur les collections et les CI.
Correctif potentiel [sn_vul_patch_orch_m2m_vuln_patch]	Stocke des données sur les correctifs et les vulnérabilités qui identifient les correctifs qui peuvent être utilisés pour résoudre une vulnérabilité.

Intégrations de Vulnerability Response Patch Orchestration avec HCL BigFix

Les intégrations développées par ServiceNow® l'ingénierie constituent le déploiement orchestré de la solution avec le produit BigFix. Les intégrations suivantes sont incluses dans l'application Réponse aux vulnérabilités Patch Orchestration Integration with HCL BigFix que vous téléchargez à partir du ServiceNow® Store.

Après avoir installé l'application d'intégration sur votre Now Platform instance, pour afficher ces intégrations, accédez à **Intégrations** > **Intégration d'orchestration de correctifs BigFix** > **Intégrations**. L'application Réponse aux vulnérabilités traite les données à intervalles de temps planifiés importés par ces intégrations avec les points de terminaison BigFix.

Intégration	Description
Intégration de la collection BigFix	• Cette intégration est planifiée pour s'exécuter quotidiennement et s'exécute en premier dans l'exécution d'intégration chaînée. • Récupère les ordinateurs et les groupes d'ordinateurs qui composent les groupes d'ordinateurs (éléments de configuration) à partir de l'application BigFix.
Intégration de fixlets BigFix	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de BigFix Collection. Vous pouvez également l'exécuter à la demande. • Récupère des informations sur tous les fixlets (correctifs) disponibles à partir du serveur BigFix.
Intégration de fixlet d'appareil BigFix	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration des fixlets BigFixlet. Vous pouvez également l'exécuter à la demande. • Récupère des informations sur les fixlets qui se trouvent actuellement sur les ordinateurs (actifs) à partir du serveur BigFix.
Intégration de BigFix Actions	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration BigFix Device Fixlet. Vous pouvez également l'exécuter à la demande. • Récupère des informations sur les correctifs planifiés par l'équipe informatique dans le serveur BigFix.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préparez-vous à l'intégration de Patch Réponse aux vulnérabilités Orchestration avec HCL BigFix

Préparez l'intégration en effectuant les tâches de configuration suivantes.

Avant de commencer

Rôles requis : administrateur pour l'installation des applications et l'affectation des rôles. D'autres rôles sont répertoriés dans la table suivante.

Pourquoi et quand exécuter cette tâche

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration.

Vous êtes prêt à Installer Patch Orchestration avec l'application Réponse aux vulnérabilités HCL BigFix.

Procédure

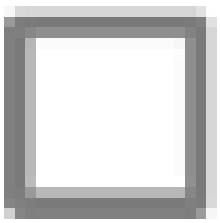
1. Pour une installation et une configuration fluides de l'application Réponse aux vulnérabilités Patch Orchestration with HCL BigFix, suivez la liste de vérification fournie.
2. Vous pouvez imprimer la liste de vérification suivante et vérifier que les éléments répertoriés sont remplis avant d'installer l'application.

   Après l'installation et la configuration, importez les informations relatives à la vulnérabilité et aux correctifs dans votre Now Platform® instance.

Tâche	Description
☐	(Facultatif) Si elle n'est pas déjà installée et activée, il peut être préférable d'installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour en savoir plus sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 16.0 ou Réponse aux vulnérabilités ultérieure.
☐	Si ce n'est pas déjà fait, obtenez les autorisations et installez une application de scanner tierce pour importer les données de vulnérabilité. Pour Intégrations de Réponse aux vulnérabilités plus d'informations sur les scanners tiers pris en charge par Réponse aux vulnérabilités. Consultez .
☐	Si ce n'est pas déjà fait, obtenez les autorisations et téléchargez l'application Vulnerability Response Patch Orchestration with HCL BigFix sur votre Now Platform® instance. Consultez .

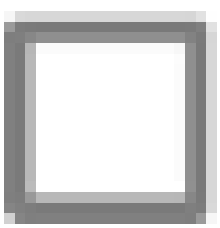
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Obtenez les informations d'identification BigFix. Vérifiez que vous disposez de tous les noms de compte, mots de passe et autres informations de service requis par vos produits BigFix afin d'y avoir accès.
	Vérifiez que vous disposez de groupes ou d'utilisateurs pour gérer les intégrations et corriger les éléments vulnérables. administrateur L'administrateur système obtient des autorisations, télécharge et installe l'application BigFix Patch Orchestration et les autres applications requises pour l'intégration. En l'absence d'affectation, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'assistant de configuration dans Réponse aux vulnérabilités ou à partir du module Administration utilisateurs. sn_vul.vulnerability_admin Une fois affecté, l'administrateur de vulnérabilité termine la configuration des intégrations BigFix et des autres applications tierces. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Ce rôle configure toutes les applications VR, les règles, les intégrations tierces, les applications Vulnerability Response Patch Orchestration et Vulnerability Solution Management. sn_vul_bigfix.configure_integration Les utilisateurs ayant ce rôle configurent l'application BigFix Patch Orchestration Integration. Ce rôle contient les rôles granulaires sn_vul_bigfix.read_integration et connection_admin qui permettent à l'utilisateur de se connecter à la console BigFix et de configurer les instances d'intégration dans votre Now Platform. sn_vul_bigfix.read_integration Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les enregistrements de l'application Réponse aux vulnérabilités BigFix Patch Orchestration Integration et les données d'orchestration des correctifs. sn_vul_patch_orch.configure_patch Les utilisateurs disposant de ce rôle peuvent configurer et appliquer des correctifs. Les correctifs demandés par cet utilisateur à partir

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	des enregistrements d'élément vulnérable et de mise à jour de correctif sont envoyés pour approbation si la gestion des changements est active et que des approbateurs sont affectés. sn_vul_patch_orch.read_patch Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les informations de correctifs sur les enregistrements. Ce rôle est hérité des rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail IT Remediation et Vulnerability Manager. Approbateurs Les utilisateurs affectés aux groupes d'approbateurs de niveau 1 et, éventuellement, d'approbateurs de niveau 2 approuvent les demandes de correctifs soumises. Par défaut, les correctifs sont soumis au groupe d'approbateurs de niveau 1 pour approbation avant le déploiement. Pour en savoir plus sur le processus d'approbation, reportez-vous Orchestration des correctifs avec Réponse aux vulnérabilitésà . Pour en savoir plus sur la configuration des approbateurs et des groupes, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. L'administrateur système effectue l'affectation initiale des rôles aux utilisateurs et aux groupes pour l'intégration. Par défaut, le groupe Vulnerability Response est disponible. Si ce n'est pas déjà fait, vous pouvez créer des groupes supplémentaires pour les rôles de spécialiste du rattrapage et d'analyste de vulnérabilité et ajouter des utilisateurs avec le module Administration des utilisateurs dans votre instance. Reportez-vous à la section Créer un groupe d'utilisateurs .
	Vérifiez que vous avez activé toutes les fonctionnalités, règles, modules d'extension de dépendance ou tâches dans votre instance requises pour l'intégration. ◦ Vulnerability Response Patch Orchestration with HCL BigFix est une intégration sur site qui nécessite l'utilisation d'un MID Server autonome. Pour plus d'informations sur les MID Servers dans votre instance, consultez Serveur MID .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	◦ Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tout** et localisez le module d'extension. S'il n'est pas installé dans votre instance, installez-le et activez-le.

Que faire ensuite
Vous êtes maintenant prêt à Installer Patch Orchestration avec l'application Réponse aux vulnérabilités HCL BigFix.

Installer Patch Orchestration avec l'application Réponse aux vulnérabilités HCL BigFix

Téléchargez l'application Vulnerability Response Patch Orchestration avec HCL BigFix à partir du ServiceNow® Store.

Avant de commencer
Rôles requis : admin pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application. Vulnerability Admin (sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)) pour configurer Vulnerability Response Patch Orchestration avec HCL BigFix et d'autres applications après leur installation.

Pourquoi et quand exécuter cette tâche
Avant d'installer l'application, vérifiez que vous avez rempli tous les éléments de la liste de vérification dans Préparez-vous à l'intégration de Patch Réponse aux vulnérabilités Orchestration avec HCL BigFix.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Procédure
1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Localisez l'application **Vulnerability Response Patch Orchestration with HCL BigFix** et cliquez sur **Installer**.

   Cette action installe l'application que vous avez téléchargée à ServiceNow Storepartir du .
3. Vous pouvez également installer des applications à partir de l'Assistant de configuration. Pour en savoir plus sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.

Que faire ensuite
Une fois l'installation terminée, accédez à **Tout** > **Intégration d'orchestration de correctifs BigFix** > **Configuration** pour poursuivre la configuration.

Configurer l'intégration d'orchestration de correctifs Réponse aux vulnérabilités avec HCL BigFix

Une fois l'application installée, configurez-la avec les informations de votre compte BigFix et validez vos informations d'identification.

Avant de commencer
Rôles requis : sn_vul.vulnerability_admin et sn_vul_bigfix.configure_integration

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Intégration d'orchestration de correctifs BigFix** > **Configuration**.
2. Renseignez les champs avec vos informations et informations d'identification BigFix.

Champ	Description
Instance d'intégration	Le nom du compte d'instance BigFix que vous souhaitez utiliser, par exemple, `intégration de gestion des correctifs BigFix`.
Nom d'hôte	Saisissez l'URL de l'hôte BigFix.
Nom d'utilisateur	Saisissez le nom d'utilisateur de votre compte BigFix.
Mot de passe	Saisissez le mot de passe de votre compte BigFix.
Serveur MID	Dans la liste, entrez le nom du serveur MID autonome que vous souhaitez utiliser. Pour Préparez-vous à l'intégration de Patch Réponse aux vulnérabilités Orchestration avec HCL BigFix plus d'informations sur les serveurs MID et sur la configuration des tâches dans votre Now Platform®.

3. Cliquez sur Enregistrer et tester les informations d'identification.
   L'état de votre connexion entre BigFix et votre Now Platform® instance est affiché dans le champ État de validation. Si le test ne réussit pas, suivez les instructions.
4. Facultatif : Séparation de domaine est pris en charge pour cette intégration.
   Vous pouvez ajouter plusieurs configurations à votre instance. Pour ajouter des configurations supplémentaires :

   a. Accédez à la **Intégration d'orchestration de correctifs BigFix Instances d'intégration**

   b. Vérifiez que le périmètre de `l'application, Vulnerability Response Patch Orchestration with HCL BigFix`, est affiché dans le champ de périmètre de l'application.

   c. Cliquez sur **Nouveau**.

   d. Remplissez le formulaire.

Champ	Description
Nom	Nom de l'instance d'intégration.
Application	Orchestration des correctifs Vulnerability Response avec HCL BigFix
Intégration	[Lecture seule] La gestion des correctifs BigFix est l'option par défaut.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	La valeur par défaut est activée (sélectionnée). Si elle est décochée, l'instance n'est pas active.

e. Cliquez sur **Envoyer**.
Votre nouvelle instance d'intégration apparaît dans la liste des instances d'intégration.

f. Répétez les étapes 1 à 3 pour configurer votre instance d'intégration et tester vos informations d'identification.

5. Configurez les approbations pour les demandes de correctifs.
Par défaut, une propriété système [**sn_vul_patch_orch.patch_approval_required**] est activée de sorte que, lorsque des déploiements de correctifs sont planifiés, ils sont soumis pour examen et approbation aux utilisateurs affectés au groupe d'approbation de niveau 1 - Mise à jour des correctifs.

Si vous souhaitez que les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch planifient des correctifs sans approbation, vous pouvez désactiver la propriété [**sn_vul_patch_orch.patch_approval_required**]. Vous préférez peut-être laisser les approbations activées afin que les correctifs planifiés n'entrent pas en conflit avec les heures de travail normales.

Remarque : Si vous désactivez la propriété système d'approbation, tout utilisateur disposant du rôle sn_vul_patch_orch.configure_patch peut planifier et déployer des correctifs sans examen ni approbation.

En tant qu'utilisateur ayant le rôle sn_vul.vulnerability_admin, pour désactiver la propriété système :

a. Accédez à la **sys.properties.list**.

b. Localisez **sn_vul_patch_orch.patch_approval_required** et cliquez dessus pour ouvrir l'enregistrement.

c. Dans le champ Valeur, tapez `false`.

d. Cliquez sur **Mettre à jour**.

6. Si vous ne désactivez pas cette propriété, vous devez affecter des approbateurs pour les demandes de correctifs.
En tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin, procédez comme suit.

a. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.

b. Si la règle d'approbation Approbation de la **mise à jour du correctif de déploiement** n'est pas affichée dans la liste, cliquez sur **Tout** à droite de l'icône de filtre vert en haut à gauche de l'écran pour afficher la liste complète.

c. Dans la liste, cliquez sur Approbation de la **mise à jour du correctif de déploiement**.

d. Dans l'enregistrement, avec l'onglet Configuration de l'approbation sélectionné, cliquez sur **Approbation de mise à jour du correctif de configuration par défaut**.

e. Pour l'enregistrement, cliquez sur **Niveau 1 - Approbation de mise à jour du correctif**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Ajoutez des utilisateurs à ce groupe.

Les utilisateurs affectés à ce groupe approuvent les demandes de correctifs soumises par les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch. Accédez à **Mes approbations** pour afficher et traiter les demandes.

7. Cliquez sur**Mettre à jour** pour enregistrer vos modifications.

8. Facultatif : Vous pouvez configurer des approbations multiniveaux de sorte que plusieurs approbations soient requises avant le déploiement des demandes de correctifs planifiées.

a. Une fois l'enregistrement d'approbation de mise à jour du correctif de configuration par défaut affiché, cliquez sur **Nouveau**.

b. Renseignez les champs.

Champ	Description
Nom	Nom du niveau d'approbation, par exemple, **Niveau 2 - Approbation de mise à jour du correctif**.
Actif	Activé par défaut, ce qui signifie que le niveau d'approbation est utilisé.
Approbation requise	Sélectionnez le nombre d'approbations requises pour le niveau sélectionné : ▪ Un approbateur requis ▪ Approbation de tous les utilisateurs requise
Ordre	Ordre d'exécution des différentes configurations au sein d'une règle. Par exemple, une configuration avec une entrée d'ordre de 100 s'exécute avant une configuration avec une entrée d'ordre de 200.
Rôle	Sélectionnez un rôle pour le groupe dans la liste.
Règle d'approbation	Contient les détails de table et de type pour la règle d'approbation.
Configuration de l'approbation	Contient les configurations d'approbation.
Affecter à l'aide de	Sélectionnez une option : ▪ Utilisateur et groupe d'utilisateurs ▪ Champ de la table des approbations ▪ Script
Groupes	Groupe de niveau de l'approbateur composé de plusieurs utilisateurs. L'utilisateur doit avoir l'un des rôles suivants que vous spécifiez.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utilisateurs	Modifier les utilisateurs répertoriés dans les groupes.

c. Cliquez sur **Envoyer** pour enregistrer vos modifications.

Affichage des données de correctif pour l'intégration d'orchestration Réponse aux vulnérabilités de correctifs avec HCL BigFix

Les données de correctif et les données de déploiement de correctif, ainsi que les informations de vulnérabilité et l'état de rattrapage de vos vulnérabilités, sont affichées dans les enregistrements de votre instance.

Affichage des données de correctifs dans les Réponse aux vulnérabilités espaces de travail

Rôles requis :

- sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs
- sn_vul_patch_orch.read_patch pour afficher (en lecture seule) les informations de correctif sur les enregistrements. Ce rôle est hérité des rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail Responsable du rattrapage informatique et de la vulnérabilité

Dans l'espace de travail de remédiation informatique, vous pouvez afficher les correctifs :

- Dans la vue d'accueil, où vous pouvez cliquer sur des tableaux de résultats pour afficher les enregistrements des solutions préférées sur les VI, des CI vulnérables et des correctifs préférés sur les VI.
- Dans la vue de liste, où vous pouvez afficher tous les enregistrements de mise à jour de correctifs (VPU) à partir des liens des correctifs, ainsi que les éléments vulnérables (VIT) qui vous sont affectés et qui ont des correctifs.

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- À partir d'une mise à jour de correctif (VPU)
- Tâche de rattrapage (RT)
- Enregistrements d'éléments détectés (SDI)

Dans Vulnerability Manager Workspace, vous pouvez afficher les correctifs :

- À partir de la vue d'accueil sur les rubriques de surveillance, où vous pouvez afficher les correctifs préférés et potentiels, les dates planifiées des correctifs et, si le correctif a été téléchargé, le tout sous l'onglet **Éléments vulnérables** .
- Depuis la vue de liste sur les efforts de rattrapage, où vous pouvez afficher les données de correctifs sur les enregistrements de VI à partir de l'onglet**Éléments vulnérables** .

À partir de la vue d'environnement classique, accédez à **Tout** > **Réponse aux vulnérabilités** > **Correctifs**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements de mise à jour de correctif dans les espaces de travail VR et dans la vue d'environnement classique

Les données de correctif et les données et l'état de déploiement de correctif sont affichés sur les enregistrements de votre instance. Les enregistrements de correctifs sont inclus dans la fonctionnalité d'orchestration de correctifs de cette intégration avec Réponse aux vulnérabilités. Affichez les enregistrements de correctifs (VPU) dans Réponse aux vulnérabilités les espaces de travail à partir de la vue Liste de l'espace de travail de remédiation informatique. Les enregistrements de mise à jour de correctif dans la vue classique et Réponse aux vulnérabilités les espaces de travail incluent les données suivantes :

- Données et informations sur les solutions de vulnérabilité provenant des fournisseurs de correctifs importées par l'application Gestion des solutions de vulnérabilité.
- État du rattrapage à la source qui inclut le nombre total d'appareils présentant une vulnérabilité donnée qui peut être corrigée par un correctif et tous les appareils pour lesquels des mises à jour sont manquantes.
- État du rattrapage qui inclut le % de VI rattrapés et le total des VI pour lesquels un correctif est préféré.
- Appareils associés, éléments vulnérables, déploiements de correctifs et demandes de correctifs sur les liens connexes des enregistrements dans la vue de classe. Ces données sont affichées sous forme d'onglets sur les Réponse aux vulnérabilités enregistrements des espaces de travail.
- Demandes de correctifs que les propriétaires de rattrapage ont soumises pour approbation.

Déploiement d'état sur les enregistrements d'éléments vulnérables

Pour en savoir plus sur le déploiement de l'état sur les enregistrements, reportez-vous Déploiement des données et de l'état des correctifs pour l'orchestration des correctifs dans Réponse aux vulnérabilitésà .

Enregistrements qui déploient des nombres de VI actifs

Pour éviter de déployer tous les correctifs sur toutes les vulnérabilités, la tâche planifiée récupère uniquement les changements apportés au nombre de VI actifs. Ces changements de nombre et les données connexes sont déployés sur les enregistrements suivants dans Réponse aux vulnérabilités:

- VIT
- RT
- Solution de vulnérabilité
- Mise à jour du correctif

Affichage des données pour les correctifs sans solutions

Pour plus d'informations sur l'affichage des correctifs sans solutions, reportez-vous à la section Afficher les correctifs sans solution dans Réponse aux vulnérabilités.

Appliquer des correctifs de données sur le Réponse aux vulnérabilités

Les tableaux de bord Gestion des vulnérabilités (PA) et CISO sont inclus dans un abonnement avec l'application Analyse des performancesRéponse aux vulnérabilités . Si vous disposez d'un abonnement à Analyse des performances, mais qu'aucune intégration

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'orchestration de correctif n'est installée, l'onglet Rattrapage s'affiche sur le tableau de bord CISO, mais il n'est pas renseigné avec les données.

Pour le tableau de bord Gestion de la vulnérabilité (PA), accédez à **Tout** > **Réponse aux vulnérabilités** > **Vue d'ensemble**. Cliquez sur l'onglet **Correction** et faites défiler vers le bas de la page pour afficher les données de mises à jour de correctifs : correctifs planifiés et non planifiés, correctifs n'ayant pas leur date cible et nombres hebdomadaires.

Pour le tableau de bord CISO, accédez à **Tout** > **Réponse aux vulnérabilités** > **Tableau de bord des CISO**. Avec l'onglet Vue d'ensemble sélectionné, faites défiler vers le bas de la page pour afficher les données de couverture des correctifs : criticité, correctifs planifiés et non planifiés, et correctifs n'ayant pas leur date cible.

Pour en savoir plus sur les tableaux de bord, reportez-vous Réponse aux vulnérabilités aux rubriques Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités, Appliquer des correctifs à Orchestration avec les Réponse aux vulnérabilités espaces de travailet Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord.

Planifier les correctifs avec l'intégration Patch Réponse aux vulnérabilités Orchestration HCL BigFix

Planifiez les correctifs à partir des enregistrements de tâche de mise à jour et de rattrapage dans l'application Réponse aux vulnérabilités de votre Now Platform instance.

Avant de commencer

À partir de la version 16.1, vous pouvez planifier des correctifs à partir des espaces de Réponse aux vulnérabilités travail ou de l'environnement classique.

Rôles requis :

- sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs
- sn_vul_patch_orch.read_patch pour afficher (en lecture seule) les informations de correctif sur les enregistrements. Ce rôle est hérité des rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail Responsable du rattrapage informatique et de la vulnérabilité

Procédure

1. Dans Vulnerability Réponse aux vulnérabilités Workspaces, en tant qu'utilisateur disposant du rôle sn_vul.remediation_owner, accédez à **Tout** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
2. Sur la page d'accueil, cliquez sur **Correctif préféré sur les VI.**
   La liste des enregistrements de mise à jour de correctifs pour les VI avec correctifs préférés qui vous sont affectés s'affiche.
3. Localisez un enregistrement que vous souhaitez ouvrir et cliquez dessus pour l'ouvrir.
4. Sinon, dans la vue de liste de l'espace de travail, cliquez sur **Correctifs** > **Tout** et localisez un enregistrement de mise à jour de correctif.
   L'enregistrement de mise à jour du correctif s'affiche. Vous préférerez peut-être examiner les données avant de planifier un correctif, car d'autres correctifs peuvent déjà être planifiés.
5. Reportez-vous au tableau suivant pour connaître les données affichées et ce que vous pouvez faire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
Cliquer sur un lien d'éléments connexes	◦ Vue d'ensemble - Affichez les détails tels que le numéro d'enregistrement de mise à jour du correctif, les ID d'article et de bulletin, la date de publication et la catégorie de la mise à jour, le nom du site pour le correctif, la cote de risque, le score de risque, la description, la solution (le cas échéant) et l'état du rattrapage. ◦ Appareils associés : liste des éléments de configuration impactés affectés par le correctif et son état. ◦ Éléments vulnérables : liste des éléments vulnérables associés à la vulnérabilité et au correctif. ◦ Déploiements de correctifs : noms et informations relatives aux déploiements de ce correctif sur les actifs ou les groupes de ressources de ce correctif. ◦ Demandes de correctifs : liste des demandes de correctifs déjà soumises pour ce correctif. Ceci s'affiche.
Cliquez sur un lien pour ouvrir un enregistrement.	Dans les listes affichées dans les enregistrements ouverts à partir des liens des éléments connexes, affichez plus de détails, y compris les messages sur les cibles manquées. Une fois ouverts, les enregistrements restent ouverts en tant qu'onglets jusqu'à ce que vous les fermiez.
Planifier le correctif	Lorsque vous êtes prêt à planifier un correctif ou à envoyer une demande, cliquez sur **Planifier le correctif**. Dans la boîte de dialogue qui s'affiche, renseignez les champs. Reportez-vous aux étapes ci-dessous pour en savoir plus.
Ajouter une note de travail ou joindre un fichier	Tout à droite de l'écran, cliquez sur l'icône **Activité** (icône d'allègement) et saisissez une note de travail. Cliquez sur l'icône pour basculer le panneau. Vous pouvez également charger un fichier.

6. Cliquez sur **Planifier le correctif**.
7. Renseignez les champs de la boîte de dialogue.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner la cible	
Ressources	Choisissez-en un dans la liste pour continuer. `Le groupe d'ordinateurs` s'affiche par défaut. ◦ Groupe d'ordinateurs : sélectionnez cette option si vous souhaitez choisir une collection (un groupe de ressources) pour ce correctif. Les groupes sont constitués d'éléments de configuration importés à partir de l'application BigFix. ◦ Liste d'ordinateurs : sélectionnez cette option si vous souhaitez choisir des ordinateurs individuels (actifs) pour ce correctif. Vous pouvez voir les données sur le fabricant, l'emplacement, la classe, la date de la dernière mise à jour et le calendrier de maintenance dans la boîte de dialogue qui s'affiche. Cliquez sur **Suivant** pour continuer.
Groupe d'ordinateurs ou liste d'ordinateurs	En fonction de votre sélection d'actifs, l'un des champs s'affiche. Choisissez dans les listes.
Calendrier	
Nom du déploiement	Entrez un nom pour le déploiement de ce correctif. Ce nom vous aide à suivre vos mises à jour.
Type de déploiement	Choisissez une option dans la liste.
Heure de date limite	Définissez la valeur de l'heure limite. Cette valeur correspond à l'heure à laquelle le correctif est disponible pour la dernière fois pour le déploiement.
Temps disponible	Définissez la valeur du moment où le correctif devient disponible.
Temps disponible basé sur	Sélectionnez un fuseau horaire dans la liste sur lequel baser votre fenêtre de temps de déploiement.
Autoriser le redémarrage	Elle est désactivée par défaut. Activez (sélectionnez) cette option pour demander aux machines du groupe de redémarrer automatiquement une fois le correctif terminé.
Description	Ajoutez plus de texte pour le patch. Ces informations sont affichées dans le champ Description des enregistrements de mise à jour de correctifs.

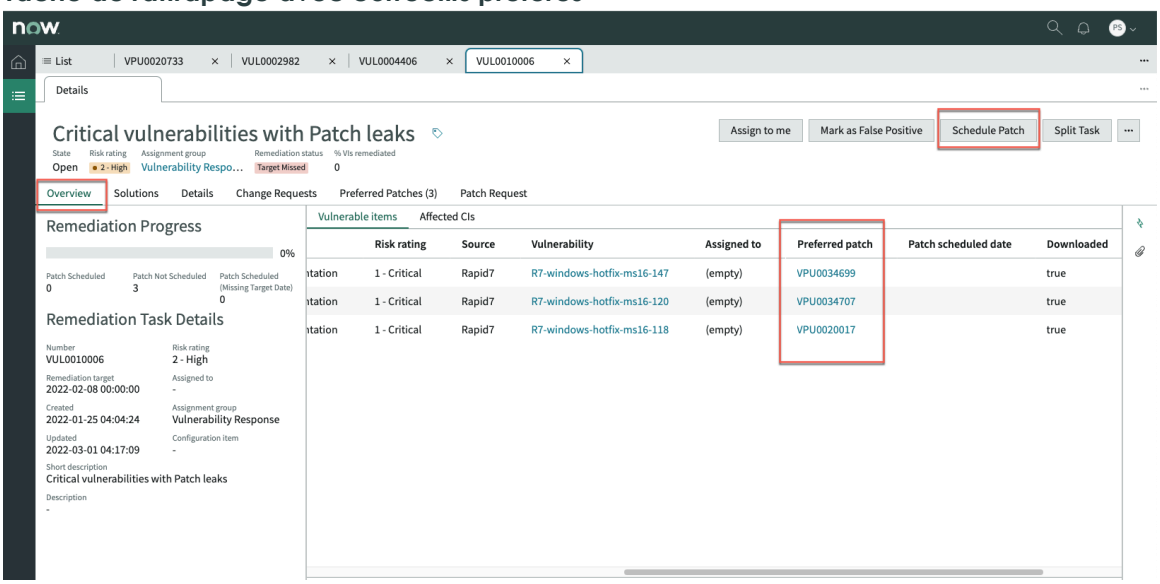
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Cliquez sur **Déployer**.
   La demande de correctif est envoyée à pour examen. Vous pouvez afficher l'état de toutes vos demandes soumises à partir de **Demandes d'exception** > **Mes demandes** dans la vue de liste.
9. Vous pouvez également planifier des correctifs à partir des tâches de rattrapage (RT) qui vous sont affectées ou qui sont affectées à votre groupe.

   Remarque : L'option permettant de planifier un correctif à partir d'un enregistrement de tâche de rattrapage n'est disponible que si des correctifs sont mappés sur les VI de la tâche (associés à ceux-ci). Ces correctifs sont affichés dans la colonne Correctif préféré si vous faites défiler vers la droite d'un enregistrement de tâche de rattrapage avec l'onglet Vue d'ensemble sélectionné.

Tâche de rattrapage avec correctifs préférés



10. Cliquez sur **Planifier le correctif** dans l'enregistrement RT et suivez les étapes énumérées ci-dessus pour le planifier dans la boîte de dialogue.
11. Vous pouvez planifier des correctifs pour les étapes répertoriées précédemment dans l'environnement classique.
    Pour localiser ces enregistrements, procédez comme suit.

    a. Dans l'environnement classique, accédez à **Réponse aux vulnérabilités** > **Correctifs** > **Tout**.

    b. Dans la liste qui s'affiche, recherchez un enregistrement de mise à jour de correctif.

    c. Pour les tâches de rattrapage, accédez à **Réponse aux vulnérabilités** > **Tâches de remédiation** et localisez un enregistrement.
    Suivez l'état du rattrapage dans l'onglet État du rattrapage. Au bas de l'enregistrement, les données de correctif sont affichées sur les liens connexes.

    d. Cliquez sur Planifier le correctif et renseignez les champs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom du déploiement	Entrez un nom pour le déploiement de ce correctif. Ce nom vous aide à suivre vos mises à jour.
Mise à jour de correctif	Choisissez-en un parmi les correctifs disponibles dans la liste.
Ressources	Sélectionner un élément : ▪ Groupe d'ordinateurs : sélectionnez cette option si vous souhaitez choisir une collection (un groupe de ressources) pour ce correctif. Les groupes sont constitués d'éléments de configuration importés à partir de l'application BigFix. ▪ Liste d'ordinateurs : sélectionnez cette option si vous souhaitez choisir des ordinateurs individuels (actifs) pour ce correctif. Vous pouvez voir les données sur le fabricant, l'emplacement, la classe, la date de la dernière mise à jour et le calendrier de maintenance dans la boîte de dialogue qui s'affiche.
Heure de début et heure de fin	Entrez les heures de début et de fin de la fenêtre horaire. Entrez le moment où vous souhaitez que le correctif commence son déploiement et le dernier jour où le correctif peut être installé.

Messages REST pour l'intégration de Vulnerability Response Patch Orchestration avec HCL BigFix

L'intégration Réponse aux vulnérabilités de l'orchestration des correctifs avec HCL BigFix Les messages REST sont utilisés pour effectuer des appels à l'API BigFix.

Connexion BigFix

Vous pouvez également utiliser les messages REST pour BigFix Login afin d'authentifier les demandes REST API. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes d'authentification adressées à BigFix.

Nom de paramètre	Valeur	Description
sourceType	cumulatif	Indique que l'intégration source extrait les données. Utilisé par code. Les changements ne sont pas recommandés.
sortDIR	Desc	Indique le sens de tri des données extraites de l'intégration. Les

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
		changements ne sont pas recommandés.
Champ de tri	severity	Indique le champ sur lequel le tri des données est basé. Les changements ne sont pas recommandés.
type	vulnérabilité	Indique le type de données à extraire de l'intégration pour l'intégration des actifs. Les changements ne sont pas recommandés.

Intégration BigFix

Vous pouvez utiliser le message REST de l'intégration BigFix pour récupérer des informations de BigFix. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes d'informations adressées à BigFix. Les messages REST contiennent les méthodes REST suivantes.

Méthodes REST

Méthode REST	Description
GET Extraire les données	Récupère les informations de BigFix concernant l'un des éléments suivants en fonction de la requête fournie : • Ordinateurs/groupes d'ordinateurs • Fixlets • Fixlets pertinents sur les ordinateurs • Actions

Nom de paramètre	Valeur	Description
URL	Valeurs dynamiques basées sur l'utilisateur	Indique le point de terminaison de la console BigFix

Correctif de déploiement BigFix

Vous pouvez utiliser le message REST de l'intégration BigFix pour planifier des correctifs de votre Now Platform® vers BigFix. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes d'informations adressées à BigFix. Les messages REST contiennent les méthodes REST suivantes.

Méthode REST	Description
POST Déployer le correctif	Programme le correctif sur la console BigFix sur un ou plusieurs ordinateurs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
URL	Valeurs dynamiques basées sur l'utilisateur	Indique le point de terminaison de la console BigFix.
Titre	Valeurs dynamiques basées sur l'utilisateur	Titre du déploiement.
settings_tag	Paramètres nommés par balise XML avec des valeurs	Indique les paramètres qui ont des paramètres différents et qui sont envoyés à BigFix lors de la planification du correctif.
computer_tag	Ordinateurs portant un nom de balise XML avec des valeurs	Indique la liste des ordinateurs sur lesquels le correctif va être planifié.
site_name	Valeur de la mise à jour du correctif	Nom du site où le fixlet est présent.
fixlet_id	Valeur de la mise à jour du correctif	ID du fixlet.

Transformation des données pour l'intégration d'orchestration de correctifs avec HCL BigFix

Les données sont récupérées à partir de l'orchestration Réponse aux vulnérabilités du correctif avec HCL BigFix Integration, traitées via un ensemble de sources de données et transformées dans votre Now Platform® instance.

Importation de collection BigFix

Les données des ressources importées (ordinateurs et groupes d'ordinateurs) sont chargées dans la table d'importation [sn_vul_bigfix_collection_import] de BigFix Collection. BigFix Computer and Computer Groups Import TM (carte de transformation ?) est utilisée pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données provenant de l'importation de la collection BigFix sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et localisez BigFix Computer et Computer Groups Import TM. La table suivante répertorie les champs de carte de transformation par intégration.

Importation d'ordinateurs BigFix et de groupes d'ordinateurs Synchronisation du script de carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application [sn_vul_bigfix] pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation d'ordinateurs BigFix et de groupes d'ordinateurs Synchronisation du script de carte de transformation (suite)

Script	Description
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour créer et mettre à jour les CI en fonction des règles et collectes de Recherche de CI, ainsi que de la relation entre elles. En fonction des résultats, ce script modifie les valeurs de la variable de champ d'application [sn_vul_bigfix]. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre de CI créés, mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Importation de fixlet BigFix

Les données des fixlets importés sont chargées dans la table d'importation de fixlets BigFix [sn_vul_bigfix_patch_update_import].

BigFix Fixlet Import TM est utilisé pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données provenant de l'importation BigFix Fixlet sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et localisez le BigFix Fixlet Import TM.

La table suivante répertorie les champs de carte de transformation par intégration.

Champs de carte de transformation d'importation de fixlet BigFix

Champ source	Champ cible	Description
u_id	article_id	ID unique d'un fixlet dans un site.
u_id	source_id	ID unique d'un fixlet dans un site.
U_site_name	Sn_vul_bigfix_site_name	Nom du site dans BigFix sur lequel le fixlet s'appuie.
U_display_name	Titre	Titre du fixlet.
[Script]	Bulletin_id	ID source de la solution.
[Script]	Sn_vul_solution	Solution basée sur l'ID source.
U_source	bulletin_source	Fournisseur source de la solution.
[Script]	Date_release	Date de libération du fixlet.
U_category	Update_category	Catégorie du fixlet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation d'importation de fixlet BigFix (suite)

Champ source	Champ cible	Description
[Script]	Is_highest_supersedence	Booléen indiquant si le fixlet est la priorité la plus élevée ou non.
[Script]	Is_downloaded	Booléen indiquant si le fixlet est téléchargé ou non.
[Script]	Integration_instance	Nom de l'instance à partir de laquelle le fixlet est importé.
U_source_severity	Source_severity	Gravité du fixlet.
U_applicable_count	Num_total	Nombre total d'appareils avec des fixlets manquants.
[Script]	Last_modified	Date de la dernière modification du fixlet.

Importation de fixlet BigFix : minutage du script de carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application [sn_vul_bigfix] pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour mettre à jour les valeurs de la variable de champ d'application [sn_vul_bigfix]. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre de fixlets créés, mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Importation de fixlet d'appareil BigFix

Les données des fixlets pertinents importés sur les ordinateurs sont chargées dans la table d'importation de fixlets de périphériques BigFix [sn_vul_bigfix_device_patch_import].

BigFix Device Fixlet TM est utilisé pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation du fixlet BigFix Device sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et localisez le BigFix Device Fixlet TM.

La table suivante répertorie les champs de carte de transformation par intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appareil BigFix Fixlet Synchronisation du script de carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application [sn_vul_bigfix] pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour créer et mettre à jour les CI en fonction des règles de recherche de CI et des collectes, ainsi que de la relation entre elles. En fonction des résultats, ce script modifie les valeurs de la variable de champ d'application [sn_vul_bigfix]. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre de CI créés, mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Importation d'actions BigFix

Les données des actions importées sont chargées dans la table BigFix Actions Import [sn_vul_bigfix_deployment_import].

BigFix Actions Import TM est utilisé pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données issues de l'importation BigFix Actions sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et localisez le BigFix Fixlet Import TM.

La table suivante répertorie les champs de carte de transformation par intégration.

Actions BigFix Importer les champs de carte de transformation

Champ source	Champ cible	Description
u_id	source_id	ID unique d'une action.
U_name	name	Nom de l'action
[Script]	Sn_vul_bigfix_discovered_item	Référence de l'élément détecté sur lequel le correctif est déployé
U_status	statut	Statut de l'action
[Script]	Sn_vul_patch_orch_update	Référence du correctif
U_apply_count	Count_success	Nombre de réussites de l'action.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions BigFix Importer les champs de carte de transformation (suite)

Champ source	Champ cible	Description
U_retry_count	retry	Nombre de nouvelles tentatives de l'action.
[Script]	Deployment_time	Heure de début de l'action.
[Script]	date limite	Heure de fin de l'action.
[Script]	Source_created	Heure de création de l'action.
[Script]	Integration_instance	Nom de l'instance à partir de laquelle l'action est importée.

Actions BigFix Importer le minutage du script de carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application [sn_vul_bigfix] pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour mettre à jour les valeurs de la variable de champ d'application [sn_vul_bigfix]. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'actions créées, mises à jour et ignorées. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Exemple de workflow pour l'intégration de Vulnerability Response patch orchestration avec HCL BigFix

Un exemple du fonctionnement de l'orchestration des correctifs avec le produit HCL BigFix.

Avant de commencer

Supposons, par exemple, que l'ensemble de votre environnement soit corrigé une fois toutes les trois semaines. La fenêtre d'application de correctif la plus récente a été terminée il y a une semaine, mais vous souhaitez appliquer un correctif pour corriger une vulnérabilité critique récemment connue. En raison de la nature critique de cette vulnérabilité, vous ne pouvez pas attendre deux semaines de plus pour le prochain correctif planifié.

Rôles requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour Vulnerability Manager Workspace.
- sn_vul.remediation_owner pour afficher l'espace de travail du propriétaire de rattrapage informatique.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs.
- sn_vul_patch_orch.read_patch pour afficher (en lecture seule) les informations de correctif sur les enregistrements. Ce rôle est hérité des rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail IT Remediation et Vulnerability Manager.

Pourquoi et quand exécuter cette tâche

En tant que gestionnaire de vulnérabilités ou analyste travaillant dans l'espace de travail du gestionnaire de vulnérabilités, vous pouvez envisager de créer des rubriques de surveillance ou de modifier des rubriques de surveillance existantes pour vous aider à capturer les éléments vulnérables importés présentant des vulnérabilités critiques. Avec l'intégration d'orchestration de correctifs, vous pouvez également voir les correctifs que vous souhaitez utiliser pour corriger et suivre ces vulnérabilités. Le tableau suivant répertorie quelques exemples avec les conditions que vous pouvez définir pour les rubriques de surveillance pour l'orchestration des correctifs. Utilisez ces exemples pour vous aider à déterminer les paramètres les mieux adaptés à votre environnement. Consultez Créer une rubrique de surveillance dans Vulnerability Manager Workspace pour plus d'informations sur la configuration de la rubrique de visualisation.

Exemple de rubriques de surveillance pour l'orchestration des correctifs dans Vulnerability Manager Workspace

Nom de la rubrique de surveillance	Description
Vulnérabilités critiques avec fuites de correctifs	`La cote de risque est de 1 - critique` ET `La raison pour laquelle le correctif n'est pas planifié`
Vulnérabilités critiques avec correctifs planifiés (SLA manquant)	`Le motif est Correctif planifié (date cible manquante)`
Vulnérabilités critiques avec correctifs planifiés	`La cote de risque est de 1 - critique` ET `La date planifiée du correctif n'est pas vide` ET `Le motif est le correctif planifié`

- En tant que gestionnaire ou analyste de vulnérabilités, après avoir créé les rubriques de surveillance et les efforts de rattrapage, vous générez des tâches de rattrapage. À partir des enregistrements de VI et des tâches de remédiation, vous pouvez explorer l'onglet Détections et localiser les enregistrements d'éléments détectés qui présentent la vulnérabilité que vous suivez, ainsi que les actifs importés par le produit BigFix.
- En tant qu'analyste de vulnérabilité ou administrateur, vous pouvez surveiller les données de correctifs associées à la vulnérabilité. Vous pouvez également déployer un ou plusieurs correctifs sur un actif spécifique (élément de configuration) à partir d'un enregistrement d'élément détecté.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En tant que spécialiste de la remédiation informatique, vous disposez d'options pour traiter la vulnérabilité avec le déploiement d'un correctif.

- Vous pouvez planifier le correctif à partir d'un enregistrement de mise à jour de correctif (VPU#).
- Si des solutions préférées sont mappées aux éléments vulnérables (VI) et qu'elles vous sont affectées, à vous ou à vos groupes, vous pouvez planifier les correctifs à partir d'une tâche de rattrapage qui comporte ces éléments vulnérables.

Procédure

1. En tant que spécialiste du rattrapage informatique, dans l'espace de travail de rattrapage informatique, cliquez sur la vue d'accueil.
2. Dans la vue d'accueil, cliquez sur le tableau de résultats des **tâches de rattrapage affectées** pour afficher les enregistrements.

   Pour les besoins de cet exemple, vous pouvez vérifier le champ Brève description sur la tâche de rattrapage (VUL#) pour tout texte qui se rapporte à votre vulnérabilité critique. Supposons, par exemple, que vous sachiez peut-être que votre gestionnaire de vulnérabilités a créé une rubrique de surveillance intitulée Vulnérabilités critiques avec fuites de correctifs pour intercepter les VI (VIT#) avec cette vulnérabilité critique.

   Une fois l'enregistrement ouvert, vous pouvez également passer en revue les VI, les correctifs préférés et voir si vous ou l'un des membres de votre groupe avez déjà soumis des demandes de correctif pour approbation.

3. Si vous disposez de suffisamment d'informations, vous pouvez soumettre une demande de correctif maintenant à partir de cette tâche de rattrapage.

   Remarque : Si les VI associés à l'enregistrement n'ont pas de correctifs mappés sur eux, le bouton **Planifier le correctif** n'est pas disponible sur l'enregistrement.

4. Cliquez sur **Planifier le correctif** et renseignez les champs de la boîte de dialogue.
   Pour en savoir plus sur la planification d'un correctif, reportez-vous à la section Planifier les correctifs avec l'intégration Patch Réponse aux vulnérabilités Orchestration HCL BigFix.
5. À partir de la vue Liste de l'espace de travail de remédiation informatique, vous pouvez également cliquer sur les liens Tâches de remédiation, Éléments vulnérables, Solutions et Correctifs pour afficher ces enregistrements.

   Dans le cas de cet exemple, au lieu d'un nom de rubrique de surveillance, vous connaissez peut-être l'ID d'article ou l'ID de bulletin et le titre du correctif. Si tel est le cas, vous voudrez peut-être vérifier si l'un des VI présentant cette vulnérabilité vous est affecté ou est affecté à vos groupes. Dans les enregistrements de mise à jour de correctifs, vous pouvez soumettre des demandes de correctifs. Dans les enregistrements de VI, vous pouvez rechercher des correctifs potentiels et ouvrir la tâche de rattrapage associée si vous souhaitez soumettre une demande de correctif.

6. Si vous n'avez pas accès aux espaces de travail, ou si vous préférez afficher les données et planifier les correctifs à partir de l'environnement classique, procédez comme suit.

   a. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Correctifs** > **Tout**.

   b. Localisez l'enregistrement de mise à jour de correctif souhaité.
      Vous préférez peut-être filtrer les enregistrements avec des scores de risque `critique` .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Passez en revue les champs des VI et du % de rattrapages des VI associés sous l'onglet État du rattrapage.
Si des correctifs sont disponibles pour les VI, le bouton **Planifier le correctif** s'affiche dans le coin supérieur droit de l'enregistrement.

d. Si vous décidez de soumettre une demande, cliquez sur **Planifier le correctif**.
Pour en savoir plus sur la planification d'un correctif, reportez-vous à la section Planifier les correctifs avec l'intégration Patch Réponse aux vulnérabilités Orchestration HCL BigFix.

e. Sinon, disons que vous n'avez pas les informations sur l'ID du correctif, mais que vous pouvez vérifier le champ Brève description sur les tâches de rattrapage qui sont affectées à votre groupe pour tout texte qui se rapporte à votre vulnérabilité critique.

f. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**.

g. Localisez l'enregistrement souhaité et cliquez dessus pour l'ouvrir.
Dans l'enregistrement ouvert, passez en revue l'onglet État du rattrapage pour les VI et le % des VI rattrapés. Cliquez sur les liens connexes pour les enregistrements de VI, les solutions préférées, les correctifs préférés et les demandes de correctifs.

> **Remarque :** Si les VI associés à l'enregistrement n'ont pas de correctifs mappés sur eux, le bouton **Planifier le correctif** n'est pas disponible sur l'enregistrement.

h. Cliquez sur **Planifier un correctif** dans l'enregistrement si vous souhaitez soumettre une demande de correctif.

Présentation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités

Gérez les correctifs et les déploiements de correctifs pour les vulnérabilités critiques sur vos actifs grâce à l'intégration Réponse aux vulnérabilitésMicrosoft au produit System Center Configuration Manager (SCCM).

Orchestration des correctifs avec Réponse aux vulnérabilités

L'orchestration des correctifs utilise Réponse aux vulnérabilités des importations planifiées à partir d'intégrations de solutions tierces, de fournisseurs de correctifs et d'analyseurs de vulnérabilité. Les données de détection des scanners associent les actifs de votre environnement aux vulnérabilités et aux mises à jour de correctifs susceptibles de les corriger. Vous soumettez des demandes de correctifs pour approbation, planifiez des mises à jour de correctifs pour résoudre les éléments vulnérables et surveillez la progression du rattrapage à partir de votre Now Platform® instance.

Réponse aux vulnérabilités l'orchestration de correctifs avec Microsoft SCCM

Lorsque Vulnerability Response Patch Orchestration with the SCCM Microsoft application est utilisé avec le , Patch ServiceNow® Gestion des solutions pour vulnérabilitésOrchestration et Réponse aux vulnérabilités les applications, les gestionnaires et analystes de vulnérabilités peuvent effectuer les tâches suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour plus d'informations sur les types de correctifs et les solutions des fournisseurs (correctifs), consultez le contexte et les informations sur les types de correctifs et les solutions des fournisseurs (correctifs).
- Affichez et surveillez les données de vulnérabilité et de solution, ainsi que la progression du rattrapage des vulnérabilités à partir des enregistrements dans les Réponse aux vulnérabilités espaces de travail.

Les spécialistes informatiques et les responsables du rattrapage peuvent effectuer les tâches suivantes :

- Déployez des correctifs pris en charge par le Microsoft produit SCCM pour leurs Windows, CentOS, MacOS, Oracleet d'autres actifs à intervalles réguliers et planifiés en dehors des heures de travail afin d'éviter les conflits avec le travail.
- Identifiez les actifs non corrigés présentant des vulnérabilités ou ceux qui n'ont pas été mis à jour correctement par les correctifs planifiés à partir de données de détection importées d'analyseurs tiers.
- Planifiez les correctifs disponibles à partir de l'espace de travail de remédiation informatique ou de l'interface utilisateur classique pour les actifs vulnérables non corrigés à partir de la mise à jour de correctif, de la tâche de rattrapage et des enregistrements d'éléments détectés.

Termes clés dans les Réponse aux vulnérabilitésMicrosoft applications et SCCM

Élément de configuration (CI)

Les CI sont les actifs existants répertoriés dans votre Base de données de gestion des configurations (CMDB)fichier . Microsoft SCCM appelle des CI, des périphériques.

Collections et collections d'appareils

Terminologie utilisée dans le Microsoft produit SCCM qui fait référence à un groupe de ressources.

Élément vulnérable

Une vulnérabilité importée qui correspond à un actif existant dans votre CMDB.

Instance

Un compte rendu distinct de l'application Microsoft SCCM. Chaque compte d'utilisateur peut être une instance de l'application Microsoft SCCM. Ce terme désigne également une adresse Web unique et sécurisée pour une Now Platform instance.

Intégration

Une intégration est une tâche planifiée dans le Now Platform qui récupère des informations à partir d'une source tierce, telle que l'intégration avec les Microsoft machines SCCM.

Solution

Il existe deux types de solutions dans le cadre de cette intégration, potentielles et préférées. Une solution potentielle est une solution qui pourrait remédier à une vulnérabilité. Les vulnérabilités ont souvent de nombreuses solutions potentielles. #Une solution privilégiée correspond à la solution la plus efficace pour une vulnérabilité spécifique détectée.

Correctifs

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mises à jour logicielles qui corrigent les vulnérabilités. Dans l'application Microsoft SCCM, les correctifs sont appelés patchs. Par exemple, Microsoft SCCM propose des correctifs pour Windows, CentOS, Oracle MAC et d'autres produits.

Correctif préféré

Les correctifs préférés sont les mises à jour logicielles destinées à corriger des vulnérabilités spécifiques. Les correctifs, une fois déployés, sont mappés aux éléments vulnérables liés à des vulnérabilités spécifiques et corrigent-les.

Tâche de rattrapage ou, avant la version 15.0 de , groupes de Réponse aux vulnérabilitésvulnérabilité

Listes des éléments vulnérables dans l'application Réponse aux vulnérabilités des actions requises pour corriger les vulnérabilités.

Déploiement

Aux fins de cette intégration, le déploiement désigne le moment où vous appliquez, lancez ou planifiez un correctif sur un ordinateur. Vous pouvez déployer les correctifs que vous avez téléchargés à partir de Microsoft SCCM dans votre Now Platform en accédant aux éléments détectés, aux correctifs ou aux tâches de remédiation à partir d'enregistrements individuels dans Réponse aux vulnérabilités. Vous pouvez déployer des correctifs avec des travaux planifiés sur des machines individuelles ou sur des groupes d'ordinateurs.

Le déploiement dans le Now Platform peut également faire référence à une intégration qui prend en charge plusieurs sources. Une existence d'intégration unique est appelée un déploiement de votre intégration. Un déploiement fait référence aux intégrations et aux produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de l'intégration de vulnérabilité Microsoft SCCM dans votre environnement.

Gestion des solutions pour vulnérabilités et l'intégration de l'orchestration Réponse aux vulnérabilités de correctifs avec Microsoft SCCM

L'application Gestion des solutions pour vulnérabilités est une Now Platform application qui met en corrélation vos résultats de vulnérabilité avec la répartition des solutions (correctifs) qui les corrigent. Identifiez les correctifs logiciels de tiers pour les produits et services, les mises à jour de configuration et les autres contrôles ayant le plus d'impact pour votre organisation. Outre les informations des scanners tiers, les applications Orchestration Réponse aux vulnérabilitésde correctif Gestion des solutions pour Réponse aux vulnérabilitésde réponse aux vulnérabilités avec Microsoft SCCM fonctionnent ensemble pour déployer les correctifs préférés de la solution à la vulnérabilité et à l'élément vulnérable pour vous aider à corriger et à fermer les vulnérabilités de votre environnement. Les Gestion des solutions pour Réponse aux vulnérabilitésapplications d'intégration SCCM , Réponse aux vulnérabilités, et Patch Réponse aux vulnérabilités Orchestration Microsoft sont toutes disponibles dans le ServiceNow® Store.

Rôles Now Platform requis

Les tâches d'intégration, d'installation, de configuration et de rattrapage nécessitent les rôles suivants dans votre Now Platform instance.

administrateur

Les utilisateurs dotés de ce rôle obtiennent des autorisations pour les applications dans le ServiceNow Store et les télécharge dans Now Platform les instances.

sn_vul.vulnerability_admin

Les utilisateurs ayant ce rôle activent les applications dans l'instance Now Platform et terminent la configuration de l'application Réponse aux

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérabilités . Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Cet utilisateur administrateur configure toutes les applications, règles et intégrations tierces VR.

sn_vul_sccm.configure_integration

Les utilisateurs ayant ce rôle configurent l'application Intégration d'orchestration de correctifs Microsoft SCCM. Ce rôle contient le rôle granulaire sn_vul_sccm.read_integration.

sn_vul_sccm.read_integration

Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les enregistrements de l'application Réponse aux vulnérabilités SCCM Patch Orchestration Integration et les Microsoft données d'orchestration des correctifs.

sn_vul_patch_orch.configure_patch

Les utilisateurs disposant de ce rôle peuvent configurer et appliquer des correctifs.

sn_vul_patch_orch.read_patch

Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les informations sur les correctifs.

Approbateurs

Affectez des utilisations aux groupes d'approbateurs de niveau 1 et d'approbateurs de niveau 2 si vous souhaitez que les demandes de correctifs soumises soient approuvées avant le déploiement.

Pour en savoir plus sur l'affectation de ces rôles à l'aide de l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.

Règles de recherche de CI

Lorsque des données sont importées de l'application Microsoft SCCM, l'application Réponse aux vulnérabilités recherche automatiquement des correspondances dans les données d'ID Base de données de gestion des configurations (CMDB) de ressource. Les règles de recherche de CI sont utilisées pour identifier les CI (actifs) et les ajouter automatiquement aux enregistrements d'éléments vulnérables (VI) lorsque des VI sont créés. Les règles de recherche de CI suivantes sont fournies avec le système de base et sont utilisées pour identifier les CI (actifs) et les ajouter aux éléments détectés.

Cette règle de recherche s'appuie sur les données apportées par Service Graph Connector avec SCCM. Vous devez installer et exécuter l'intégration CMDB avant d'exécuter les intégrations SCCM. Si vous avez plusieurs installations du serveur SCCM, vous pouvez configurer l'alias de connexion Service Graph Connector dans la page de configuration de l'orchestration des correctifs SCCM.

Serveur MID

Vulnerability Response Patch Orchestration with Microsoft SCCM est une intégration locale. Il nécessite un serveur MID autonome Windows qui ne fait pas partie d'une grappe de serveurs MID. Le MID Server doit exécuter des scripts sur des machines distantes à partir de votre instance afin d'importer des données à partir du serveur SCCM. Les API pour cette intégration sont appelées à l'aide des MID Servers que vous configurez dans votre Now Platform instance. Préparation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations et dépendances du correctif Vulnerability Response Orchestration avec l'application Microsoft SCCM

Les applications de produits et de dépendances suivantes sont requises pour l'intégration de Vulnerability Response Patch Orchestration avec Microsoft System Center Configuration Manager (SCCM). Ces applications sont disponibles dans le ServiceNow® Store

Versions disponibles des applications et dépendances requises pour l'intégration d'orchestration de correctifs

Pour afficher les données d'orchestration des correctifs et les mises à jour disponibles (correctifs) dans les espaces de travail et l'interface utilisateur classique dans Réponse aux vulnérabilités, les applications suivantes sont requises. Toutes les applications répertoriées sont disponibles dans le ServiceNow® Storefichier . Certaines applications nécessitent des abonnements distincts.

Pour plus d'informations sur la compatibilité des versions avec les applications requises et les versions de famille, consultez l'article Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production dans la base de connaissances HI.

Application et version de mise en production
Réponse aux vulnérabilités
Gestion des solutions pour vulnérabilités
Application Orchestration de correctif pour Vulnerability Response
Orchestration des correctifs Vulnerability Response avec l'application Microsoft SCCM
Security Support Common
Orchestration de support de sécurité
Connecteur du graphe de services avec SCCM

Réponse aux vulnérabilités Tables de l'application Orchestration de correctifs

L'application Réponse aux vulnérabilités Patch Orchestration contient les tables suivantes :

Table	Description
Mise à jour de correctif [sn_vul_patch_orch_update]	Stocke des informations sur les correctifs disponibles sur des instances distinctes.
Mise à jour de l'appareil [sn_vul_patch_orch_m2m_src_ci_update]	Stocke les données relatives aux correctifs déployés, ainsi que l'état de déploiement, qui sont affichés sur les enregistrements d'éléments détectés.
Collecte [sn_vul_patch_orch_collection]	Stocke les données de collection provenant d'instances distinctes.
Collection d'appareils [sn_vul_patch_orch_m2m_src_ci_collection]	Stocke les données de collection sur les éléments détectés.
Déploiement de correctif [sn_vul_patch_orch_deployment]	Stocke des informations sur les correctifs déployés, sur les collections et les CI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Correctif potentiel [sn_vul_patch_orch_m2m_vuln_patch]	Stocke des données sur les correctifs et les vulnérabilités qui identifient les correctifs qui peuvent être utilisés pour résoudre une vulnérabilité.

Orchestration des correctifs de réponse aux vulnérabilités avec Microsoft intégrations SCCM

Les intégrations développées par ServiceNow® l'ingénierie constituent le déploiement orchestré de la solution avec le Microsoft produit SCCM. Les intégrations suivantes sont incluses dans l'application Microsoft SCCM Patch Orchestration Integration que vous téléchargez à partir du ServiceNow® Store.

Après avoir installé l'application d'intégration sur votre Now Platform instance, pour afficher ces intégrations, accédez à **Intégrations** > **Intégration d'orchestration de correctifs SCCM** > **Intégrations**. L'application Réponse aux vulnérabilités traite les données sur des intervalles de temps planifiés importés par ces intégrations avec Microsoft des points de terminaison SCCM.

Intégration	Description
Microsoft Intégration de collection SCCM	• Cette intégration est planifiée pour s'exécuter quotidiennement et s'exécute en premier dans l'exécution d'intégration chaînée. • Récupère les ensembles d'appareils à partir des ensembles SCCM.
Microsoft Intégration de la collection d'appareils SCCM	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de collection SCCM. Vous pouvez également l'exécuter à la demande. • Cette intégration récupère les appareils sous chaque collection. Cette intégration crée des enregistrements dans la table des éléments détectés et dans la table Collection d'appareils.
Microsoft Intégration de la mise à jour du correctif SCCM	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de la collection d'appareils SCCM. Vous pouvez également l'exécuter à la demande. • Récupère des informations à partir du serveur SCCM sur les correctifs qui sont installés ou manquants sur les appareils (actifs).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
Microsoft Intégration des déploiements SCCM	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de mise à jour des correctifs. Vous pouvez également l'exécuter à la demande. • Récupère des informations sur les correctifs planifiés par l'équipe informatique sur le serveur SCCM.

Préparation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités

Préparez l'intégration en effectuant les tâches de configuration suivantes.

Avant de commencer

Rôles requis : administrateur pour l'installation des applications et l'affectation des rôles. D'autres rôles sont répertoriés dans la table suivante.

Pourquoi et quand exécuter cette tâche

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration.

Procédure

1. Pour une installation et une configuration fluides de l'application Orchestration des correctifs de réponse aux vulnérabilités avec Microsoft SCCM, suivez la liste de vérification fournie ci-dessous.
2. Vous pouvez imprimer la liste de vérification suivante et vérifier que les éléments répertoriés sont complétés avant d'installer l'application et d'importer les informations relatives à la vulnérabilité et aux correctifs dans votre Now Platform® instance.

Tâche	Description
☐	(Facultatif) Si elle n'est pas déjà installée et activée, il peut être préférable d'installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour en savoir plus sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 16.1 ou Réponse aux vulnérabilités ultérieure.
☐	Si ce n'est pas déjà fait, obtenez les autorisations et installez une application de scanner tierce pour importer les données de vulnérabilité. Pour Intégrations de Réponse aux vulnérabilités plus d'informations sur les scanners tiers pris en charge par Réponse aux vulnérabilités. Consultez .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
☐	Si ce n'est pas déjà fait, obtenez les autorisations et téléchargez l'application Vulnerability Response Patch Orchestration with Microsoft SCCM sur votre Now Platform® instance. Consultez .
☐	Obtenir les informations d'identification Microsoft SCCM. Vérifiez que vous disposez de tous les noms de compte, mots de passe et autres informations de service requis par vos Microsoft produits afin d'y avoir accès.
☐	Vérifiez que vous disposez de groupes ou d'utilisateurs pour gérer les intégrations et corriger les éléments vulnérables. administrateur L'administrateur système obtient des autorisations, télécharge et installe l'application Microsoft SCCM Patch Orchestration et les autres applications requises pour l'intégration. En l'absence d'affectation, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'assistant de configuration dans Réponse aux vulnérabilités ou à partir du module Administration utilisateurs. sn_vul.vulnerability_admin Une fois affecté, l'administrateur de vulnérabilité termine la configuration des intégrations SCCM et des Microsoft autres applications tierces. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Ce rôle configure toutes les applications VR, les règles, les intégrations tierces, Réponse aux vulnérabilités l'orchestration des correctifs et les applications de gestion des solutions en matière de vulnérabilité. sn_vul_sccm.configure_integration Les utilisateurs ayant ce rôle configurent l'application Intégration d'orchestration de correctifs Microsoft SCCM. Ce rôle contient les rôles granulaires sn_vul_sccm.read_integration et connection_admin qui permettent à l'utilisateur de se connecter à la console

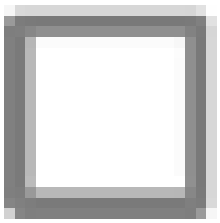
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	SCCM et de configurer les instances d'intégration dans votre Now Platform. sn_vul_sccm.read_integration Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les enregistrements de l'application Réponse aux vulnérabilités SCCM Patch Orchestration Integration et les Microsoft données d'orchestration des correctifs. sn_vul_patch_orch.configure_patch Les utilisateurs disposant de ce rôle peuvent configurer et appliquer des correctifs. Les correctifs demandés par cet utilisateur à partir des enregistrements d'élément vulnérable et de mise à jour de correctif sont envoyés pour approbation si la gestion des changements est active et que des approbateurs sont affectés. sn_vul_patch_orch.read_patch Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les informations de correctifs sur les enregistrements. Ce rôle est hérité des rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail IT Remediation et Vulnerability Manager. Approbateurs Les utilisateurs affectés aux groupes d'approbateurs de niveau 1 et, éventuellement, d'approbateurs de niveau 2 approuvent les demandes de correctifs soumises. Par défaut, les correctifs sont soumis au groupe d'approbateurs de niveau 1 pour approbation avant le déploiement. Pour en savoir plus sur le processus d'approbation, reportez-vous Configurer l'orchestration des correctifs de réponse aux vulnérabilités avec Microsoft l'intégration SCCMà . Pour en savoir plus sur la configuration des approbateurs et des groupes, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. L'administrateur système effectue l'affectation initiale des rôles aux utilisateurs et aux groupes pour l'intégration. Par défaut, le Réponse aux vulnérabilités groupe est disponible. Si ce n'est pas déjà fait, vous pouvez créer des groupes supplémentaires pour les rôles de spécialiste du rattrapage et d'analyste de vulnérabilité et ajouter des utilisateurs avec le module Administration des utilisateurs

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	dans votre instance. Reportez-vous à la section Créer un groupe d'utilisateurs .
	Vérifiez que vous avez activé toutes les fonctionnalités, règles, modules d'extension de dépendance ou tâches dans votre instance requises pour l'intégration. ◦ Vulnerability Response Patch Orchestration with Microsoft SCCM est une intégration locale qui nécessite l'utilisation d'un Windows serveur MID autonome. Pour plus d'informations sur les MID Servers dans votre instance, consultez Serveur MID . ◦ Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tout** et localisez le module d'extension. S'il n'est pas installé dans votre instance, installez-le et activez-le.

Installer l'application Réponse aux vulnérabilités Patch Orchestration with Microsoft SCCM

Téléchargez l'application à partir du ServiceNow Storefichier .

Avant de commencer

Avant d'installer l'application, vérifiez que vous avez rempli tous les éléments de la liste de vérification dans Préparation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités.

Rôles requis : admin pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application. Vulnerability admin (sn_vul.vulnerability_admin ou sn_vul.admin (obsolète) pour configurer Patch Réponse aux vulnérabilités Orchestration Microsoft SCCM et d'autres applications après leur installation.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de sous-production ou de développement, il n'est pas nécessaire d'obtenir l'autorisation, passez à .

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Localisez l'application **Vulnerability Response Patch Orchestration with Microsoft SCCM** et cliquez sur **Installer**.

   Cette action installe l'application que vous avez téléchargée à ServiceNow Storepartir du .
3. Vous pouvez également installer des applications à partir de l'Assistant de configuration. Pour en savoir plus sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.

Que faire ensuite

Une fois l'installation terminée, accédez à **Tout** > **Intégration d'orchestration de correctifs SCCM Microsoft** > **Configuration** pour poursuivre la configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'orchestration des correctifs de réponse aux vulnérabilités avec Microsoft l'intégration SCCM

Une fois l'application installée, configurez-la avec les informations de votre compte et validez vos informations d'identification.

Avant de commencer

Rôles requis : sn_vul.vulnerability_admin et sn_vul_sccm.configure_integration

Procédure

1. Accédez à la **Tout** > **Intégration d'orchestration de correctifs SCCM Microsoft** > **Configuration**.
2. Remplissez les champs avec vos informations SCCM et vos Microsoft informations d'identification.

Champ	Description
Instance d'intégration	Le nom du compte d'instance Microsoft SCCM que vous souhaitez utiliser, par exemple, `Microsoft SCCM Patch Management Integration`.
Nom d'hôte	Entrez l'URL de l'hôte Microsoft SCCM.
Nom d'utilisateur	Saisissez le nom d'utilisateur de votre Microsoft compte SCCM.
Mot de passe	Saisissez le mot de passe de votre Microsoft compte SCCM.
Serveur MID	Dans la liste, entrez le nom du serveur MID autonome que vous souhaitez utiliser. Pour Préparation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités plus d'informations sur les serveurs MID et sur la configuration des tâches dans votre Now Platform®.

3. Cliquez sur Enregistrer et tester les informations d'identification.
   L'état de votre connexion entre Microsoft SCCM et votre Now Platform® instance est affiché dans le champ État de validation. Si le test ne réussit pas, suivez les instructions.
4. Facultatif : Séparation de domaine est pris en charge pour cette intégration.
   Vous pouvez ajouter plusieurs configurations à votre instance. Pour ajouter des configurations supplémentaires :

   a. Accédez à la **Tout** > **Intégration d'orchestration de correctifs SCCM Microsoft Instances d'intégration**

   b. Vérifiez que le périmètre de l'application, `Orchestration des correctifs Vulnerability Response avec Microsoft SCCM`, est affiché dans le champ Périmètre de l'application.

   c. Cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Remplissez le formulaire.

Champ	Description
Nom	Nom de l'instance d'intégration.
Application	Orchestration des correctifs Vulnerability Response avec Microsoft SCCM
Intégration	[Lecture seule] Microsoft La gestion des correctifs SCCM est l'option par défaut.
Actif	La valeur par défaut est activée. Si elle est décochée, l'instance n'est pas active.

e. Cliquez sur **Envoyer**.
Votre nouvelle instance d'intégration apparaît dans la liste des instances d'intégration.

f. Répétez les étapes 1 à 3 pour configurer votre instance d'intégration et tester vos informations d'identification.

5. Configurez les approbations pour les demandes de correctifs.
Par défaut, une propriété système [**sn_vul_patch_orch.patch_approval_required**] est activée de sorte que, lorsque des déploiements de correctifs sont planifiés, ils sont soumis pour examen et approbation aux utilisateurs affectés au groupe d'approbation de niveau 1 - Mise à jour des correctifs.

Si vous souhaitez que les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch planifient des correctifs sans approbation, vous pouvez désactiver la propriété [**sn_vul_patch_orch.patch_approval_required**]. Vous préférez peut-être laisser les approbations activées afin que les correctifs planifiés n'entrent pas en conflit avec les heures de travail normales.

Remarque : Si vous désactivez la propriété système d'approbation, tout utilisateur disposant du rôle sn_vul_patch_orch.configure_patch peut planifier et déployer des correctifs sans examen ni approbation.

En tant qu'utilisateur ayant le rôle sn_vul.vulnerability_admin, pour désactiver la propriété système :

a. Accédez à la **Tout** > **sys.properties.list**.

b. Localisez **sn_vul_patch_orch.patch_approval_required** et cliquez dessus pour ouvrir l'enregistrement.

c. Dans le champ Valeur, tapez `false`.

d. Cliquez sur **Mettre à jour**.

6. Si vous ne désactivez pas cette propriété, vous devez affecter des approbateurs pour les demandes de correctifs.
En tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin, procédez comme suit.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.

b. Si la règle d'approbation Approbation de la **mise à jour du correctif de déploiement** n'est pas affichée dans la liste, cliquez sur **Tout** à droite de l'icône de filtre vert en haut à gauche de l'écran pour afficher la liste complète.

c. Dans la liste, cliquez sur Approbation de la **mise à jour du correctif de déploiement**.

d. Dans l'enregistrement, avec l'onglet Configuration de l'approbation sélectionné, cliquez sur **Approbation de mise à jour du correctif de configuration par défaut**.

e. Pour l'enregistrement, cliquez sur **Niveau 1 - Approbation de mise à jour du correctif**.

f. Ajoutez des utilisateurs à ce groupe.

Les utilisateurs affectés à ce groupe approuvent les demandes de correctifs soumises par les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch. Accédez à **Mes approbations** pour afficher et traiter les demandes.

7. Cliquez sur**Mettre à jour** pour enregistrer vos modifications.

8. Facultatif : Vous pouvez configurer des approbations multiniveaux de sorte que plusieurs approbations soient requises avant le déploiement des demandes de correctifs planifiées.

a. Une fois l'enregistrement d'approbation de mise à jour du correctif de configuration par défaut affiché, cliquez sur **Nouveau**.

b. Renseignez les champs.

Champ	Description
Nom	Nom du niveau d'approbation, par exemple, **Niveau 2 - Approbation de mise à jour du correctif**.
Actif	Activé par défaut, ce qui signifie que le niveau d'approbation est utilisé.
Approbation requise	Sélectionnez le nombre d'approbations requises pour le niveau sélectionné : ▪ Un approbateur requis ▪ Approbation de tous les utilisateurs requise
Ordre	Ordre d'exécution des différentes configurations au sein d'une règle. Par exemple, une configuration avec une entrée d'ordre de 100 s'exécute avant une configuration avec une entrée d'ordre de 200.
Rôle	Sélectionnez un rôle pour le groupe dans la liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Règle d'approbation	Contient les détails de table et de type pour la règle d'approbation.
Configuration de l'approbation	Contient les configurations d'approbation.
Affecter à l'aide de	Sélectionnez une option : ▪ Utilisateur et groupe d'utilisateurs ▪ Champ de la table des approbations ▪ Script
Groupes	Groupe de niveau de l'approbateur composé de plusieurs utilisateurs. L'utilisateur doit avoir l'un des rôles suivants que vous spécifiez.
Utilisateurs	Modifier les utilisateurs répertoriés dans les groupes.

c. Cliquez sur **Envoyer** pour enregistrer vos modifications.

Affichage des données de correctifs et du déploiement des données de correctifs pour l'intégration de Patch Réponse aux vulnérabilités Orchestration avec Microsoft SCCM

Les données de correctif et les données de déploiement de correctif, ainsi que les informations de vulnérabilité et l'état de rattrapage de vos vulnérabilités sont affichées dans les enregistrements de votre instance.

Affichage des données de correctifs dans les Réponse aux vulnérabilités espaces de travail

Rôles requis :

- sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs
- sn_vul_patch_orch.read_patch pour afficher (en lecture seule) les informations de correctif sur les enregistrements. Ce rôle est hérité des rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail Responsable du rattrapage informatique et de la vulnérabilité

Dans l'espace de travail de remédiation informatique, vous pouvez afficher les correctifs :

- Dans la vue d'accueil, où vous pouvez cliquer sur des tableaux de résultats pour afficher les enregistrements des solutions préférées sur les VI, des CI vulnérables et des correctifs préférés sur les VI.
- Dans la vue de liste, où vous pouvez afficher tous les enregistrements de mise à jour de correctifs (VPU) à partir des liens des correctifs, ainsi que les éléments vulnérables (VIT) qui vous sont affectés et qui ont des correctifs.

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- À partir d'une mise à jour de correctif (VPU)
- Tâche de rattrapage (RT)
- Enregistrements d'éléments détectés (SDI)

Dans Vulnerability Manager Workspace, vous pouvez afficher les correctifs :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- À partir de la vue d'accueil sur les rubriques de surveillance, où vous pouvez afficher les correctifs préférés et potentiels, les dates planifiées des correctifs et, si le correctif a été téléchargé, le tout sous l'onglet **Éléments vulnérables** .
- Depuis la vue de liste sur les efforts de rattrapage, où vous pouvez afficher les données de correctifs sur les enregistrements de VI à partir de l'onglet**Éléments vulnérables** .

À partir de la vue d'environnement classique, accédez à **Tout** > **Réponse aux vulnérabilités** > **Correctifs**.

Enregistrements de mise à jour de correctif dans les espaces de travail VR et dans la vue d'environnement classique

Les données de correctif et les données et l'état de déploiement de correctif sont affichés sur les enregistrements de votre instance. Les enregistrements de correctifs sont inclus dans la fonctionnalité d'orchestration de correctifs de cette intégration avec Réponse aux vulnérabilités. Affichez les enregistrements de correctifs (VPU) dans Réponse aux vulnérabilités les espaces de travail à partir de la vue Liste de l'espace de travail de remédiation informatique. Les enregistrements de mise à jour de correctif dans l'environnement classique et Réponse aux vulnérabilités les espaces de travail incluent les données suivantes :

- Données et informations sur les solutions de vulnérabilité provenant des fournisseurs de correctifs importées par l'application Gestion des solutions de vulnérabilité.
- État du rattrapage à la source qui inclut le nombre total d'appareils présentant une vulnérabilité donnée qui peut être corrigée par un correctif. De plus, il inclut également tous les appareils qui n'ont pas de mises à jour.
- État du rattrapage qui inclut le % de VI rattrapés et le total des VI pour lesquels un correctif est préféré.
- Appareils associés, éléments vulnérables, déploiements de correctifs et demandes de correctifs sur les liens connexes des enregistrements dans la vue de classe. Ces données sont affichées sous forme d'onglets sur les Réponse aux vulnérabilités enregistrements des espaces de travail.
- Demandes de correctifs que les propriétaires de rattrapage ont soumises pour approbation.

Déploiement d'état sur les enregistrements d'éléments vulnérables

Pour en savoir plus sur le déploiement de l'état sur les enregistrements, reportez-vous Déploiement des données et de l'état des correctifs pour l'orchestration des correctifs dans Réponse aux vulnérabilitésà .

Enregistrements qui déploient des nombres de VI actifs

Pour éviter de déployer tous les correctifs sur toutes les vulnérabilités, la tâche planifiée récupère uniquement les changements apportés au nombre de VI actifs. Ces changements de nombre et les données connexes sont déployés sur les enregistrements suivants dans Réponse aux vulnérabilités:

- VIT
- RT
- Solution de vulnérabilité
- Mise à jour du correctif

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage des données pour les correctifs sans solutions

Pour plus d'informations sur l'affichage des correctifs sans solutions, reportez-vous à la section Afficher les correctifs sans solution dans Réponse aux vulnérabilités.

Appliquer des correctifs de données sur le Réponse aux vulnérabilités

Les tableaux de bord Gestion des vulnérabilités (PA) et CISO sont inclus dans un abonnement avec l'application Analyse des performancesRéponse aux vulnérabilités . Si vous disposez d'un abonnement à Analyse des performances, mais qu'aucune intégration d'orchestration de correctif n'est installée, l'onglet Rattrapage s'affiche sur le tableau de bord CISO, mais il n'est pas renseigné avec les données.

Pour le tableau de bord Gestion de la vulnérabilité (PA), accédez à **Tout** > **Réponse aux vulnérabilités** > **Vue d'ensemble**. Cliquez sur l'onglet **Correction** et faites défiler vers le bas de la page pour afficher les données de mises à jour de correctifs : correctifs planifiés et non planifiés, correctifs n'ayant pas leur date cible et nombres hebdomadaires.

Pour le tableau de bord CISO, accédez à **Tout** > **Réponse aux vulnérabilités** > **Tableau de bord des CISO**. Avec l'onglet Vue d'ensemble sélectionné, faites défiler vers le bas de la page pour afficher les données de couverture des correctifs : criticité, correctifs planifiés et non planifiés, et correctifs n'ayant pas leur date cible.

Pour en savoir plus sur les tableaux de bord, reportez-vous Réponse aux vulnérabilités aux rubriques Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités, Appliquer des correctifs à Orchestration avec les Réponse aux vulnérabilités espaces de travailet Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord.

Planifier les correctifs avec l'intégration Microsoft SCCM avec Réponse aux vulnérabilités

Planifiez les correctifs à partir des enregistrements de tâche de mise à jour et de rattrapage dans l'application Réponse aux vulnérabilités de votre Now Platform instance.

Avant de commencer

À partir de la version 16.1, vous pouvez planifier des correctifs à partir des espaces de Réponse aux vulnérabilités travail ou de l'environnement classique.

Rôles requis :

- sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs
- sn_vul_patch_orch.read_patch pour afficher (en lecture seule) les informations de correctif sur les enregistrements. Ce rôle est hérité des rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail Responsable du rattrapage informatique et de la vulnérabilité

Procédure

1. Dans Vulnerability Réponse aux vulnérabilités Workspaces, en tant qu'utilisateur disposant du rôle sn_vul.remediation_owner, accédez à **Tout** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
2. Sur la page d'accueil, cliquez sur **Correctif préféré sur les VI.**
   La liste des enregistrements de mise à jour de correctifs pour les VI avec correctifs préférés qui vous sont affectés s'affiche.
3. Localisez un enregistrement que vous souhaitez ouvrir et cliquez dessus pour l'ouvrir.
4. Sinon, dans la vue de liste de l'espace de travail, cliquez sur **Correctifs** > **Tout** et localisez un enregistrement de mise à jour de correctif.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'enregistrement de mise à jour du correctif s'affiche. Vous préférerez peut-être examiner les données avant de planifier un correctif, car d'autres correctifs peuvent déjà être planifiés.

5. Consultez le tableau suivant pour en savoir plus sur les données affichées dans IT Remediation Workspace et sur ce que vous pouvez faire.

Tâche	Description
Cliquez sur un lien d'éléments connexes	◦ Vue d'ensemble - Affichez les détails tels que le numéro d'enregistrement de mise à jour du correctif, les ID d'article et de bulletin, la date de publication et la catégorie de la mise à jour, le nom du site pour le correctif, la cote de risque, le score de risque, la description, la solution (le cas échéant) et l'état du rattrapage. ◦ Appareils associés : liste des éléments de configuration impactés affectés par le correctif et son état. ◦ Éléments vulnérables : liste des éléments vulnérables associés à la vulnérabilité et au correctif. ◦ Déploiements de correctifs : noms et informations relatives aux déploiements de ce correctif sur les actifs ou les groupes de ressources de ce correctif. ◦ Demandes de correctifs : liste des demandes de correctifs déjà soumises pour ce correctif.
Cliquez sur un lien pour ouvrir un enregistrement.	Dans les listes affichées dans les enregistrements ouverts à partir des liens des éléments connexes, affichez plus de détails, y compris les messages sur les cibles manquées. Une fois ouverts, les enregistrements restent ouverts en tant qu'onglets jusqu'à ce que vous les fermiez.
Planifier le correctif	Lorsque vous êtes prêt à planifier un correctif ou à envoyer une demande, cliquez sur **Planifier le correctif**. Dans la boîte de dialogue qui s'affiche, renseignez les champs. Reportez-vous aux étapes ci-dessous pour en savoir plus.
Ajouter une note de travail ou joindre un fichier	Tout à droite de l'écran, cliquez sur l'icône **Activité** (icône d'allègement) et saisissez une note de travail. Cliquez sur l'icône pour basculer le panneau. Vous pouvez également charger un fichier.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Planifier le correctif**.
7. Renseignez les champs de la boîte de dialogue.

Champ	Description
Étape 1 : Sélectionner la cible	
Collection	Choisissez une collection (groupe d'actifs) dans la liste pour continuer. Il s'agit des collections importées du SCCM.
Étape 2 : Calendrier	
Nom du déploiement	Entrez un nom pour le déploiement de ce correctif. Ce nom vous aide à suivre vos mises à jour.
Type de déploiement	Choisissez une option dans la liste. ◦ Requis : ce correctif est une mise à jour requise. ◦ Disponible : ce correctif n'est pas requis, mais disponible pour le déploiement.
Heure de date limite	Fixez la date limite. Cette valeur indique le dernier jour où le correctif peut être installé.
Temps disponible	Définissez la valeur du moment où le correctif devient disponible pour la première fois pour le déploiement.
Temps disponible basé sur	Sélectionnez un fuseau horaire dans la liste sur lequel baser votre fenêtre de temps de déploiement.
Autoriser le redémarrage	Elle est désactivée par défaut. Activez (sélectionnez) cette option pour demander aux machines du groupe de redémarrer automatiquement une fois le correctif terminé.
Description	Ajoutez plus de texte pour le patch. Ces informations s'affichent dans le champ Description de l'enregistrement de mise à jour des correctifs.

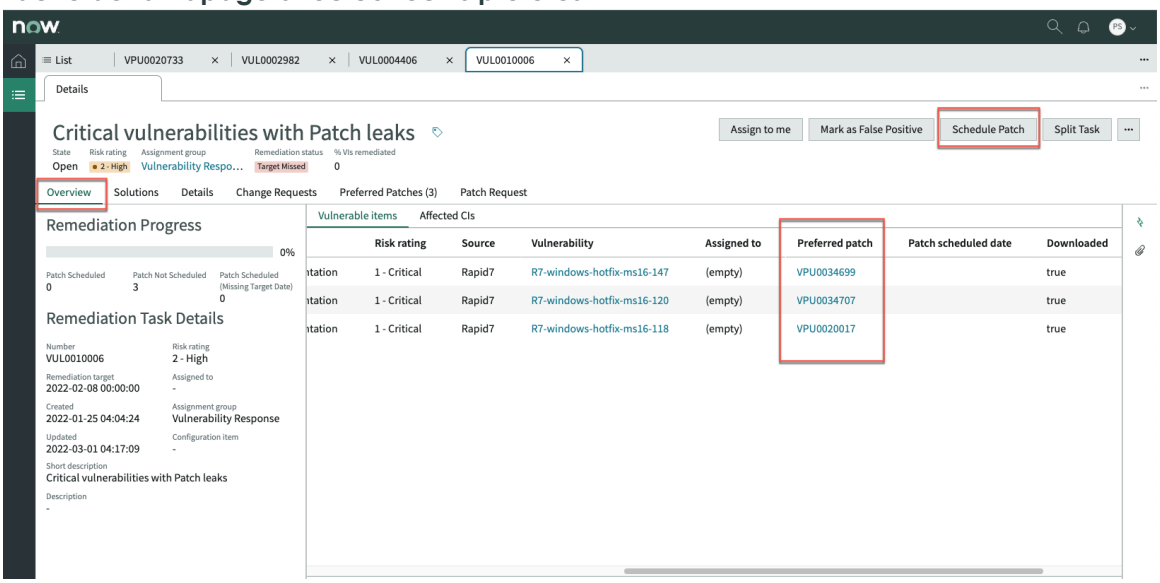
8. Cliquez sur **Déployer**.
   La demande de correctif est envoyée à pour examen. Vous pouvez afficher l'état de toutes vos demandes soumises à partir de **Demandes d'exception** > **Mes demandes** dans la vue de liste.
9. Vous pouvez également planifier des correctifs à partir des tâches de rattrapage (RT) qui vous sont affectées ou qui sont affectées à votre groupe.

> **Remarque :** L'option permettant de planifier un correctif à partir d'un enregistrement de tâche de rattrapage n'est disponible que si des correctifs sont mappés sur les VI de la tâche (associés à ceux-ci). Ces correctifs sont affichés dans la colonne Correctif préféré si vous faites défiler vers la droite d'un enregistrement de tâche de rattrapage avec l'onglet Vue d'ensemble sélectionné.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de rattrapage avec correctifs préférés



10. Cliquez sur **Planifier le correctif** dans l'enregistrement RT et suivez les étapes énumérées ci-dessus pour le planifier dans la boîte de dialogue.
11. Facultatif : Vous pouvez planifier des correctifs pour les étapes précédemment dans l'environnement classique.
    Pour localiser ces enregistrements, procédez comme suit.

    a. Dans l'environnement classique, accédez à **Tout** > **Réponse aux vulnérabilités** > **Correctifs** > **Tout**.

    b. Dans la liste qui s'affiche, recherchez un enregistrement de mise à jour de correctif.

    c. Pour les tâches de rattrapage, accédez à **Réponse aux vulnérabilités** > **Tâches de remédiation** et localisez un enregistrement.
    Suivez l'état du rattrapage dans l'onglet État du rattrapage. Au bas de l'enregistrement, les données de correctif sont affichées sur les liens connexes.

    d. Cliquez sur **Planifier le correctif** et renseignez les champs.

Champ	Description
Nom du déploiement	Entrez un nom pour le déploiement de ce correctif. Ce nom vous aide à suivre vos mises à jour.
Description	Ajoutez plus de texte pour le patch. Ces informations s'affichent dans le champ Description de l'enregistrement de mise à jour des correctifs.
Type de déploiement	Choisissez une option dans la liste. ▪ Requis : ce correctif est une mise à jour requise. ▪ Disponible : ce correctif n'est pas requis, mais disponible pour le déploiement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Collection	Choisissez une collection (groupe d'actifs) dans la liste pour continuer. Ces groupes sont les collections d'actifs importées de SCCM.
Temps disponible basé sur	Sélectionnez un fuseau horaire dans la liste sur lequel baser votre fenêtre de temps de déploiement.
Temps disponible	Définissez la valeur du moment où le correctif devient disponible pour la première fois pour le déploiement.
Date limite	Fixez la date limite. Cette valeur indique le dernier jour où le correctif peut être installé.

e. Cliquez sur **Déployer**.

Messages REST pour Patch Réponse aux vulnérabilités Orchestration with Microsoft SCCM

Vulnerability Response Patch Orchestration with Microsoft SCCM utilise les classes WMI (Windows Management Instrumentation) SCCM pour effectuer des appels à l'API du serveur SCCM.

Vue d'ensemble

Le fournisseur de SMS fournit à l'API un accès d'interopérabilité via HTTPS, appelé service d'administration. Le service d'administration est une API REST (Representational State Transfer) basée sur le protocole Open Data (OData) v4.

Consultez Qu'est-ce que le service d'administration dans Configuration Manager pour plus d'informations sur l'utilisation du service d'administration avec cette intégration.

Étant donné que l'authentification requise utilise le protocole Windows New Technology LAN Manager NTLM, les appels aux API sont effectués via le MID Server à l'aide de scripts PowerShell.

Microsoft Intégration SCCM

Vous pouvez utiliser le message REST pour l'intégration Microsoft SCCM afin de récupérer des informations à partir de Microsoft SCCM. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes de récupération d'informations adressées au Microsoft SCCM. Les messages REST contiennent les méthodes REST suivantes.

Noms des classes WMI :

- SMS_Collection
- SMS_DeploymentSummary

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
URL	Valeurs dynamiques basées sur l'utilisateur	Indique le point de terminaison de la console SCCM

Microsoft Correctif de déploiement SCCM

Vous pouvez utiliser le message REST pour l'intégration Microsoft SCCM afin de planifier des correctifs de Ur Now Platform® vers le Microsoft SCCM. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes de récupération d'informations adressées au SCCM. Les messages REST contiennent les méthodes REST suivantes.

Méthode REST	Description
POST Déployer le correctif	Planifie la mise à jour sur la console SCCM sur un ou plusieurs ordinateurs.

Nom de paramètre	Valeur	Description
URL	Valeurs dynamiques basées sur l'utilisateur	Indique le point de terminaison de la console SCCM.
Titre	Valeurs dynamiques basées sur l'utilisateur	Titre du déploiement.
settings_tag	Paramètres nommés par balise XML avec des valeurs	Indique les paramètres qui ont des paramètres différents et qui sont envoyés au SCCM lors de la planification du correctif.
computer_tag	Ordinateurs portant un nom de balise XML avec des valeurs	Indique la liste des ordinateurs sur lesquels le correctif va être planifié.
site_name	Valeur de la mise à jour du correctif	Nom du site où le correctif est présent.
Patch_id	Valeur de la mise à jour du correctif	ID du correctif.

Transformation des données pour l'orchestration des correctifs avec Microsoft l'intégration SCCM

Les données sont récupérées à partir de Patch Orchestration avec Microsoft l'intégration SCCM, traitées via un ensemble de sources de données et transformées dans votre Now Platform® instance.

Importation de collection SCCM

Les données des collections importées sont chargées dans la table Importation de collections SCCM [sn_vul_sccm_collection_import]. Les collections SCCM (carte de transformation) permettent de transformer les informations importées.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les modifications apportées à cette carte de transformation modifient le traitement des données provenant de l'importation de la collection SCCM.

Pour accéder à cette carte de transformation, accédez à **Tout** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation de collection SCCM. La table suivante répertorie les champs de carte de transformation par intégration.

Champ source	Champ cible	Description
u_collectionid	source_id	ID unique de la collection.
u_name	name	Nom de la collection.
u_membercount	device_count	Nombre d'appareils dans cette collection.
[script]	integration_instance	Nom de l'instance à partir de laquelle le correctif est importé.

Importation collection SCCM Synchroniser le script de la carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour mettre à jour les valeurs de la variable de champ d'application [sn_vul_sccm]. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Importation de la mise à jour du correctif SCCM

Les données des correctifs importés sont chargées dans la table d'importation [sn_vul_sccm_patch_update_import] de mise à jour du correctif SCCM.

La transformation de mise à jour du correctif SCCM est utilisée pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient le traitement des données issues de l'importation de la mise à jour du correctif SCCM.

Pour accéder à cette carte de transformation, accédez à **Tout** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation de mise à jour du correctif SCCM.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La table suivante répertorie les champs de carte de transformation par intégration.

Importation de la mise à jour du correctif SCCM Champs de carte de transformation

Champ source	Champ cible	Description
[Script]	URL	URL du correctif.
u_nummissing	num_missing	Nombre d'appareils manquants pour ce correctif.
[Script]	date_release	Date de sortie du correctif.
u_bulletinid	bulletin_id	ID du bulletin pour le correctif.
u_numtotal	num_total	Nombre total d'appareils.
u_localizeddescription	description	Description du correctif.
[Script]	is_highest_supersedence	C'est le patch avec la plus grande priorité.
u_numnotapplicable	num_not_applicable	Nombre d'appareils non applicables pour ce correctif.
u_iscontentprovisioned	is_downloaded	Si le correctif est téléchargé sur le serveur SCCM.
u_numunknown	num_unknown	Nombre total d'appareils inconnus.
u_articleid	article_id	ID d'article du correctif.
u_localizeddisplayname	Titre	Titre du patch.
u_ci_id	source_id	ID unique du correctif dans SCCM.
u_numpresent	num_present	Nombre d'appareils sur lesquels le correctif est installé.
[Script]	integration_instance	Nom de l'instance à partir de laquelle le correctif est importé.
[Script]	sn_vul_solution	Solution basée sur l'ID source.
[Script]	last_modified	Date de la dernière modification du correctif.
u_severity	source_severity	Gravité du correctif.

Importation de la mise à jour du correctif SCCM Synchronisation du script de carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à une

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation de la mise à jour du correctif SCCM Synchronisation du script de carte de transformation (suite)

Script	Description
	utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour mettre à jour les valeurs de la variable de champ d'application [sn_vul_sccm]. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Importation de la mise à jour du correctif de l'appareil SCCM

Les données des correctifs pertinents importés sur les appareils sont chargées dans la table Importation de mise à jour de correctif d'appareil SCCM [sn_vul_sccm_device_patch_import].

La transformation de mise à jour du correctif de l'appareil SCCM est utilisée pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient le traitement des données provenant de l'importation de la mise à jour du correctif de l'appareil SCCM.

Pour accéder à cette carte de transformation, accédez à **Tout** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation de mise à jour du correctif de l'appareil SCCM.

La table suivante répertorie les champs de carte de transformation par intégration.

Mise à jour du correctif de l'appareil SCCM Synchroniser le script de la carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour créer et mettre à jour les CI en fonction des règles de recherche de CI et des correctifs, ainsi que de la relation entre eux. En fonction des résultats, ce script modifie les valeurs de la variable de champ d'application [sn_vul_sccm]. Ce script est

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise à jour du correctif de l'appareil SCCM Synchroniser le script de la carte de transformation (suite)

Script	Description
	destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Importation de la collection des appareils SCCM

Les données des collections d'appareils importées sont chargées dans la table Importation d'une collection d'appareils SCCM [sn_vul_sccm_device_collection_import].

La transformation d'importation de collection d'appareils SCCM est utilisée pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient le traitement des données de l'importation de la collection d'appareils SCCM.

Pour accéder à cette carte de transformation, accédez à **Tout** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation de la collection d'appareils SCCM.

La table suivante répertorie les champs de carte de transformation par intégration.

Importation d'une collection d'appareils Synchroniser le script de carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour créer et mettre à jour les CI en fonction des règles de recherche de CI et des collectes, ainsi que de la relation entre elles. En fonction des résultats, ce script modifie les valeurs de la variable de champ d'application [sn_vul_sccm]. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation de la collection d'appareils SCCM Champs de carte de transformation

Champ source	Champ cible	Description
u_id	source_id	ID unique d'une action.
U_name	name	Nom de l'action
[Script]	Sn_vul_sccm_discovered_item	Référence de l'élément détecté sur lequel le correctif est déployé
U_status	statut	Statut de l'action
[Script]	Sn_vul_patch_orch_update	Référence du correctif
U_apply_count	Count_success	Nombre de réussites de l'action.
U_retry_count	retry	Nombre de nouvelles tentatives de l'action.
[Script]	Deployment_time	Heure de début de l'action.
[Script]	date limite	Heure de fin de l'action.
[Script]	Source_created	Heure de création de l'action.
[Script]	Integration_instance	Nom de l'instance à partir de laquelle l'action est importée.

Importation du déploiement SCCM

Les données des déploiements importés sont chargées dans la table Importation de déploiement SCCM [sn_vul_sccm_deployment_import].

La transformation d'importation de déploiement SCCM permet de transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation de déploiement SCCM sont traitées.

Pour accéder à cette carte de transformation, accédez à **Tout** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation du déploiement SCCM.

Déploiement SCCM Champs de carte de transformation

Champ source	Champ cible	Description
u_id	source_id	ID unique d'un déploiement.
u_name	name	Nom du déploiement.
[Script]	date limite	Heure limite pour le déploiement.
u_numberinprogress	count_progress	Nombre d'appareils en cours pour le déploiement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déploiement SCCM Champs de carte de transformation (suite)

Champ source	Champ cible	Description
[Script]	deployment_time	Heure de début du déploiement.
[Script]	integration_instance	Nom de l'instance à partir de laquelle le déploiement est importé.
[Script]	source_created	Heure de création du déploiement.
[Script]	sn_vul_patch_orch_update	Référence du correctif
[Script]	sn_vul_patch_orch_collection	Référence de l'élément détecté sur lequel le correctif est déployé.
u_softwarename	name	Nom du déploiement.
u_numberother	count_other	Autre nombre d'appareils pour le déploiement.
u_numberunknown	count_unknown	État inconnu : nombre d'appareils pour le déploiement.
u_deploymentid	source_id	Identificateur unique du déploiement.
u_numbersuccess	count_success	Nombre correct d'appareils pour le déploiement.
u_numbererrors	count_error	Nombre d'erreurs d'appareils pour le déploiement.
u_numbertargeted	count_total	Nombre total d'appareils pour le déploiement.

Importation déploiement SCCM Synchroniser le script de la carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé la transformation).	Script utilisé pour initialiser les valeurs de la variable de champ d'application [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Script utilisé pour mettre à jour les valeurs de la variable de champ d'application [sn_vul_sccm]. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation déploiement SCCM Synchroniser le script de la carte de transformation (suite)

Script	Description
	script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Exemple de workflow pour l'intégration de Réponse aux vulnérabilités Patch Orchestration avec Microsoft SCCM

Un exemple du fonctionnement de l'orchestration des correctifs avec Microsoft SCCM.

Avant de commencer

Supposons, par exemple, que l'ensemble de votre environnement soit corrigé une fois toutes les trois semaines. La fenêtre d'application de correctif la plus récente a été terminée il y a une semaine, mais vous souhaitez appliquer un correctif pour corriger une vulnérabilité critique récemment connue. En raison de la nature critique de cette vulnérabilité, vous ne pouvez pas attendre deux semaines de plus pour le prochain correctif planifié.

Rôles requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour Vulnerability Manager Workspace.
- sn_vul.remediation_owner pour afficher l'espace de travail du propriétaire de rattrapage informatique.
- sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs.
- sn_vul_patch_orch.read_patch pour afficher (en lecture seule) les informations de correctif sur les enregistrements. Ce rôle est hérité des rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail IT Remediation et Vulnerability Manager.

Pourquoi et quand exécuter cette tâche

En tant que gestionnaire de vulnérabilités ou analyste travaillant dans l'espace de travail du gestionnaire de vulnérabilités, vous pouvez envisager de créer des rubriques de surveillance ou de modifier des rubriques de surveillance existantes pour vous aider à capturer les éléments vulnérables importés présentant des vulnérabilités critiques. Avec l'intégration d'orchestration de correctifs, vous pouvez également voir les correctifs que vous souhaitez utiliser pour corriger et suivre ces vulnérabilités. Le tableau suivant répertorie quelques exemples avec les conditions que vous pouvez définir pour les rubriques de surveillance pour l'orchestration des correctifs. Utilisez ces exemples pour vous aider à déterminer les paramètres les mieux adaptés à votre environnement. Consultez Créer une rubrique de surveillance dans Vulnerability Manager Workspace pour plus d'informations sur la configuration de la rubrique de visualisation.

Exemple de rubriques de surveillance pour l'orchestration des correctifs dans Vulnerability Manager Workspace

Nom de la rubrique de surveillance	Description
Vulnérabilités critiques avec fuites de correctifs	`La cote de risque est de 1 - critique` ET `La raison pour laquelle le correctif n'est pas planifié`

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de rubriques de surveillance pour l'orchestration des correctifs dans Vulnerability Manager Workspace (suite)

Nom de la rubrique de surveillance	Description
Vulnérabilités critiques avec correctifs planifiés (SLA manquant)	`Le motif est Correctif planifié (date cible manquante)`
Vulnérabilités critiques avec correctifs planifiés	`La cote de risque est de 1 - critique` ET `La date planifiée du correctif n'est pas vide` ET `Le motif est le correctif planifié`

- En tant que gestionnaire ou analyste de vulnérabilités, après avoir créé les rubriques de surveillance et les efforts de rattrapage, vous générez des tâches de rattrapage. À partir des enregistrements de VI et des tâches de rattrapage, vous pouvez explorer l'onglet Détections et localiser les enregistrements d'éléments détectés qui présentent la vulnérabilité que vous suivez, ainsi que les actifs importés par le produit SCCM.
- En tant qu'analyste de vulnérabilité ou administrateur, vous pouvez surveiller les données de correctifs associées à la vulnérabilité. Vous pouvez également déployer un ou plusieurs correctifs sur un actif spécifique (élément de configuration) à partir d'un enregistrement d'élément détecté.

En tant que spécialiste de la remédiation informatique, vous disposez d'options pour traiter la vulnérabilité avec le déploiement d'un correctif.

- Vous pouvez planifier le correctif à partir d'un enregistrement de mise à jour de correctif (VPU#).
- Si des solutions préférées sont mappées aux éléments vulnérables (VI) et qu'elles vous sont affectées, à vous ou à vos groupes, vous pouvez planifier les correctifs à partir d'une tâche de rattrapage qui comporte ces éléments vulnérables.

Procédure

1. En tant que spécialiste du rattrapage informatique, dans l'espace de travail de rattrapage informatique, cliquez sur la vue d'accueil.
2. Dans la vue d'accueil, cliquez sur le tableau de résultats des **tâches de rattrapage affectées** pour afficher les enregistrements.

   Pour les besoins de cet exemple, vous pouvez vérifier le champ Brève description sur la tâche de rattrapage (VUL#) pour tout texte qui se rapporte à votre vulnérabilité critique. Supposons, par exemple, que vous sachiez peut-être que votre gestionnaire de vulnérabilités a créé une rubrique de surveillance intitulée Vulnérabilités critiques avec fuites de correctifs pour intercepter les VI (VIT#) avec cette vulnérabilité critique.

   Une fois l'enregistrement ouvert, vous pouvez également passer en revue les VI, les correctifs préférés et voir si vous ou l'un des membres de votre groupe avez déjà soumis des demandes de correctif pour approbation.

3. Si vous disposez de suffisamment d'informations, vous pouvez soumettre une demande de correctif maintenant à partir de cette tâche de rattrapage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si les VI associés à l'enregistrement n'ont pas de correctifs mappés sur eux, le bouton **Planifier le correctif** n'est pas disponible sur l'enregistrement.

4. Cliquez sur **Planifier le correctif** et renseignez les champs de la boîte de dialogue.
   Pour en savoir plus sur la planification d'un correctif, reportez-vous à la section Planifier les correctifs avec l'intégration Microsoft SCCM avec Réponse aux vulnérabilités.
5. À partir de la vue Liste de l'espace de travail de remédiation informatique, vous pouvez également cliquer sur les liens Tâches de remédiation, Éléments vulnérables, Solutions et Correctifs pour afficher ces enregistrements.
   Dans le cas de cet exemple, au lieu d'un nom de rubrique de surveillance, vous connaissez peut-être l'ID d'article ou l'ID de bulletin et le titre du correctif. Si tel est le cas, vous voudrez peut-être vérifier si l'un des VI présentant cette vulnérabilité vous est affecté ou est affecté à vos groupes. Dans les enregistrements de mise à jour de correctifs, vous pouvez soumettre des demandes de correctifs. Dans les enregistrements de VI, vous pouvez rechercher des correctifs potentiels et ouvrir la tâche de rattrapage associée si vous souhaitez soumettre une demande de correctif.
6. Si vous n'avez pas accès aux espaces de travail, ou si vous préférez afficher les données et planifier les correctifs à partir de l'environnement classique, procédez comme suit.

   a. Accédez à la **Réponse aux vulnérabilités** > **Correctifs** > **Tout**.

   b. Localisez l'enregistrement de mise à jour de correctif souhaité.
   Vous préférez peut-être filtrer les enregistrements avec des scores de risque `critique` .

   c. Passez en revue les champs des VI et du % de rattrapages des VI associés sous l'onglet État du rattrapage.
   Si des correctifs sont disponibles pour les VI, le bouton **Planifier le correctif** s'affiche dans le coin supérieur droit de l'enregistrement.

   d. Si vous décidez de soumettre une demande, cliquez sur **Planifier le correctif**.
   Pour en savoir plus sur la planification d'un correctif, reportez-vous à la section Planifier les correctifs avec l'intégration Microsoft SCCM avec Réponse aux vulnérabilités.

   e. Sinon, disons que vous n'avez pas les informations sur l'ID du correctif, mais que vous pouvez vérifier le champ Brève description sur les tâches de rattrapage qui sont affectées à votre groupe pour tout texte qui se rapporte à votre vulnérabilité critique.

   f. Accédez à la **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**.

   g. Localisez l'enregistrement souhaité et cliquez dessus pour l'ouvrir.
   Dans l'enregistrement ouvert, passez en revue l'onglet État du rattrapage pour les VI et le % des VI rattrapés. Cliquez sur les liens connexes pour les enregistrements de VI, les solutions préférées, les correctifs préférés et les demandes de correctifs.

   Remarque : Si les VI associés à l'enregistrement n'ont pas de correctifs mappés sur eux, le bouton **Planifier le correctif** n'est pas disponible sur l'enregistrement.

   h. Cliquez sur **Planifier un correctif** dans l'enregistrement si vous souhaitez soumettre une demande de correctif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Présentation de Qualys Vulnerability Integration

Les Qualys capteurs du produit collectent les données et les envoient automatiquement à l'application, qui analyse et corrèle Qualys les informations en continu. Il s'intègre Réponse aux vulnérabilitésQualys Vulnerability Integration facilement pour mapper les vulnérabilités aux CI et aux services d'entreprise afin de déterminer l'impact et la priorité des menaces potentiellement malveillantes.

Configurer votre Qualys Vulnerability Integration utilisation **Vulnérabilité** > **Administration** > **Assistant de configuration** pour rendre la récupération de données plus flexible et évolutive.

Si vous avez plusieurs déploiements de l'application Qualys Cloud Platform , vous pouvez ajouter une intégration pour chaque déploiement. Les actifs, identifiés par plusieurs déploiements tiers et leurs vulnérabilités, sont consolidés et rapprochés avec votre CMDB. Cette consolidation se produit même lorsque les processus d'analyse se chevauchent entre les différents déploiements. Les données provenant de chaque déploiement sont identifiées et disponibles dans une instance unique de Réponse aux vulnérabilités. Qualys Vulnerability Integration Les enregistrements de la base de connaissances sont normalisés entre les déploiements, ce qui garantit que les instances de la même vulnérabilité dans tous les déploiements sont traitées comme la même vulnérabilité.

Remarque : Vous ne pouvez pas supprimer l'intégration de vulnérabilité d'origine, mais vous pouvez la désactiver. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Remarque : Bien que l'crée des intégrations pour la liste des appliances, le groupe d'actifs Qualys Vulnerability Integration , la liste de recherche dynamique et la liste de recherche statique, elles ne sont pas nécessaires pour un fonctionnement normal.

Versions disponibles

Version de mise en production pour Xanadu	**Notes de publication**
Qualys Vulnerability Integration v12.7, v12.8	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Composants installés

Pour obtenir la liste à jour des rôles, des tâches d'intégration et des tables installés avec l'intégration, ainsi qu'un lien vers des instructions permettant d'afficher ce qui est actuellement installé dans votre instance, reportez-vous Composants installés avec l' Qualys Vulnerability Integrationà .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations principales et prises en charge

Qualys Les intégrations principales et prises en charge enrichissent les données de vulnérabilité sur votre instance en récupérant les données à partir de Qualys Vulnerability Integration. Une série de travaux planifiés invoque automatiquement les intégrations. Vous pouvez également les exécuter manuellement. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités. Les intégrations principales et de prise en charge peuvent être modifiées.

Les Qualys intégrations sont exécutées en tant que travaux planifiés. Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Cette valeur ne doit pas être modifiée.

Remarque : L'échec de la définition d'un utilisateur d'exécution en tant que valide entraîne la récupération de plusieurs pièces jointes, souvent en double, récupérées sur les enregistrements de source de données, à chaque exécution de l'intégration. Plusieurs pièces jointes sur la source de données augmentent le temps de traitement, ce qui entraîne des résultats de transformation incohérents.

Au cours de l'importation, les enregistrements CVE, qui ne sont pas déjà présents, sont créés en tant qu'enregistrements NVD et référencés par défaut dans des entrées Qualys tierces.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Intégrations principales

Une intégration primaire est un point d'entrée vers l'interaction Qualys Cloud Platform avec l'API invoquée dans un Qualys calendrier.

Affichez les intégrations principales en accédant à **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.

Prise en charge des intégrations

Une intégration de prise en charge est un processus qui n'est pas destiné à s'exécuter selon un calendrier ni sans invocation par une intégration primaire.

Afficher les intégrations de prise en charge en accédant à **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations prises en charge**.

Connecteur du graphe de services pour Qualys

À partir de la version 2.2, Connecteur du graphe de services pour Qualys est disponible à partir du ServiceNow® Store. Consultez Connecteur du graphe de services pour Qualys (2.0.0) pour plus d'informations.

Les données des champs de source de Qualys données sont importées avec l'API Global Asset et l'API Gestion des actifs et de balisage.

API d'actif global :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Une licence CSAM est requise.
- Les informations sur les actifs comprennent des détails tels que la catégorie de matériel et la catégorie de système d'exploitation.

API de gestion des actifs et de balisage :

- Aucune licence CSAM n'est requise
- Les informations sur les actifs n'incluent pas de détails sur la catégorie de matériel et la catégorie de système d'exploitation.

Pour plus d'informations, voir API Connecteur du graphe de services pour Qualys

.

Créer des CI à l'aide du moteur Identification et rapprochement (IRE)

Vous pouvez utiliser le moteur Identification et rapprochement pour créer de nouveaux CI lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte importé à partir d'un scanner tiers. Activez le module d'extension Modèles de classe CI CMDB pour créer des CI à l'aide des nouvelles classes, sinon des CI sans correspondance sont créés dans les classes CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement. Pour en savoir plus sur la configuration de la catégorisation des ressources cloud inégalées dans votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

Listes de recherches

Les listes de recherche sont utilisées pour Qualys créer des groupes personnalisés de vulnérabilités. Vous pouvez les enregistrer et les utiliser pour créer des tickets et personnaliser les analyses et les rapports de vulnérabilité. Le module Listes de recherches vous permet de télécharger les données de liste de recherches de Qualys vers votre instance de manière planifiée.

Les listes de recherche sont extraites à l'aide des cartes de transformation de données d'importation de liste de recherches dynamiques et/ou d'importation de listes deQualys recherches statiques. Dans chacune de ces transformations, vous pouvez définir des calendriers pour effectuer l'importation.

Profils d'option

Les profils d'option sont disponibles avec Qualys des paramètres de numérisation. Un profil d'option est requis lorsque vous lancez une analyse à partir de votre Now Platformfichier .

Les profils d'option Qualys sont importés à partir du produit par l'intégration de la liste des profils d'options. Il est peut-être préférable d'exécuter l'intégration de la liste de profils d'options après une importation à partir des intégrations de listes de recherche, de liste Qualys de recherche dynamique et Qualys de liste de recherche statique afin de voir quelles listes de recherches sont associées aux profils d'options.

Groupes d'actifs

Les groupes de ressources sont configurés dans la Qualys plateforme. Les groupes d'actifs identifient les dispositifs de scanner utilisés pour analyser les adresses IP correspondantes lorsqu'une analyse est lancée à partir du Now Platform.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les groupes d'actifs auxquels des dispositifs sont associés sont extraits par l'intégration de la liste des groupes d'actifs Qualys .

Lancez l'intégration de la liste des dispositifs après avoir importé des groupes de ressources pour renseigner les champs Nom du dispositif et État du dispositif sur les Qualys enregistrements Applications par défaut dans votre Now Platform.

Balises d'hôtes

Toutes les balises d'hôte sont importées dans le cadre de l'intégration de la liste d'hôtes Qualys . Les balises d'hôte sont principalement utilisées pour le filtrage dans les Réponse aux vulnérabilités règles d'affectation et de groupe de vulnérabilité. Ils sont affichés dans le formulaire Élément détecté.

Remarque : L'intégration de la Qualys liste d'hôtes doit être exécutée avant la création de règles Réponse aux vulnérabilités de tâche d'affectation ou de rattrapage afin que toutes les balises puissent être présentes dans les règles et avant que les éléments vulnérables ne soient importés et regroupés.

- Le stockage des balises n'est pas sensible à la casse. Si une balise **San Diego** est créée, une balise **SAN DIEGO** ne peut pas être stockée dans la table de balises Host. 'San Diego' et 'SAN DIEGO' sont considérés comme étant la même balise d'hôte. La balise qui a été importée en premier gagne.
- L'utilisation de balises d'hôte en tant que clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises hôtes sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises hôtes sont contrôlées par la propriété système globale **sn_vul.import_host_tags**. Cette propriété est définie sur vrai par défaut. La désactivation des balises les désactive dans toutes les instances.

Les balises d'hôte (également appelées balises d'actif) sont utilisées pour organiser et suivre les actifs de votre organisation. Vous pouvez affecter des balises à vos ressources hôte. Ensuite, lors du lancement des analyses, vous pouvez sélectionner des balises associées aux hôtes que vous souhaitez analyser. Le module Balises d'hôte vous permet de télécharger des données de balises d'hôte Qualys vers votre instance de manière planifiée.

Rouvrir les éléments vulnérables résolus non fermés par les analyses

Les éléments vulnérables définis sur « Résolu » dans votre Now Platform instance, mais pas sur « Fermé/Résolu » par l'exécution de l'intégration tierce, sont rouverts s'ils sont détectés lors des nouvelles analyses.

Pour Qualys les détections, si le scanner continue de trouver des VI qui ont été définis comme « Résolu » mais qui ne sont pas passés à « Fermé/Fixe » par les analyses suivantes, ces VI reviennent à « Ouvert » lorsque la dernière date trouvée est ultérieure à la date de résolution.

Limites de la récupération de données

Par défaut, il n'y a aucune restriction sur la façon dont les données sont extraites à partir de Qualys. De nombreux enregistrements peuvent être liés à des vulnérabilités de faible gravité qu'un client n'est pas disposé à corriger à l'aide de son processus Vulnerability Response. La mise à jour des paramètres correspondants du message/de la méthode REST peut modifier ce comportement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le message/la méthode REST responsable de cette mise à jour est **Qualys Host Detection – Standard/post**. Pour mettre à jour les valeurs, ajoutez un nouveau paramètre de requête HTTP à la méthode post avec les valeurs suivantes :

- Nom : gravités
- Valeur : 3-5 (ou toute autre gravité appropriée souhaitée)

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Information associée

Messages REST Qualys

Se préparer à la Qualys Vulnerability Integration

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Il est essentiel que vous prépariez l'intégration en effectuant ces procédures. L'suppose Qualys Vulnerability Integration que vous connaissez et exécutez les analyses Qualys Cloud Platform dans votre environnement.

Remarque : Apportez les modifications de configuration nécessaires en fonction de vos besoins avant d'exécuter les intégrations.

Conditions préalables importantes

Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service et assistance client.

Utilisez le filtrage pour limiter le nombre d'éléments pour l'importation initiale et phaser votre déploiement en ajustant les filtres dans les importations ultérieures.

Les Qualys scanners sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Ré-analyse** n'est pas disponible.

Mesures à prendre

- Déterminez une date de début initiale pour les intégrations **d'importation de liste de détection d'hôte** .

  Envisagez de définir le champ **Heure de début** sur quelques heures ou quelques jours dans le passé. Idéalement, choisissez la date de la dernière analyse Qualys. La date de début peut inclure les vulnérabilités découvertes avant d'utiliser la solution de gestion des vulnérabilités. Définissez l'heure de début la plus proche utilisée pour le début de votre cycle d'analyse. Donc, s'il faut une semaine avant que tous les hôtes ne soient analysés, définissez cette valeur sur une semaine avant cette heure.

- Ajoutez des utilisateurs aux rôles administrateur, sn_vuln.admin et sn_vul_qualys.admin. Pour plus d'informations, reportez-vous à la section Affecter un rôle à un utilisateur .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.
- Si vous n'utilisez pas de calculateurs de vulnérabilité, Désactiver le calculateur de vulnérabilité par défaut s'il n'est pas utilisé, en plus de tous les autres que vous avez définis. Les calculateurs de vulnérabilité s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est créé ou mis à jour, ce qui peut avoir un impact sur les performances d'importation initiales.
- Lors de l'importation initiale des enregistrements, certaines règles métier liées aux notifications peuvent entraîner la génération de nombreuses notifications, ce qui a un impact sur les performances. Avant votre importation initiale, désactivez les règles métier.
- Si vous souhaitez utiliser un scanner différent de celui par défaut de Qualys, reportez-vous à la section Configuration des dispositifs de scanner.
- Munissez-vous de l'URL de votre serveur Qualys et de vos informations d'authentification. Les informations d'identification doivent fournir les autorisations nécessaires pour récupérer les informations de connaissances, d'analyse et de détection pour un abonnement Qualys.
- Si vous prévoyez d'utiliser des balises d'hôte dans Réponse aux vulnérabilités les règles d'affectation ou de groupe de vulnérabilité, assurez-vous que l'intégration de la liste d'hôtes Qualys a été exécutée avant de créer des règles.

Installer Qualys Vulnerability Integration

Avant d'exécuter le Qualys Vulnerability Integration dans votre instance, vous devez installer et configurer l'application Qualys Vulnerability Integration . Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Rôle requis : admin pour télécharger et installer l'application

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
Obtenez des autorisations pour l'application Qualys Vulnerability Integration et téléchargez-la sur votre Now Platform® instance.	Si l'application n'est pas déjà téléchargée sur votre instance, reportez-vous à la section .
Préparez-vous pour l'intégration.	Consultez Se préparer à la Qualys Vulnerability Integration.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.

   Après quelques instants, les applications disponibles pour installation sur votre instance s'affichent.

2. Localisez la Qualys Vulnerability Integration vignette et cliquez sur **Installer**.
3. Suivez les instructions de l'assistant de configuration.
   Pour en savoir plus sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.
4. Accédez à **Configuration d'intégration>Intégrations de scanner dans l'Assistant** de configuration pour poursuivre la configuration.
   Pour plus d'informations sur la complémentarité des invites fournies dans l'Assistant de configuration, reportez-vous à la section Configurer l'utilisation de l'assistant de Qualys Vulnerability Integration configuration.

Que faire ensuite

Activez les scanners car ils sont inactifs par défaut dans l'application Réponse aux vulnérabilités . Pour plus d'informations sur l'activation des Qualys scanners, reportez-vous à la section Activer les Qualys scanners.

Activer les Qualys scanners

Vous devez activer les scanners après l'installation car Qualys Vulnerability Integration les scanners sont désactivés par défaut dans l'application Réponse aux vulnérabilités .

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Ré-analyse** n'est pas disponible.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Localisez le produit de scanner que vous souhaitez activer et sélectionnez l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher **Activé**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Mettre à jour**.
5. Le produit que vous avez activé s'affiche dans le champ **Source** sur un élément vulnérable et des enregistrements de tâche de rattrapage après la prochaine importation, et **l'action Analyser de nouveau** est disponible.

Composants installés avec l' Qualys Vulnerability Integration

Les rôles, tâches d'intégration et tables suivants sont installés avec le Qualys Vulnerability Integration.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Afficher les listes filtrées pour les composants installés avec une application

Filtrez la table Fichiers d'applications afin que seuls les rôles, les travaux planifiés et les tables installés avec une application s'affichent. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés sur l'instance et dans la table de métadonnées. Procédez comme suit pour afficher les listes filtrées à partir de la table Fichiers d'applications.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application. Par exemple : **Application** > **est** > **Réponse aux vulnérabilités**.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, sélectionnez **ET**, puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
sn_vul_qualys.read	Dispose d'un Qualys Vulnerability Integration accès en lecture aux enregistrements.	
sn_vul_qualys.utilisateur	Utilisateur pour Qualys Vulnerability Integration. Peut lire et écrire des enregistrements	sn_vul_qualys.read
sn_vul_qualys.admin	Administrateur pourQualys Vulnerability Integration. Par exemple, vous pouvez modifier les dates de début d'intégration et effectuer certains paramètres de configuration avancés.	• sn_vul_qualys.utilisateur • sn_vul.vulnerability_analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
sn_vul.configure_qualys_integration	Peut configurer l' Qualys Vulnerability Integration	sn_vul_qualys.admin

Tâches d'intégration installées

Tâche d'intégration	Description
Qualys Intégration de liste de recherches statiques	Synchronise les listes de recherche pour trouver les Qualys entrées vulnérables. Récupère uniquement les enregistrements de type liste statique.
Qualys Intégration complète de la détection d'hôte	Récupère les données d'hôte et de Qualys vulnérabilité et les traite dans votre instance. Il coordonne les appels de message REST à l'API de détection d'hôte. La sortie de cette intégration est constituée d'éléments vulnérables. Cette intégration importe tous les états de la vulnérabilité : Nouveau, Corrigé, Actif et Rouvert. Par défaut, cette intégration est inactive et s'exécute chaque semaine. **Remarque :** Une fois cette intégration activée, la tâche globale quotidienne importe uniquement les états Nouveau, Fixe et Rouvert.
Qualys Intégration de la liste d'hôtes	Récupère les données d'analyse d'hôte authentifiées et non authentifiées et les balises d'hôte une Qualys fois par semaine et les stocke dans le module Éléments détectés de votre instance. Permet d'identifier les actifs qui n'ont pas été analysés récemment.
Qualys Intégration de la détection d'hôte	Récupère les données d'hôte et de Qualys vulnérabilité et les traite dans votre instance. Il coordonne les appels de message REST à l'API de détection de liste d'hôtes. Les sorties de cette intégration sont des éléments vulnérables. Qualys Les balises hôtes sont importées dans cette intégration.
Qualys Intégration de ticket	Récupère les Qualys tickets et les ajoute à votre instance. Il coordonne les appels de message REST à l'API de liste de tickets. Il y a souvent moins de tickets que de détections d'hôte, car Qualys les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche d'intégration	Description
	paramètres peuvent limiter les détections qui aboutissent à un ticket.
Qualys Intégration de la liste des profils d'options	Récupère les profils d'option du Qualys produit. Les profils d'option incluent des paramètres d'analyse qui sont requis lorsque vous lancez des analyses à partir de votre Now Platform instance.
Qualys Intégration de la liste des dispositifs	Récupère les informations sur le dispositif de scanner à partir de Qualys.
Qualys Intégration de groupes d'actifs	Récupère les informations sur le groupe d'actifs à partir de Qualys. Les groupes de ressources sont utilisés pour identifier les dispositifs de scanner à utiliser pour analyser les éléments de configuration correspondants.
Qualys Base de connaissances (remplissage)	Récupère les entrées de la base de Qualys connaissances. Planifié pour s'exécuter après l'intégration de la détection d'hôte Qualys . Met à jour votre instance avec tous les QID qui ont été référencés dans l'intégration de la détection d'hôte, mais qui n'existaient pas dans le système.
Qualys Base de connaissances	Récupère les entrées de la base de Qualys connaissances. Les données récupérées sont basées sur la date à laquelle les vulnérabilités ont été mises à jour et Qualys depuis la dernière exécution de l'intégration. Ces données sont utiles pour renseigner les données historiques dans votre instance et pour s'assurer que les Qualys identificateurs (QID) sont à jour.
Qualys Intégration de liste de recherches dynamiques	Synchronise les listes de recherche pour trouver les Qualys entrées vulnérables et récupère les enregistrements de type liste dynamique.
Correction des détections pour la clé mise à jour pour Qualys	Une combinaison hachée de champs qui fournit un moyen d'identifier et de lier une détection à un Qualys élément vulnérable.
Qualys Mettre à jour les éléments détectés existants avec l'identificateur de partition de réseau	Met à jour vos éléments détectés existants. Les CI de vos données d'intégration de vulnérabilité existantes Qualys sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables installées

Table	Description
Vulnérabilité de la liste de recherches sn_vul_qualys_m2m_search_list_vul	Stocke le mappage entre la Qualys liste de recherche et une vulnérabilité.
Qualys Scanner de vulnérabilité sn_vul_qualys_scanner	Table qui étend les scanners de vulnérabilité pour stocker les informations du scanner pour la fonctionnalité de Qualys nouvelle analyse.
Qualys Liste de recherches sn_vul_qualys_search_list	Stocke les listes de recherche récupérées par l'intégration de la Qualys liste de recherche.
Qualys Importation du dispositif sn_vul_qualys_appliance_imp	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de la réponse est traitée directement avec le script onComplete.
Qualys CI sn_vul_qualys_ci	Table n'est plus utilisée.
Pagination de détection d'hôte sn_vul_qualys_host_detection_pagination	Table n'est plus utilisée.
Qualys Exécution de l'intégration sn_vul_qualys_integration_run	Table n'est plus utilisée.
Qualys Intégration sn_vul_qualys_integration	Table étendant l'intégration de vulnérabilité et stockant toutes les intégrations qui correspondent à Qualys.
Qualys Importation de liste de recherches statiques sn_vul_qualys_static_search_list_imp	Table étendant la ligne de jeu d'importation. Les cartes de champs sont utilisées pour transformer les données vers la table cible, Qualys les listes de recherche.
Qualys Base de connaissances sn_vul_qualys_knowledge_base	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de la réponse est traitée directement avec le script onComplete.
Qualys Liste des tickets sn_vul_qualys_ticket_list_imp	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de la réponse est traitée directement avec le script onComplete.
Qualys Profil d'option sn_vul_qualys_option_profile	Table stockant les profils d'option récupérés à partir de Qualys. Cette table est utilisée avec la nouvelle analyse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Qualys Importation de liste de recherches dynamiques sn_vul_qualys_dynamic_search_list_imp	Table étendant la ligne de jeu d'importation. Les cartes de champs sont utilisées pour transformer les données vers la table cible, Qualys les listes de recherche.
Qualys Réexécution du jeu d'importation sn_vul_qualys_import_rerun	Table n'est plus utilisée.
Qualys Importation du profil de l'option sn_vul_qualys_option_profile_import	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de la réponse est traitée directement avec le script onComplete.

Mettre à jour les éléments de configuration avec l'identificateur de partition de réseau pour le Qualys Vulnerability Integration

Créez des éléments de configuration (CI) uniques pour les actifs de votre environnement qui partagent des adresses IP. Identifiez les actifs distincts dans votre environnement et mettez automatiquement à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous donner plus de détails sur vos vulnérabilités.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Par défaut, dans l'application Réponse aux vulnérabilités , l'adresse IP est l'un des moyens d'identifier vos actifs. Dans certains cas, les actifs peuvent partager des adresses IP, mais ils sont stockés en tant que CI unique dans votre CMDB.

Par exemple, comme le montrent les tables suivantes, plusieurs actifs (CI) de votre environnement peuvent partager des adresses IP, mais ont des ID de réseau et de référentiel uniques. Toutefois, par défaut, ces ressources sont généralement identifiées et stockées comme un seul CI `(CI 1)` lors de la recherche d'adresse IP.

Recherche d'adresses IP et création de CI par défaut

Source	Adresse IP	NETWORK_ID	Élément de configuration
Qualys Vulnerability Integration: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	Adresse IP	REPOSITORY_ID	Élément de configuration
Qualys Vulnerability Integration: Intégrations d'actifs	123.12.12.141	12	CI 1

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Source	Adresse IP	REPOSITORY_ID	Élément de configuration
et de vulnérabilités fixes et ouvertes			
	123.12.12.141	13	CI 1

Vous pouvez créer des CI individuels pour les actifs qui ont la même adresse IP afin de pouvoir les identifier en tant qu'actifs distincts. À partir d'une importation de données actualisée, vous pouvez mettre à jour vos CI existants avec une plus grande granularité incluant l'identificateur de partition de réseau [network_partition_identifier] en exécutant la tâche planifiée. *Update existing discovered items with network partition identifier*

Cette tâche planifiée est désactivée par défaut. Activez cette fonctionnalité pour les intégrations d'actifs et de vulnérabilités Qualys Vulnerability Integration fixes et ouvertes dans l'assistant de configuration afin d'afficher cet identificateur dans vos enregistrements.

Lorsqu'elle est activée, cette tâche planifiée ajoute l'identificateur de partition de réseau [network_partition_identifier] aux enregistrements de CI existants à partir des données importées. Les CI existants créés par l'IRE sont également mis à jour. La tâche planifiée crée également des CI qui incluent l'identificateur de partition de réseau à partir de la prochaine importation. Vous pouvez également lancer la tâche à la demande pour mettre à jour vos données existantes.

À partir des versions 14.0 et Réponse aux vulnérabilités 12.1 de l'intégration Qualys Vulnerability Integration de vulnérabilité, les modèles de classe CI CMDB (1.0.21.) sont pris en charge. Les modèles de classe ont l'identificateur de partition de réseau [network_partition_identifier] dans les règles d'identification Identification et rapprochement (IRE).

Option	Description
Exécutez les travaux planifiés sur demande.	Mettez à jour vos éléments détectés existants. Les CI de vos données existantes Qualys Vulnerability Integration sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau. Les éléments détectés, les éléments vulnérables et les enregistrements de détection sont tous mis à jour avec les nouveaux CI.
Attendez les importations de données fraîches des intégrations avec les prochains travaux planifiés.	Créez des CI pour chaque nouvel actif à l'aide de l'identificateur de partition de réseau en commençant par la tâche planifiée suivante. Les enregistrements de CI, d'élément vulnérable et de détection sont tous mis à jour pour inclure la nouvelle granularité. De nouveaux CI sont créés lorsqu'aucune correspondance exacte n'est trouvée.

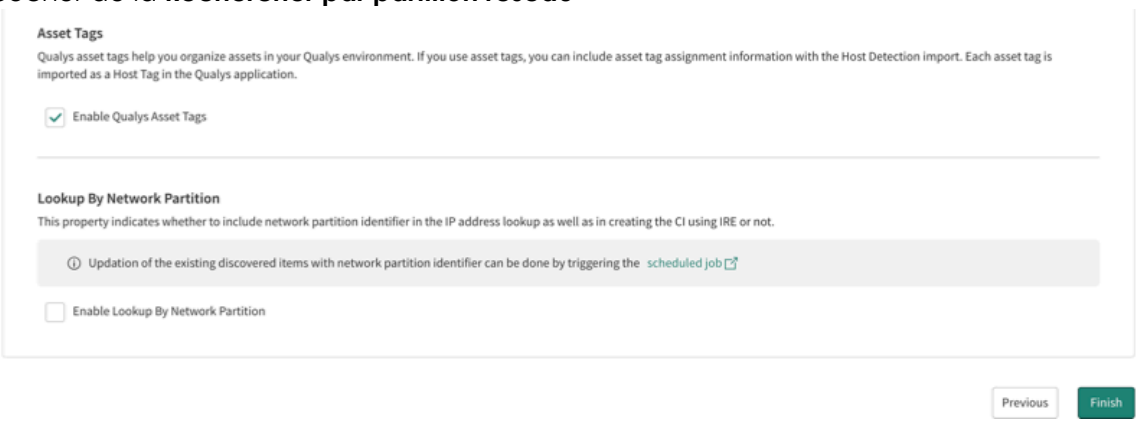
Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
2. Choisissez Qualys Vulnerability Integration.
3. **Modifiez** l'intégration requise.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Choisir **Configuration de la détection d'hôte**.
5. Choisir **Activer la recherche par partition de réseau** case à cocher de la **Rechercher par partition réseau**



section.

6. Cliquez sur **Terminer**.

Les identificateurs de partition de réseau NETWORK_ID et REPOSITORY _ID inclus dans la recherche d'adresses IP et la création de CI

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Éléments CI : actifs avec identificateur de partition de réseau
Qualys Vulnerability Integration: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Source	Adresse IP	REPOSITORY_ID	CI pour les actifs sans identificateur de partition de réseau	Éléments CI : actifs avec identificateur de partition de réseau
Qualys : Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Les règles de recherche d'identification CI d'adresse IP et d'adresse IP incomplète incluent automatiquement l'attribut d'identificateur de partition de réseau pour une importation de données à partir des intégrations d'actifs et de vulnérabilités fixes et ouvertes pour Qualys Vulnerability Integration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après avoir activé la tâche planifiée et enregistré les enregistrements, vous pouvez également mettre à jour vos éléments détectés existants avec des CI qui incluent l'identificateur de partition de réseau en lançant les travaux planifiés sur demande. Les CI de vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection sont automatiquement mis à jour.

Modifications Qualys facultatives

Configurez les modifications facultatives et rationalisez certaines données spécifiquement pour l'intégration Qualys.

Vous pouvez réinitialiser cette date de début dans l'Assistant réglages ou à partir de l'intégration principale, ou modifier les règles métier pour les désactiver lors d'une importation initiale.

Désactiver les règles métier liées à la notification avant l'importation initiale de l'enregistrement

Lors de l'importation initiale des enregistrements, certaines règles métier liées aux notifications peuvent générer de nombreuses notifications, ce qui a un impact sur les performances. Ces règles métier doivent être modifiées pour les désactiver lors de l'importation.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la**Tout** > **Définition du système** > **Règles métier**.
2. **Recherchez les notifications de CI affectés**.
3. Ouvrez la règle métier et insérez cette condition : `current.sys_class_name != « sn_vul_vulnerable_item »`.
4. Cliquez sur **Mettre à jour**.
5. Répétez cette procédure pour les règles métier suivantes :
   - Notifications des centres de coûts affectés
   - Notifications des groupes affectés
   - Notifications d'emplacements affectés

Remarque : Une fois l'importation d'enregistrement initiale terminée, vous pouvez réactiver ces règles métier. Cependant, envisagez de les laisser handicapés. Elles peuvent générer un grand nombre de notifications et avoir un impact sur les performances de votre instance.

Modifier une date de début initiale

Lors de l'installation à l'aide de l'Assistant de configuration, vous définissez une date de début initiale pour les intégrations Qualys. Vous pouvez réinitialiser cette date de début dans l'Assistant de configuration ou à partir de l'intégration principale, comme indiqué ci-dessous.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
2. Cliquez sur **Qualys Host Detection Integration**.
3. Cliquez sur **Détails de l'intégration**.
4. Définissez le champ **Heure de début** sur une valeur passée, de sorte que toutes les vulnérabilités analysées et détectées depuis cette heure soient détectées.

   Si vous avez configuré Qualys à l'aide de l'Assistant de configuration, le champ **Heure de début** est pré-rempli, initialement jusqu'à trois mois avant la date d'aujourd'hui, puis jusqu'à la date d'aujourd'hui.

   Remarque : Envisagez de définir la valeur à un maximum d'un mois dans le passé. Cela permet d'éviter qu'une grande quantité de données ne dépasse les limites de débit de l'API Qualys et de déclencher des délais d'exécution.

5. Cliquez sur **Envoyer** ou **Mettre à jour**.
6. Facultatif : Cliquez sur **Exécuter maintenant** pour l'exécuter immédiatement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurations et modifications avancées de Qualys

Configurez les modifications facultatives avancées et rationalisez certaines données spécifiquement pour l'intégration Qualys. La plupart de ces modifications nécessitent un codage ou une expertise avancée ServiceNowQualys Cloud Platform .

Modifier les valeurs de mappage de priorité et d'état Qualys vers ServiceNow

Modifiez les valeurs de mappage pour la priorité et l'état en fonction de vos besoins.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Il s'agit d'une option de personnalisation avancée.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Règles métier**.
2. **Recherchez Mapper les valeurs Qualys** et ouvrez-le.
3. Cliquez sur l'onglet **Avancé** .
4. Modifiez selon vos besoins.
   Les modifications les plus courantes incluent l'ajout de nouvelles valeurs d'état ou la révision de la criticité ou de la priorité.
5. Cliquez sur **Mettre à jour**.

Restreindre la possibilité d'écrire dans un enregistrement en fonction d'un groupe d'affectation

Vous pouvez restreindre les droits d'écriture/lecture sur les enregistrements en fonction de l'appartenance à un groupe affecté. Modifiez les conditions et le script en fonction des besoins spécifiques.

Avant de commencer
Rôle requis : security_admin (rôle élevé à partir de l'administrateur)

Remarque : Cette action est effectuée dans le périmètre de vulnérabilité.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Contrôle d'accès (ACL)**.
2. Recherchez les ACL commençant par `sn_vul`.
3. Choisissez un enregistrement de contrôle d'accès, par exemple, `sn_vul_vulnerable_item`, **Opération d'écriture**.
4. Cochez la case **Avancé** dans l'enregistrement, si nécessaire, pour afficher les entrées de **rôle** .
5. Modifiez le script de **rôle** en fonction de vos besoins.
   Script : Exemple de modification d'un accès par groupe.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
return result;
}
```

6. Cliquez sur **Mettre à jour**.

Configurer des dispositifs de scanner

Si vous lancez des analyses à partir de votre Now Platform® instance plutôt que directement à partir de Qualys, vous pouvez configurer des analyses pour les plages d'adresses IP.

Avant de commencer

Les données proviennent de l'intégration basée sur Qualys les Qualys groupes d'actifs et leurs dispositifs par défaut associés (scanners).

Si aucun dispositif n'est configuré pour les plages d'adresses IP ciblées, l'appliance définie par défaut pour l'instance d'intégration est utilisée pour l'analyse.

Rôle requis : sn_vul_qualys.admin

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Dispositifs de scanner**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom du dispositif	Vous êtes invité à remplir ce champ lorsque vous créez un enregistrement manuellement. Entrez le nom du dispositif de Qualys scanner à utiliser pour l'appel d'analyses afin de faire correspondre les éléments de configuration. Utilisez la valeur `Externe` lorsque vous souhaitez que l'analyse soit lancée avec un scanner externe.
ID du dispositif	Entrez l'identificateur du dispositif de Qualys scanner à utiliser pour appeler des analyses pour établir une correspondance avec les éléments de configuration. Vous êtes invité à remplir ce champ lorsque vous créez un enregistrement manuellement. Utilisez la valeur `0` lorsque vous souhaitez que l'analyse soit lancée avec un scanner externe.
États des dispositifs	Affiche le dernier état du dispositif de scanner sur les données retournées par l'intégration Qualys . Pour les enregistrements créés manuellement, l'état n'est mis à jour que si un **ID de dispositif** valide est spécifié.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID du groupe de ressources	Affiche l'identificateur du Qualys groupe de ressources qui a créé cet enregistrement. Ce champ affiche une valeur uniquement pour les enregistrements créés par l'intégration Qualys .
Nom du groupe de ressources	Affiche le nom du Qualys groupe de ressources qui a créé cet enregistrement. Ce champ affiche une valeur uniquement pour les enregistrements créés par l'intégration Qualys .
Ordre	Entrez une valeur à utiliser pour déterminer la priorité d'analyse. Pour les dispositifs présentant des critères contradictoires, une solution avec une valeur d'ordre inférieure se voit accorder une priorité plus élevée.
Créés manuellement	Indique si cet enregistrement a été créé manuellement par l'utilisateur.
Utiliser un groupe de filtres	Cochez cette case pour spécifier un groupe de filtres afin de trouver les éléments de configuration correspondants pour l'analyse.
Groupe de filtres	Sélectionnez le groupe de filtres que vous souhaitez utiliser pour trouver les éléments de configuration correspondants pour l'analyse. Ce champ s'affiche uniquement si vous avez sélectionné **Utiliser un groupe de filtres**.
IP	Liste séparée par des virgules d'adresses IP ou de plages d'adresses IP à utiliser par ce dispositif lors de l'appel d'analyses.
Instance d'intégration	Instance d'intégration Qualys associée à ce dispositif.
Profil d'option	Sélectionnez le profil d'option que vous souhaitez utiliser pour les analyses visant à établir une correspondance avec les éléments de configuration.

3. Cliquez sur **Mettre à jour**.

Configurer et gérer Qualys les scanners et analyses de vulnérabilité

Qualys Les analyses de vulnérabilité peuvent être effectuées pour trouver les vulnérabilités logicielles qui affectent vos CI. Vous pouvez lancer des analyses à partir d'un enregistrement d'élément vulnérable ou en créant un enregistrement d'analyse directement pour les éléments de configuration (CI) et les adresses IP.

Si vous numérisez Qualys des éléments vulnérables directement à partir de l'écran Éléments vulnérables, vous avez également la possibilité d'analyser plusieurs éléments vulnérables en même temps.

Si Réponse aux incidents de sécurité elle est activée, vous pouvez également lancer une analyse à partir du catalogue des incidents de sécurité, d'un enregistrement d'incident de sécurité ou d'une demande d'analyse de sécurité.

Les analyses soumises à partir d'éléments vulnérables, d'incidents de sécurité ou de demandes d'analyse QualysCatalogue des incidents de sécuritéde sécurité sont effectuées par le scanner par défaut Qualys .

Vous pouvez sélectionner le profil d'option que vous souhaitez utiliser pour les analyses afin de faire correspondre les éléments de configuration.

- Les profils d'option contiennent Qualys des paramètres d'analyse.
- Un profil d'option est requis lorsque vous lancez une Qualys analyse à partir de votre Now Platform®fichier .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'analyse IP initiée Qualys par ServiceNow

Le Qualys scanner inclus avec le système de base fournit une intégration de base de référence pour lancer des analyses en fonction des adresses IP.

Avant de commencer

Vous pouvez sélectionner le profil d'option que vous souhaitez utiliser pour les analyses afin de faire correspondre les éléments de configuration.

- Les profils d'option contiennent Qualys des paramètres d'analyse.
- Un profil d'option est requis lorsque vous lancez une analyse Qualys à partir de votre Now Platform®fichier .

Rôle requis : sn_vul_qualys.admin

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Ouvrez l'enregistrement Qualys .
3. Cochez les cases**Actif** et **Par défaut** .

   Sélectionner **Actif** est nécessaire pour utiliser le Qualys scanner afin d'analyser Qualys automatiquement les VI. Vous n'avez pas non plus besoin de sélectionner **Par défaut** pour qu'il s'exécute automatiquement.

   Avant la version 12.0, **Active** est requis pour utiliser l'analyseur. Si **l'option Par défaut** est également sélectionnée, le scanner est automatiquement utilisé sans qu'il soit nécessaire de le sélectionner pendant la numérisation.

4. Pour le champ Intégration source, cliquez sur l'icône de recherche et sélectionnez l'option pour **Qualys**, par exemple, **Qualys Cloud Platform**.
5. Cliquez sur **Mettre à jour**.
6. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
7. **Ouvrez l'intégration de la liste des groupes de ressources Qualys**.
   a. Sélectionnez la case à cocher **Activé**.
   b. Cliquez sur **Exécuter maintenant**.
8. Procédez comme suit pour renseigner vos dispositifs de scanner.

> **Remarque :** Il est peut-être préférable d'exécuter l'intégration de la liste de profils d'options après une importation à partir des intégrations de listes de recherches, de la liste de recherche dynamique Qualys et des intégrations de listes de recherches statiques Qualys, afin de voir quelles listes de recherches sont associées aux profils d'options.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Ouvrez **l'intégration de la liste des profils d'options Qualys**.

b. Sélectionnez la case à cocher **Activé**.

c. Cliquez sur **Exécuter maintenant**.

d. Suivez les étapes répertoriées dans Configurer des dispositifs de scanner pour configurer vos dispositifs de scanner.
Revenez ici une fois que vous avez terminé ces étapes pour poursuivre la configuration.

e. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.

f. Ouvrez **l'intégration de la liste des dispositifs Qualys**.

g. Sélectionnez la case à cocher **Activé**.

h. Cliquez sur **Exécuter maintenant**.
Vos Qualys dispositifs de scanner sont maintenant correctement remplis.

Information associée

Présentation de Qualys Vulnerability Integration

Analyser plusieurs Qualys vulnérabilités ou éléments vulnérables

Vous pouvez analyser simultanément plusieurs Qualys vulnérabilités ou éléments vulnérables qui contiennent au moins un élément de configuration (CI) affecté ou une adresse IP renseignée sur le formulaire.

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Effectuez l'une des actions suivantes :
   - Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
   - Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tous les éléments vulnérables**.
2. Cochez les cases des enregistrements que vous souhaitez numériser.
3. Cliquez sur la liste **Actions sur les lignes sélectionnées** , puis cliquez sur **Analyser à nouveau pour les éléments vulnérables**.
   Un message s'affiche avec un lien vers l'analyse et les notes de travail sont mises à jour.
4. Cliquez sur le lien pour afficher la progression ou les résultats de l'analyse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'analyse automatique pour les Qualys tâches de rattrapage résolues

Vous pouvez planifier l'analyse qui s'exécute automatiquement pour mettre à jour vos Qualys éléments vulnérables.

Avant de commencer

Lorsqu'une tâche de rattrapage est passée à **l'état Résolu**, une analyse est lancée automatiquement pour mettre à jour l'état des éléments vulnérables associés.

- L'analyse est désactivée par défaut.
- Activez l'analyse avec le **paramètre d'instance** d'intégration scan_on_resolved dans l'enregistrement **Qualys** situé à **Tout** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration** > **Qualys**. Consultez les étapes suivantes pour plus d'informations.
- Cette analyse est spécifique à l'instance. Si vous disposez de plusieurs instances et que vous souhaitez activer ou désactiver cette analyse, vous devez désactiver le paramètre **scan_on_resolved** dans les paramètres d'instance d'intégration de chaque instance que vous souhaitez modifier.
- Lorsque l'analyse est activée, vous pouvez la lancer à la demande ou planifier l'exécution de l'analyse uniquement dans une fenêtre de temps spécifiée. Reportez-vous à la rubrique Configurer Qualys les nouvelles analyses pour qu'elles s'exécutent uniquement dans les intervalles planifiés pour savoir comment définir les heures de début et de fin de la fenêtre horaire.

Rôle requis : sn_vul_qualys.admin

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Administration** > **Instances d'intégration**.
2. Sélectionnez **Qualys** pour ouvrir l'enregistrement.
   Les paramètres de l'instance d'intégration sont Qualys affichés dans un onglet.
3. Pour activer l'analyse automatique, localisez le *scan_on_resolved* paramètre.
4. Dans la colonne Valeur de la propriété, saisissez `vrai`.
5. Cliquez sur **Mettre à jour**.

Configurer Qualys les nouvelles analyses pour qu'elles s'exécutent uniquement dans les intervalles planifiés

Pour l'intégration Qualys de vulnérabilité, définissez les paramètres d'heure de début et de fin de l'analyse de sorte que les nouvelles analyses s'exécutent ou ne soient disponibles que pendant les heures souhaitées.

Avant de commencer

Cette configuration s'applique à la fois aux réanalyses planifiées et aux nouvelles analyses que vous lancez manuellement dans le Qualys produit à partir de votre Now Platform® instance.

La définition des paramètres d'heure de début et de fin d'analyse pour les instances d'intégration vous permet de spécifier des fenêtres de temps lorsque de nouvelles analyses sont disponibles dans le Qualys produit. Par exemple, vous pouvez préférer spécifier que les nouvelles analyses ne sont disponibles qu'en dehors des heures de travail, par exemple, de minuit à 10 heures.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce paramètre est spécifique à l'instance. Si vous disposez de plusieurs instances, vous devez configurer les valeurs scan_start_time et scan_end_time dans les paramètres d'instance d'intégration de chaque instance que vous souhaitez modifier.

Rôle requis : sn_vul_qualys.admin

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration** > **Qualys**.
2. Cliquez sur **Qualys** pour ouvrir l'enregistrement.
   Les paramètres de l'instance d'intégration pour Qualys sont affichés.
3. Pour le paramètre scan_start_time, dans la colonne Valeur, entrez l'heure dans le fuseau horaire UTC au format 24 heures (00:00 à 24:00) pour l'heure de début de la fenêtre pour laquelle vous souhaitez que de nouvelles analyses soient disponibles.
4. Pour le scan_end_time, dans la colonne Valeur, entrez les heures au même format (00:00 à 24:00) pour l'heure de fin de la fenêtre disponible.
   Par exemple, si vous entrez une heure de début de 00h00 pour le paramètre de scan_start_time et une scan_end_time de 10h00 le matin même, les analyses planifiées ou lancées manuellement en dehors de la fenêtre horaire de minuit à 10h sont mises en file d'attente et lancées à l'heure de début de la fenêtre horaire du lendemain, 00h00.

   Dans le même exemple, si un propriétaire de rattrapage lance manuellement une nouvelle analyse à 11h00, la nouvelle analyse n'est pas immédiatement lancée, car elle se trouve en dehors des heures d'analyse configurées disponibles. La demande d'analyse reste en file d'attente jusqu'au début de la fenêtre horaire du jour suivant, dans cet exemple (00:00).
5. Cliquez sur **Mettre à jour** pour enregistrer vos paramètres.

Qualys Limites des taux d'analyse de vulnérabilité

Vous pouvez définir la fréquence à laquelle différents types d'analyses sont effectués pour limiter le nombre de demandes envoyées à un scanner externe. Une fois que vous avez défini des limites de débit, vous pouvez les appliquer aux Qualys scanners.

Définir les Qualys limites de taux d'analyse

Vous pouvez définir la fréquence à laquelle différents types d'analyses sont effectués pour équilibrer la charge dans votre file d'attente d'analyse. Les conditions définies dans la limite de taux déterminent si les limites de taux sont appliquées aux entrées en file d'attente.

Avant de commencer

Rôle requis : sn_vul.admin

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Définitions de limite d'évaluation**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définition de limite de taux

Champ	Description
Nom	Fournissez un nom descriptif qui identifie les conditions que l'entrée de file d'attente doit remplir. Par exemple, analyses par minute
Conditions de la file d'attente	Entrez les conditions utilisées pour déterminer si une entrée d'analyse en file d'attente est soumise à cette limite de taux. Les conditions ne doivent pas être spécifiques à un scanner particulier.
Script d'évaluation	Écrivez un script avec la logique pour évaluer l'entrée en file d'attente. Il est important que le script retourne vrai/faux pour définir si l'entrée est traitée. En outre, basez le script d'évaluation sur l'entrée en file d'attente évaluée.

4. Cliquez sur **Envoyer**.

Appliquer des limites de taux d'analyse aux Qualys scanners

Une fois que vous avez défini des limites de taux d'analyse à l'aide **de définitions de limite de débit**, vous pouvez appliquer des limites de taux à des scanners spécifiques Qualys .

Avant de commencer

Rôle requis : sn.vul_admin

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Limites de taux des analyseurs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Limite de taux du scanner

Champ	Description
Scanner	Sélectionnez le scanner auquel vous souhaitez appliquer une limite de taux.
Limite du taux	Sélectionnez la limite de taux que vous souhaitez appliquer à ce scanner.
Seuil	Entrez le seuil auquel vous souhaitez soumettre le scanner sélectionné pour la limite de taux sélectionnée. Par exemple, si le scanner autorise 4 analyses par minute et que la limite de débit est définie comme requêtes par minute, le seuil sera 4.

4. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher la file d'attente de l'analyse de Qualys vulnérabilité

Les demandes d'analyse de vulnérabilité soumises à l'intégration de l'analyse des vulnérabilités sont mises en file d'attente Qualys afin de ne pas surcharger les ressources système. Vous pouvez afficher l'état des demandes en file d'attente, selon les besoins.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche
Dans la liste des analyses en file d'attente, chaque analyse comprend un nom d'analyse généré automatiquement qui identifie le CI qui a été analysé.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **File d'attente de l'analyse**.
   Toutes les Qualys demandes d'analyse qui ont été soumises sont affichées dans une liste. La colonne **État** affiche l'état actuel de chaque entrée en file d'attente. Un état **Terminé** indique que l'analyse a quitté la file d'attente. Cela n'indique pas nécessairement que le traitement de l'analyse est terminé. Lorsque les analyses ont été terminées ou si elles ont échoué, la colonne **Traitement** affiche le texte des notes de travail approprié.

   Remarque : Si une valeur de hachage a été soumise à l'analyse et que le scanner ne parvient pas à trouver un résultat, **l'état** indique **Terminé** et la note de travail dans la colonne **Traitement** indique **Inconnu**.

2. Une fois le traitement d'une analyse terminée, cliquez sur un enregistrement en file d'attente pour afficher les détails de la demande d'analyse.

Activer le filtre du système de base pour les importations de détection confirmées

Activez un filtre par défaut utilisant des paramètres d'intégration pour importer uniquement les détections confirmées à partir de Qualys Cloud Platform.

Avant de commencer
Rôle requis : sn_vul_qualys.admin, sn_vul.vr_import_admin

Pourquoi et quand exécuter cette tâche
Un paramètre d'instance d'intégration du système de base « include_only_confirmed » est disponible pour importer une liste filtrée de détections à partir de .Qualys Cloud Platform Par défaut, ce paramètre est défini sur *FAUX* et toutes les détections, qu'elles soient potentielles, confirmées ou informatives, sont importées.

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Administration** > **Instances d'intégration**.
2. Ouvrez Qualys Cloud Platform Integration à partir de la liste Instances d'intégration.
3. Dans la liste Paramètres de l'instance d'intégration, ouvrez le paramètre «*include_only_confirmed*».

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Mettez à jour la valeur par défaut sur *Vrai*.
5. Cliquez sur **Mettre à jour**.
   Vous avez activé le filtre pour importer les détections confirmées à partir de l'intégration Qualys Cloud Platform .

Résultats

Par défaut, seules les détections confirmées à partir de l'intégration Qualys Cloud Platform sont importées lors de l'exécution de la prochaine importation de vulnérabilité Qualys. Toutes les autres détections, qu'elles soient informatives ou potentielles, sont ignorées et ne sont pas importées. Pour plus d'informations, consultez Afficher les données de détection d'éléments vulnérables de Vulnerability Response.

Lancer une nouvelle analyse pour le Qualys Vulnerability Integration

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans le Qualys produit à partir de votre Now Platform application à la demande.

Avant de commencer

Vous pouvez lancer de nouvelles analyses à partir des espaces de travail Vulnerability Response. Pour plus d'informations, consultez Analyser à nouveau les enregistrements et les tâches de rattrapage dans Vulnerability Manager Workspace et Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT.

Pour les nouvelles analyses dans l'environnement classique, consultez les sections suivantes pour savoir comment lancer de nouvelles analyses.

Configuration requise pour les nouvelles analyses dans le Qualys produit lancées à partir de votre Now Platform:

Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Qualys produit à partir de votre Now Platform® instance.

Pour aider à réduire les frais généraux et le volume impliqués par les analyses complètes planifiées, les responsables des rattrapages, les spécialistes informatiques, les analystes de vulnérabilité ou les gestionnaires de vulnérabilités peuvent lancer de nouvelles analyses ciblées sur demande pour des vulnérabilités spécifiques sur des actifs (éléments de configuration) dans leurs environnements. Vous pouvez lancer de nouvelles analyses dans le Qualys produit à partir d'enregistrements d'éléments vulnérables (VI), de tâches de rattrapage (RT), d'entrée tierce (TPE) ou d'éléments détectés depuis votre Now Platform instance.

Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, vos correctifs et vos autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Cas d'utilisation:

À titre d'exemple, supposons que l'ensemble de votre environnement soit analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été effectuée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines la prochaine analyse planifiée pour vérifier qu'elle a été corrigée. Pour vérifier que votre correctif corrige avec succès une vulnérabilité critique détectée lors d'une analyse précédente, vous pouvez lancer une nouvelle analyse ciblée à partir de votre Now Platform recherche Qualys d'éléments vulnérables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez lancer de nouvelles analyses pour les VI dont la source se trouve Qualys dans des états autres que Fermé. Consultez Analyser à nouveau les enregistrements et les tâches de rattrapage dans Vulnerability Manager Workspace et Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT.

Vérifiez que vous avez terminé la configuration suivante, requise pour les nouvelles analyses. Pour plus d'informations, reportez-vous aux étapes commençant par Configurer et gérer Qualys les scanners et analyses de vulnérabilité répertoriés dans les sections précédentes.

Rôle requis : sn_vul_manually_initiate_rescan

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Vous ne pouvez lancer de nouvelles analyses que pour les VI dont Qualys la source est la source. Verify Qualys s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le Créateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue Liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône**Personnaliser la liste** (icône Engrenage) et utilisez la zone de sélection pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**, **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers**ou aux **éléments détectés** pour les enregistrements de tâche de rattrapage, d'entrée tierce ou d'éléments détectés, respectivement, que vous souhaitez utiliser pour la nouvelle analyse.

   En fonction de votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

   - Sur un enregistrement de VI unique, le VI doit provenir du Qualys produit et se trouver dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent être Qualys la source et être dans un état autre que **Fermé**.
   - Sur un enregistrement RT, la tâche de rattrapage peut être dans n'importe quel état autre que **Fermé**, et tous les VI associés doivent avoir Qualys comme source.
   - Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé dans un état autre que **Fermé** avec Qualys comme source.
   - Sur un enregistrement d'élément détecté, l'élément de configuration a au moins un VI Qualys associé comme source dans n'importe quel état autre que **Fermé**.

4. Dans l'angle supérieur droit de l'enregistrement que vous avez choisi, cliquez sur **Analyser à nouveau**.
   Dans la boîte de dialogue qui s'affiche, choisissez-en un pour continuer.

Option	Description
Cochez la case **Spécifier les profils d'option** .	Dans la liste, choisissez le profil d'option Qualys du scanner que vous souhaitez utiliser pour la nouvelle numérisation. Il s'agit des appliances (scanners) que vous avez configurées et répertoriées dans **Intégration de vulnérabilité Qualys** > **Dispositifs de scanner**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Décochez la case **Spécifier les profils d'option** (non cochée).	Le Qualys profil d'option du scanner que vous avez défini comme scanner par défaut dans la liste Dispositifs de scanner est utilisé pour l'analyse. Pour plus d'informations sur la définition des scanners par défaut que vous lancez à partir de votre Now Platform, configurez les dispositifs de scanner répertoriés dans la section précédente pour plus d'informations.

5. Cliquez sur **Demander l'analyse**.

   Un message s'affiche pour indiquer que votre analyse est en cours de traitement. L'état de toutes les nouvelles analyses peut être consulté à tout moment sous les listes connexes Analyse des enregistrements VI, RT, TPE et d'éléments détectés que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

   Votre instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine correctement ou jusqu'à l'expiration de la période de suivi définie, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de votre Now Platform nouvelle analyse a cessé, et non à la date à laquelle la nouvelle analyse elle-même s'est arrêtée.

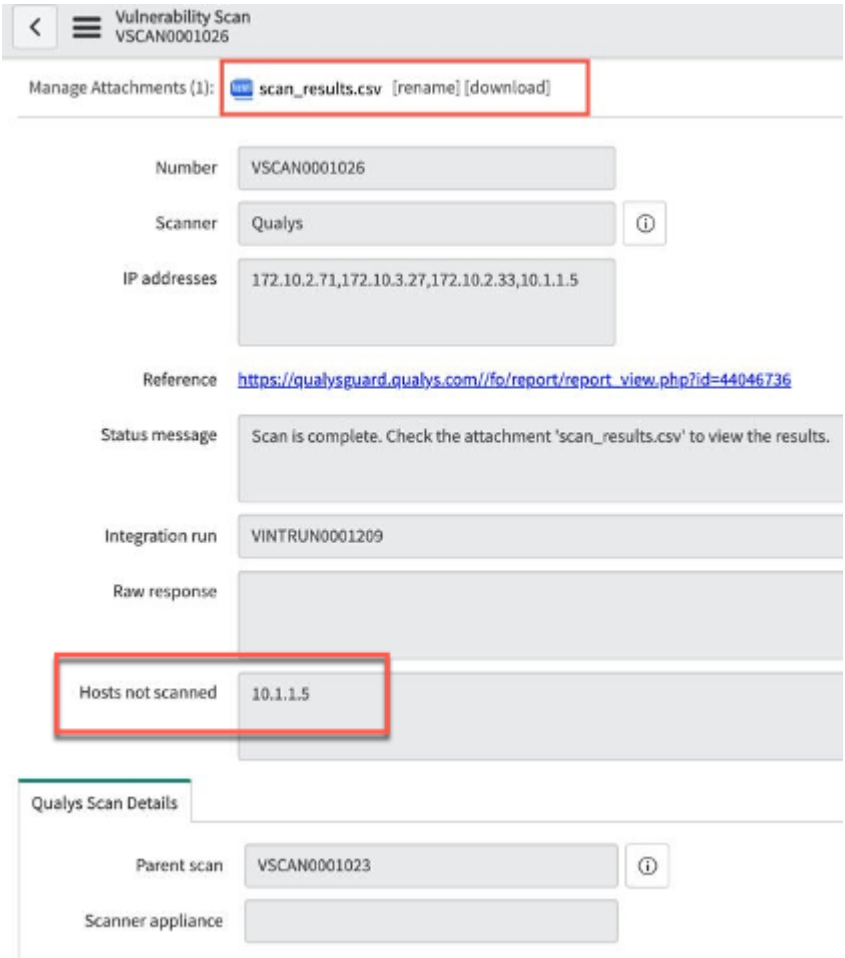
   Une fois la nouvelle analyse terminée avec succès, l'intégration de la détection d'hôte Qualys est automatiquement lancée pour mettre à jour vos éléments vulnérables. En fonction du nombre d'éléments vulnérables que vous avez, vos détections, éléments vulnérables et éléments vulnérables sont mis à jour une fois l'analyse de l'intégration de la Qualys détection d'hôte terminée. Accédez à ces enregistrements pour afficher les mises à jour une fois l'intégration de la détection d'hôte terminée.

   Cette analyse est spécifique à l'instance et peut être désactivée. Pour en savoir plus sur les Qualys intégrations et sur l'affichage des intégrations, reportez-vous à la section Présentation de Qualys Vulnerability Integration.

Que faire ensuite

Vous pouvez afficher une pièce jointe .csv sur l'enregistrement d'analyse pour afficher les détails des nouvelles analyses.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Comme le montre l'image précédente, lors de la nouvelle analyse, si les hôtes (éléments de configuration) de votre environnement ne sont pas accessibles, les détections et les VI associés à ces actifs ne sont pas mis à jour lorsque la nouvelle analyse est terminée. Pour vous aider à comprendre pourquoi ils ne sont pas inclus, une fois la nouvelle analyse terminée, les adresses IP des actifs pour ces CI sont répertoriées dans les enregistrements de vulnérabilité dans le champ Hôtes non analysés.

Qualys Métadonnées pour les vulnérabilités

L'intégration Qualys de la détection d'hôte a été améliorée pour inclure davantage de champs à partir de Qualys. Ces champs aident à filtrer les vulnérabilités non exploitables Linux . Cette amélioration améliore l'intégration au niveau de la détection et au niveau de l'élément vulnérable (VI).

Importer des métadonnées supplémentaires à partir de Qualys

Importez des métadonnées supplémentaires pour les éléments de vulnérabilité (VI) afin de filtrer les vulnérabilités en fonction de l'impact sur un noyau ou un service.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.
2. Sous Configuration de l'intégration, cliquez sur **Intégrations de scanners**.
3. Sous Application installée, cliquez sur **Modifier** pour l'application Qualys .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Configuration de la détection d'hôte**.
5. Accédez à la **Importer des métadonnées supplémentaires pour les détections**.
6. Pour importer des métadonnées supplémentaires à partir de Qualys, cochez manuellement l'une des cases suivantes dont vous avez besoin.
   - **Métadonnées du noyau** : identifie les vulnérabilités trouvées sur les noyaux Linux en cours d'exécution ou non.

     Si la valeur des métadonnées renvoyées est **Non**, cela signifie que la vulnérabilité n'est pas exploitable en raison d'un noyau qui ne s'exécute pas. Pour plus d'informations sur les valeurs récupérées, reportez-vous à la section Qualys Valeurs de métadonnées pour les vulnérabilités.
   - **Métadonnées de service** : identifie les vulnérabilités trouvées sur les ports ou les services en cours d'exécution ou non.
   - **Métadonnées de configuration exploitables** : identifie les vulnérabilités qui peuvent être exploitables ou non en raison de la configuration actuelle de l'hôte.

   Remarque : Par défaut, ces cases ne sont pas cochées.
7. Exécuter l'intégration de détection d'hôte Qualys avec une date rétroactive. Pour en savoir plus sur la définition de la date de début, reportez-vous à la section Modifications Qualys facultatives.

Résultats
Les métadonnées ont été importées.

Que faire ensuite
Pour afficher les métadonnées importées, saisissez `sn_vul_detection.list` dans le menu Filtrer la navigation. La liste des détections d'éléments vulnérables s'affiche. Pour plus d'informations sur les valeurs affichées dans les colonnes nouvellement ajoutées, reportez-vous à la section Qualys Valeurs de métadonnées pour les vulnérabilités.

Qualys Valeurs de métadonnées pour les vulnérabilités

Lorsque les métadonnées du noyau, les métadonnées de service et les métadonnées de configuration sont importées, certaines valeurs sont également récupérées. Les valeurs **0**, **1** et **Non disponible** sont traitées dans le back-end et converties respectivement en **Non**, **Oui** et **Vide** .

Ces valeurs sont renseignées dans les colonnes suivantes de la liste Détections d'éléments de vulnérabilité et Éléments de vulnérabilité :

- Affecte la colonne de service en cours d'exécution
- Affecte la colonne de configuration exploitable
- Affecte l'exécution des colonnes de noyau

Remarque :

- Ces colonnes ne sont pas visibles par défaut. Pour en savoir plus sur la configuration de la mise en page de formulaire, voir Configurer la mise en page de formulaire
- Pour les détections plus anciennes, les valeurs de ces colonnes peuvent être vides. Pour mettre à jour les données, exécutez une intégration antidatée de la détection d'hôte Qualys. Pour en savoir plus sur la définition de la date de début, reportez-vous à la section Modifications Qualys facultatives.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le tableau suivant présente les valeurs récupérées et leur signification.

Valeurs de champ récupérées et leur signification

Champ	Valeur	Importance
AFFECT_RUNNING_KERNEL	0	La vulnérabilité se trouve sur un noyau non exécuté. La vulnérabilité n'est pas exploitable.
AFFECT_RUNNING_KERNEL	1	La vulnérabilité se trouve sur un noyau en cours d'exécution. La vulnérabilité est exploitable.
AFFECT_RUNNING_KERNEL	Non disponible	La vulnérabilité n'est pas une vulnérabilité liée au noyau.
AFFECT_RUNNING_SERVICE	1	La vulnérabilité se trouve sur les ports ou les services qui ne sont pas en cours d'exécution. La vulnérabilité n'est pas exploitable.
AFFECT_RUNNING_SERVICE	0	La vulnérabilité se trouve sur les ports ou les services en cours d'exécution. La vulnérabilité est exploitable.
AFFECT_RUNNING_SERVICE	Non disponible	La vulnérabilité n'est pas une vulnérabilité connexe.
AFFECT_EXPLOITABLE_CONFIG	1	La vulnérabilité n'est pas exploitable en raison de la configuration de l'hôte.
AFFECT_EXPLOITABLE_CONFIG	0	La vulnérabilité est exploitable en raison de la configuration de l'hôte.
AFFECT_EXPLOITABLE_CONFIG	Non disponible	La vulnérabilité n'est pas une vulnérabilité connexe.

Définir des paramètres de filtre supplémentaires pour Qualys les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec la Qualys Vulnerability Integration pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec les intégrations prises en charge Qualys .

Avant de commencer

Cas d'utilisation : en tant que gestionnaire ou analyste des vulnérabilités, vous souhaiterez peut-être filtrer les données de vos requêtes afin de ne pouvoir examiner que certains détails de vulnérabilité. Par exemple, supposons que vous souhaitiez afficher les vulnérabilités importées qui sont filtrées par des adresses IP ou des plages d'adresses IP spécifiques. Vous pouvez également importer uniquement les machines qui se trouvent dans votre champ d'application, par exemple, les seules machines de votre réseau d'entreprise qui ne sont pas des périphériques externes.

Pour vous aider à collecter ces données, vous pouvez ajouter Qualys des paramètres pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

Sans ajouter d'appels d'API ou de codage supplémentaires, cette fonctionnalité vous permet de personnaliser les informations de votre requête HTTP à l'aide Qualys des paramètres de votre Now Platformfichier . Vous modifiez ou ajoutez ces valeurs à votre enregistrement de méthode HTTP sous la méthode REST pour les intégrations prises en charge Qualys du Qualys Vulnerability Integration.

Rôle requis : sn_vul.vulnerability_admin

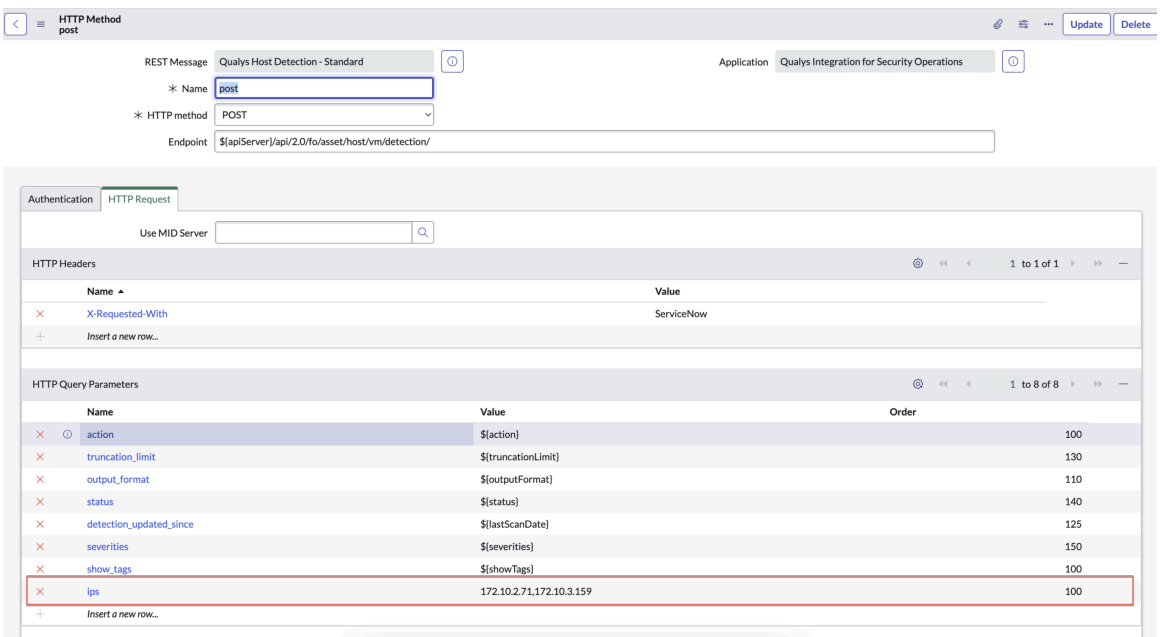
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Localisez les paramètres pris en charge par le Qualys produit sur le site développeur que vous souhaitez utiliser pour votre filtrage.
   Les paramètres et valeurs que vous entrez à partir Qualys du produit ne sont pris en charge qu'au niveau de l'instance d'intégration dans votre Now Platform. Toutes les Qualys intégrations prennent en charge le filtrage à l'aide de paramètres de requête.
2. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
3. Sur la Qualys page de liste Intégrations, cliquez sur l'enregistrement de l'intégration que vous souhaitez ouvrir.
4. Une fois l'onglet Qualys Détails REST sélectionné, localisez et cliquez sur l'icône d'informations (I) pour la méthode REST, puis sur **Ouvrir l'enregistrement** pour ouvrir l'enregistrement de la méthode HTTP.
5. Sélectionnez l'onglet **de demande HTTP** .
6. Dans les paramètres de requête HTTP du corps de la demande, ajoutez les valeurs que vous avez obtenues du site développeur Qualys .

   Dans l'image suivante, à titre d'exemple, le paramètre qui ingère uniquement certaines adresses `ips={value}` /plages IP a été ajouté. Dans ce cas, la **valeur** correspond à une ou plusieurs adresses IP/plages que vous spécifiez. Plusieurs entrées sont séparées par des virgules, `172.10.2.71, 172.10.3.159`, et une plage est spécifiée par un trait d'union, `10.10.10.1-10.10.10.100`. Consultez le site du Qualys développeur pour plus d'informations.



   Si vous souhaitez entrer plusieurs paramètres, reportez-vous à la documentation pour plus d'informations sur la Qualys séparation de chaque valeur.

   Remarque : Vous devez connaître vos exigences en matière d'API. Vous devrez peut-être ajouter ces propriétés API aux paramètres de requête ou au contenu du corps.

   Voici d'autres paramètres qui pourraient vous être utiles sur le Qualys site développeur :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- *ag_ids* - ID de listes de groupes d'actifs à récupérer. Ce paramètre garantit que seules les machines sous votre périmètre sont importées.
- *qids* - Ce paramètre limite les résultats à certaines vulnérabilités seulement (QID dans la table Third-Party Entry). Cela évite d'inonder votre système d'enregistrements d'informations.

7. Cliquez sur **Mettre à jour**.

Résolution des problèmes d'intégration de vulnérabilité Qualys

Certains problèmes fréquemment rencontrés, ainsi que des solutions de contournement, sont discutés.

Les pièces jointes n'apparaissent pas après l'importation

Si les pièces jointes n'apparaissent pas comme prévu pour les sources de données ou lors d'un incident de sécurité après des importations d'intégration tierce, vérifiez vos restrictions IP.

Les restrictions d'accès IP peuvent empêcher les pièces jointes d'être vues, sauf si vous êtes connecté à partir d'une adresse IP sécurisée. Étant donné qu'une nouvelle pièce jointe est ajoutée à chaque importation, cela peut entraîner des doublons que vous devez supprimer.

Par exemple, lorsque vous exécutez une intégration d'importation d'hôte tiers, si vous ne voyez aucune pièce jointe sur vos sources de données, vérifiez vos restrictions IP et ajoutez des utilisateurs à la liste de sécurité avant l'importation.

Modifier les cartes de transformation

Les cartes de transformation sont fournies avec des configurations de base et sont généralement suffisantes. Vous pouvez modifier les mappages de transformation en fonction des besoins de votre organisation.

Avant de commencer
Rôle requis : sn_vul_qualys.admin + import_admin

Procédure

1. Accédez à la **Tout** > **Ensembles de données à importations système** > **Administration** > **Cartes de transformation** pour afficher les messages REST.
2. Filtrez la liste résultante par application et limitez la liste à l'application **Qualys Vulnerability Integration** .
3. Modifiez les cartes de transformation selon les besoins du client.

   Pour plus d'informations sur les données fournies par l'API Qualys, consultez la documentation de l'API Qualys .

Vérifier la taille de propriété de la pièce jointe XML

Vérifie que la propriété de pièce jointe XML est suffisante pour les fichiers volumineux.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Importer/exporter**.
2. Faites défiler vers le bas jusqu'à **Propriétés d'importation** > **Format XML** en bas de la page.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Si nécessaire, remplacez la valeur par 250 et cliquez sur **Enregistrer**.

Information associée

Propriétés système disponibles

Limites de la récupération de données

Par défaut, il n'existe aucune restriction sur la façon dont les données sont récupérées à partir de Qualys. De nombreux enregistrements peuvent être liés à des vulnérabilités de faible gravité qu'un client n'est pas disposé à corriger à l'aide de son processus Vulnerability Response. La mise à jour des paramètres correspondants du message/de la méthode REST peut modifier ce comportement.

Le message/la méthode REST responsable de cette mise à jour est **Qualys Host Detection – Standard/post**. Pour mettre à jour les valeurs, ajoutez un nouveau paramètre de requête HTTP à la méthode post avec les valeurs suivantes :

- Nom : gravités
- Valeur : 3-5 (ou toute autre gravité appropriée souhaitée)

Résolution de l'échec de l'intégration de la base de connaissances Qualys

Résolvez Qualys l'échec de l'intégration de la base de connaissances en réduisant la taille de la pièce jointe de la charge utile Qualys reçue jusqu'à la limite spécifiée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Assurez-vous que la taille de la pièce jointe de la charge utile se trouve dans la limite spécifiée.
   a. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration**.
   b. Sélectionnez l'onglet **Paramètres de l'instance d'intégration** .
   c. Sélectionnez **max_delta_days** et remplacez la valeur par défaut par 3.
2. Si l'intégration échoue toujours, procédez comme suit :
   a. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Intégrations principales**.
   b. Sélectionnez **la base de connaissances Qualys**.
   c. Sélectionnez l'onglet **Détails de l'intégration** .
   d. Dans le champ **Heure de début** , sélectionnez la date actuelle pour ignorer l'exécution de l'exécution pour ce jour.
   e. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Sélectionnez l'onglet **Paramètres de l'instance d'intégration** .

g. Sélectionnez **kb_backfill_full_import** et remplacez la valeur par défaut par vrai.

Résultats
L'exécution de l'intégration du remplissage de la base de connaissances Qualys met à jour toutes les entrées tierces (TPE) dans le système. Alors que l'intégration de la détection d'hôte Qualys crée une entrée d'espace réservé, l'intégration du remplissage de la base de connaissances Qualys la met à jour.

Qualys Vulnerability Integration Rapports

La Qualys Cloud Platform vue d'ensemble est une vue exécutive de l'activité de vulnérabilité. En fournissant des tendances, des rapports et des analyses détaillées de données spécifiques, un administrateur ou un analyste peut rapidement identifier les zones de préoccupation. Les graphiques sont renseignés avec des données après la récupération des éléments vulnérables et des données de la Qualys base de connaissances.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à suivre la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en visualisant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Reportez-vous à la rubrique Réponse aux vulnérabilités Espaces de travailet Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Versions antérieures de Réponse aux vulnérabilités

Les analystes de vulnérabilité peuvent également utiliser les tableaux de bord par défaut dans l'environnement classique pour surveiller les données de vulnérabilité. Consultez Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités pour plus d'informations.

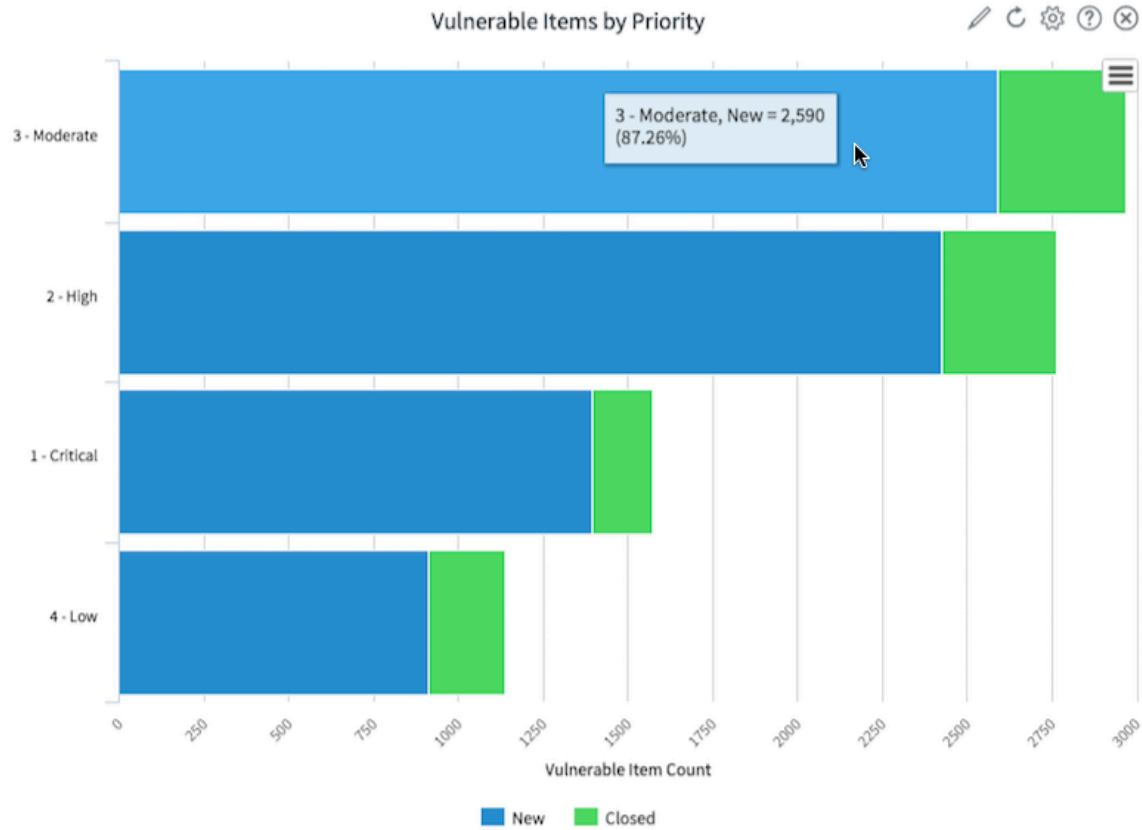
Remarque : L'utilisation de l'intégration de vulnérabilité suppose que le réglage, les tests et le Qualys Cloud Platform déploiement ont eu lieu dans votre instance. Ces fonctions sont des domaines qui ne relèvent pas du cadre de la documentation produit. Pour obtenir de l'aide, contactez Service et assistance client.

Dans chaque graphique, vous pouvez pointer sur n'importe quelle partie d'un graphique (barre, secteurs, point de données, etc.) pour afficher des données générales spécifiques à cette pièce. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de Qualys Vulnerability Integration diagramme



Les rapports suivants sont disponibles sur la page d'accueil Qualys Cloud Platform .

Qualys Vulnerability Integration Rapports de vue d'ensemble

Nom	Visuel	Description
CI synchronisés avec Qualys	Histogramme	Affiche le nombre d'éléments vulnérables ouverts enregistrés pour chaque CI, du plus au moins élevé.
Ouvrir les éléments vulnérables Qualys	Histogramme	Affiche le nombre d'éléments vulnérables ouverts associés à des vulnérabilités (enregistrements CVE), du plus au moins élevé.
Total des éléments vulnérables Qualys	Histogramme	Affiche le nombre d'éléments vulnérables ignorés dont l'expiration est planifiée dans les 7 jours.
Éléments vulnérables par priorité	Graphique de tendance	Affiche le nombre d'entrées de vulnérabilité enregistrées chaque semaine.
Prévalence QID	Histogramme	Affiche le nombre d'éléments vulnérables enregistrés pour chaque modèle, du plus au moins élevé.
Ouvrir les éléments vulnérables Qualys	Liste	Affiche le nombre d'éléments vulnérables enregistrés pour chaque éditeur, du plus au moins élevé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Qualys Graphique d'état de l'exécution de l'intégration

Le Qualys module État d'exécution de l'intégration est une vue graphique de l'état des exécutions d'intégration Qualys .

Pour afficher l'état des exécutions d'intégration, accédez à **Intégration de vulnérabilité Qualys** > **État de l'exécution de l'intégration**.

À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

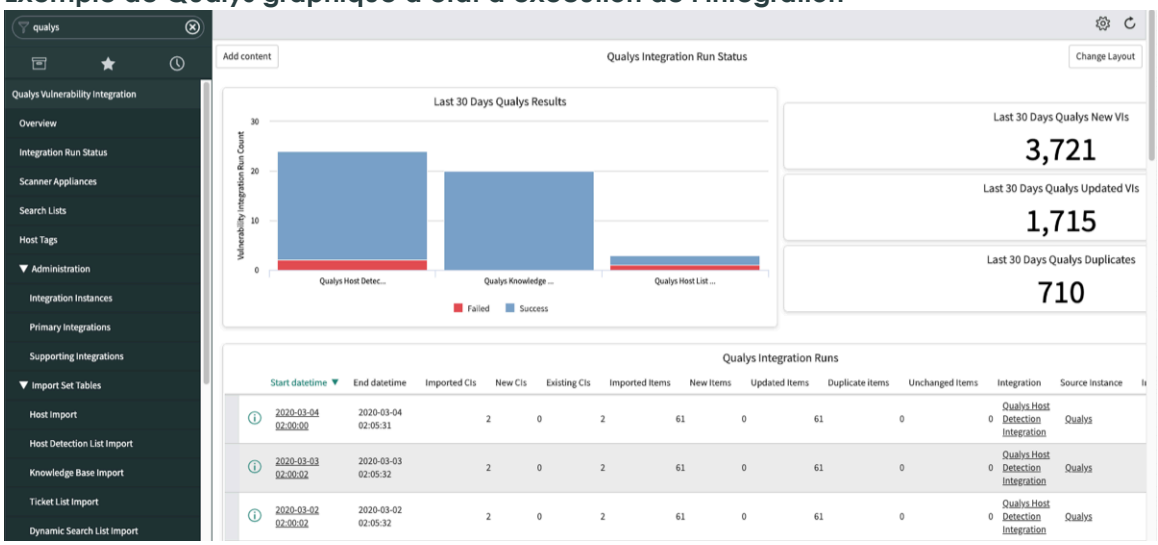
Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Dans le graphique, pointez sur n'importe quelle pièce (barre, secteur, point de données, etc.) pour afficher des données générales spécifiques à cette pièce. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

L'état Qualys de l'exécution de l'intégration affiche l'état de l'exécution de l'intégration de vulnérabilité au cours des 30 derniers jours. Le nombre de VI mis à jour Qualys[qualys] indique le nombre de détections uniques dans le même actif. Le VI est ensuite mis à jour avec la nouvelle détection.

Remarque : Le nombre d'exécutions de l'intégration de vulnérabilité n'est affiché que pour les intégrations qui sont définies sur l'état actif. Accédez à la **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales** et définissez l'état sur actif.

Exemple de Qualys graphique d'état d'exécution de l'intégration



- Les valeurs de la colonne Éléments importés représentent le nombre total d'enregistrements créés à partir d'une exécution d'intégration.
- La colonne Nouveaux éléments affiche le nombre d'enregistrements créés à partir d'une exécution d'intégration.
- La colonne Éléments dupliqués n'est plus renseignée. Vous préférez peut-être supprimer cette colonne de l'affichage.
- La colonne Éléments mis à jour affiche le nombre de fois où les enregistrements sont mis à jour au cours d'une exécution d'intégration. Cette valeur n'est pas le nombre d'enregistrements uniques qui sont mis à jour. Si, par exemple, un enregistrement est mis

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à jour deux fois au cours de l'exécution de l'intégration, il est compté deux fois et affiché sous la forme `de 2` éléments mis à jour.

- La colonne Éléments inchangés affiche les enregistrements trouvés pendant l'exécution de l'intégration qui existent déjà dans la base de données mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

Remarque : L'intégration s'exécute avec zéro résultat pour les quatre valeurs suivantes : **Nouveaux CI**, **CI existants**, **Nouveaux éléments** et **Éléments mis à jour** sont exclus de la liste des **exécutions d'intégration Qualys** .

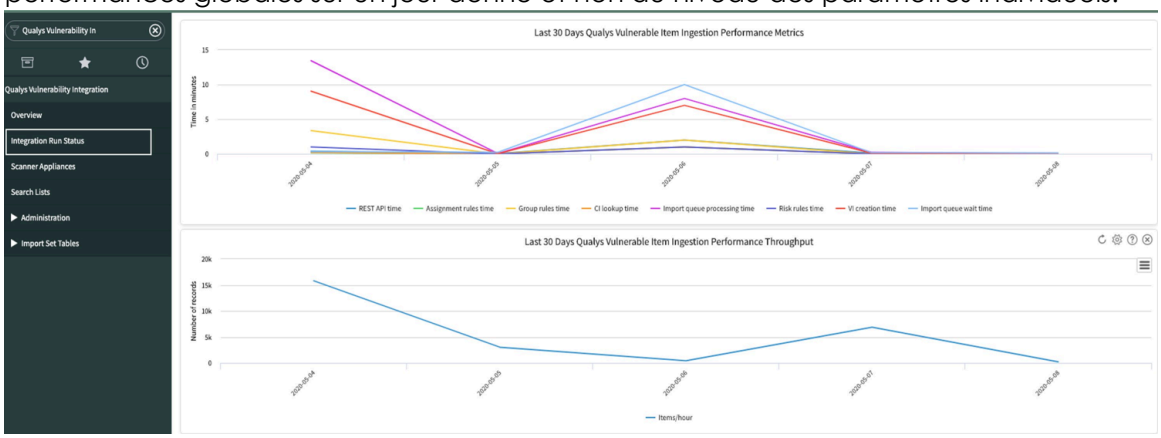
Qualys Rapports de graphiques d'état de l'exécution de l'intégration

Nom	Description
Résultats des 30 derniers jours Qualys	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Exécuter dans un visuel de barre.
Nouveaux VI au cours des 30 derniers jours Qualys	Nombre de nouveaux enregistrements importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour au cours des 30 derniers jours Qualys	Nombre d'enregistrements mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Doublons des 30 derniers jours Qualys	Nombre d'enregistrements en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Qualys Exécutions des intégrations	L'exécution de l'intégration enregistre dans une liste. **Remarque : V16.1 :** Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection de la *sn_vul_detection* table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, après la fin de l'exécution de l'intégration.
Mesures de performance d'ingestion d'élément vulnérables au cours des 30 derniers jours Qualys	Mesures de performances quotidiennes pour les éléments vulnérables comparées au cours des 30 derniers jours.
Rendement de performance d'ingestion d'élément vulnérable au cours des 30 derniers jours Qualys	Débit quotidien d'ingestion d'éléments vulnérables mesuré pour l'intégration de détection d'hôte Qualys au cours des 30 derniers jours.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Plusieurs facteurs peuvent avoir un impact sur les performances de l'exécution de l'intégration, comme la quantité de données et le temps nécessaire pour traiter ces données. Deux graphiques comparent les mesures de performance :

- Qualys Mesures de performances d'ingestion d'éléments vulnérables : comparez les mesures de performances quotidiennes pour les règles d'affectation, les règles de groupe, les règles de risque, le temps d'attente en file d'attente, le temps de traitement de la file d'attente et d'autres statistiques pour les éléments vulnérables au cours des 30 derniers jours, afin d'identifier la cause de tout écart de performance. La performance est calculée en fonction du temps pris pour chaque activité. Ces paramètres sont calculés et associés au niveau de l'exécution de l'intégration. Chaque paramètre est codé par couleur pour faciliter l'identification.
- Qualys Rendement de performance d'ingestion d'éléments vulnérables : comparez le débit quotidien d'ingestion d'éléments vulnérables pour l'intégration de la détection d'hôte Qualys . Le débit est mesuré en éléments par heure. Ce rapport affiche les performances globales sur un jour donné et non au niveau des paramètres individuels.



Transformation des données Qualys

Les données extraites de Qualys sont traitées par un ensemble de sources et de transformations de données.

La plupart des transformations sont effectuées à Qualys Vulnerability Integration l'aide de scripts de transformation. Ces scripts sont destinés à un usage interne. La suppression n'est pas recommandée. Les modifications nécessitent un codage ou Qualys Vulnerability Integration une expertise avancéeServiceNow. Les cartes restantes sont répertoriées dans cette section et utilisent des cartes de champ.

Remarque : Lors de l'installation, des cartes de gravité normalisées, qui transforment les niveaux de gravité importés Qualys Cloud Platform en niveaux de gravité standard ServiceNow , sont installées dans le module de mappage de Réponse aux vulnérabilités gravité normalisée. Consultez Créer une carte de Réponse aux vulnérabilités gravité pour plus d'informations.

Importation de liste de recherches dynamiques

La carte de transformation de liste de recherche dynamique Qualys permet de transformer et d'importer des listes de recherches dynamiques Qualys. Les modifications apportées à cette transformation modifient la façon dont les listes de recherche dynamique sont traitées et insérées dans le système.

Pour accéder à cette carte de transformation, accédez à **Intégration de vulnérabilité Qualys** > **Tables des jeux d'importation** > **Importation de liste de recherches dynamiques**.

La table affiche les champs en cours de transformation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation de liste de recherche dynamique Qualys

Champ source	Champ cible	Description
u_id	id	Utilisé comme identificateur de la liste de recherche dynamique Qualys.
[Script]	list_type	Le type de liste de recherche. Dynamique est la valeur par défaut pour la transformation de liste de recherches dynamiques.
u_title	Titre	Nom dans Qualys de cette liste de recherche.

Outre les mappages de champs, un script de transformation est exécuté au cours du processus de transformation.

La table suivante indique quand ce script est exécuté et à quoi il sert.

Calendrier et objectif du script de carte de transformation de liste de recherches dynamiques Qualys

Lorsque le script est exécuté	Objectif du script
onAfter (une fois la transformation terminée d'un jeu d'importation).	Crée les relations entre les listes de recherche et leurs vulnérabilités connexes. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Importation de liste de recherches statiques

La carte de transformation de liste de recherches statiques Qualys permet de transformer et d'importer des listes de recherches statiques Qualys. Les modifications apportées à cette transformation modifient la façon dont les listes de recherches statiques sont traitées et insérées dans le système.

Pour accéder à cette carte de transformation, accédez à **Intégration de vulnérabilité Qualys** > **Tables des jeux d'importation** > **Importation de liste de recherches statiques**.

La table affiche les champs en cours de transformation.

Champs de carte de transformation de liste de recherche statique Qualys

Champ source	Champ cible	Description
u_id	id	Utilisé comme identificateur de la liste de recherches statiques Qualys.
u_title	Titre	Nom dans Qualys de cette liste de recherche.
[Script]	list_type	Le type de liste de recherche. Statique est la valeur par défaut pour la transformation de liste de recherches statiques.

Outre les mappages de champs, un script de transformation est exécuté au cours du processus de transformation.

La table suivante indique quand ce script est exécuté et à quoi il sert.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calendrier et objectif du script de carte de transformation de liste de recherches statiques Qualys

Lorsque le script est exécuté	Objectif du script
onAfter (une fois la transformation terminée d'un jeu d'importation).	Crée les relations entre les listes de recherche et leurs vulnérabilités connexes. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Importation d'un groupe de ressources

La carte de transformation du dispositif Qualys Asset Group est utilisée pour transformer les données du groupe d'actifs Qualys afin de créer des enregistrements de dispositif de scanner. Les changements apportés à cette transformation modifient la façon dont les dispositifs de scanner sont créés et modifiés.

Pour accéder à cette carte de transformation, accédez à **Intégration de vulnérabilité Qualys** > **Tables des jeux d'importation** > **Importation d'un groupe de ressources**.

La table affiche les champs en cours de transformation.

Champs de carte de transformation des groupes d'actifs Qualys

Champ source	Champ cible	Description
u_id	id	Utilisé comme identificateur pour le groupe d'actifs Qualys.
[Script]	Manuelle	Valeur scriptée pour déterminer la façon dont l'enregistrement cible a été créé. Lorsqu'il est créé via des transformations, ce champ est toujours défini sur faux.
[Script]	ip	Adresses IP associées au groupe d'actifs en cours de transformation.
u_default_appliance_id	appliance_id	L'identificateur d'équipement Qualys pour l'équipement par défaut dans ce groupe d'actifs.
u_title	asset_group_name	Nom du groupe d'actifs Qualys.

Outre les mappages de champs, un script de transformation est exécuté au cours du processus de transformation.

La table suivante indique quand ce script est exécuté et à quoi il sert.

Calendrier et objectif du script de carte de transformation du groupe d'actifs Qualys

Lorsque le script est exécuté	Objectif du script
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Le script qui contraint le groupe d'actifs importe uniquement vers les groupes d'actifs avec un dispositif par défaut et un ensemble d'adresses IP mappées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calendrier et objectif du script de carte de transformation du groupe d'actifs Qualys (suite)

Lorsque le script est exécuté	Objectif du script
	Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Importation du dispositif

La carte de transformation du dispositif Qualys est utilisée pour transformer les données du dispositif Qualys en enregistrements de dispositif. Permet de mettre à jour les enregistrements de dispositif qui seraient initialement créés à partir de l'importation du groupe d'actifs. Les changements apportés à cette transformation modifient la façon dont les enregistrements de dispositif sont mis à jour avec les détails du dispositif.

Pour accéder à cette carte de transformation, accédez à **Intégration de vulnérabilité Qualys** > **Tables des jeux d'importation** > **Importation du dispositif**.

La table affiche les champs en cours de transformation.

Champs de carte de transformation d'appliance Qualys

Champ source	Champ cible	Description
u_name	appliance_name	Nom du dispositif de scanner Qualys.
u_status	appliance_status	Dernier état signalé du dispositif de scanner Qualys.
u_id	appliance_id	L'identificateur d'appliance Qualys.

Outre les mappages de champs, un script de transformation est exécuté au cours du processus de transformation.

La table suivante indique quand ce script est exécuté et à quoi il sert.

Calendrier et objectif du script de carte de transformation d'appliance Qualys

Lorsque le script est exécuté	Objectif du script
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Utilisé pour mettre à jour les noms et les états des dispositifs pour l'ID donné. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Messages REST Qualys

Les messages REST Qualys sont utilisés pour effectuer des appels à l'API Qualys.

À partir de la version 12.9.2 de Qualys, vous avez le choix entre l'authentification de base ou OAuth. Le paramètre d'instance La méthode Qualys Cloud Authentication est préconfigurée pour l'authentification de base. Si vous préférez utiliser OAuth, vous devez modifier le paramètre d'instance d'intégration, puis configurer le message REST directement pour OAuth.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Message REST de détection d'hôte Qualys

Le message REST de détection d'hôte Qualys effectue l'appel initial à l'API de détection de liste d'hôtes pour l'intégration de détection d'hôte Qualys.

Paramètres de message REST de détection d'hôte Qualys

Nom de paramètre	Valeur	Description
action	liste	Indique le type d'opération demandée. Paramètres requis. Les changements ne sont pas nécessaires.
output_format	XML	Définit le format du rapport renvoyé par Qualys. Les différents scripts et transformations supposent du XML, il n'est donc pas recommandé de modifier la valeur.
detection_processed_after	${lastScanDate}	Affiche uniquement les détections dont l'état de détection a changé après une date et une heure certaines. Pour les détections qui n'ont jamais changé, la date est appliquée à la dernière date de détection.
truncation_limit	500	Nombre d'hôtes à partir desquels récupérer les données, en fonction de la demande. Ce paramètre est utilisé à des fins de pagination. La valeur par défaut est 500, mais des valeurs plus grandes ou plus petites peuvent être utilisées. Ne définissez pas à moins de 100 car cela augmente considérablement la charge du système. Les valeurs plus petites nécessitent plus d'appels à l'API Qualys et les valeurs plus grandes entraînent des ensembles de résultats à traiter plus volumineux et des délais potentiels de récupération/traitement des données.
statut	Nouveau, Corrigé, Actif, Rouvert	États de détection à récupérer à partir de Qualys. La valeur par défaut récupère tous les états. Pour les extractions de données volumineuses (souvent l'extraction initiale de données), il peut être avantageux d'exclure les états fixes de cette liste. Il est important d'inclure l'état Corrigé lors de la mise à jour des vulnérabilités déjà présentes dans le système.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pagination de détection d'hôte Qualys Message REST

Le message REST de pagination de détection d'hôte gère les demandes de pagination adressées à l'API de détection d'hôte.

Lors de l'exécution de la détection de l'hôte principal, si l'API Qualys fournit une URL pour extraire la page de données suivante, ce message REST récupère ces données supplémentaires. Ces données sont utilisées par le gestionnaire de pagination de détection d'hôte.

Pagination de détection d'hôte REST est un message REST spécialisé et n'est pas destiné à être modifié.

Base de connaissances Qualys (remplissage) Message REST

Le message REST de la base de connaissances Qualys (remplissage) récupère les données de la base de connaissances Qualys en fonction de l'horodatage du dernier horodatage modifié des données de vulnérabilité pour l'intégration de la base de connaissances Qualys.

Les modifications apportées à l'enregistrement de méthode de message REST impactent la demande faite à Qualys pour récupérer les informations de la base de connaissances.

La table suivante répertorie les paramètres de demande qui sont envoyés.

Base de connaissances Qualys (remplissage) Paramètres de messages REST

Paramètre	Valeur	Description
action	liste	Indique le type d'opération demandé. Paramètres requis. Les changements ne sont pas recommandés.
Détails	Tout	Indique le niveau de détail affiché pour les vulnérabilités récupérées. Vous pouvez le modifier en toute sécurité au besoin.
ids	${qids}	Spécifie les QID à extraire de Qualys. Référencé dans le code. Aucune modification n'est recommandée.

Base de connaissances Qualys (basée sur la date) Message REST

Le message REST de la base de connaissances Qualys (basé sur la date) est utilisé pour récupérer les données de la base de connaissances Qualys en fonction de l'horodatage du dernier horodatage modifié des données de vulnérabilité. Ce message est utilisé par l'intégration de la base de connaissances Qualys.

Les modifications apportées à l'enregistrement de méthode de message REST impactent la demande faite à Qualys pour récupérer les informations de la base de connaissances.

La table suivante répertorie les paramètres de demande qui sont envoyés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Base de connaissances Qualys (basée sur la date) Paramètres de message REST

Champ source	Champ cible	Description
action	liste	Indique le type d'opération demandée. Paramètres requis. Les changements ne sont pas recommandés.
Détails	Tout	Indique le niveau de détail affiché pour les vulnérabilités récupérées. Vous pouvez le modifier en toute sécurité au besoin.
last_modified_after	${dateDébut}	Indique quand commencer à récupérer les données historiques. Utilisé par le code pour déterminer à la fois l'heure de début et pour aider à la pagination. Aucune modification ou suppression n'est recommandée.
last_modifiedbefore	${datede fin}	Indique quand mettre fin à la récupération des données historiques. Utilisé par le code pour déterminer à la fois l'heure de fin et pour aider à la pagination. Aucune modification ou suppression n'est recommandée.

Tickets Qualys Message REST

Le message REST des tickets Qualys récupère les informations de ticket Qualys pour Qualys Ticket Integration. Les modifications apportées à l'enregistrement de méthode de message REST impactent les demandes adressées à Qualys pour récupérer les informations du ticket.

La table affiche les paramètres de demande qui sont envoyés.

Tickets Qualys Paramètres de message REST

Nom de paramètre	Valeur	Description
modified_since_datetime	${lastRunDatetime}	Indique la date de dernière exécution de l'intégration et la date après laquelle extraire les données. Utilisé par code. Les changements ne sont pas recommandés.
since_ticket_number	${lastTicketNumber}	Indique quel ticket a été récupéré pour la dernière fois à partir de Qualys. Utilisé pour la pagination. Les changements ne sont pas recommandés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tickets Qualys Paramètres de message REST (suite)

Nom de paramètre	Valeur	Description
show_vuln_details	1	Indique si les détails de la vulnérabilité ont été récupérés.

Présentation de Intégration des vulnérabilités Rapid7

Le utilise ServiceNow® Intégration des vulnérabilités Rapid7 des données importées de l'entrepôt Rapid7 de données ou Rapid7 InsightVM des produits pour vous aider à déterminer l'impact et la priorité des menaces potentiellement malveillantes.

Rapid7 NexposeLes capteurs collectent les données et les envoient automatiquement à l'entrepôt de données (sur site) ou Rapid7 InsightVM aux produits (basés sur le cloud), qui analysent et corrèlent Rapid7 les informations en permanence. Il s'intègre ServiceNow® Réponse aux vulnérabilités facilement pour mapper les vulnérabilités aux CI et aux services. Enrichit les données de vulnérabilité sur Intégration des vulnérabilités Rapid7 votre instance.

Rapid7 Les intégrations sont des points d'entrée qui interagissent avec l'entrepôt de données ou Rapid7 InsightVM les Rapid7 produits, appelés en tant que travaux planifiés. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités. Les travaux planifiés sont exécutés automatiquement et dans l'ordre spécifié. Vous pouvez également exécuter manuellement des travaux planifiés individuels.

Remarque :

Si vous utilisez à la fois Rapid7 un entrepôt de données et Rapid7 InsightVM comme sources pour vos données, vous courez le risque d'avoir des enregistrements de vulnérabilité en double.

Remarque : Lors de la migration du type d'intégration **Entrepôt de données** vers le type **InsightVM** , vous pouvez dédupliquer vos enregistrements d'entrepôt de données existants. Consultez Dédupliquer les enregistrements d'entrepôt de Intégration des vulnérabilités Rapid7 données pour plus d'informations.

Si vous avez plusieurs déploiements de l'intégration Rapid7 InsightVM de vulnérabilité, vous pouvez ajouter une intégration pour chaque déploiement. Les actifs, identifiés par plusieurs déploiements tiers et leurs vulnérabilités, sont consolidés et rapprochés avec votre CMDB. Cette consolidation se produit même lorsque les processus d'analyse se chevauchent entre les différents déploiements. Les données provenant de chaque déploiement sont identifiées et disponibles dans une instance unique de Réponse aux vulnérabilités.

Remarque : Vous ne pouvez pas supprimer l'intégration de vulnérabilité d'origine, mais vous pouvez la désactiver. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions disponibles

Version de mise en production pour Xanadu	Notes de publication
Intégration des vulnérabilités Rapid7 v13.6 et 13.7	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Rôles

Rapid7 Les tâches d'intégration de vulnérabilité impliquent les rôles suivants.

- sn_vul_r7.admin : peut lire, écrire et supprimer des enregistrements.
- sn_vul_r7.user : peut lire et écrire des enregistrements.
- sn_vul_r7.read : peut lire des enregistrements.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Intégrations de Intégration des vulnérabilités Rapid7

Pour afficher le Intégration des vulnérabilités Rapid7, accédez à **Rapid7** > **Administration** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base.

Rapid7 Intégrations d'entrepôts de données

Intégration	Description
Intégration des vulnérabilités Rapid7	Récupère les données de Rapid7 Nexpose vulnérabilité et les traite dans votre instance.
Rapid7 Intégration de la liste des actifs	Récupère les données d'analyse une fois par semaine à partir de l'entrepôt de Rapid7 Nexpose données et les stocke dans le module Éléments détectés de votre instance. Permet d'identifier les actifs qui n'ont pas été analysés récemment à l'aide de la **date de la dernière analyse** . Affichez l'heure de **la dernière analyse** dans la liste des éléments détectés dans Réponse aux vulnérabilités.
Rapid7 Intégration de catégorie	Récupère les informations de catégorie à partir de Rapid7 Nexpose. Les catégories fournissent une classification de haut niveau pour les vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapid7 Intégrations d'entrepôts de données (suite)

Intégration	Description
Rapid7 Intégration d'exploit	Récupère les informations sur l'exploitation à partir du Rapid7 Nexposefichier .
Rapid7 Intégration de Malware Kit	Récupère les informations sur le kit malware à partir du Rapid7 Nexposefichier .
Rapid7 Intégration de référence	Récupère les références à des documents de référence externes tels que les CVE ou les références de vulnérabilité spécifiques au fournisseur.
Rapid7 Intégration de solution	Récupère les données de solution à partir de Rapid7 Nexpose, qui fournit des solutions recommandées pour des vulnérabilités spécifiques.
Rapid7 Intégration de solution de remplacement	Récupère des informations sur les solutions qui sont remplacées par d'autres solutions.
Rapid7 Intégration de solution prérequise	Récupère des informations sur les solutions qui sont des prérequis pour d'autres solutions. Lorsque cette intégration s'exécute, elle récupère le mappage des solutions et des solutions prérequises à partir de l'entrepôt Rapid7 de données. **Remarque :** Cette intégration fonctionne uniquement si le module d'extension Gestion des solutions pour vulnérabilités est activé.
Rapid7 Intégration de la carte de solution de vulnérabilité	Récupère le mappage pour associer des solutions à des vulnérabilités.
Rapid7 Intégration d'éléments vulnérables	Récupère les données d'éléments Rapid7 Nexpose vulnérables et les traite dans votre instance. Les sorties de cette intégration sont des éléments vulnérables.
Rapid7 Intégration de résolution des éléments vulnérables	Récupère des informations sur les éléments vulnérables marqués comme fermés et Rapid7 Nexpose ferme les éléments vulnérables correspondants dans Réponse aux vulnérabilités.
Rapid7 Intégration de site	Récupère les données du site à partir du Rapid7 Nexposefichier . Un site est une collection d'actifs ciblés pour une analyse.
Rapid7 Intégration de la liste des actifs	Récupère les balises d'hôte et les données d'analyse une fois par semaine à partir de l'entrepôt Rapid7 de données et les stocke dans le module Éléments détectés de votre instance. Permet d'identifier les actifs qui n'ont pas été analysés récemment à l'aide de la **date de la dernière analyse** . Afficher l'heure de la **dernière analyse** dans la liste des éléments détectés dans Réponse aux vulnérabilités

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapid7 Intégrations d'entrepôts de données (suite)

Intégration	Description
Rapid7 Intégration complète des éléments vulnérables	Importe toutes les détections Rapid7 pour tous les éléments de configuration analysés depuis la dernière exécution réussie de l'intégration. En fonction des données importées les plus récentes, les éléments vulnérables qui n'ont pas été trouvés récemment lors des analyses passent automatiquement à l'état « Fermé » lorsque le module Fermer automatiquement les éléments vulnérables périmés est activé.

Intégrations de Rapid7 InsightVM

Intégration	Description
Rapid7 Intégration d'éléments vulnérables : API	Récupère les données d'éléments vulnérables à partir d'InsightVM Rapid7 et les traite dans votre instance.
Intégration des vulnérabilités Rapid7 — L'API	Récupère les données de référence, de catégorie, d'exploitation, de kit de logiciels malveillants et de vulnérabilité d'InsightVM Rapid7 et les traite dans votre instance.
Rapid7 Intégration de la liste des actifs : API	Récupère les balises d'hôte et les données d'analyse Rapid7 InsightVM une fois par semaine et les stocke dans le module Éléments détectés de votre instance. Permet d'identifier les actifs qui n'ont pas été analysés récemment à l'aide de la **date de la dernière analyse** . Affichez l'heure de **la dernière analyse** dans la liste des éléments détectés dans Réponse aux vulnérabilités.
Rapid7 Intégration complète des éléments vulnérables : API	Importe toutes les détections Rapid7 pour tous les éléments de configuration analysés depuis la dernière exécution réussie de l'intégration. En fonction des données importées les plus récentes, les éléments vulnérables qui n'ont pas été trouvés récemment lors des analyses passent automatiquement à l'état « Fermé » lorsque le module Fermer automatiquement les éléments vulnérables périmés est activé.
Rapid7 Intégration de site	Récupère les données du site à partir du Rapid7 InsightVM produit. Cette intégration est définie pour s'exécuter chaque semaine à 00:00:00.

Au cours de l'importation, les enregistrements CVE qui ne sont pas déjà présents sont créés en tant qu'enregistrements NVD et référencés dans des entrées tierces par Rapid7 défaut. L'intégration du modèle ne Rapid7 peut pas être supprimée. Désactivez-le plutôt.

Connecteur du graphe de services pour Rapid7

À partir de la version 2.0, Connecteur du graphe de services pour Rapid7 est disponible à partir du ServiceNow® Store. Consultez Connecteur du graphe de services pour Rapid7 (2.0.0) pour plus d'informations.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles de recherche de CI

Les règles de recherche de CI déterminent comment renseigner le champ **Élément de configuration** dans un enregistrement d'élément vulnérable.

Pour plus d'informations sur le fonctionnement des règles de recherche de CI, reportez-vous à Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Pour créer ou modifier des règles de recherche, reportez-vous Créer une règle de recherche de CI de Vulnerability Responseà .

Remarque : Les règles, une fois supprimées, ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Éléments détectés

Ce module répertorie les éléments de configuration détectés lors de l'importation à partir des intégrations d'éléments Rapid7 vulnérables (entrepôt de données ou API InsightVM) et de l'intégration de liste Rapid7 des actifs - API. L'API Rapid7 d'intégration de liste des actifs importe tous les actifs Rapid7 analysés pour détecter les vulnérabilités depuis la dernière exécution de l'intégration. L'intégration de la liste des actifs de l'entrepôt Rapid7 de données est incluse.

Remarque : Le filtre par défaut de cette liste est défini sur **Sans correspondance**. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour plus d'informations sur le module Éléments détectés, reportez-vous à Réponse aux vulnérabilités la section Éléments détectés In.

Balises d'hôtes

Les balises d'hôte sont importées dans le cadre de l'intégration de la liste des actifs - intégration de l'API Rapid7 pour Rapid7 InsightVM. Elles sont principalement utilisées pour le filtrage dans Réponse aux vulnérabilités les règles de tâches d'affectation et de rattrapage de .Rapid7 InsightVM Ils sont affichés dans le formulaire Élément détecté.

Balises d'hôtes

Remarque : L'intégration Rapid7 de la liste des actifs : l'intégration de l'API doit être exécutée avant de créer des règles Réponse aux vulnérabilités de tâche d'affectation ou de rattrapage afin que toutes les balises puissent être présentes dans les règles et avant que les éléments vulnérables ne soient importés et regroupés.

- Le stockage des balises n'est pas sensible à la casse. Si une balise **San Diego** est créée, une balise **SAN DIEGO** ne peut pas être stockée dans la table de balises Host. « San Diego » et « SAN DIEGO » sont considérés comme étant la même balise d'hôte. La balise qui a été importée en premier gagne.
- L'utilisation de balises d'hôte en tant que clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises hôtes sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises hôtes sont contrôlées par la propriété système globale **sn_vul.import_host_tags**. Cette propriété est définie sur vrai par défaut. La désactivation des balises les désactive dans toutes les instances.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sites

Un site est une collection d'actifs ciblés pour une analyse. Un site se compose d'actifs cibles, d'un modèle d'analyse, d'un ou de plusieurs moteurs d'analyse et d'autres paramètres liés à l'analyse tels que les calendriers ou les alertes. Les sites sont gérés par Rapid7 les applications.

Intégration des vulnérabilités Rapid7 Le filtrage de site pendant la configuration vous permet de classer et de demander des actifs par site pendant l'importation. Pour plus d'informations sur le filtrage des importations, consultez la section Filtrage par Rapid7 sites

L'entrepôt Rapid7 de données et Rapid7 InsightVM les intégrations de sites importent des sites sous la forme d'une tâche planifiée hebdomadaire.

Pour afficher les sites importés dans une liste, accédez à **Rapid7** > **Sites**.

Rouvrir les éléments vulnérables résolus non fermés par les analyses

Les éléments vulnérables définis sur « Résolu » dans votre Now Platform instance, mais qui ne sont pas passés à l'état « Fermé/Résolu » par les exécutions d'intégration suivantes, sont rouverts s'ils sont détectés lors des nouvelles analyses.

Pour Rapid7 les détections, une option est désormais disponible sur la page de configuration Rapid7 de votre instance pour rouvrir les VI résolus par âge. Si cette option est activée, les VI définis sur « Résolu », mais qui ne sont pas ensuite transférés vers « Fermé/Fixe » par les analyses suivantes, reviennent à l'état « Ouvert » après le nombre de jours que vous entrez.

Créer des CI à l'aide du moteur Identification et rapprochement (IRE)

Vous pouvez utiliser le moteur Identification et rapprochement pour créer de nouveaux CI lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte importé à partir d'un scanner tiers. Activez le module d'extension Modèles de classe CI CMDB pour créer des CI à l'aide des nouvelles classes, sinon des CI sans correspondance sont créés dans les classes CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement. Pour en savoir plus sur la configuration de la catégorisation des ressources cloud inégalées dans votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

Analyser à nouveau les éléments vulnérables

Lancez de nouvelles analyses dans la Rapid7 plateforme pour vérifier que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Consultez Lancer une nouvelle analyse pour l'intégration de Rapid7 vulnérabilité.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Rapid7 Gestion des solutions

Si vous avez activé le module d'extension Gestion des solutions pour vulnérabilités , les solutions pour l'entrepôt Rapid7Rapid7 de données et Rapid7 InsightVM la table Solutions en matière de vulnérabilité [sn_vul_solution]. Toutefois, si vous n'avez pas activé

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le module d'extension Gestion des solutions pour vulnérabilités , alors Intégration des vulnérabilités Rapid7 fonctionne tel quel et importe les solutions dans la table personnalisée [sn_vul_r7_solution]. Pour plus d'informations, consultez Rapid7 Gestion des solutions.

Se préparer à la Intégration des vulnérabilités Rapid7

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Préparez l'intégration en effectuant ces tâches. Le Intégration des vulnérabilités Rapid7 suppose que vous connaissez et exécutez Rapid7 des analyses d'entrepôt de données ou Rapid7 InsightVM de produits dans votre environnement.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Les Rapid7 scanners sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Ré-analyse** n'est pas disponible.

Avant de télécharger l'application Intégration des vulnérabilités Rapid7 à partir de et ServiceNow® Store de l'installer sur votre instance, passez en revue les informations suivantes sur les types d'intégration et les informations de configuration :

Deux types d'intégrations sont inclus dans le Intégration des vulnérabilités Rapid7 qui est disponible dans :ServiceNow® Store

- Rapid7 InsightVM
- Rapid7 entrepôt de données

Le type d'entrepôt Rapid7 de données :

- Nécessite l'URL de votre Rapid7 serveur d'entrepôt de données et vos informations d'identification d'authentification
- nécessite un serveur MID
- Utilise un pilote PostgresSQL pour exécuter des requêtes sur l'entrepôt de données
- Ne prend pas en charge plusieurs instances

Le type d'intégration Rapid7 InsightVM :

- Est basé sur le cloud et utilise une API REST. Cette intégration nécessite une clé API à partir de votre Rapid7 compte Insight.
- Prend en charge plusieurs instances.

Consultez Configurer pour l'intégration de l'entrepôt de Rapid7 données (entrepôt de données) et Configurer pour l'intégration Rapid7 InsightVM pour plus d'informations sur les exigences de configuration pour ces types d'intégration.

Configurer pour l'intégration de l'entrepôt de Rapid7 données

L'intégration Rapid7 de l'entrepôt de données est l'un des types d'intégration inclus avec le Intégration des vulnérabilités Rapid7 Intégration des vulnérabilités Rapid7.

Avant de commencer

Avant d'exécuter l'intégration de l'entrepôt Rapid7 de données, effectuez les tâches de configuration suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Procurez-vous le module complémentaire d'entrepôt Rapid7 de données. Consultez le Rapid7 site Web et la documentation pour acquérir et installer ce module complémentaire.
- Obtenez le pilote PostgresSQL le plus récent. Accédez à https://jdbc.postgresql.org/ et téléchargez le pilote le plus récent.
- Un MID Server pour exécuter des requêtes vers l'entrepôt de données Reportez-vous à la section Serveur MID pour plus d'informations sur la configuration d'un serveur MID.

  Notez le nom de l'entrepôt de données. Le type d'intégration Rapid7 de l'entrepôt de données prend uniquement en charge les MID Server autonomes. Les serveurs MID en grappe ne sont pas pris en charge.

- Obtenez l'URL et les informations d'identification d'authentification de votre Rapid7 serveur d'entrepôt de données et accédez-les.

Rôle requis : L'administrateur système [admin] télécharge et installe l'application. Le sn_vul.vulnerability_admin ou sn_vul.admin supervise la configuration et vérifie les résultats attendus.

Procédure

1. Connectez-vous à l'instance sur laquelle Now Platform vous souhaitez installer l'application Intégration des vulnérabilités Rapid7 .
2. Installez le fichier JAR PostgreSQL que vous avez téléchargé dans les tâches de configuration répertoriées précédemment.

   a. Dans votre Now Platform instance, accédez à **Tout** > **Serveur MID** > **Fichiers JAR**.

   b. Cliquez sur **Nouveau**.

   c. Entrez le nom du pilote PostgresSQL que vous avez téléchargé précédemment.

      Si vous le souhaitez, entrez les informations de **version**, **de source** et **de description** . Laissez la case **Actif** cochée.

   d. Joignez le fichier JAR téléchargé à l'aide de l'icône de dans l'en-tête.

   e. Cliquez sur **Envoyer**.

   Vous avez terminé la configuration de l'intégration de l'entrepôt Rapid7 de données. Si vous n'avez pas passé en revue les exigences relatives à l'intégrationRapid7 InsightVM, avant d'installer les fichiers , consultez Intégration des vulnérabilités Rapid7Configurer pour l'intégration Rapid7 InsightVM et Se préparer à la Intégration des vulnérabilités Rapid7.

   Pour connaître la procédure à suivre pour obtenir des autorisations, télécharger et installer le , reportez-vous à la Intégration des vulnérabilités Rapid7section Installer Intégration des vulnérabilités Rapid7.

Configurer pour l'intégration Rapid7 InsightVM

L'intégration Rapid7 InsightVM est l'un des types d'intégration inclus avec le Intégration des vulnérabilités Rapid7 Intégration des vulnérabilités Rapid7.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Avant d'exécuter l'intégration Rapid7 InsightVM , effectuez les tâches de configuration suivantes.

Rôle requis : L'administrateur système [admin] télécharge et installe l'application. Le sn_vul.vulnerability_admin ou sn_vul.admin supervise la configuration et vérifie les résultats attendus.

Procédure

1. Pour le type d'intégration Rapid7 InsightVM , préparez votre région et votre clé API.
   Contact Rapid7 pour obtenir la région et la clé API appropriées.
   Vous avez terminé la configuration de l'intégration Rapid7 InsightVM . Si vous n'avez pas passé en revue les exigences relatives à l'intégration de l'entrepôt Rapid7 de données, avant d'installer les fichiers , consultez Intégration des vulnérabilités Rapid7Configurer pour l'intégration de l'entrepôt de Rapid7 données et Se préparer à la Intégration des vulnérabilités Rapid7.
2. Pour connaître la procédure à suivre pour obtenir des autorisations, télécharger et installer le , reportez-vous à la Intégration des vulnérabilités Rapid7section Installer Intégration des vulnérabilités Rapid7.

Installer Intégration des vulnérabilités Rapid7

Une fois que vous avez terminé les étapes de configuration de l'intégration afin qu'elle s'intègre correctement à Réponse aux vulnérabilités, obtenez les autorisations, téléchargez et installez l'application sur votre Now Platform® instance.

Avant de commencer

Rôles requis : administrateur pour le téléchargement et l'installation, sn_vuln.admin supervise la configuration et vérifie les résultats attendus.

1. Reportez-vous à la section Se préparer à la Intégration des vulnérabilités Rapid7, Configurer pour l'intégration de l'entrepôt de Rapid7 données et Configurer pour l'intégration Rapid7 InsightVM pour plus d'informations sur les types d'intégration et les exigences de configuration du Intégration des vulnérabilités Rapid7.
2. Remplissez la liste de vérification de configuration suivante avant le téléchargement et l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.
3. Une fois l'application activée, procédez comme suit pour configurer le Intégration des vulnérabilités Rapid7fichier .

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que vous disposez des rôles requis Now Platform pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus. Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités. • L'administrateur système [admin] installe l'application. S'il n'est pas déjà affecté, l'administrateur affecte le rôle d'administrateur de vulnérabilité [sn_vul.vulnerability_admin ou sn_vul.admin]. • L'administrateur de vulnérabilité supervise la configuration et vérifie les résultats attendus. Le Rapid7 rôle administrateur est hérité lorsqu'un rôle administratif vous est affecté dans l'application Réponse aux vulnérabilités (VR).
Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables que vous prévoyez d'importer.	Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service et assistance client.
Configurer le filtrage	Utilisez le filtrage pour limiter le nombre d'éléments pour l'importation initiale et phaser votre déploiement en ajustant les filtres dans les importations ultérieures.
Désactiver les calculateurs de vulnérabilité	Si vous n'utilisez pas de calculateurs de vulnérabilité, Désactiver le calculateur de vulnérabilité par défaut s'il n'est pas utilisé, en plus de tous les autres que vous avez définis. Les calculateurs de vulnérabilité s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	créé ou mis à jour, ce qui peut avoir un impact sur les performances d'importation initiales.
Conserver la valeur par défaut pour l'exécution en tant qu'utilisateur	Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.
Utilisation des balises d'hôte	Si vous prévoyez d'utiliser des balises d'hôte dans Réponse aux vulnérabilités les règles de tâche d'affectation ou de rattrapage, exécutez l'intégration de la liste des actifs Rapid7 avant de créer des règles.
Dédupliquer les enregistrements de données existants	Lorsque vous migrez du type d'intégration **Entrepôt de données** vers le type **InsightVM** , vous pouvez dédupliquer vos enregistrements d'entrepôt de données existants. Consultez Dédupliquer les enregistrements d'entrepôt de Intégration des vulnérabilités Rapid7 données pour plus d'informations.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer l'application Intégration des vulnérabilités Rapid7 .
2. Accédez au ServiceNow Store et connectez-vous.
3. Dans le ServiceNow Store, recherchez l'application Intégration des vulnérabilités Rapid7 .

   Remarque : Dans le , l'application ServiceNow Storeest appelée Rapid7 Integration for Security Operations. Cette application nécessite un abonnement.

4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **Dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Dans votre Now Platform instance, accédez à **Applications système** > **Toutes les applications** > **Tout**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Dans la boîte de dialogue Installer, l'état de votre dépendance s'affiche. Si vous avez besoin d'une application de dépendance, l'application dont vous avez besoin s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suivez les invites de la boîte de dialogue pour installer l'application Intégration des vulnérabilités Rapid7 sur votre instance.

Remarque : L'administrateur de vulnérabilité peut maintenant terminer la configuration de l'application. Consultez Configurez la Intégration des vulnérabilités Rapid7..

Configurez la Intégration des vulnérabilités Rapid7.

Configurez le Intégration des vulnérabilités Rapid7 après l'installation et l'activation de l'application sur votre Now Platform®.

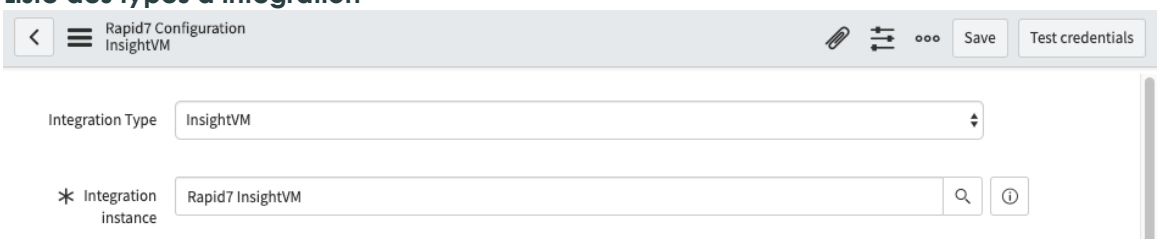
Avant de commencer

Rôle requis : L'administrateur [admin] télécharge et installe l'application. Le sn_vul.vulnerability_admin ou sn_vul.admin supervise la configuration et vérifie les résultats attendus.

Procédure

1. Une fois l'application activée (installée), accédez à **Rapid7 Vulnerability Integration** > **Administration** > **Configuration**.
2. Sélectionnez un type d'intégration dans la liste.

Liste des types d'intégration



3. Sélectionnez une instance d'intégration.
   L'instance d'intégration par défaut Rapid7 InsightVM est sélectionnée par défaut. Si tel correspond au type d'intégration que vous souhaitez, procédez comme suit. Si vous souhaitez configurer le type d'intégration de l'entrepôt de données, passez à l'étape Rapid7 4.

   a. Avec l'onglet **Configuration de l'intégration** sélectionné sur le formulaire qui s'affiche, renseignez les champs :

Onglet Configuration de l'intégration pour le type d'intégration InsightVM

Champ	Description
Région InsightVM	L'URL du serveur que vous avez acquise sur le Rapid7 site.
Clé API	La clé API que vous avez acquise à partir de votre Rapid7 compte Insight.
État de validation	Lecture seule : état du processus de validation des informations d'identification.

   b. Vérifiez la configuration correcte en cliquant sur **Tester les informations d'identification**.
   Si un message d'erreur s'affiche pendant la configuration, saisissez à nouveau vos données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Après un test réussi, cliquez sur **Enregistrer**.

d. Cliquez sur l'onglet **Configuration de l'importation** .

Renseignez les champs du formulaire qui s'affiche.

Onglet Configuration de l'importation pour InsightVM

Champ	Description
Score CVSS min.	Score CVSS de l'élément vulnérable minimum utilisé pour filtrer les éléments vulnérables pendant l'importation.
Score CVSS max.	Score CVSS d'élément vulnérable maximal utilisé pour filtrer les éléments vulnérables pendant l'importation.
Filtre de site	Limite les données aux Rapid7 InsightVM sites choisis dans la liste Sites. Consultez Filtrage par Rapid7 sites. Vous pouvez choisir plusieurs sites. La valeur par défaut (vide) concerne tous les sites. Pour pré-remplir la liste des sites, exécutez l'API Rapid7 Site Integration avant de définir ce champ. Pour plus d'informations sur l'utilisation du filtrage de site, reportez-vous à la section Filtrage par Rapid7 sites.
Créer automatiquement une entrée CVE	La propriété système permettant de créer une entrée CVE est active (vraie) par défaut. Les espaces réservés CVE sont créés automatiquement avec l'ingestion de connaissances Rapid7 si l'ID CVE n'existe pas. Si vous souhaitez que cette fonctionnalité soit inactive, désactivez la propriété [sn_vul_r7.create_cve_for_vulnerabilities] dans la liste des propriétés système.
Réouverture résolue par âge	Lorsque cette option est sélectionnée, les éléments vulnérables sont automatiquement rouverts lorsque le nombre de jours pendant lesquels ils ont été résolus mais non fermés correspond à la valeur affichée dans le champ **Rouvrir résolu après** .

e. Cliquez sur **Enregistrer**.

Pour plusieurs déploiements du type d'intégration Rapid7 InsightVM :

f. Dans le champ **Instance d'intégration** , ouvrez de la liste de recherche, sélectionnez une instance d'intégration existante ou cliquez sur **Nouveau** dans le menu contextuel.

g. Pour **Nouveau**, saisissez un **nom** pour l'instance d'intégration et cliquez sur **Soumettre**.
Le type d'intégration apparaît dans le formulaire de Rapid7 configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez supprimer n'importe quelle instance d'intégration à l'exception de la valeur par défaut. La suppression d'une instance supprime les éléments suivants (à l'exclusion des VI) :

- Intégrations
- Paramètres d'instance
- Exécutions des intégrations
- Processus d'intégration
- La colonne d'instance sur le VI est marquée comme vide

h. Vérifiez la configuration correcte en cliquant sur **Tester les informations d'identification**.

i. Après un test réussi, cliquez sur **Enregistrer**.

4. Dans le champ Type d'intégration, développez la liste et cliquez sur **Entrepôt de données**.

a. Sélectionnez l'onglet **Configuration de l'intégration** .

Renseignez les champs du formulaire qui s'affiche.

Onglet Configuration de l'intégration pour l'entrepôt de données Type d'intégration

Champ	Description
Nom d'identification JDBC	Nom des informations d'identification de votre entrepôt de données.
Nom d'utilisateur	Nom d'utilisateur de l'entrepôt de données Rapid7.
Mot de passe	Mot de passe de l'entrepôt de données Rapid7.
État de validation	Lecture seule : état du processus de validation des informations d'identification.
Détail de validation	Lecture seule : entrepôt de données uniquement. Affiche des informations supplémentaires sur le contrôle de validation après avoir cliqué au moins une fois sur Informations d'identification de test. Cela peut être utile pour déboguer votre configuration (par exemple, pour valider si votre MID Server est mal configuré ou si vous avez simplement des informations d'identification erronées).
Serveur de base de données DNS/ IP	Adresse DNS ou IP de votre entrepôt de données.
Port de la base de données	Port à utiliser pour l'intégration de votre entrepôt de données.
Nom de base de données	Nom de votre entrepôt de données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Décalage du retard de données (en jours)	Le décalage du retard de données tient compte du délai entre les données en temps réel du Rapid7 Nexpose scanner et les données de l'entrepôt de données.
Serveur MID	Serveur MID à utiliser. Seuls les MID Servers autonomes sont pris en charge. Les MID Servers en grappe ne sont pas pris en charge.
Délai d'expiration du serveur MID (min)	Nombre de minutes à attendre que le serveur MID réponde avant expiration de l'exécution de l'intégration.

b. Vérifiez la configuration correcte en cliquant sur **Tester les informations d'identification**.

c. Après un test réussi, cliquez sur **Enregistrer**.

d. Cliquez sur l'onglet **Configuration de l'importation** .

Renseignez les champs du formulaire qui s'affiche.

Onglet Configuration de l'importation pour l'entrepôt de données

Champ	Description
Avant la version 12.0 : case à cocher Créer une entrée CVE	Lorsque cette option est cochée, les espaces réservés pour les CVE, qui ne sont pas déjà présents, sont créés en tant qu'enregistrements NVD et référencés dans l'entrée tierce pour Rapid7. Lorsque cette option n'est pas cochée, ces CVE sont ignorées.
Score CVSS min.	Score CVSS de l'élément vulnérable minimum utilisé pour filtrer les éléments vulnérables pendant l'importation.
Score CVSS max.	Score CVSS d'élément vulnérable maximal utilisé pour filtrer les éléments vulnérables pendant l'importation.
Filtre de site	Limite les données d'intégration de sites importées aux sites choisis. Vous pouvez en choisir plusieurs. **Remarque :** Étant donné que le paramètre par défaut est d'importer des données à partir de tous les sites, vous n'avez pas besoin d'utiliser le filtre si vous voulez tous les sites. Cela ralentit la demande.
Réouverture résolue par âge	Lorsque cette option est sélectionnée, les éléments vulnérables sont automatiquement rouverts lorsque le nombre de jours pendant lesquels ils ont été résolus mais non fermés correspond à la valeur affichée dans le champ **Rouvrir résolu après** .

5. Cliquez sur **Enregistrer**.

6. Facultatif : Si vous souhaitez définir une date de début dans les Rapid7 enregistrements Intégration de vulnérabilité - API et Intégration d'élément vulnérable Rapid7 - API pour récupérer des données historiques lors de votre importation initiale à partir de l'analyse Rapid7 , suivez ces étapes.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez utiliser ces données pour vous aider avec Fermeture des détections obsolètes dans Réponse aux vulnérabilités.

a. Accédez à la **Rapid7 Vulnerability Integration** > **Administration** > **Intégrations**.
La Rapid7 liste des intégrations s'affiche.

b. Cliquez sur l'un des enregistrements d'intégration pour l'ouvrir.

(Optional) En haut du formulaire, cliquez sur le lien **ici** pour modifier l'enregistrement.

Le champ **Importer depuis** la date dans les intégrations est vide par défaut, à l'exception Rapid7 de l'API et de l'intégration Rapid7 d'éléments vulnérables Rapid7 : API. Pour ces intégrations, ces champs sont définis sur 1998-12-31 ou 1999-01-01.

Pour récupérer des données historiques lors de votre importation initiale à partir de l'analyse Rapid7 , définissez une date de début dans les enregistrements d'intégration appropriés. Ce processus fonctionne pour toute Rapid7 intégration, avec les exceptions suivantes :

- Les Rapid7 intégrations Exploit et Malware Kit n'affichent pas le champ **Importer depuis** , car elles n'effectuent pas de mises à jour Delta et n'utilisent donc pas ce champ.
- L'intégration Rapid7 de la liste des actifs ignore le champ, car son intention est de récupérer toutes les données.
- Pour l'exécution initiale de l'API Rapid7 InsightVM Intégration complète des éléments vulnérables lorsque le module Fermer automatiquement les éléments vulnérables périmés est activé et que le champ **Importer depuis** est laissé vide.

  Lorsque vous activez la fonctionnalité de fermeture automatique, une exécution réussie de l'intégration complète des éléments vulnérables Rapid7 ou de l'intégration complète des éléments vulnérables Rapid7 - API est requise. Ces intégrations sont désactivées par défaut.

  Lorsque vous activez l'intégration complète des Rapid7 InsightVM éléments vulnérables – API, si vous laissez le champ **Importer depuis** vide sur la page de configuration de l'intégration, la valeur du champ **Il y a jours** du formulaire Fermer automatiquement les éléments vulnérables périmés est également utilisée pour la date **d'importation depuis** lors de la première exécution de l'intégration. La valeur par défaut pour Fermer automatiquement les éléments vulnérables périmés est de (90 jours).

  Par exemple, si le champ **jours plus tôt** du formulaire Éléments vulnérables périmés à fermeture automatique est 90 et que le champ **Importer depuis** de la page Intégration complète des éléments vulnérables Rapid7 : page de configuration de l'API est vide, la première exécution de l'intégration importe les données des 90 derniers jours.

  Cette relation entre les champs **Importer depuis** et **jours plus tôt** s'applique uniquement à la première exécution d'intégration. Par la suite, la modification du champ **« jours plus tôt** » du formulaire Fermer automatiquement les éléments vulnérables périmés n'affecte pas le champ **Importer depuis sur** la page Intégration d'élément vulnérable complet Rapid7 : page de configuration de l'API. Le champ est remplacé par l'heure de début de la première exécution afin que les exécutions d'intégration suivantes importent uniquement les informations delta

  Le champ **Importer depuis** est modifiable ; vous pouvez entrer les valeurs de votre choix pour chacune des intégrations.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Accédez à la **Tout** > **sn_sec_int_impl.liste** > **Rapid7 InsightVM**.

   a. Le paramètre **d'instance** d'intégration import_startime_buffer_comprehensive définit un temps tampon de 24 heures avant l'heure spécifiée dans le champ **Importer depuis** afin que les actifs analysés à partir de ce temps tampon soient récupérés pendant l'exécution de l'intégration **complète des éléments vulnérables Rapid7 - API** . Vous pouvez modifier cette durée tampon en fonction de vos besoins.

   b. Facultatif : Définissez le paramètre **close_stale_detections***sur true* pour fermer les détections obsolètes qui ne proviennent plus de l'API Rapid7 pour les actifs qui sont analysés et récupérés via l'API Rapid7 via l'API **Rapid7 Comprehensive Vulnerable Item Integration - API.**

   Vous avez terminé avec succès les étapes d'installation, d'installation et de configuration pour le Intégration des vulnérabilités Rapid7. Vous êtes maintenant prêt à examiner et à vérifier les données importées.

Que faire ensuite

Les Rapid7 analyseurs et Qualys sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Ré-analyse** n'est pas disponible.

Pour activer ces analyseurs, en tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin :

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Localisez le produit de scanner que vous souhaitez activer et cliquez sur l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher Activé.
4. Cliquez sur **Mettre à jour**.

   Le produit que vous avez activé s'affiche dans le champ Source sur les enregistrements d'éléments vulnérables et de tâches de rattrapage après la prochaine importation, et **l'action Analyser de nouveau** est disponible.

Si votre environnement nécessite des importations séparées par domaine, reportez-vous à la section Créer des importations séparées par domaine pour une intégration.

Pour créer ou affiner vos règles de recherche avant l'importation, reportez-vous à la section Créer une règle de recherche de CI de Vulnerability Response.

Filtrage par Rapid7 sites

Filtrez par site pour les types d'intégration ainsi que Rapid7 Nexpose les Rapid7 InsightVM types d'intégration d'entrepôt de données.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'utilisation du filtrage de site peut avoir un impact sur les performances. Pour plus d'informations sur les performances et d'autres considérations avant d'utiliser le filtrage de site, consultez KB0789221 .

Pourquoi et quand exécuter cette tâche

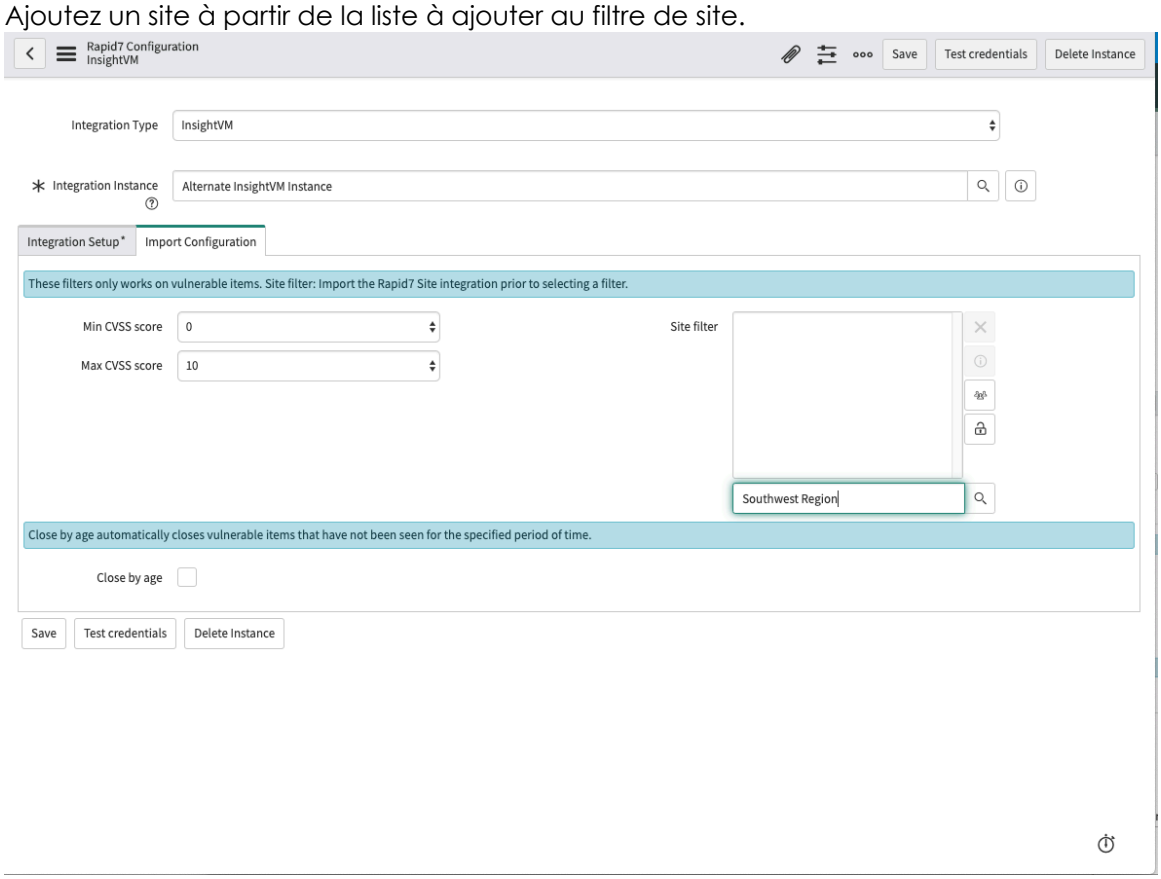
Procédure

1. Accédez à la **Tout** > **Rapid7 Vulnerability Integration** > **Configuration**.
2. Sélectionnez une instance d'intégration.
3. Cliquez sur l'onglet **Configuration de l'importation** .

   Remarque : Si vous voulez tous les sites, laissez le champ de filtre de site vide. Aucun filtre de site n'équivaut à ajouter tous les sites.

   Les sites sont spécifiques à l'instance d'intégration. La liste de recherche pour le filtrage de site affiche à la fois les sites d'instance d'intégration de l'entrepôt de Rapid7 InsightVM données et Rapid7 Nexpose ceux de l'entrepôt de données. Assurez-vous que le site que vous choisissez correspond à l'instance d'intégration que vous avez sélectionnée. Par exemple, si vous choisissez un site d'entrepôt de données, par erreur, ce site ne fonctionnera pas pour le filtrage de site par Rapid7 InsightVM.

4. Cliquez sur la liste de recherche pour afficher les enregistrements du site pour l'instance d'intégration actuelle.
5. Ajoutez un site à partir de la liste à ajouter au filtre de site.



6. Répétez la sélection pour ajouter d'autres sites.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Enregistrer**.
   Ces sites sont utilisés pour filtrer par site lors de la prochaine importation. Pour plus d'informations sur l'ajout du préfixe SITE aux données de votre site, reportez-vous à la section Ajoutez SITE à vos balises de site Rapid7 InsightVM .

Ajoutez SITE à vos balises de site Rapid7 InsightVM

Ajoutez le préfixe SITE à vos Rapid7 InsightVM balises de site pour les mettre en surbrillance dans votre liste de balises.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Remarque : Si nécessaire, changez de périmètre pour Rapid7 Integration for Security Operations.

Procédure

1. Dans la boîte de navigation de gauche, tapez : *sys_properties.list*.
2. Sous **Nom**, recherchez : *sn_vul_r7.prefix_site_to_rapid7_tags*.
3. Ouvrez *sn_vul_r7.prefix_site_to_rapid7_tags*.
4. Remplacez **la valeur** par **vrai**.
5. Cliquez sur **Mettre à jour**.
   Les balises de site nouvelles et existantes sont précédées lors de la prochaine importation de Rapid7 InsightVM.

Dédupliquer les enregistrements d'entrepôt de Intégration des vulnérabilités Rapid7 données

Lors de la migration vers le type d'intégration **InsightVM** à partir du type d'intégration **Entrepôt de données** , vous pouvez dédupliquer les éléments vulnérables de l'entrepôt de données existants tant qu'ils appartiennent aux mêmes données sources que vos Rapid7 InsightVM données.

Avant de commencer

Rôle requis : sn_vul_r7.admin, sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

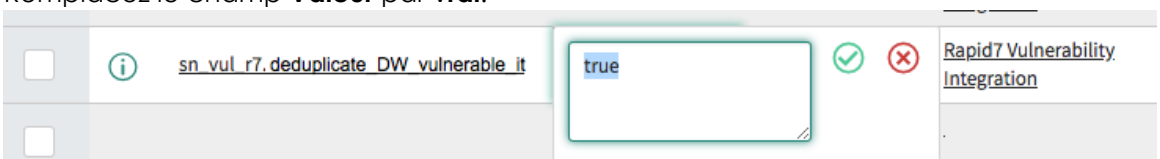
Pourquoi et quand exécuter cette tâche

Cette déduplication fonctionne uniquement lors de la migration de l'entrepôt Rapid7 Nexpose de données vers l'intégration Rapid7 InsightVM des éléments vulnérables.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Rapide 7** > **Intégrations**.
2. Définir toutes les Rapid7 Nexpose intégrations d'entrepôt de données Paramètres de colonnes **Actifs** sur **Faux**, ce qui désactive les intégrations.
3. Saisissez `sys_properties.list` dans le panneau de navigation de gauche.
4. Recherchez le **nom** : `sn_vul_r7.deduplicate_DW_vulnerable_item`.
5. Remplacez le champ **Valeur** par **vrai**.



6. Cliquez sur l'icône de coche verte .
   Lors de la prochaine Rapid7 InsightVM importation d'intégration d'élément vulnérable, toute correspondance avec des enregistrements d'entrepôt de données existants empêche la création d'un élément vulnérable en double.

Intégration des vulnérabilités Rapid7 Exécuter le graphique d'état

Rapid7 NexposeLes capteurs collectent les données et les envoient automatiquement aux produits de la salle d'opérationRapid7 InsightVM, qui analysent et corrèlent Rapid7 Nexpose en permanence les informations.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à suivre la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en visualisant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Reportez-vous à la rubrique Réponse aux vulnérabilités Espaces de travailet Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Intégration des vulnérabilités Rapid7 permet de mapper facilement Réponse aux vulnérabilités les vulnérabilités aux CI et aux services aux entreprises afin de déterminer l'impact et la priorité des menaces potentiellement malveillantes. Le Intégration des vulnérabilités Rapid7 module État d'exécution est une vue graphique de l'état des Intégration des vulnérabilités Rapid7 exécutions.

Pour afficher ces données dans la vue héritée, accédez à **Tout** > **Toutes les intégrations de vulnérabilités Rapid7** > **État de l'exécution de l'intégration**.

À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions précédentes de Réponse aux vulnérabilités

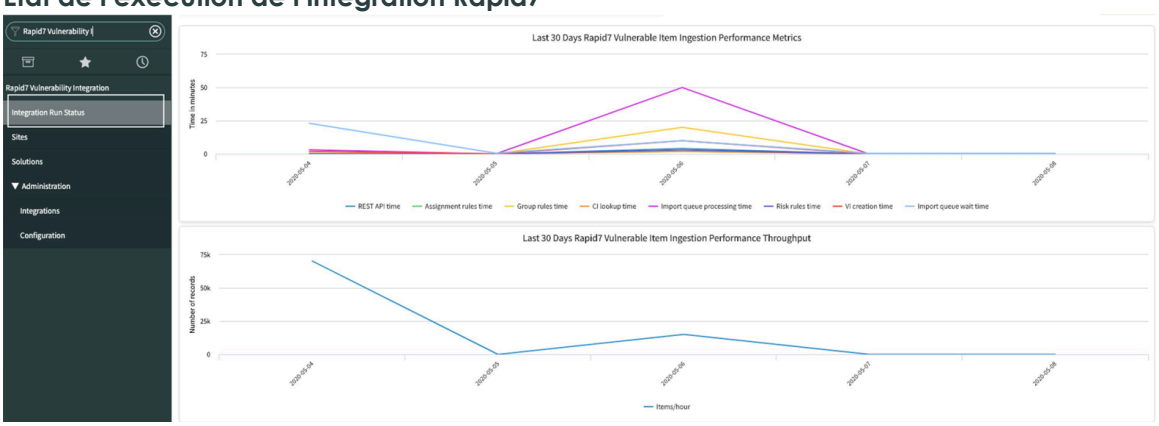
Dans le graphique, pointez sur n'importe quelle pièce (barre, secteur, point de données, etc.) pour afficher des données générales spécifiques à cette pièce. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

Plusieurs facteurs peuvent avoir un impact sur les performances de l'exécution de l'intégration, comme la quantité de données et le temps nécessaire pour traiter ces données. Deux nouveaux graphiques ont été ajoutés pour comparer les mesures de performance :

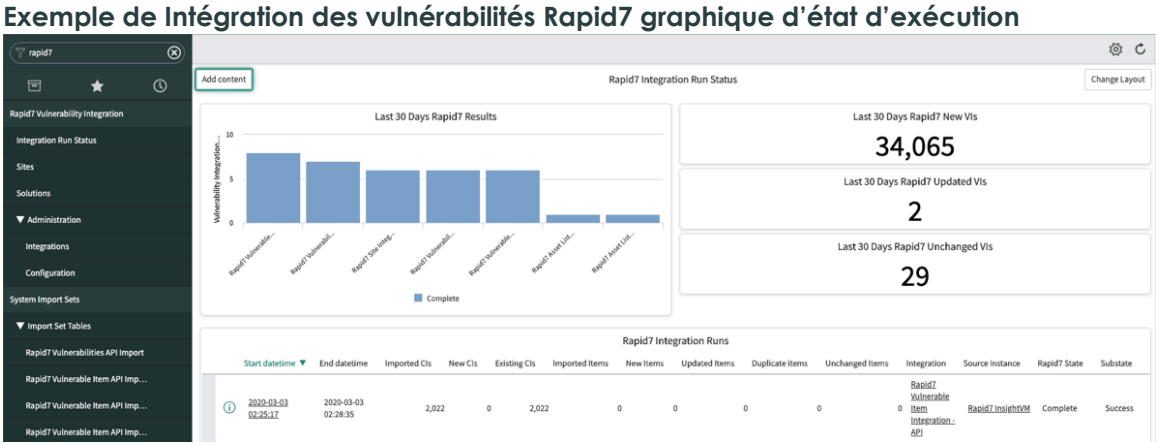
- Rapid7 Mesures de performances d'ingestion d'éléments vulnérables : comparez les mesures de performances quotidiennes pour les règles d'affectation, les règles de groupe, les règles de risque, le temps d'attente en file d'attente, le temps de traitement de la file d'attente et d'autres statistiques pour les éléments vulnérables au cours des 30 derniers jours, afin d'identifier la cause de tout écart de performance.
- Rapid7 Rendement de performance d'ingestion d'éléments vulnérables : comparez le débit quotidien d'ingestion d'éléments vulnérables pour l'intégration d'éléments Rapid7 vulnérables - API. Le débit est mesuré en éléments par heure.

Remarque : Dans Rapid7, ces graphiques sont pris en charge uniquement pour l'intégration d'Insight VM.

État de l'exécution de l'intégration Rapid7



Exemple de Intégration des vulnérabilités Rapid7 graphique d'état d'exécution



- La valeur de la colonne Éléments importés représente le nombre total d'éléments vulnérables créés à partir d'une exécution d'intégration.
- La colonne Nouveaux éléments affiche le nombre d'éléments vulnérables créés à partir d'une exécution d'intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La colonne Éléments dupliqués n'est plus renseignée. Vous préférez peut-être supprimer cette colonne de l'affichage.
- La colonne Éléments mis à jour affiche le nombre de fois où des éléments vulnérables sont mis à jour au cours d'une exécution d'intégration. Cette valeur n'est pas le nombre d'éléments vulnérables uniques qui sont mis à jour. Si, par exemple, un élément vulnérable est mis à jour deux fois au cours de l'exécution de l'intégration, il est compté deux fois et affiché sous la forme `de 2` éléments mis à jour.
- La colonne Éléments inchangés affiche les éléments vulnérables trouvés pendant l'exécution de l'intégration qui existent déjà dans la base de données, mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

Remarque : L'intégration s'exécute avec zéro résultat pour les quatre valeurs suivantes : **les nouveaux CI**, les **CI existants**, les **nouveaux éléments** et les **éléments mis à jour** sont exclus de la liste des **exécutions de l'intégration Rapid7** .

Intégration des vulnérabilités Rapid7 Exécuter des rapports de graphique d'état

Nom	Description
Résultats des 30 derniers jours Rapid7	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Exécuter dans un visuel de barre.
Nouveaux VI au cours des 30 derniers jours Rapid7	Nombre de nouveaux éléments vulnérables importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour au cours des 30 derniers jours Rapid7	Nombre d'éléments vulnérables mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Doublons des 30 derniers jours Rapid7	Nombre d'éléments vulnérables en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Rapid7 Exécutions des intégrations	L'exécution de l'intégration enregistre dans une liste. **Remarque : V16.1 :** Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection de la *sn_vul_detection* table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, après la fin de l'exécution de l'intégration.
Mesures de performance d'ingestion d'élément vulnérables au cours des 30 derniers jours Rapid7	Mesures de performances quotidiennes pour les éléments vulnérables comparées au cours des 30 derniers jours.
Rendement de performance d'ingestion d'élément	Débit quotidien d'ingestion d'éléments vulnérables pour l'intégration d'éléments Rapid7 vulnérables : API mesuré au cours des 30 derniers jours.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration des vulnérabilités Rapid7 Exécuter des rapports de graphique d'état (suite)

Nom	Description
vulnérable au cours des 30 derniers jours Rapid7	

Afficher le tableau de bord de l'état des exécutions d'importation Intégration des vulnérabilités Rapid7

Utilisez le tableau de bord d'état de l'exécution de l'importation Rapid7 de vulnérabilité pour vérifier la réussite de vos exécutions d'intégration, localiser les problèmes et prendre des décisions de rattrapage.

Avant de commencer

Rôles requis : sn_vuln.admin

Pourquoi et quand exécuter cette tâche

Cette procédure repose sur les hypothèses suivantes.

- Vous avez Réponse aux vulnérabilités et le Intégration des vulnérabilités Rapid7 installé et configuré.
- Intégration des vulnérabilités Rapid7 Les importations sont planifiées et en cours d'exécution.
- Rapid7 Les graphiques d'état d'exécution de l'intégration sont en cours d'utilisation.

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 19.0 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite les données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Rapid7** > **État de l'exécution de l'intégration**.

   À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

   Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

2. Si vous n'utilisez pas le graphique d'état d'exécution de l'intégration Rapid7 , accédez à **Rapid7** > **Intégrations**.
   a. Choisissez une intégration.
   b. Cliquez sur la liste connexe **Exécutions de l'intégration de vulnérabilité** .
3. Vérifiez que toutes les importations ont réussi.

   Trouble?

   Les causes les plus courantes d'un échec d'exécution :

   - Interruption du réseau
   - Désintégration du bit dans le transfert de données, ce qui entraîne la corruption des données pendant la transformation

   Pour toutes ces conditions, cliquez sur **Exécuter maintenant** et réexécutez l'intégration.

Lancer une nouvelle analyse pour l'intégration de Rapid7 vulnérabilité

Lancez de nouvelles analyses dans la Rapid7 plateforme pour vérifier que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés.

Avant de commencer

Remarque : Les nouvelles analyses des éléments vulnérables de Rapid7 l'entrepôt de données ne sont pas prises en charge.

Vous pouvez lancer de nouvelles analyses à partir des espaces de travail Vulnerability Response. Pour plus d'informations, consultez Analyser à nouveau les enregistrements et les tâches de rattrapage dans Vulnerability Manager Workspace et Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT.

Rôles requis : Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Pourquoi et quand exécuter cette tâche

Pour les nouvelles analyses dans l'environnement classique, reportez-vous aux sections suivantes.

Les nouvelles analyses sont prises en charge. Vous pouvez lancer une nouvelle analyse sur demande pour les éléments vulnérables importés à partir d'intégrations Rapid7 InsightVM à partir de votre Now Platform® instance.

Remarque : Le Rapid7 scanner est désactivé par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont Rapid7 une application comme source, le bouton Ré-analyse n'est pas disponible.

Pour aider à réduire les frais généraux et le volume impliqués par les analyses complètes planifiées, les responsables des rattrapages, les spécialistes informatiques, les analystes de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérabilité ou les gestionnaires de vulnérabilités peuvent lancer de nouvelles analyses ciblées sur demande pour des vulnérabilités spécifiques sur des actifs (éléments de configuration) dans leurs environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de remédiation (RT), d'entrée tierce (TPE) ou d'éléments détectés à partir de votre Now Platform® instance.

Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, vos correctifs et vos autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

À titre d'exemple, l'ensemble de votre environnement est analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été effectuée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines la prochaine analyse planifiée pour vérifier qu'elle a été corrigée. Pour vérifier que votre correctif corrige avec succès une vulnérabilité critique détectée lors d'une analyse précédente, vous pouvez lancer une nouvelle analyse ciblée à partir de votre Now Platform recherche Rapid7 d'éléments vulnérables. Vous pouvez afficher les résultats mis à jour sur vos éléments vulnérables lors de la prochaine importation planifiée de vulnérabilité et d'intégrations d'éléments Rapid7 InsightVM vulnérables.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

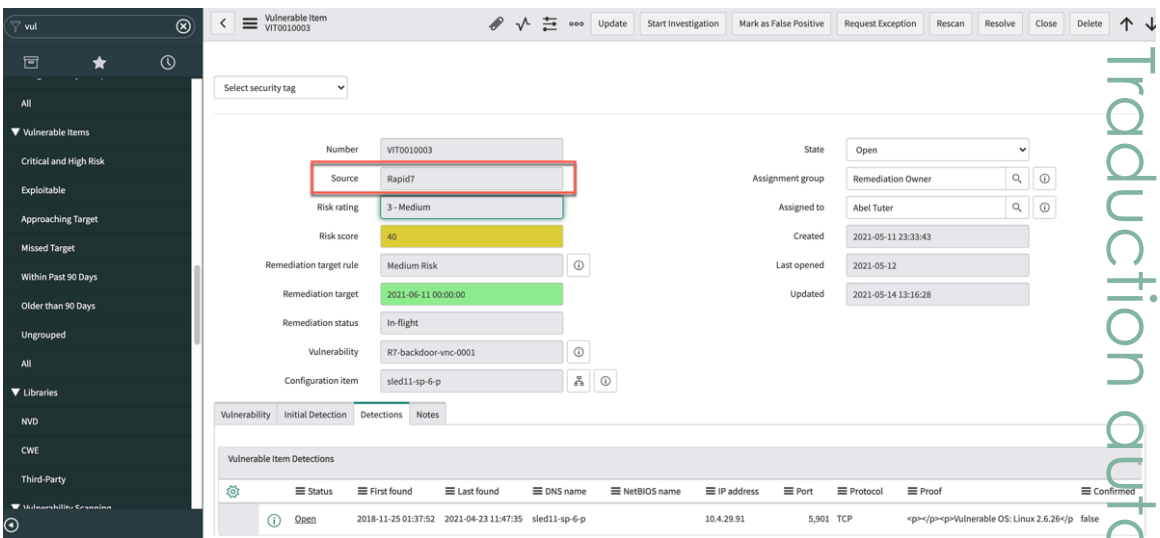
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lancer de nouvelles analyses pour les VI avec Rapid7 comme source. Verify Rapid7 s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le Créateur de conditions pour regrouper les VI par source. Ou, si la colonne **Source** n'est pas affichée dans la vue Liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône d'engrenage et déplacez **Source** de **Disponible** à **Sélectionné**.

Lorsque vous lancez de nouvelles analyses, évitez de déclencher simultanément des analyses pour un ID source à partir de plusieurs sources. La dernière demande d'analyse génère une erreur.

Par exemple, si vous lancez une nouvelle analyse pour un VI à partir d'un enregistrement de VI et que vous demandez également une autre nouvelle analyse à partir d'un enregistrement de tâche de rattrapage qui contient ce même VI, il est probable que la deuxième demande échoue.



3. Vous pouvez également accéder à **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **tiers** pour la tâche de rattrapage ou les enregistrements d'entrées de tiers, respectivement, que vous souhaitez utiliser pour la nouvelle analyse.

   En fonction de votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

   - Sur un enregistrement de VI unique, le VI doit provenir du Rapid7 produit et se trouver dans un état autre que Fermé. Pour plusieurs enregistrements de VI, tous les VI que vous sélectionnez dans la vue de liste doivent provenir du produit et se trouver dans un état autre que Fermé Rapid7 .
   - Sur un enregistrement de tâche de rattrapage, la tâche de rattrapage peut être dans n'importe quel état autre que Fermé et tous les éléments vulnérables associés doivent provenir du Rapid7 produit.
   - Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du produit dans un Rapid7 état autre que Fermé.
   - Sur un enregistrement d'élément détecté, le VI doit provenir du Rapid7 produit et être dans un état autre que **Fermé**.

4. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour les vues de listes, sélectionnez les VI que vous souhaitez réanalyser dans la liste et, dans la liste **Action sur les lignes sélectionnées** , sélectionnez **Analyser à nouveau**.

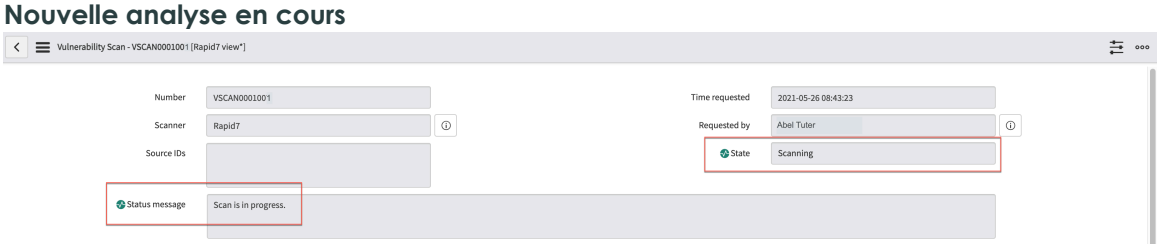
5. Dans la fenêtre contextuelle qui s'affiche, confirmez la nouvelle analyse.
   Un message s'affiche indiquant que votre analyse est en cours de traitement (**Mis en file d'attente**). Dans le message, cliquez sur le lien **Afficher les détails** pour vérifier l'état de la nouvelle analyse (analyse enfant) et afficher toutes les autres nouvelles analyses lancées à partir de l'enregistrement. L'état de toutes les nouvelles analyses peut être consulté à tout moment sous la liste connexe Analyses au bas des enregistrements de VI, de tâche de rattrapage, de TPE et d'élément détecté que vous utilisez pour lancer les nouvelles analyses.

   Lorsque l'analyse est en cours, le champ État passe à **Analyse** et le champ Message d'état affiche **Scan is in progress (L'analyse est en cours**).

   Remarque : Chaque nouvelle analyse prend en charge 500 actifs par analyse. Si votre demande comporte plus de 500 actifs, d'autres analyses enfants sont demandées.

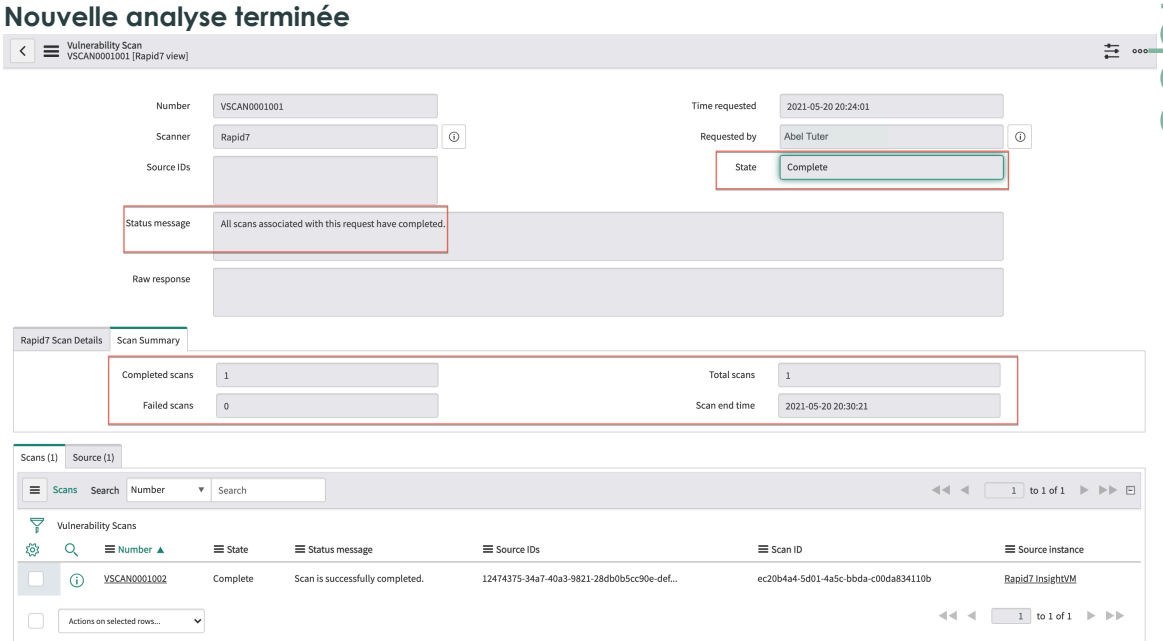
Votre Now Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine correctement ou jusqu'à l'expiration de la période de suivi définie, selon la première éventualité.

Nouvelle analyse en cours



Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de votre Now Platform® nouvelle analyse a cessé, et non à la date à laquelle la nouvelle analyse elle-même s'est arrêtée. Tous les VI qui sont passés ou passeront à l'état Fermé/Fixe sont importés avec la prochaine importation planifiée des Rapid7 intégrations.

Nouvelle analyse terminée



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

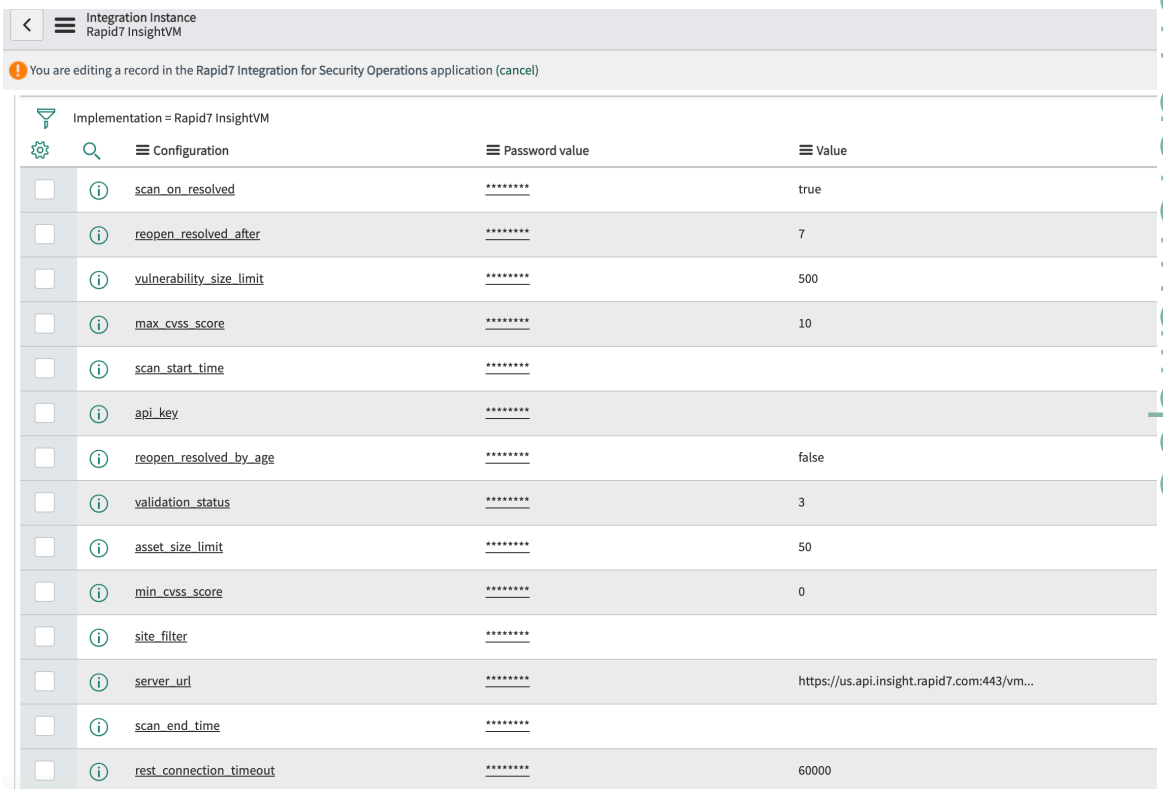
Vous pouvez également lancer une nouvelle analyse à la demande pour une vulnérabilité spécifique sur un actif spécifique. Vous pouvez afficher les résultats de ces analyses une fois l'analyse terminée sur les enregistrements actualisés de VI, de tâche de rattrapage, de TPE et d'élément détecté à partir desquels vous avez lancé l'analyse.

La valeur du champ État sur les enregistrements d'analyse de vulnérabilité est importée à partir de Rapid7. Lorsque l'analyse est terminée avec succès, l'état est défini sur Terminé. Si l'analyse ne se termine pas avec succès, une valeur d'erreur s'affiche.

Analyses automatiques et analyses planifiées

En tant que gestionnaire ou analyste des vulnérabilités, vous pouvez spécifier et planifier le moment où de nouvelles analyses sont lancées pour les VI et les RT. Vous pouvez également activer les analyses automatiques pour les VI et les tâches de rattrapage définies sur Résoudre.

6. Pour modifier les paramètres d'intégration sur l'instance d'intégration, accédez à **Rapid7 Vulnerability Integration** > **Administration** > **Configuration**.
7. Dans l'enregistrement de configuration Rapid7, s'il n'est pas sélectionné, dans la liste **Type d'intégration**, sélectionnez **Rapid7 InsightVM.**
8. À droite du champ **Instance d'intégration** , cliquez sur l'icône d'informations, puis sur **Ouvrir l'enregistrement**.
9. Sur l'enregistrement Rapid7 InsightVM de l'instance d'intégration, localisez les paramètres de planification des analyses et modifiez-les si nécessaire.



scan_on_resolved Indique si l'analyse est lancée lorsqu'une vulnérabilité est résolue. La valeur par défaut est **false** (désactivée).

Si ce paramètre est défini sur `vrai`, chaque fois qu'un élément vulnérable ou une tâche de rattrapage est défini sur Résolu, le workflow permettant d'analyser à nouveau l'élément vulnérable et la tâche de rattrapage respectifs est déclenché automatiquement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

scan_start_time

Définissez l'heure de début de l'analyse au format **HH :mm** (format 24 heures) dans le fuseau horaire UTC pour l'heure de début de la fenêtre pour laquelle vous souhaitez que de nouvelles analyses soient disponibles.

La valeur par défaut est `00:00`.

scan_end_time

Définissez l'heure de fin de l'analyse au format **HH :mm** (format 24 heures) dans le fuseau horaire UTC pour l'heure de fin de la fenêtre d'analyse disponible.

La valeur par défaut est `23:59`.

Si une analyse est lancée dans la fenêtre de temps prévue, elle est lancée instantanément. Si l'analyse est lancée en dehors de la fenêtre, elle est mise en file d'attente pour la prochaine fenêtre planifiée.

Par exemple, si vous entrez une heure de début de `00:00` pour le *`scan_start_time`* paramètre et *`scan_end_time`* une de 10:00 le matin même, les analyses planifiées ou lancées manuellement en dehors de la fenêtre horaire de minuit à 10 heures sont mises en file d'attente et lancées à l'heure de début de l'intervalle de temps du jour suivant `00:00`.

Dans le même exemple, si vous lancez manuellement une nouvelle analyse à 11h00, la nouvelle analyse n'est pas immédiatement lancée, car elle se trouve en dehors des heures d'analyse configurées disponibles. La demande d'analyse reste en file d'attente jusqu'au début de la fenêtre horaire du jour suivant, dans cet exemple `00:00`.

Définir des paramètres de filtre supplémentaires pour Rapid7 InsightVM les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec la Intégration Rapid7 pour Opérations de sécurité pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec le Rapid7 InsightVM produit.

Avant de commencer

Cas d'utilisation : en tant que gestionnaire ou analyste des vulnérabilités, vous souhaiterez peut-être filtrer les données de vos requêtes afin de ne pouvoir examiner que certains détails de vulnérabilité. Par exemple, vous pouvez afficher uniquement les vulnérabilités importées qui sont `critiques` et `sévères`.

Pour vous aider à collecter ces données, ajoutez Rapid7 des paramètres pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

Sans ajouter d'appels d'API ou de codage supplémentaires, à partir de la version 13.4, la fonctionnalité vous permet de personnaliser les informations de votre requête HTTP à l'aide Rapid7 InsightVM des paramètres de votre Now Platformfichier . Les intégrations suivantes Rapid7 InsightVM prennent en charge le filtrage en ajoutant du contenu JSON dans le corps de la demande :

- Rapid7 InsightVM API d'intégration d'élément vulnérable
- Rapid7 InsightVM API d'intégration de vulnérabilité
- Rapid7 InsightVM

Vous devez savoir comment utiliser JSON des chaînes pour cette fonctionnalité.

Rôle requis : sn_vul.vulnerability_admin

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

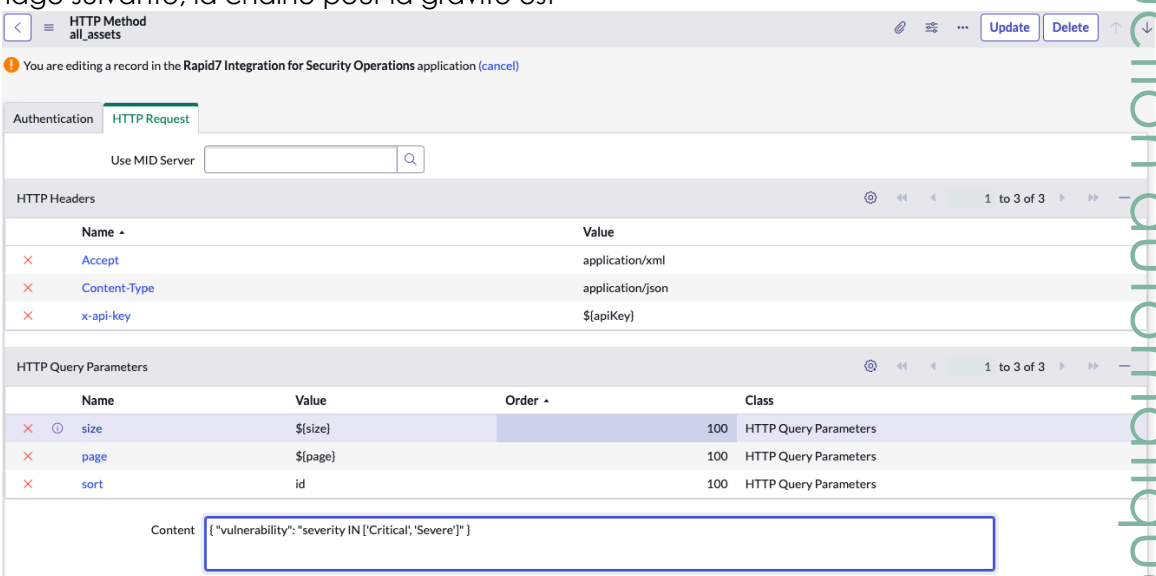
Procédure

1. Localisez les paramètres pris en charge par le Rapid7 InsightVM produit sur le site développeur Rapid7 que vous souhaitez utiliser pour votre filtrage.

   Vous pouvez créer les paramètres du corps de la demande en vous référant à la Rapid7 documentation. Les paramètres et les valeurs que vous entrez à partir du produit ne sont pris en charge qu'au niveau de l'instance d'intégration Rapid7 InsightVM .

2. Accédez à la **Tout** > **Rapid7 Vulnerability Integration** > **Administration** > **Intégrations**.
3. Sur la page de liste Intégrations Rapid7, cliquez sur l'enregistrement de l'intégration Rapid7 InsightVM que vous souhaitez ouvrir.
4. À droite de la page, cliquez sur l'icône d'information (I) pour le message REST, puis sur **Ouvrir l'enregistrement**.
5. Avec l'onglet de demande HTTP sélectionné, sous Méthodes HTTP, dans la colonne Nom, cliquez sur un élément pour ouvrir ses paramètres de requête HTTP.
6. Sous Enregistrement de méthode HTTP, sous Paramètres de requête HTTP, dans le champ Contenu, entrez les valeurs de paramètre que vous avez trouvées sur le site développeur Rapid7 .

   Dans l'image suivante, la chaîne pour la gravité est ajoutée.



   Si vous souhaitez entrer plusieurs paramètres, reportez-vous à la documentation pour plus d'informations sur la Rapid7 séparation de chaque valeur.

7. Cliquez sur **Mettre à jour**.

Présentation de Shodan Exploit Integration

L'application ServiceNow® Shodan Exploit Integration utilise les Shodan données importées du moteur de recherche pour vous aider à déterminer l'impact et la priorité des exploits potentiellement malveillants.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Shodan Exploit Integration

Le Shodan moteur de recherche collecte des données d'exploitation et l'API Shodan met cette base de données à la disposition du Now Platform®. Il s'intègre facilement à l'application ServiceNow® Réponse aux vulnérabilités pour mapper les exploits aux vulnérabilités tierces, enrichissant ainsi les données d'exploitation dans votre instance.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Chaque jour, les travaux planifiés invoquent automatiquement les intégrations dans l'ordre où elles sont répertoriées. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Versions disponibles

Version de mise en production pour Xanadu	**Notes de publication**
Intégration d'exploit Shodan v10.6 et 10.7	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Rôles

Shodan Les tâches d'intégration d'exploit impliquent les rôles suivants.

- sn_vul_shodan.admin : les utilisateurs disposant de ce rôle peuvent lire, écrire et supprimer des enregistrements.
- sn_vul_shodan.user : les utilisateurs disposant de ce rôle peuvent lire et écrire des enregistrements.
- sn_vul_shodan.read : les utilisateurs disposant de ce rôle peuvent lire les enregistrements.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Intégrations d'exploits Shodan

Pour afficher les intégrations d'exploits Shodan , accédez à **Tout** > **Shodan Exploit Integration** > **Intégrations**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les intégrations suivantes sont incluses dans le système de base. Ces intégrations sont actives par défaut.

Intégrations d'exploits Shodan

Intégration	Description
Intégration Shodan ExploitDB	Récupère les données ExploitDB et enrichit vos données de Shodan vulnérabilité tierces. Cette intégration est définie pour s'exécuter quotidiennement à 03:15:00.
Intégration de Shodan Metasploit	Récupère les informations Metasploit à partir de vos données de Shodan vulnérabilité tierces et les enrichit. Cette intégration est définie pour s'exécuter quotidiennement à 01:15:00.

Pour modifier l'heure de début par défaut des importations d'intégration planifiées, reportez-vous à la section Définir Shodan l'heure d'importation de l'intégration de l'exploit.

Pour afficher les données d'exploitation dans les vulnérabilités tierces, reportez-vous à la section Afficher Réponse aux vulnérabilités les bibliothèques de vulnérabilité.

La modification d'autres paramètres d'Exploit Shodan Integration nécessite un niveau avancé ServiceNow et Réponse aux vulnérabilités une expertise et dépasse le cadre de la documentation du produit.

Préparation de l'intégration d'Exploit Shodan

Une intégration réussie Shodan d'Exploit nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Préparez l'intégration en effectuant ces tâches. L'intégration d'Exploit Shodan suppose que vous connaissez le moteur de recherche et l'API Shodan .

Avant de commencer

Exploit Shodan Integration nécessite une clé API. Inscrivez-vous sur le Shodan site web pour un abonnement gratuit afin d'acquérir cette clé.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter l'intégration, apportez les changements de configuration nécessaires en fonction de vos besoins.

- Si vous n'avez pas importé de données NIST Vulnerability Database (NVD) dans Réponse aux vulnérabilités, faites-le avant d'installer Exploit Shodan Integration. L'importation des données NVD garantit que vos données CVE (Common Vulnerability and Exposure) remplissent automatiquement les enregistrements d'exploit.

  En l'absence de données NVD, un espace réservé est créé dans l'enregistrement de l'exploit et n'est pas saisi avant la prochaine mise à jour NVD. Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces.

- Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installez et configurez le Intégration d'exploit Shodan pour Opérations de sécurité

Avant de pouvoir exécuter la Intégration d'exploit Shodan dans votre instance, téléchargez-la et installez-la à partir du ServiceNow Store. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que vous disposez d'autorisations valides ServiceNow pour l'application et pour l'application Intégration d'exploit ShodanRéponse aux vulnérabilitésOpérations de sécurité.	Pour vérifier les autorisations, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Pour plus d'informations sur l'obtention d'autorisations pour une Opérations de sécurité application à partir de , reportez-vous à la ServiceNow Storesection .
(Facultatif) Si elle n'est pas déjà installée et activée, il peut être préférable d'installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce.	Pour en savoir plus sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités.
Munissez-vous de la clé API d'Exploit Shodan Integration.	Consultez Préparation de l'intégration d'Exploit Shodan.

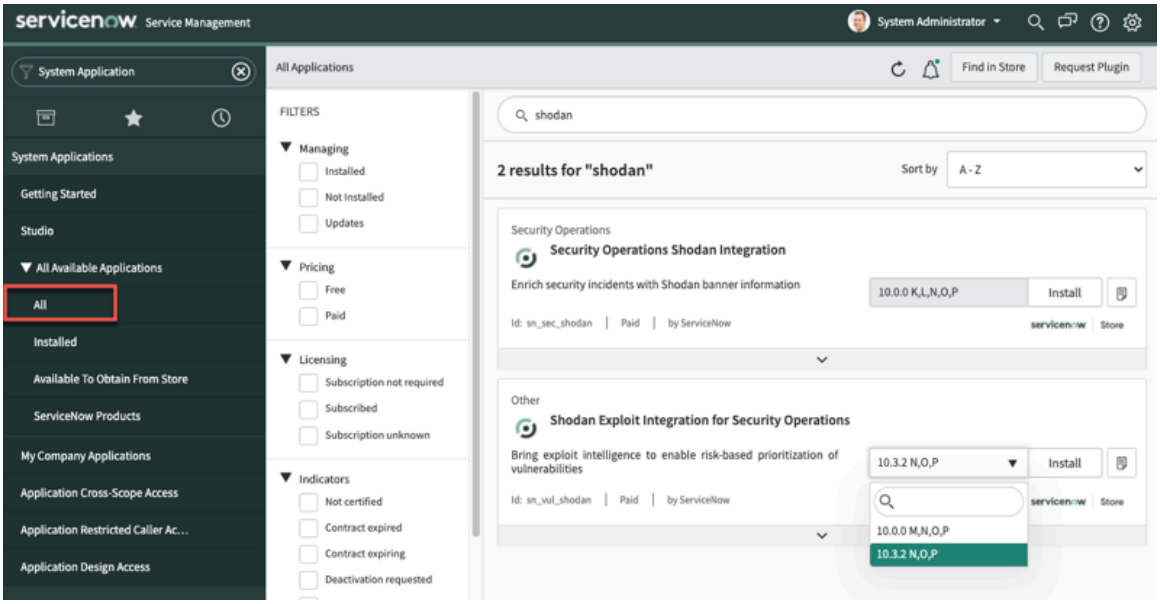
Rôle requis : administrateur

Procédure

1. Connectez-vous à l'instance sur laquelle Now Platform vous souhaitez installer l'application Intégration d'exploit Shodan .
2. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tout**.
3. Recherchez l'application Intégration d'exploit ShodanOpérations de sécurité , sélectionnez la version souhaitée et cliquez sur **Installer**.

Traduction automatique

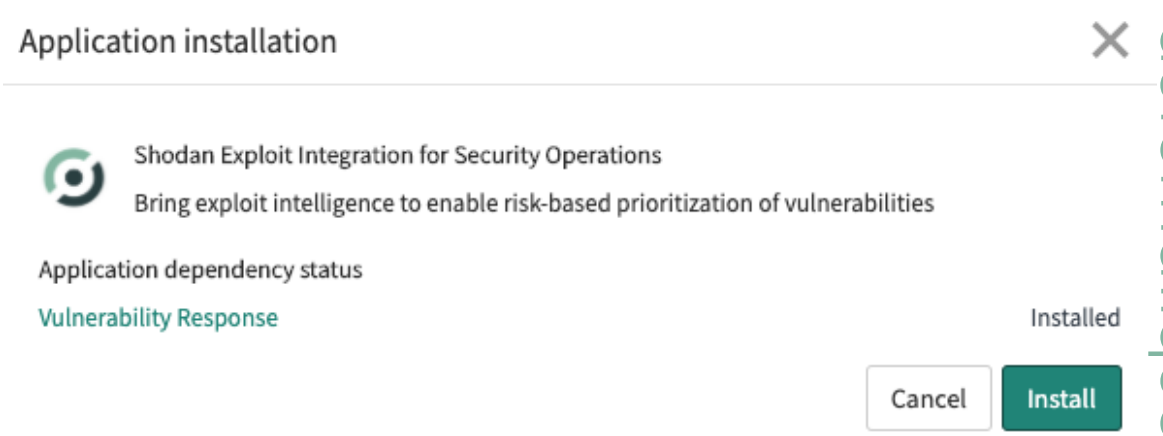
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Si vous avez droit à une mise à jour pour cette application, le bouton **Mettre à jour** s'affiche.

La boîte de dialogue d'installation de l'application affiche l'état de dépendance de l'application. Toutes les dépendances requises qui ne sont pas encore installées sont automatiquement installées avec l'application.

4. Dans la boîte de dialogue, cliquez sur **Installer**.

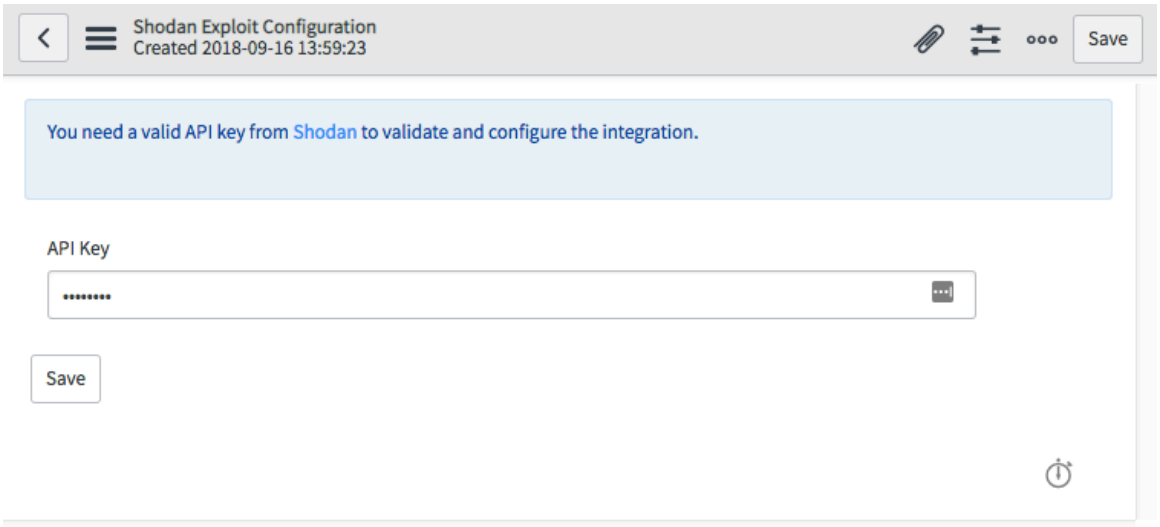


La boîte de dialogue Installer indique quand l'installation est terminée avec succès.

5. Fermez la boîte de dialogue Installer.
6. Accédez à la **Shodan Exploit Integration** > **Configuration**.
7. Entrez votre Shodan clé API.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Cliquez sur **Enregistrer**.
   Votre Intégration d'exploit Shodan configuration est terminée.

Définir Shodan l'heure d'importation de l'intégration de l'exploit

Pour plus de commodité, vous pouvez réinitialiser l'heure de début pour les intégrations d'exploits Shodan .

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Après l'importation initiale, Shodan les intégrations d'exploits importent des données de différentiel, sauf si une importation complète est demandée. Voir Effectuer une importation manuelle Shodan d'exploit pour plus d'informations sur les importations complètes.

Procédure

1. Accédez à la **Tout** > **Shodan Exploit Integration** > **Intégrations**.
2. Choisissez une intégration.
3. Cliquez sur le lien pour modifier l'enregistrement.
4. Définissez les nouvelles options **Exécution** et **Temps** .
   L'heure est calculée en heures dans l'heure locale. L'heure par défaut pour les importations d'exploits est 03 Shodan :15:00.
5. Cliquez sur **Mettre à jour**.
   La nouvelle heure est utilisée pour la prochaine importation planifiée.

Effectuer une importation manuelle Shodan d'exploit

Si votre importation initiale a échoué, ou si vous ne souhaitez pas attendre l'importation initiale planifiée, vous pouvez effectuer une importation de données complète indépendamment de la tâche planifiée quotidienne.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Shodan Exploit Integration** > **Intégrations**.
2. Choisissez une intégration.
3. Cochez la case **Importation complète des données** .
4. Cliquez sur **Exécuter maintenant**.
   Une fois l'importation terminée, la case est décochée et les importations delta reprennent.

Afficher l'état de l'exécution de l'importation d'Exploit Shodan Integration

Utilisez la liste connexe Exécutions de l'intégration de vulnérabilité pour vérifier la réussite de vos exécutions d'intégration, localiser les problèmes et prendre des décisions de rattrapage.

Avant de commencer

Pour afficher l'état de l'exécution de l'importation Shodan :

- L'application Réponse aux vulnérabilités et l'intégration Exploit Shodan doivent être installées et configurées.
- Les importations d'intégration Shodan d'exploit doivent être planifiées et en cours d'exécution.

Rôle requis : sn_vuln.admin

Pourquoi et quand exécuter cette tâche

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Shodan Exploit Integration** > **Intégrations**.
2. Sélectionnez une intégration.
3. Cliquez sur la liste connexe **Exécutions de l'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.

Trouble?

Les causes les plus courantes d'un échec d'exécution sont les suivantes :

- Interruption du réseau
- Désintégration du bit dans le transfert de données, ce qui entraîne la corruption des données pendant la transformation

Si vous rencontrez l'une de ces conditions, cochez la case **Importation complète des données** , cliquez sur **Exécuter maintenant** et réexécutez l'intégration.

Présentation de l'intégration Tenable Vulnerability

L'application Intégration de Réponse aux vulnérabilités à Tenable développée par ServiceNow l'ingénierie pour Tenable Vulnerability Integration utilise des données importées des Tenable.io produits et Tenable.sc pour vous aider à hiérarchiser et à corriger les vulnérabilités de vos actifs. L'application est disponible avec un abonnement distinct à partir du ServiceNow® Storefichier .

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

L'intégration de vulnérabilité Tenable utilise deux intégrations Tenable.io Tenable et Tenable.sc, pour importer des données d'analyseurs tiers concernant vos actifs et vos vulnérabilités. L'application Intégration de Réponse aux vulnérabilités à Tenable prend en charge le produit à partir de la Tenable.sc version 5.13.

- Tenable.io est une intégration d'entreprise basée sur le cloud.
- Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le produit et votre Tenable.scNow Platform instance se trouvent dans le même environnement.
- Si le produit et votre Tenable.scNow Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID.

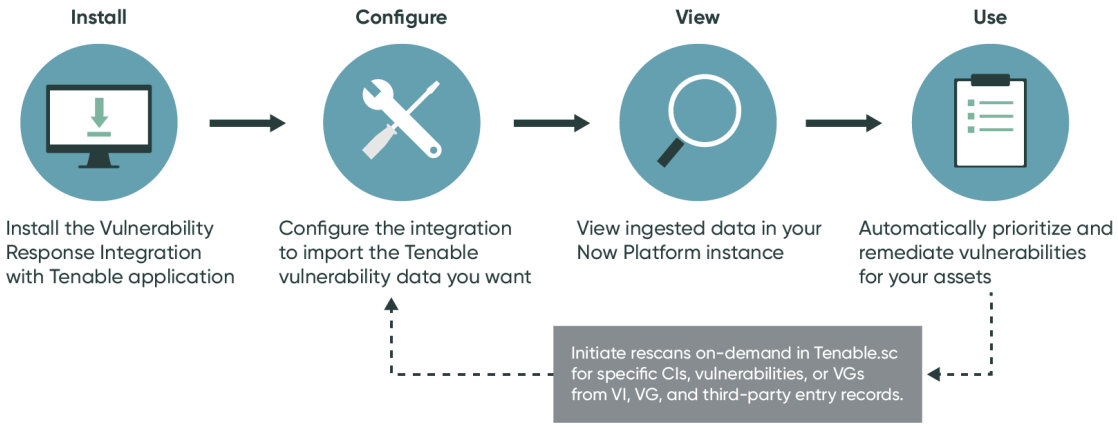
L'application Intégration de Réponse aux vulnérabilités à Tenable est disponible sur le ServiceNow Store avec un abonnement séparé.

Pour obtenir des listes et des descriptions des intégrations dans , consultez Tenable Vulnerability IntegrationTenable.ioIntégrations avec les applications ET Réponse aux vulnérabilitésConformité de la configuration et Tenable.scIntégrations avec l'application Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration de vulnérabilité tenable



Versions disponibles pour Xanadu

Version	Notes de publication
Intégration de Réponse aux vulnérabilités à Tenable v3.5, v3.6	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Termes et fonctionnalités clés des intégrations

Éléments vulnérables et vulnérabilités

Un élément vulnérable est créé dans votre instance lorsque :Now Platform

- Une vulnérabilité importée à partir d'un scanner tiers est mise en correspondance avec un actif existant (un élément de configuration dans votre CMDB). Le produit Tenable qualifie ces **correspondances de vulnérabilités**.
- Une vulnérabilité importée à partir d'un scanner tiers ne correspond pas à un actif existant dans votre CMDB. Dans ce cas, un CI sans correspondance est également créé ainsi qu'un élément vulnérable.

  Pour les CI sans correspondance, vous pouvez également utiliser le moteur Identification et réconciliation (IRE) pour créer des CI dans deux nouvelles classes lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte. Dans le cas contraire, des CI sans correspondance sont créés dans les classes de CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement.

Entrées et modules d'extension de vulnérabilité tiers

Les entrées de vulnérabilité tierces sont importées à partir d'analyseurs tiers et répertoriées dans la table Entrées de vulnérabilité tierces de votre Now Platform instance. Les entrées de vulnérabilité tierces de Tenable sont ingérées et mises en Réponse aux vulnérabilités correspondance avec les actifs existants répertoriés dans votre CMDBfichier . Tenable fait référence aux entrées de vulnérabilité tierces en tant que **modules d'extension.**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément de configuration (CI)

Les éléments de configuration sont les actifs existants répertoriés dans votre CMDBfichier .

Élément détecté

Les ressources ingérées à partir de l'importation d'actif Tenable sont mises en correspondance avec des éléments de configuration existants dans votre CMDB. Les actifs importés sont mis à jour.

Si aucune correspondance n'est trouvée, un CI est créé dans la classe CI sans correspondance du CMDB. Si le module d'extension Modèles de classe CI CMDB est activé, le moteur Identification et réconciliation (IRE) crée de nouveaux CI à l'aide de nouvelles classes. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement. Si le CI d'origine, sans correspondance, est reclassé, les enregistrements d'éléments détectés sont mis à jour pour refléter l'état. Les éléments détectés vous donnent une visibilité sur la façon dont les actifs sont identifiés et mappés aux CI dans le CMDB.

Règles de recherche de CI

Lorsque les données sont importées à partir d'une intégration tierce, Vulnerability Response utilise automatiquement les données de l'hôte (actif) pour rechercher des correspondances dans la base de données de gestion des configurations (CMDB). Les règles de recherche de CI sont utilisées pour identifier les CI et les ajouter aux enregistrements de VI lorsque des VI sont créés pour vous aider à y remédier.

Nouvelle analyse et analyse de rattrapage

Vous pouvez lancer une commande de nouvelle analyse ciblée sur un élément de configuration, une tâche de rattrapage ou une entrée de tiers spécifique directement à partir des enregistrements d'élément vulnérable, de tâche de rattrapage et d'entrée de vulnérabilité tiers dans votre Now Platform instance. Tenable fait référence à cette nouvelle analyse en tant **qu'analyse de rattrapage**.

Fermer automatiquement les VI plus anciens

Le module Fermer automatiquement les éléments vulnérables périmés de votre Now Platform, vous pouvez nettoyer les éléments vulnérables (VI) anciens et périmés qui n'ont pas été trouvés récemment par vos intégrations tierces. Le déplacement de ces VI vers **Fermé** vous aide à réduire le nombre d'éléments vulnérables actifs et de tâches de rattrapage, ainsi qu'à rapprocher les actifs dans votre CMDB. Vous pouvez utiliser toutes les intégrations avec le Intégration de Réponse aux vulnérabilités à Tenable pour fermer automatiquement les VI périmés.

Instance

Ce terme fait référence à une occurrence distincte de votre Now Platform® application.

Intégration

Une intégration est une référence spécifique à un produit d'une intégration, comme l'intégration des actifs ou l'intégration Tenable.io du module d'extension Tenable.sc . Il s'agit des intégrations distinctes qui appartiennent à des produits Tenable spécifiques dans l'intégration de vulnérabilité Tenable de votre instance.

Instance d'intégration

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce terme désigne les intégrations Tenable distinctes répertoriées par leur Tenable.io et Tenable.sc leurs produits.

Déploiement

Lorsqu'une intégration prend en charge plusieurs sources, une existence d'intégration unique et distincte est appelée déploiement de votre intégration. Le terme est utilisé pour désigner la ou les intégrations et les produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de diverses intégrations des produits et Tenable.ioTenable.sc dans votre environnement.

Les Tenable.io intégrations et Tenable.sc incluent également les fonctionnalités clés suivantes :

- Les résultats de l'évaluation de configuration, c'est-à-dire les résultats des tests, ainsi que les politiques, les tests de configuration (contrôles) et les citations avec des sources de référence peuvent être importés dans l'application Conformité de la configuration avec le Tenable.io produit. Consultez Tenable.ioIntégrations avec les applications ET Réponse aux vulnérabilitésConformité de la configuration et Explorer Conformité de la configuration pour en savoir plus sur le fonctionnement de cette intégration avec l'application Conformité de la configuration .
- À partir de la version 2.1 du , créez des éléments de Tenable Vulnerability Integrationconfiguration (CI) uniques qui incluent différents identificateurs de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. Identifiez les actifs distincts dans votre environnement et mettez à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous donner plus de détails sur vos vulnérabilités.
- Vous pouvez planifier le moment où vous souhaitez que les tâches s'exécutent pour toutes les Tenable.io intégrations and Tenable.sc . Vous pouvez également exécuter manuellement des travaux planifiés sur demande.
- Pour les importations d'actifs avec Tenable.io, vous pouvez activer les balises d'actif pour organiser et suivre les actifs répertoriés dans CMDB votre Tenable.io environnement.
- Les Tenable.io intégrations et Tenable.sc vous permettent de configurer des règles de recherche de CI pour définir la manière dont les données d'actifs de sources tierces sont utilisées pour identifier les éléments de configuration (CI) dans votre Now Platform CMDB.
- Les Tenable.io intégrations et Tenable.sc vous permettent de définir des filtres d'importation sur l'importation des vulnérabilités afin d'importer uniquement les vulnérabilités de Tenable que vous souhaitez. Pour Tenable.io, vous avez la possibilité d'importer des vulnérabilités **corrigées** de Tenable avec l'importation des vulnérabilités.
- Pour Tenable.sc, vous pouvez lancer de nouvelles analyses sur demande directement à partir d'enregistrements d'éléments vulnérables, de tâches de rattrapage et d'entrées tierces dans votre Now Platform instance. Si des VI sont passés à **l'état Fermé/Fixe** , mais ne sont pas encore mis à jour dans votre instance, vous pouvez vérifier que les vulnérabilités sur des éléments de configuration spécifiques ont été corrigées. Consultez Lancer une nouvelle analyse pour l'intégration Tenable.sc.

Les sections suivantes répertorient plus d'informations sur les intégrations Tenable.

Rôles Now Platform requis

Les tâches d'intégration nécessitent les rôles suivants dans votre Now Platform instance.

administrateur

L'administrateur système utilise l'Assistant de configuration pour installer l'application Intégration de Réponse aux vulnérabilités à Tenable . Si elle

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'Assistant de configuration.

sn_vul.vulnerability_admin

Une fois cette affectation effectuée, l'administrateur de vulnérabilité termine la configuration des intégrations Tenable dans l'assistant de configuration. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. L'administrateur de vulnérabilité configure toutes les applications et toutes les règles de réalité virtuelle pour les intégrations tierces installées.

sn_vul_tenable.configure_integration

Ce rôle contient le rôle granulaire sn_vul_tenable.read_integration et les utilisateurs dotés de ce rôle peuvent configurer l'application Intégration de Réponse aux vulnérabilités à Tenable .

sn_vul_tenable.read_integration

Les utilisateurs disposant de ces rôles peuvent afficher (lire) mais pas modifier les enregistrements de l'application Intégration de Réponse aux vulnérabilités à Tenable .

Groupe Vulnerability Response

Par défaut, le groupe Vulnerability Response est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Vulnerability Response héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner.

Éléments vulnérables

Les éléments vulnérables sont regroupés en tâches de rattrapage en fonction des règles de tâche de rattrapage et affectés pour le rattrapage en fonction de vos règles d'affectation. Pour plus d'informations, consultez Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage et Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Règles de recherche d'éléments de configuration (CI)

Les règles de recherche de CI identifient les CI et déterminent quand les ajouter à un élément vulnérable. Pour plus d'informations sur le fonctionnement des règles de recherche de CI, reportez-vous à Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Remarque : Les règles, une fois supprimées, ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Les règles de recherche suivantes Tenable.io sont fournies avec le système de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- Nom d'hôte
- DNS
- IP

Les règles de recherche suivantes Tenable.sc sont fournies avec le système de base.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Remarque : Plusieurs valeurs pour ip_address, mac_address, FQDNS et network_interfaces sont utilisées pour un actif. Toutes les valeurs sont prises en compte dans les règles de recherche de CI pour la correspondance. Toutes les valeurs sont utilisées pour créer plusieurs cartes réseau à l'aide d'IRE.

Pour en savoir plus sur la configuration de la catégorisation des ressources cloud inégalées dans votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

Nouvelles propriétés pour ignorer les adresses IP

Dans Tenable.io, deux propriétés sont disponibles si vous souhaitez ignorer plusieurs adresses IP ou plusieurs adresses Mac dans le cadre de vos règles de recherche de CI :

ignoreIPAddress

Une liste d'adresses IP à ignorer pour la recherche de CI et la création de CI.

ignoreMacAddress

Une liste d'adresses MAC à ignorer pour la recherche de CI ou la création de CI.

Éléments détectés

Ce module répertorie les éléments de configuration détectés lors de l'importation à partir des intégrations d'éléments vulnérables Tenable et d'actifs Tenable.

Remarque : Le filtre par défaut de cette liste est défini sur `Sans correspondance`. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour plus d'informations sur le module Éléments détectés, reportez-vous à la section Éléments détectés.

Balises d'actifs

Les balises d'actif (également appelées balises d'hôte) sont utilisées pour organiser et suivre les actifs de votre organisation. Vous pouvez affecter des balises à vos ressources. Ensuite, lors du lancement des analyses, vous pouvez sélectionner des balises associées aux ressources que vous souhaitez analyser. Le module Balises d'actif vous permet de télécharger les données des balises d'actif Tenable.io depuis votre instance de manière planifiée. Les données d'actif Tenable.io qui incluent des balises d'actif sont extraites et transformées à l'aide des cartes de transformation d'intégration Tenable.io Asset Transform .

Toutes les balises d'actif sont importées dans le cadre de l'intégration d'actif Tenable.io . Les balises d'actifs sont généralement utilisées pour le filtrage dans Réponse aux vulnérabilités les règles d'affectation et les règles de tâche de rattrapage. Les balises sont affichées dans le formulaire Élément détecté.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Exécutez l'intégration Tenable.io des actifs avant de créer Réponse aux vulnérabilités des règles d'affectation ou des règles de tâche de rattrapage dans l'application afin que toutes les balises soient disponibles pour ces règles avant que Réponse aux vulnérabilités les éléments vulnérables ne soient importés et regroupés. Notez également les points suivants concernant les balises :

- Le stockage des balises n'est pas sensible à la casse. Par exemple, si vous créez une balise pour décrire les actifs de votre emplacement San Diego, et que vous créez la balise `San Diego` , vous ne pouvez pas également créer une balise `SAN DIEGO` et la stocker dans la table Balise d'actif. `San Diego` et `SAN DIEGO` sont considérés comme étant la même balise d'actif par le système. La balise importée en premier est celle qui est stockée et reconnue à l'avenir.
- L'utilisation de balises d'actifs en tant que clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises d'actif sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises d'actifs sont contrôlées par la propriété système globale sn_vul.import_asset_tags. Cette propriété est définie sur `vrai` par défaut. La désactivation des balises les désactive dans toutes les Now Platform® instances.

Filtres de récupération de données

Les paramètres de récupération de données vous aident à déterminer spécifiquement le type et le périmètre des données que vous souhaitez importer de l'application Tenable vers votre Now Platform® instance. Pour obtenir la liste des paramètres les plus couramment utilisés, reportez-vous à la section Paramètres de récupération de données pour Tenable Vulnerability Integration.

Évaluation de priorité de vulnérabilité (VPR)

L'évaluation de priorité de vulnérabilité (VPR) est un attribut du produit Tenable qui est importé et utilisé avec un nouveau calculateur de risque par défaut dans Réponse aux vulnérabilités. La règle de risque Tenable est installée avec l'application dans le Intégration de Réponse aux vulnérabilités à Tenable cadre du calculateur de risque par défaut dans les calculateurs de vulnérabilité à partir de Réponse aux vulnérabilités.

Cette règle de risque est désactivée par défaut.

En activant la règle du calculateur de risque Tenable, les valeurs VPR importées sont utilisées pour calculer le score de risque pour les éléments vulnérables. Distribution de pondération par défaut pour ce calculateur de risque : VPR = 70 %, Actif = 15 % et Criticité opérationnelle = 15 %. L'activation de cette règle du calculateur de risque Tenable peut avoir un impact sur vos performances d'ingestion de données. Pour en savoir plus sur Réponse aux vulnérabilités les calculateurs et la règle du calculateur de risque Tenable, reportez-vous à la section Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.

Installation et configuration

Après avoir téléchargé le Intégration de Réponse aux vulnérabilités à Tenable à partir du , l'installation ServiceNow® Storeet la configuration sont prises en charge par l'assistant de configuration dans Réponse aux vulnérabilités. Consultez Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration pour plus d'informations.

Tenable.ioIntégrations avec les applications ET Réponse aux vulnérabilitésConformité de la configuration

Les Tenable.io intégrations dans l'application Intégration de Réponse aux vulnérabilités à Tenable sont disponibles dans les Réponse aux vulnérabilités applications et Conformité de la configuration .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste des Tenable.io intégrations

Multisource est pris en charge pour toutes les Tenable.io intégrations .Tenable.sc Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'Assistant de configuration dans Réponse aux vulnérabilités. Vous pouvez également installer et configurer l'application à partir de l'Assistant Intégration de Réponse aux vulnérabilités à Tenable de configuration.

Tenable.io est une intégration d'entreprise basée sur le cloud. Consultez le tableau suivant pour connaître les noms et les descriptions des intégrations prises en charge pour le Tenable.io produit.

L'intégration Tenable.io des résultats de conformité et l'intégration du remplissage des Tenable.io résultats de conformité sont inactives par défaut.

Pour les activer :

1. Accédez à la **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.
2. Dans la liste Intégrations Tenable, cliquez sur un nom d'intégration pour ouvrir l'enregistrement et cochez la case **Actif** pour l'activer. Vous préférerez peut-être conserver les paramètres de calendrier dans leurs valeurs par défaut pour que ces intégrations démarrent.

Intégrations de Tenable.io

Intégration	Description
Tenable.io Intégration des actifs	• Récupère toutes les données d'actif, y compris les balises d'actif, du Tenable.io produit et les traite dans votre instance. • À partir de la version 3.0, si l'intégration des résultats de conformité est activée, vous pouvez importer des données d'évaluation Tenable.io de configuration sécurisée ainsi que des données d'actif importées. Ces données peuvent vous aider à identifier et à répondre aux vulnérabilités liées à la configuration sur vos actifs. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API Asset. • La sortie de cette intégration est les éléments détectés. • Les données sont importées par blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours. • À partir de la version 2.2, *Last Scan Time* les actifs présentant des vulnérabilités sont importés et mis à jour uniquement.
Tenable.io Intégration des résultats de conformité	• À partir de la version 3.0, les données d'évaluation de la configuration sécurisée importées à partir de l'intégration des résultats de conformité, ainsi que les données

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	importées à partir de l'intégration des actifs, peuvent vous aider à identifier les vulnérabilités liées à la configuration sur vos actifs et à y répondre. • Si cette option est activée, elle récupère les données d'évaluation de la configuration sécurisée de haut niveau et les traite dans votre Now Platform instance. Les données importées comprennent les résultats des tests, ainsi que les politiques, les tests de configuration (contrôles) et les citations avec des sources de référence. • Les données d'évaluation pour les actifs manquants ou les actifs sans ID d'actif ne sont pas importées. • Si un résultat de test est importé et que son actif correspondant ne peut pas être mis en correspondance dans votre instance, le résultat du test est ignoré et l'ID de l'actif manquant est stocké dans un enregistrement temporaire dans la table [sn_vul_tenable_missing_asset]. • La valeur totale des actifs **ignorés (manquants**) est répertoriée dans le champ CI ignorés de l'onglet **Configuration** de l'enregistrement d'exécution de l'intégration pour cette intégration.
Tenable.io Intégration du remplissage des résultats de conformité	• Lorsqu'elle est activée, cette intégration s'exécute automatiquement une fois l'intégration des actifs terminée avec succès dans le cadre d'une exécution d'intégration chaînée. Cette intégration associe les données d'évaluation de la configuration aux actifs manquants répertoriés dans la table [sn_vul_tenable_missing_asset]. • Importe jusqu'à 200 ID d'actifs pour tous les actifs manquants détectés ou présents dans l'instance une fois l'importation de l'intégration des actifs terminée avec succès. • Supprime les enregistrements temporaires de la table [sn_vul_tenable_missing_asset] lorsque les actifs peuvent être mis en correspondance avec les données d'évaluation de configuration correspondantes.
Tenable.io Intégration des informations d'identification de numérisation	• Cette intégration récupère les informations d'identification de numérisation configurées dans Tenable.io. • Coordonne les appels de message REST à l'API d'informations d'identification. • Le résultat de cette intégration est les informations d'identification d'analyse renseignées dans la table [sn_vul_tenable_scan_credential].

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	• Les informations d'identification importées sont utilisées pour accéder au scanner lorsque des demandes d'analyse sont lancées à partir du Now Platform. • Cette intégration est planifiée pour s'exécuter chaque semaine.
Tenable.io Intégration de modèle	Un enregistrement de modèle est envoyé lors de la Tenable.io nouvelle analyse. Cette intégration récupère les informations d'identification disponibles Tenable.io à utiliser pour les nouvelles analyses. Les informations d'identification sont spécifiques à l'instance et un enregistrement de modèle unique est importé et stocké temporairement en toute sécurité sur la table [sn_vul_tenable_io_template].
Tenable.io Intégration du module d'extension	• Récupère les données du module d'extension à partir du Tenable.io produit. Les données récupérées sont basées sur la date à laquelle les modules d'extension ont été mis à jour pour la dernière fois par une exécution d'intégration Tenable.io . • Cette importation garantit que les Tenable.io identificateurs (dix ID) sont à jour. • Coordonne les appels de message REST à l'API du module d'extension. • La sortie de cette intégration est constituée de vulnérabilités tierces.
Tenable.io Intégration des vulnérabilités corrigées	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.io produit et les traite dans votre instance. Les éléments vulnérables sont créés pour les enregistrements de détection qui sont dans les états **Ouvert** et **Rouvert** , car ces enregistrements nécessitent une correction. Les éléments vulnérables existants sont mis à jour par Vulnerability Response si les détections sont **corrigées**, mais les éléments vulnérables ne sont pas créés pour les détections **corrigées** par défaut, car Tenable considère les vulnérabilités **corrigéescomme atténuées**. • Lorsque le marqueur **Créer des temps de vulnérabilité pour les détections de vulnérabilité fixes** est activé dans l'Assistant de configuration, de nouveaux éléments vulnérables sont créés à l'état **Fixe** afin que vous ayez une visibilité sur les détections qui les ont créés. Étant donné que les VI sont créés pour les détections **fixes** qui n'existent pas déjà dans votre instance, cela peut avoir un impact négatif sur vos performances d'importation. Vous préférez peut-être laisser cette fonctionnalité désactivée afin que les détections **corrigées** ne fassent

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	que mettre à jour l'état des éléments vulnérables existants. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API de vulnérabilités. • La sortie de cette intégration est les éléments vulnérables (VI) **fermés/fixes** . Il crée également des actifs et des entrées tierces s'ils n'existent pas. • Les données sont importées par blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours. Cette exécution d'intégration est planifiée. Il s'agit d'une intégration enchaînée, ce qui signifie qu'une fois qu'une exécution est terminée avec succès, l'intégration des vulnérabilités ouvertes décrite ci-dessous est déclenchée. À partir de la version 3.3 de Tenable, vous pouvez afficher les informations suivantes pour les exécutions d'intégration de vulnérabilité : • **Blocs totaux :** Nombre total de blocs générés par Tenable • **Blocs disponibles :** Nombre de blocs disponibles au téléchargement pour ServiceNow
Tenable.io Intégration des vulnérabilités ouvertes	• Cette intégration est déclenchée une fois l'intégration Tenable.io des vulnérabilités corrigée terminée. • Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.io produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API de vulnérabilités. • La sortie de cette intégration est des éléments vulnérables (VI) **nouveaux/rouverts** . Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas. Tenable considère les vulnérabilités **actives comme cumulatives** (actuelle). • Les données sont importées par blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	À partir de la version 3.3 de Tenable, vous pouvez afficher les informations suivantes pour les exécutions d'intégration de vulnérabilité : • **Blocs totaux :** Nombre total de blocs générés par Tenable • **Blocs disponibles :** Nombre de blocs disponibles au téléchargement pour ServiceNow

Tenable.scIntégrations avec l'application Réponse aux vulnérabilités

Les Tenable.sc intégrations dans l'application Intégration de Réponse aux vulnérabilités à Tenable .

À partir de la Réponse aux vulnérabilités version 20.0, si un actif est analysé par un agent, la colonne L'agent existe affiche la valeur (vrai) dans la liste Éléments détectés qui indique qu'il s'agit d'une analyse authentique.

Liste des Tenable.sc intégrations

Multisource est pris en charge pour toutes les Tenable.io intégrations .Tenable.sc Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'Assistant de configuration dans Réponse aux vulnérabilités. Vous pouvez également installer et configurer l'application à partir de l'Assistant Intégration de Réponse aux vulnérabilités à Tenable de configuration.

- Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le produit et votre Tenable.scNow Platform instance se trouvent dans le même environnement.
- Si le produit et votre Tenable.scNow Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID.

Intégrations de Tenable.sc

Intégration	Description
Tenable.sc Intégration des actifs	Pour éviter de créer des éléments détectés en double avec des données d'actif importées, l'intégration des actifs du Tenable.sc produit est composée de deux intégrations. Intégration Tenable.sc des actifs ouverts Cette intégration importe les données de vulnérabilité de vos actifs que Tenable considère **comme cumulatifs** (actuels) ou **ouverts**. Les éléments vulnérables (VI) créés dans votre instance avec ces données d'actif importées sont considérés comme ouverts, c'est-à-dire à l'état **Ouvert** . Ces éléments vulnérables nécessitent une enquête et peuvent nécessiter une correction. L'intégration Tenable.sc des actifs immobilisés Cette intégration importe les données de vulnérabilité de vos actifs que Tenable

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	considère comme **atténuées** (n'étant plus vulnérables) ou **corrigées**. Les éléments vulnérables de ces actifs passent de l'état **Ouvert** à l'état **Fermé/Fixe** dans votre instance, car les résultats des analyses montrent qu'ils ne sont plus vulnérables. • Récupère toutes les données d'actif du Tenable.sc produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API Assets. • La sortie de cette intégration est les éléments détectés. • Le filtre de requête Tenable que vous sélectionnez dans l'assistant de configuration s'applique également à l'intégration Tenable.sc des actifs. Seuls les actifs présentant les vulnérabilités qui correspondent aux conditions du filtre de requête sont importés.
Tenable.sc Intégration du module d'extension	• Récupère les données du module d'extension à partir du Tenable.sc produit. Les données récupérées sont basées sur la date à laquelle les modules d'extension ont été mis à jour pour la dernière fois par une exécution d'intégration Tenable.sc . • Cette importation garantit que les Tenable.sc identificateurs (dix ID) sont à jour et que seules les vulnérabilités actives sont importées. • Coordonne les appels de message REST à l'API des modules d'extension. • La sortie de cette intégration est constituée de vulnérabilités tierces.
Tenable.sc Intégration des vulnérabilités corrigées	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.sc produit et les traite dans votre instance. Les éléments vulnérables sont créés pour les enregistrements de détection qui sont dans les états **Ouvert** et **Rouvert** , car ces enregistrements nécessitent une correction. Les éléments vulnérables existants sont mis à jour par Vulnerability Response si les détections sont **corrigées**, mais les éléments vulnérables ne sont pas créés pour les détections **corrigées** par défaut, car Tenable considère les vulnérabilités **corrigéescomme atténuées**. • Lorsque le marqueur **Créer des temps vulnérables pour les détections de vulnérabilité fixes** est activé dans l'Assistant de configuration, il crée de nouveaux VI à l'état

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	Fixe afin que vous ayez une visibilité sur les détections qui les ont créés. Étant donné que les VI sont créés pour les détections **fixes** qui n'existent pas déjà dans votre instance, cela peut avoir un impact négatif sur vos performances d'importation. Vous préférez peut-être laisser cette fonctionnalité désactivée afin que les détections **corrigées** ne fassent que mettre à jour l'état des éléments vulnérables existants. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API de vulnérabilités. • La sortie de cette intégration est les éléments vulnérables (VI) **fermés/fixes** . Il crée également des actifs et des entrées tierces s'ils n'existent pas. Cette exécution d'intégration est une exécution planifiée. Il s'agit d'une intégration chaînée, ce qui signifie qu'une fois qu'une exécution est terminée avec succès, l'intégration Tenable.sc des vulnérabilités ouvertes décrite ci-dessous est déclenchée. **Remarque :** Par défaut, les ID de famille 0 et 39 sont exclus de cette intégration.
Tenable.sc Intégration des vulnérabilités ouvertes	• Cette intégration est déclenchée une fois l'intégration Tenable.sc des vulnérabilités corrigée terminée. • Récupère les données de vulnérabilité en fonction des filtres de requête sélectionnés dans le Tenable.sc produit et les traite dans votre instance. • Crée des éléments vulnérables correspondants pour les vulnérabilités actives. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API de vulnérabilités. • Le résultat de cette intégration est **Mettre à jour/Créer de nouveaux** éléments vulnérables (VI) s'ils n'existent pas déjà. Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas. **Remarque :** Par défaut, les ID de famille 0 et 39 sont exclus de cette intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
Tenable.sc Intégration des informations d'identification de numérisation	• Cette intégration récupère les informations d'identification de numérisation configurées dans Tenable.sc. • Coordonne les appels de message REST à l'API d'informations d'identification. • Le résultat de cette intégration est les informations d'identification d'analyse renseignées dans la table [sn_vul_tenable_scan_credential]. • Les informations d'identification importées sont utilisées pour accéder au scanner lorsque des demandes d'analyse sont lancées à partir du Now Platform. • Cette intégration est planifiée pour s'exécuter chaque semaine.
Tenable.sc Intégration des vulnérabilités de remplissage	• Cette intégration de remplissage importe toutes les vulnérabilités ouvertes et corrigées qui auraient pu être manquées lors d'une importation. • Cette intégration importe les vulnérabilités ouvertes et corrigées des sept derniers jours pour mettre à jour vos détections et éléments vulnérables. • Cette intégration peut avoir un impact sur vos performances. • Cette intégration est désactivée par défaut. • Pour mettre à jour vos données de vulnérabilité et éviter d'éventuels problèmes de performances, vous préférez peut-être planifier l'exécution des intégrations des vulnérabilités corrigées Tenable.sc et des vulnérabilités ouvertes lorsqu'aucune autre analyse n'est en cours d'exécution. • Le résultat de cette intégration est : ◦ Éléments vulnérables (VI) **fermés/fixes**. Il crée également des actifs et des entrées tierces s'ils n'existent pas. ◦ **pour mettre à jour/créer de nouveaux** éléments vulnérables (VI) s'ils n'existent pas déjà. Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas.

Authentification utilisateur et Tenable.sc

L'authentification utilisateur est prise en charge par votre instance et la Now Platform® version 5.13 du Tenable.sc produit. L'authentification de l'utilisateur est requise si vous utilisez la version 5.12 ou antérieure du Tenable.sc produit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous sélectionnez l'authentification utilisateur pour les intégrations, les jetons peuvent expirer et être remplacés lors de l'exécution de l'intégration Tenable.sc . Dans la colonne Notes de l'enregistrement d'exécution de l'intégration de vulnérabilité (VIN), le message suivant s'affiche pour un processus à l'expiration d'un jeton, `Erreur : échec de la validation du jeton`. Aucune action n'est requise si ce message s'affiche. Les jetons expirés sont automatiquement actualisés en arrière-plan et le message n'indique pas une pause ou une erreur dans le processus d'intégration.

Préparation de l'intégration Tenable Vulnerability

Préparez l'intégration Tenable ServiceNow® Vulnerability en effectuant les tâches de configuration suivantes.

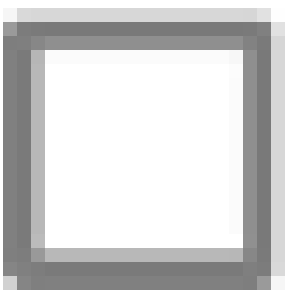
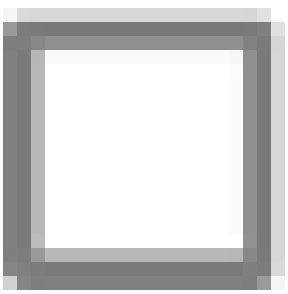
Avant de commencer

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Pour une installation et une configuration fluides de l'application Intégration de Réponse aux vulnérabilités à Tenable , il est préférable d'imprimer la liste de vérification suivante et de vérifier que les éléments répertoriés sont terminés avant d'installer l'application et d'importer les données de vulnérabilité dans votre Now Platform® instance.

Remarque : Si vous avez importé des données avec l'intégration créée par Tenable et que vous souhaitez commencer à utiliser Vulnerability ServiceNow® Response Integration avec Tenable, consultez le

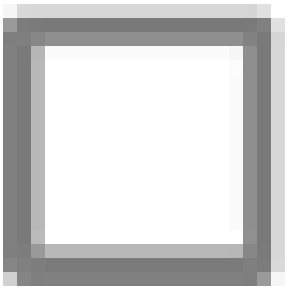
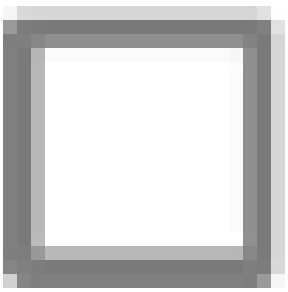
Pour obtenir des informations actuelles sur le nettoyage et la migration des données de l'intégration créée par Tenable vers l'intégration créée par ServiceNow, consultez l'article Directives pour migrer de l'intégration Tenable Vulnerability Response vers l'intégration ServiceNow Vulnerability Response avec Tenable [KB0960667].

Rôle requis : admin pour télécharger et installer l'application.

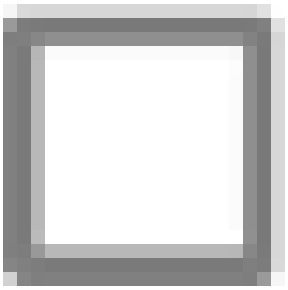
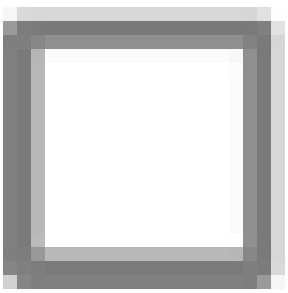
Tâche	Description
	(Facultatif) Si elle n'est pas déjà installée et activée, il peut être préférable d'installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour en savoir plus sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 12.1 ou Réponse aux vulnérabilités ultérieure.
	Si vous ne l'avez pas déjà sur votre instance, obtenez les autorisations et téléchargez l'application Intégration de Réponse aux vulnérabilités à Tenable sur votre Now Platform® instance. L'application Intégration de Réponse aux vulnérabilités à Tenable prend en charge le produit à partir de la Tenable.sc version 5.13. Consultez .

Traduction automatique

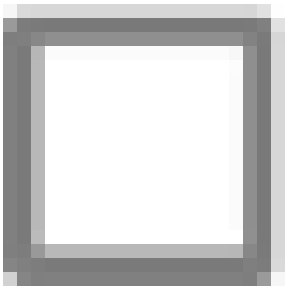
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Estimez le nombre d'éléments vulnérables que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, ou si vous avez besoin d'aide, contactez ServiceNow® le support technique.
	Vérifiez que vous disposez de groupes ou d'utilisateurs pour gérer les intégrations et corriger les éléments vulnérables. administrateur L'administrateur système utilise l'Assistant de configuration pour installer l'application Intégration de Réponse aux vulnérabilités à Tenable . Si elle n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'Assistant de configuration. sn_vul.vulnerability_admin Une fois cette affectation effectuée, l'administrateur des vulnérabilités termine la configuration des intégrations Tenable. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Configure toutes les applications et les règles de VR et configure les intégrations tierces. sn_vul_tenable.configure_integration Peut configurer l'intégration de vulnérabilité Tenable. Ce rôle contient le rôle granulaire sn_vul_tenable.read_integration. sn_vul_tenable.read_integration Peut afficher (lire) les enregistrements de l'intégration de vulnérabilité Tenable. Groupe Vulnerability Response Par défaut, le groupe Vulnerability Response est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Vulnerability Response héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner. L'administrateur système effectue l'affectation initiale des rôles aux utilisateurs et aux groupes dans l'Assistant de configuration pour l'intégration. Par défaut, le groupe Vulnerability Response est disponible. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance avant d'utiliser l'Assistant de configuration. Reportez-vous à la section Créer un groupe d'utilisateurs .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Des rôles granulaires et de profil sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.
	Pour améliorer les performances de votre première importation, vous pouvez désactiver certaines fonctionnalités, règles ou tâches dans votre instance. • Désactivez les calculateurs de vulnérabilité si vous ne les utilisez pas. Ces calculateurs, ainsi que ceux que vous avez définis, s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est créé ou mis à jour. Reportez-vous à la section Désactiver les calculateurs de vulnérabilité. • Lors de l'importation initiale des enregistrements, certaines règles métier liées aux notifications peuvent entraîner la génération de nombreuses notifications, ce qui a un impact sur les performances. Avant votre importation initiale, vous préférerez peut-être désactiver les règles métier liées aux notifications, comme décrit dans .Importer les modifications pour l'intégration de vulnérabilité Tenable
	Vérifiez que vous avez activé toutes les fonctionnalités, règles, modules d'extension de dépendance ou tâches dans votre instance requises pour l'intégration. • Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le produit et votre Intégration de Réponse aux vulnérabilités à TenableNow Platform instance se trouvent dans le même environnement. Si le produit et votre Tenable.scNow Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID. Pour plus d'informations sur les MID Servers dans votre instance, consultez Serveur MID . • Vérifiez que le module d'extension Centre d'intégration est installé et activé. Ce module d'extension permet aux composants du système de base d'appeler des systèmes externes à l'aide d'API d'intégration et active les étapes de protocole telles que REST. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tout** et localisez le module d'extension. S'il n'est pas installé dans votre instance, installez-le et activez-le.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Obtenez les informations d'identification Tenable. Vérifiez que vous disposez de tous les noms de compte, mots de passe et autres informations de service requis par vos produits Tenable afin d'y avoir accès. Tenable.io nécessite l'accès Administrateur avec un attribut d'autorisation supérieur ou égal à 64. Tenable.sc nécessite l'accès Analyste ou Gestionnaire de sécurité. **Remarque :** À partir de la version 3.8 de Intégration de Réponse aux vulnérabilités à Tenable, l'accès Tenable.io ne nécessite plus de privilèges d'administrateur. Un utilisateur de base avec un attribut d'autorisation égal à 16 peut également accéder au produit.

Vous êtes prêt à Installer l'application à l'aide de l'Assistant Intégration de Réponse aux vulnérabilités à Tenable de configuration.

Installer l'application à l'aide de l'Assistant Intégration de Réponse aux vulnérabilités à Tenable de configuration

Avant d'exécuter Tenable ServiceNow® Vulnerability Integration, vous devez télécharger l'application Intégration de Réponse aux vulnérabilités à Tenable à partir de et ServiceNow Store l'installer et la configurer à l'aide de l'assistant de configuration de l'application Réponse aux vulnérabilités .

Avant de commencer

Avant d'installer l'application Tenable, vérifiez que vous avez rempli tous les éléments de la liste de vérification dans Préparation de l'intégration Tenable Vulnerability.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Rôles requis : admin pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application Tenable dans l'Assistant de configuration. Administrateur de vulnérabilité (sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) pour configurer l'application dans l'Assistant de configuration après son installation.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation de l'application d'intégration**.

   Après quelques instants, les applications disponibles pour installation sur votre instance s'affichent.

2. Localisez la vignette **Tenable (Tenable Platform)** et cliquez sur **Installer**.

   Cette action installe l'application Intégration de Réponse aux vulnérabilités à Tenable que vous avez téléchargée à ServiceNow Storepartir du .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Suivez les instructions fournies dans l'assistant de configuration pour poursuivre l'installation.
4. Pour en savoir plus sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.

Que faire ensuite

Une fois l'installation terminée dans l'Assistant de configuration, accédez à **Configuration d'intégration>Intégrations de scanners dans l'Assistant** de configuration pour poursuivre la configuration. Si vous souhaitez plus d'informations pour compléter les invites fournies dans l'Assistant de configuration, reportez-vous à la section Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration.

Paramètres de récupération de données pour Tenable Vulnerability Integration

Les paramètres de récupération de données suivants vous aident à déterminer spécifiquement le type et le périmètre des données que vous souhaitez importer de Tenable ServiceNow® Vulnerability Integration vers votre Now Platform® instance.

Les paramètres décrits dans les sections suivantes vous aident à contrôler les données que vous souhaitez importer. En outre, vous pouvez définir les valeurs de ces filtres dans les instances d'intégration. Pour afficher les instances d'intégration, accédez à **Intégration de vulnérabilité tenable** > **Instances d'intégration** et cliquez sur votre intégration, Tenable.io ou Tenable.scsur .

Sur la page Instance d'intégration qui s'affiche, cliquez sur Paramètres de l'instance d'intégration pour afficher une liste des paramètres ou sur les onglets Intégrations de vulnérabilité pour un calendrier, Détails REST, Détails de l'intégration, Sources de données et Informations sur l'exécution de l'intégration.

Paramètres et filtres courants de gravité et de récupération pour Tenable.io et Tenable.sc dans votre Now Platform instance

Les paramètres suivants sont disponibles pour les Tenable.io intégrations et Tenable.sc dans votre Now Platform instance. Ces paramètres de configuration, ainsi que d'autres, sont affichés sur la page Instance d'intégration de votre Now Platform instance. Vous préférerez peut-être laisser ces paramètres dans leurs valeurs par défaut pour les premières exécutions d'intégration.

Tenable.io

insert_fixed

Si vous activez le marqueur **insert_fixed** dans l'assistant de configuration pour l'intégration d'importation des vulnérabilités, de nouveaux VI sont créés pour les détections à l'état **Fixe** qui n'existent pas déjà dans votre instance.

severity_critical

Ce filtre est activé par défaut (vrai) pour recevoir les vulnérabilités de gravité critique des intégrations de vulnérabilités ouvertes et Tenable.io des Tenable.io vulnérabilités corrigées.

severity_high

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de gravité élevée à partir des intégrations des vulnérabilités ouvertes et Tenable.io des Tenable.io vulnérabilités corrigées.

severity_medium

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce filtre est désactivé par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité moyenne à partir des intégrations de vulnérabilités ouvertes et Tenable.io de Tenable.io vulnérabilités corrigées.

severity_info

Ce filtre est désactivé par défaut (faux). Activez ce filtre pour recevoir les vulnérabilités de gravité au niveau des informations des intégrations de vulnérabilités ouvertes et Tenable.io des Tenable.io vulnérabilités corrigées.

severity_low

Ce filtre est désactivé par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité de faible niveau à partir des intégrations de vulnérabilités ouvertes et Tenable.io de Tenable.io vulnérabilités corrigées.

taille

Ce paramètre définit le nombre d'enregistrements de module d'extension à inclure dans l'ensemble de résultats à partir de l'intégration des modules d'extension Tenable.io . Doit être au format int32. La valeur par défaut est 1 000. La taille maximale est de 10 000 personnes.

num_assets

Le nombre maximal de vulnérabilités par bloc exporté à partir des intégrations Tenable.io des vulnérabilités corrigées et Tenable.io des vulnérabilités ouvertes. La valeur par défaut est 50.

chunk_size

Spécifie le nombre d'actifs par bloc exporté par l'intégration Tenable.io des actifs. La valeur par défaut est 1 000.

Tenable.sc

async_request

Ce paramètre est désactivé par défaut (faux). Activez ou désactivez ce paramètre pour effectuer des appels d'API asynchrones ou synchrones avec Tenable.sc , respectivement. Pour les appels synchrones, s'il y a un délai d'attente à 30 secondes, contactez l'assistance du produit Tenable pour régler le boîtier. Ce paramètre, une fois activé, est applicable pour toutes les intégrations de Tenable.sc. Pour les clients existants utilisant des appels asynchrones, un script correctif est disponible, qui ajoute un nouveau paramètre async_request aux instances d'intégration existantes Tenable.sc . Pour afficher les scripts correctifs, accédez à **Définition du système** > **Scripts correctifs**.

insert_fixed

Si vous activez le marqueur **insert_fixed** dans l'assistant de configuration pour l'intégration d'importation des vulnérabilités, de nouveaux VI sont créés pour les détections à l'état **Fixe** qui n'existent pas déjà dans votre instance.

décalage

Spécifie le nombre d'actifs, de modules d'extension et de vulnérabilités importés en une seule exécution d'intégration.

Filtres de requête

Les filtres de requête sont configurés à partir de la console Tenable. Ces filtres de requête ont des ID qui peuvent être sélectionnés à partir de l'Assistant de configuration ou de la page Instances d'intégration de votre Now Platform instance. Ces filtres sont appliqués lors de la récupération des données à partir des Tenable.sc intégrations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Messages REST pour l'intégration Tenable Vulnerability

Les ServiceNow® messages REST de l'intégration de vulnérabilité de Tenable sont utilisés pour effectuer des appels à l'API de Tenable.

Tenable.io Message REST Actifs

Le Tenable.io message REST Actifs récupère les informations sur les actifs pour l'intégration Tenable.io des actifs. Les modifications apportées à l'enregistrement de méthode de message REST ont un impact sur les demandes effectuées pour Tenable.io récupérer les informations sur les actifs. La tâche d'exportation des actifs est soumise avec les filtres suivants :

- « is_deleted » : faux
- « is_licensed » : vrai

Tenable.io Modules d'extension Message REST

Le Tenable.io message REST Modules d'extension récupère les informations du module d'extension pour l'intégration du module d'extension Tenable.io . Les changements apportés à l'enregistrement de méthode de message REST impactent les demandes effectuées pour récupérer des informations sur les modules d'extension Tenable.io .

Tenable.io Vulnérabilités Message REST

Le Tenable.io message REST Vulnérabilités récupère les informations sur la vulnérabilité pour les vulnérabilités ouvertes et fermées à partir de l'intégration Tenable.io de vulnérabilité. Les changements apportés à l'enregistrement de méthode de message REST ont un impact sur les demandes effectuées pour Tenable.io récupérer des informations sur les vulnérabilités.

Requêtes Tenable.sc Message REST

Le message REST Requêtes Tenable.sc récupère les informations du filtre de requête pour l'intégration des actifs Tenable.sc et des vulnérabilités Tenable.sc où le filtre de requête est configuré.

Tenable.sc Modules d'extension Message REST

Le Tenable.sc message REST du module d'extension récupère les informations du module d'extension pour l'intégration des modules d'extension Tenable.sc . Les modifications apportées au message REST Obtenir l'enregistrement de méthode des modules d'extension ont un impact sur les demandes effectuées pour récupérer les informations sur les modules d'extension Tenable.sc .

Nom de paramètre	Valeur	Description
type	Actif	Indique la source à partir de laquelle Tenable extrait les données. Utilisé par code. Les changements ne sont pas recommandés.
champs	id, description, cvssVector,cvssV3Vector, cvssV3TemporalVector, synopsis, cvssVector, baseScore,temporalScore,	Indique la liste des champs importés de Tenable.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
	cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, family, riskFactor, cpe, seeAlso, solution, exploitAvailable, exploitFrameworks, type, copyright, version, sourceFile, dependencies, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	

Tenable.sc Vulnérabilités Message REST

Le Tenable.sc message REST de vulnérabilités récupère les informations de vulnérabilité à partir de l'intégration Tenable.sc . Les modifications apportées au message REST Extraire les vulnérabilités ou la méthode Extraire les vulnérabilités corrigées ou, à partir des versions 14.0 Réponse aux vulnérabilités et v2.2 de Tenable Vulnerability Integration, l'extraction de l'enregistrement des vulnérabilités de remplissage ont un impact sur les demandes faites Tenable.sc pour récupérer les informations sur les vulnérabilités.

Tenable.sc Informations d'identification de numérisation Message REST

Tenable.sc Message REST de la politique

Le Tenable.sc message REST POST de politique ajoute une politique pour les modules d'extension demandés. La politique générée sera utilisée dans Tenable.sc les demandes d'analyse.

Tenable.sc Analyser le message REST

Le message POST REST de l'analyse Tenable.sc ajoute une analyse qui dépend de l'accès et de l'autorisation définis dans le corps de la demande du message REST. Il utilise la politique, l'ID de module d'extension et la ou les adresses IP dans le corps de la demande d'analyse.

Tenable.sc Résultat de l'analyse Message REST

Le Tenable.sc message REST Résultat de l'analyse GET fournit les détails de l'analyse générée à l'aide du message REST d'analyse. Il utilise scanResultId dans la réponse des messages REST de l'analyse et récupère les détails de l'analyse pour l'analyse déclenchée.

Tenable.sc Informations d'identification de numérisation

Le Tenable.sc message REST des informations d'identification d'analyse récupère les informations d'identification à partir de Tenable.sc. Les changements apportés à l'enregistrement de méthode « Importation » du message REST ont un impact sur les demandes effectuées Tenable.sc pour récupérer les informations d'identification.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
champs	id,nom,description,type	Indique la liste des champs importés à partir de Tenable.sc
filtre	utilisable	Indique que l'intégration extrait uniquement les informations d'identification utilisables de Tenable.sc Il n'est pas recommandé de modifier l'un ou l'autre des paramètres.

Transformation des données pour l'intégration Tenable Vulnerability

Une fois que vous avez identifié les données à importer, celles-ci sont récupérées à partir du produit Tenable et traitées via un ensemble de sources de données et de transformations dans votre instance.

Lors de l'installation, les cartes de gravité normalisées sont installées dans le module Mappage de gravité normalisée. Ces cartes transforment les niveaux de gravité Tenable importés en niveaux de gravité standard pour le traitement dans votre instance. Pour plus d'informations sur la création de cartes de gravité, consultez Créer une carte de gravité Vulnerability Response dans la Réponse aux vulnérabilités documentation.

Importation d'actif Tenable.io

Les données d'actif importées sont d'abord chargées dans la table d'importation d'actifs Tenable.io [sn_vul_tenable_io_asset_import].

La carte de transformation d'intégration des actifs Tenable.io est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données provenant de l'importation d'actifs Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. `Recherchez Tenable.io transformation d'actif`.

Les tables suivantes répertorient les champs de carte de transformation par intégration.

Champs de carte de transformation d'actif Tenable.io

Champ source	Champ cible	Description
u_id	source_id	Tenable fournit un ID unique pour les actifs et les mappe à l'enregistrement d'élément détecté et est utilisé pour la recherche de CI.
u_ipv4s	ip_address	Mappe la première valeur IP au champ ip_address sur l'enregistrement de l'élément détecté.
u_mac_addresses	mac_address	Mappe la première valeur mac_address au

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation d'actif Tenable.io (suite)

Champ source	Champ cible	Description
		champ d'adresse MAC sur l'enregistrement de l'élément détecté.
u_fqdns	fqdn	Mappe la première valeur de nom de domaine complet au champ de nom de domaine complet sur l'enregistrement d'élément détecté.
u_netbios_names	Netbios	Mappe la première valeur netbios au champ netbios sur l'enregistrement de l'élément détecté.
u_operating_systems	système d'exploitation	Mappe la première valeur de système d'exploitation au champ système d'exploitation sur l'enregistrement de l'élément détecté.
(Avant les versions 14.0 Réponse aux vulnérabilités et 2.2 de Tenable Vulnerability Integration)u_last_scan_time	last_scan_date	Mappé au champ last_scan_date sur l'enregistrement de l'élément détecté.
u_last_authenticated_scan_date	last_auth_scan_date	Mappe au champ last_auth_scan_date sur l'enregistrement de l'élément détecté.
[script]	name	Mappe le nom d'hôte à l'aide de la logique du script.
u_tags		Les balises sont enregistrées dans sn_sec_cmn_host_tag. Le mappage des balises aux ressources est enregistré dans sn_sec_cmn_m2m_src_ci_tag.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Délai et objectif du script de la carte de transformation des actifs Tenable.io

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque le script est exécuté	Objectif
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs dans l'hôte et vérifier si l'hôte existe déjà. En fonction des résultats, modifie les valeurs d'un import_set. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Intégration des modules d'extension Tenable.io

La carte de transformation des modules d'extension Tenable.io est utilisée pour transformer les modules d'extension importés à partir de Tenable.io.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données reçues des modules d'extension Tenable sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la transformation du module d'extension Tenable.io.

La charge utile des modules d'extension tenable.io contient tous les champs de la colonne u_attributes de la table sn_vul_tenable_io_plugin_import. Le champ d'attributs est analysé et mappé aux enregistrements de table d'entrée tiers, tels que répertoriés dans la table suivante.

Champ source	Champ cible	Description
id	id	Mappe l'ID à partir de la source et lui ajoute le préfixe TEN-. Par exemple, si l'ID reçu est 12345, l'ID de la table cible est TEN-12345.
Description	résumé	Mappe la description du module d'extension à la colonne Résumé.
[script]	source	La source du TPE importé est Tenable.io.
[script]	source_instance	Référence au déploiement Tenable qui importe cet enregistrement.
famille	catégorie	Mappe la famille de module d'extension à la colonne de catégorie
plugin_modification_date	last_modified	Mappe la plugin_modification_date au champ de la dernière modification.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
plugin_publication_date	date_published	Mappe le plugin_publication_date à la date de publication.
has_patch	remediation_type	Mappe le type de rattrapage à partir de has_patch valeur.
synopsis	menace	Mappe les informations sur la menace concernant cette vulnérabilité.
cvss_base__score	score	Mappe le score de base CVSS à la colonne de score dans la table d'entrée tierce.
solution	solution	Mappe la solution fournie par le scanner à la colonne de solution dans la table d'entrée tierce.
exploit_available	exploit	Mappe les exploit_available fournies par le scanner à la colonne Exploit dans la table d'entrée tierce
vpr.score	source_risk_score	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 – 7 – Moyen • 0-4 - Faible
vpr.drivers.age_of_vuln	age_of_vuln	Mappe l'âge de la vulnérabilité du scanner à la colonne age_of_vuln dans la table d'entrée tierce.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
vpr.drivers.product_coverage	product_coverage	Mappe la couverture du produit depuis le scanner jusqu'au product_coverage dans la table d'entrée tierce.
vpr.drivers.threat_sources_last28	threat_sources	Mappe les sources de menace au cours des 28

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		derniers jours, du scanner au threat_sources dans la table tierce.
vpr.drivers.threat_intensity_last28	threat_intensity	Mappe l'intensité de la menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_intensity dans la table d'entrée tierce.
vpr.drivers.threat_recency	threat_recency	Mappe les informations de récence de la menace du scanner à threat_recency dans la table d'entrée tierce.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mappe le score d'impact cvss3 à v3_impact_subscore colonne dans la table d'entrée tierce.
cvss_temporal_score	cvss_temporal_score	Mappe le score temporel pour CVSS v2.
cvss_v3_temporal_score	v3_temporal_score	Mappe le score temporel pour CVSS v3.
risk_factor	source_severity	Mappé à la gravité de la source dans la table d'entrée tierce.
name	name	Mappe le nom du module d'extension au nom dans la table d'entrée tierce.
stig_severity	stig_severity	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
plugin_type	check_type	Mappe le type de module d'extension au check_type dans la table d'entrée tierce.
unsupported_by_vendor	unsupported_by_vendor	Mappe le champ de unsupported_by_vendor à la colonne unsupported_by_vendor.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction de exploit_available et v3_attack_vector de colonnes.

En plus des champs directs, d'autres informations sont ajoutées sous forme de listes connexes aux entrées de tiers.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
cve	Insère les données liées aux CVE dans la table de référence (sn_vul_nvd_entry). Si la même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvée, elle associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
offre	La liste des traqs de bogues est ajoutée en tant que référence.
see_also	La liste des URL est ajoutée en tant que référence.
xrefs	La liste de X-REF est ajoutée en tant que référence.
[script]	Liste des exploits pour ce module d'extension et insère le mappage pour le cadre de travail de l'exploit applicable et le module d'extension à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs de l'entrée tierce et vérifier si l'entrée tierce existe déjà. En fonction des résultats, modifie les valeurs d'une entrée de tiers. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

L'include de script TenableIOPluginsImportProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de Tenable.io intégration des modules d'extension et la transforme en Now Platform entrées de vulnérabilité tierces. Toute modification apportée à cet include de script peut altérer la transformation des données de Tenable.io modules d'extension dans la table d'entrée tierce.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation des vulnérabilités Tenable.io

Les Tenable.io cartes de transformation des éléments vulnérables sont utilisées pour transformer les informations sur les vulnérabilités ouvertes et corrigées importées depuis Tenable.io.

Remarque : Les changements apportés à cette carte de transformation modifient la façon dont les données provenant de l'importation des vulnérabilités Tenable sont traitées.

La même carte de transformation est utilisée pour l'intégration des vulnérabilités fixes Tenable.io et l'intégration des vulnérabilités ouvertes Tenable.io. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la `carte de transformation de l'élément vulnérable Tenable.io`.

Champ source	Champ cible	Description
u_asset.uuid	id	Uuid est mappé au champ d'ID de l'enregistrement de cmdb_ci.
u_asset.ipv4	ip_address	Le champ ipv4 est mappé au champ d'adresse ip de l'enregistrement cmdb_ci.
u_asset .last_authenticated_results	last_auth_scan_date	La date de la dernière analyse authentifiée est mappée à la date de la dernière analyse d'authentification de l'enregistrement cmdb_ci.
u_asset.mac_addess	mac_address	L'adresse Mac est mappée au champ d'adresse MAC de l'hôte de l'enregistrement cmdb_ci.
u_asset.netbios_name	Netbios	Netbios est mappé au champ netbios de cmdb_ci enregistrement.
u._plugin.cvss3_base_score	v3_base_score	Le score de base CVSS v3 est mappé au score de base v3 de l'enregistrement d'entrée tierce.
u._plugin.cvss3_temporal_score	v3_temporal_score	Le score temporel CVSS v3 est mappé au score temporel v3 dans l'enregistrement d'entrée tierce.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u._plugin.cvss_base_score	score	Le score de base CVSS est mappé au champ de score de l'enregistrement d'entrée tierce.
u._plugin.cvss_temporal_score	temporal_score	Le score temporel est mappé au score temporel dans l'enregistrement d'entrée tierce.
u_plugin.description	résumé	La description est mappée au champ Résumé dans l'enregistrement d'entrée tierce.
u_plugin.famille	catégorie	Mappe la famille de module d'extension à la colonne de catégorie de l'enregistrement d'entrée tierce.
u_plugin.modification_date	last_modified	La dernière date modifiée est mappée à la date de la dernière modification du module d'extension dans l'enregistrement d'entrée tierce.
u_plugin.date_publication_	date_published	La date de publication est mappée au champ Date de publication de l'enregistrement d'entrée tierce.
u_plugin.risque_facteur	source_severity	Le facteur de risque est mappé au champ source_severity de l'enregistrement d'entrée tierce.
u_plugin.solution	solution	La solution est mappée au champ de solution de l'enregistrement d'entrée tierce.
u_plugin.synopsis	menace	Le synopsis est mappé au champ de menace de l'enregistrement d'entrée de tiers.
u_severity_id	Priorité	La priorité est mappée à l'ID de gravité de la

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		charge utile. La valeur par défaut est de 5.
u_plugin.exploit_disponible	exploit	Mappe les exploit_available fournies par le scanner à la colonne Exploit dans la table d'entrée tierce.
vpr.score	source_risk_score	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 – 7 – Moyen • 0-4 - Faible
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	Mappe l'âge de vulnérabilité depuis le scanner jusqu'aux age_of_vuln dans la table d'entrée tierce.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mappe la couverture du produit depuis le scanner jusqu'au product_coverage dans la table d'entrée tierce.
u_plugin.vpr.drivers.threat_sources_last_28	threat_sources	Mappe les sources de menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_sources dans la table d'entrée tierce.
u_plugin.vpr.drivers.threat_intensity_last_28	threat_intensity	Mappe l'intensité de la menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_intensity dans la table d'entrée tierce.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_plugin.vpr.drivers.threat_recency	threat_recency	Mappe les informations de récence de la menace du scanner aux threat_recency dans la table d'entrée tierce.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mappe le score d'impact CVSS3 v3 à v3_impact_subscore colonne dans la table d'entrée tierce.
u_plugin.type	check_type	Mappe le type de module d'extension au check_type dans la table d'entrée tierce.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Mappe le champ unsupported_by_vendor du module d'extension à la colonne unsupported_by_vendor.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction de exploit_available et v3_attack_vector de colonnes.
u_plugin.family_id	Family_id	Mappe l'ID de famille de modules d'extension à family_id colonne de la table d'entrée tierce.
port	port	Le port est mappé au champ port de l'enregistrement d'élément vulnérable.
protocol	protocol	Le protocole est mappé au champ Protocole de l'enregistrement d'élément vulnérable.
u_first_found	first_found	Le premier trouvé est mappé au champ du premier trouvé de l'enregistrement d'élément vulnérable.
u_last_found	last_found	Dernier trouvé est mappé au champ Dernier trouvé de l'enregistrement d'élément vulnérable.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_state	État	L'état est mappé au champ État dans l'enregistrement de l'élément vulnérable
[script]	source	La source de l'intégration est renseignée. Les éléments vulnérables créés à partir de cette intégration ont Tenable.io comme source.
[script]	integration_instance	Le integration_instance est le nom de l'instance à partir de laquelle l'élément vulnérable est importé.
u_plugin.name	name	Mappe le nom du module d'extension au nom dans la table d'entrée tierce.
u_plugin.stig_severity	stig_severity	Mappe la gravité stig du module d'extension à la colonne gravité stig dans la table d'entrée tierce

En plus des champs directs, d'autres informations sont ajoutées sous forme de listes connexes aux entrées de tiers.

Champ source	Description
cve	Insère les données liées aux CVE dans la table de référence (sn_vul_nvd_entry). Si la même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvée, elle associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
offre	La liste des traqs de bogues est ajoutée en tant que référence.
see_also	La liste des URL est ajoutée en tant que référence.
xrefs	La liste de X-REF est ajoutée en tant que référence.
[script]	Liste des exploits pour ce module d'extension et insère le mappage de l'infrastructure de l'exploit applicable et du module d'extension à sn_vul_m2m_framework_vul.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation déclenche TenableIOVulnerabilitiesProcessor qui importe les données des Tenable.io à l'aide du jeu d'importation et charge chaque enregistrement dans la table CI CMDB, la table des éléments vulnérables et la table de vulnérabilité tierce. Pour un usage interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction permettant de vérifier si l'entrée et les détections tierces existent déjà. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour mettre à jour le nombre de CI, de VI et de détections tels qu'importés à partir de Tenable.io. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Importation d'actif Tenable.sc

Les données d'actif importées à partir de Tenable.sc sont d'abord chargées dans la table d'importation d'actifs Tenable.sc (sn_vul_tenable_sc_asset_import). La carte de transformation de l'intégration des actifs Tenable.sc est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données provenant de l'importation d'actifs Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la `transformation de l'actif Tenable.sc`.

Champ source	Champ cible	Description
u_uuid	id	L'uuid n'étant pas renseigné à partir de l'API Tenable, l'attribut « u_uniqueness » est donc utilisé pour créer un champ uuid unique pour les actifs et le mapper à l'enregistrement cmdb_ci.
u_ip	ip_address	Mappe le champ IP de l'API au champ ip_address d'un enregistrement cmdb_ci.
u_macaddress	mac_address	Mappe le champ macaddress de l'API au

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		champ d'adresse sur l'enregistrement cmdb_ci.
u_dnsname	fqdn	Mappe le champ dnsname de l'API au champ fqdn de l'enregistrement cmdb_ci.
u_netbiosname	Netbios	Mappe le champ netbios de l'API au champ netbios de l'enregistrement cmdb_ci.
u_oscpe	système d'exploitation	Les informations sur le système d'exploitation sont extraites de l'attribut oscpe dans la charge utile et les mappent au champ système d'exploitation de l'enregistrement cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mappe le champ lastauthrun de l'API au champ last_auth_scan_date sur l'enregistrement de l'élément détecté.
u_lastauthrun et u_lastunauthrun	last_scan_date	Le lastauthrun est extrait de l'api Tenable ou du lastunauthrun. En fonction de la valeur qui apparaît dans la charge utile, le champ last_scan_date de l'enregistrement de l'élément détecté est renseigné.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs dans l'hôte et vérifier si l'hôte existe déjà. En fonction des résultats, modifie les valeurs d'un import_set. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.sc Importation des modules d'extension

Les données des modules d'extension importées à partir de Tenable.sc sont d'abord chargées dans la table d'importation des modules d'extension Tenable.sc (sn_vul_tenable_sc_plugin_import). La carte de transformation du module d'extension Tenable.sc est utilisée pour transformer les informations des modules d'extension qui ont été importées. Les changements apportés à cette transformation modifient la façon dont les données provenant de l'importation du module d'extension Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez `Tenable.sc carte de transformation de module d'extension`.

Champ source	Champ cible	Description
u_id	id	Mappe l'ID à partir de la source et ajoute le préfixe TEN-. Par exemple, si l'ID reçu est 12345, l'ID de la table cible est TEN-12345.
u_description	résumé	Mappe la description du module d'extension à la colonne Résumé.
[script]	source	Le TPE importé à partir de cette intégration a Tenable.sc comme source.
[script]	source_instance	Référence au déploiement Tenable qui importe cet enregistrement.
u_family	catégorie	Mappe le champ Nom dans l'objet de famille du module d'extension à la colonne Catégorie.
u_plugin_modification_date	last_modified	Mappe la plugin_modification_date au champ de la dernière modification.
u_plugin_publication_date	date_published	Mappe le plugin_publication_date à la date de publication.
u_has_patch	Remediation_type	Mappe le type de rattrapage à partir de has_patch valeur.
u_synopsis	menace	Mappe les informations sur la menace concernant cette vulnérabilité.
u_cvss_base_score	score	Mappe le score de base CVSS à la colonne de score dans la table d'entrée tierce.
u_solution	solution	Mappe la solution fournie par le scanner à la colonne

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		de solution dans la table d'entrée tierce.
u_cvss_temporal_score	cvss_temporal_score	Mappe le score temporel pour CVSS v2.
u_cvss_v3_temporal_score	v3_temporal_score	Mappe le score temporel pour CVSS v3.
u_risk_factor	Gravité de la source	Mappé à la gravité de la source dans la table d'entrée tierce.
u_cvss_v3_base_score	v3_base_score	Mappe le score de base CVSS dans la table d'entrée tierce.
u_exploit_available	exploit	Mappe l'exploitDisponible fourni par le scanner à la colonne Exploit dans la table d'entrée tierce.
u_vpr_score	source_risk_score	Mappe le score VPR du scanner au score du risque source dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 – 7 – Moyen • 0-4 - Faible
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mappe l'âge de la vulnérabilité depuis le scanner jusqu'aux age_of_vuln dans la table d'entrée tierce.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_vpr_context[id=product_coverage]	product_coverage	Mappe la couverture du produit depuis le scanner jusqu'au product_coverage dans la table d'entrée tierce.
u_vpr_context[id="threat_sources_last_28"]	threat_sources	Mappe les sources de menace au cours des 28 derniers jours, du scanner à l'threat_sources dans la table tierce.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_vpr_context[id="threat_intensity_last_28"]	threat_intensity	Mappe l'intensité de la menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_intensity dans la table d'entrée tierce.
u_vpr_context[id="threat_recency"]	threat_recency	Mappe les informations de récence de la menace du scanner aux threat_recency de la table d'entrée tierce.
u_vpr_context[id=cvssV3_impact_score]	v3_impact_subscore	Mappe le score d'impact CVSS v3 du scanner au v3_impact_subscore dans la table d'entrée tierce.
u_name	name	Mappe le nom du module d'extension à la colonne nom dans la table d'entrée tierce.
u_stig_severity	stig_severity	Mappe le champ stig_severity du module d'extension à stig_severity dans la table d'entrée tierce.
u_check_type	check_type	Mappe le type de chèque au check_type dans la table d'entrée tierce.
u_family.id	family_id	Mappe les family_id de module d'extension aux family_id dans la table d'entrée tierce.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction de exploit_available et v3_attack_vector de colonnes.

En plus des champs directs, d'autres informations sont ajoutées sous forme de listes connexes aux entrées de tiers.

Champ source	Description
u_cpe	La liste des CPE est ajoutée à titre de référence.
u_see_also	La liste des URL est ajoutée en tant que référence.
u_exploit_frameworks	Liste des exploits pour ce module d'extension et insère le mappage pour le cadre de travail de l'exploit

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
	applicable et le module d'extension à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs dans l'entrée tierce et vérifier si l'entrée tierce existe déjà. En fonction des résultats, modifie les valeurs d'une entrée de tiers. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation permet de définir les valeurs des modules d'extension créés et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

L'include de script TenableSCPluginsImportProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de l'intégration des modules d'extension Tenable.sc et la transforme en entrées de vulnérabilité tierces ServiceNow. Toute modification apportée à cet include de script peut altérer la transformation des données de Tenable.sc modules d'extension dans la table d'entrée tierce.

Tenable.sc Importation des vulnérabilités

La carte de transformation des vulnérabilités ouvertes Tenable.sc est utilisée pour transformer les données importées de l'intégration des vulnérabilités ouvertes Tenable.sc, et la carte de transformation des vulnérabilités Tenable.sc et corrigées est utilisée pour transformer les données importées de l'intégration des vulnérabilités corrigées Tenable.sc.

Remarque : Les changements apportés à ces cartes de transformation modifient la façon dont les données provenant de l'importation des vulnérabilités Tenable corrigées/ouvertes sont traitées.

Pour accéder aux cartes de transformation des vulnérabilités ouvertes et corrigées Tenable.sc, naviguez vers **Intégration de vulnérabilité tenable** > **Administration** > **Instances d'intégration** > **Tenable.sc Intégration des vulnérabilités corrigées/ouvertes** > **Sources de données** > **Tenable.sc vulnérabilités ouvertes/corrigées** > **Transformations**.

Champ source	Champ cible	Description
u_pluginID	ID	Utilisé comme identificateur pour le module d'extension.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		Ce champ est mappé à l'ID du module d'extension dans l'enregistrement d'entrée tierce.
u_riskfactor	source_severity	Ce champ est mappé à source_severity dans l'enregistrement d'entrée tierce.
u_severity	Priorité	Le champ de priorité est mappé avec la gravité. La valeur par défaut est de 5.
u_hasbeenmitigated	État	Hasbeenmitigated est mappé au champ d'état de l'enregistrement de vulnérabilité. Pour l'intégration des vulnérabilités corrigées, tous les VI sont à l'état « Fermé ».
u_ip	ip_address	L'adresse IP est mappée au champ IP de l'hôte de cmdb_ci table.
u_port	port	Le port est mappé au champ port de l'enregistrement d'élément vulnérable.
u_protocol	protocol	Le protocole est mappé au champ de port de l'enregistrement de l'élément vulnérable.
u_firstSeen	first_found	La première valeur vue est mappée au premier champ trouvé de l'enregistrement VI.
u_lastSeen	last_found	La dernière valeur observée est mappée au dernier champ trouvé de l'enregistrement VI.
u_exploitAvailable	exploit	ExploitAvailable est mappé au champ Exploit dans l'enregistrement d'entrée tierce.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_synopsis	menace	Le synopsis est mappé au champ Menace dans l'enregistrement d'entrée tierce.
u_description	résumé	La description est mappée au champ Résumé dans l'enregistrement d'entrée tierce.
u_solution	solution	La solution est mappée au champ de solution dans l'enregistrement d'entrée tierce.
u_basescore	score	Le score de base est mappé au champ de score dans l'enregistrement de l'entrée tierce.
u_temporalScore	temporal_score	Le score temporel est mappé au score temporel dans l'enregistrement d'entrée tierce.
u_cvssv3basescore	v3_base_score	Cvssv3basescore est mappé au score de base v3 dans l'enregistrement d'entrée tierce.
u_cvsstemporalscore	v3_temporal_score	Le score temporel Cvssv3 est mappé au score temporel v3 dans l'enregistrement d'entrée tierce.
u_pluginpubdate	date_published	La date de publication du module d'extension est mappée à la date de publication du module d'extension dans l'enregistrement d'entrée tierce.
u_pluginmoddate	last_modified	La dernière date modifiée est mappée à la date de la dernière modification du module d'extension dans l'enregistrement d'entrée tierce.
u_dnsname	fqdn	DnsName est mappé au champ FQDN

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		de l'enregistrement cmdb_ci.
u_macaddress	mac_address	MacAddress est mappé au champ mac_address de l'enregistrement cmdb_ci.
u_netbiosName	Netbios	NetbiosName est mappé au champ NETBIOS de l'enregistrement cmdb_ci.
u_ip	ip	L'adresse IP est mappée au champ IP de cmdb_ci enregistrement.
hostUniqueness	uuid	L'unicité de l'hôte n'est mappée à aucun champ, mais est utilisée pour déterminer l'uuid de l'hôte.
u_family	catégorie	Mappe le champ de nom dans l'objet de famille du module d'extension à la colonne de catégorie de l'enregistrement d'entrée tiers.
u_plugintext	proof	Le texte du module d'extension est mappé à la preuve dans l'enregistrement TPE.
[script]	source	La source de l'intégration est renseignée. Les éléments vulnérables créés à partir de cette intégration ont Tenable.sc comme source.
[script}	integration_instance	Le integration_instance est le nom de l'instance à partir de laquelle l'élément vulnérable est importé.
u_vpr_score	source_risk_score	Mappe le score VPR du scanner au score du risque source dans la table d'entrée tierce.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 – 7 – Moyen • 0-4 - Faible
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mappe l'âge de la vulnérabilité depuis le scanner jusqu'aux age_of_vuln dans la table d'entrée tierce.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_vpr_context[id=product_coverage]	product_coverage	Mappe la couverture du produit depuis le scanner jusqu'au product_coverage dans la table d'entrée tierce.
u_vpr_context[id="threat_sources_last_28]	threat_sources	Mappe les sources de menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_sources dans la table tierce.
u_vpr_context[id="threat_intensity_last_28]	threat_intensity	Mappe l'intensité de la menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_intensity dans la table d'entrée tierce.
u_vpr_context[id="threat_recency"]	threat_recency	Mappe les informations de récence de la menace du scanner aux threat_recency de la table d'entrée tierce.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mappe le score d'impact CVSS v3 du scanner au v3_impact_subscore

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		dans la table d'entrée tierce.
u_pluginname	name	Mappe le nom du module d'extension à la colonne nom dans la table d'entrée tierce.
u_stigseverity	stig_severity	Mappe le champ stig_severity du module d'extension à stig_severity dans la table d'entrée tierce.
u_checktype	check_type	Mappe le type de vérification à check_type dans la table d'entrée tierce.
u_family.id	family_id	Mappe les family.id de module d'extension aux family_id dans la table d'entrée tierce.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table third_party_entry est renseignée en fonction de exploit_available et v3_attack_vector de colonnes.

Champ source	Description
u_cve	Insère les données liées aux CVE dans la table de référence (sn_vul_nvd_entry). Si la même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvée, elle associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
u_bid	La liste des traqs de bogues est ajoutée en tant que référence.
u_cpe	La liste des CPE est ajoutée à titre de référence.
u_seealso	La liste des URL est ajoutée en tant que référence.
u_xrefs	La liste des X-REF est ajoutée à titre de référence.
u_exploitframeworks	Liste des exploits pour ce module d'extension et insère le mappage de l'infrastructure de l'exploit

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
	applicable et du module d'extension à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs de la vulnérabilité et vérifier si la vulnérabilité existe déjà. En fonction des résultats, modifie les valeurs d'une table d'éléments vulnérables. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux VI créés et des VI qui ont été mis à jour et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Définir des paramètres de filtre supplémentaires pour Tenable.io les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec la Tenable Vulnerability Integration pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec le Tenable.io produit.

Avant de commencer

Cas d'utilisation : en tant que gestionnaire ou analyste des vulnérabilités, vous souhaiterez peut-être filtrer les données de vos requêtes afin de ne pouvoir examiner que certains détails de vulnérabilité. Par exemple, supposons que vous souhaitiez afficher les vulnérabilités importées qui sont filtrées par *cidr_range*, *num_assets*, *indexed_at*et *plugin_family*. Supposons que vous souhaitiez exécuter une Tenable.io intégration de sorte qu'une exécution importe uniquement les vulnérabilités critiques toutes les quatre heures et qu'une autre s'exécute toutes les 24 heures pour récupérer toutes les autres vulnérabilités non critiques.

Pour vous aider à collecter ces données, vous pouvez ajouter des paramètres pris en charge par Tenable pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

Sans ajouter d'appels d'API ou de codage supplémentaires, cette fonctionnalité vous permet de personnaliser les informations de votre requête HTTP avec les paramètres Tenable dans votre Now Platformfichier . Les intégrations suivantes Tenable.io prennent en charge le filtrage en fournissant du contenu JSON dans le corps de la demande :

- Intégration des actifs
- Intégration de vulnérabilité fixe
- Intégration des vulnérabilités ouvertes

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous devez savoir comment utiliser JSON des chaînes pour cette fonctionnalité.

Rôle requis : sn_vul.vulnerability_admin

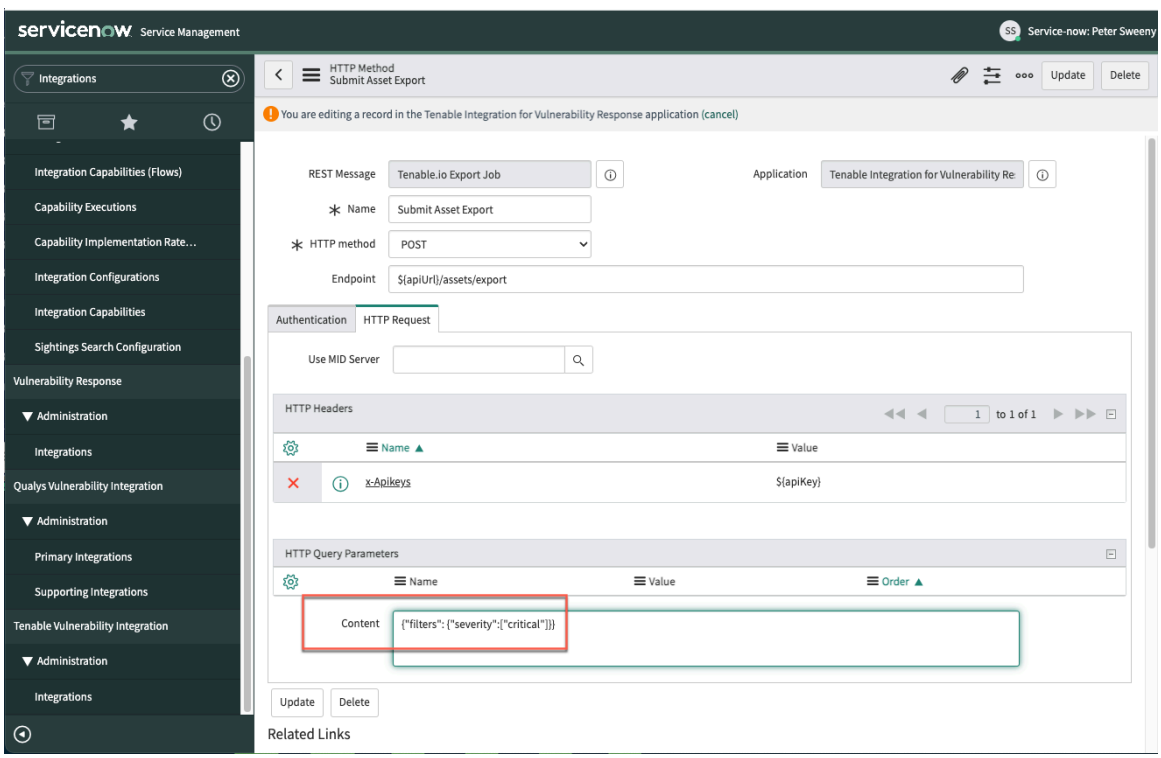
Procédure

1. Localisez les paramètres pris en charge par le Tenable.io produit sur le site développeur que vous souhaitez utiliser pour votre filtrage.

   Les paramètres et les valeurs que vous entrez à partir du produit ne sont pris en charge qu'au niveau de l'instance d'intégration Tenable.io .

2. Accédez à la **Tout** > **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.
3. Sur la page de liste Intégrations Tenable, cliquez sur l'enregistrement de l'intégration Tenable.io que vous souhaitez ouvrir.
4. Une fois l'onglet Méthodes REST Tenable sélectionné, cliquez sur l'icône d'informations (I) pour la méthode REST, puis sur **Ouvrir l'enregistrement**.
5. Sélectionnez l'onglet **de demande HTTP** .
6. Pour modifier l'enregistrement, en haut de la page, cliquez sur le lien, Pour modifier l'enregistrement, cliquez **ici**.
7. Dans l'enregistrement Méthode REST, dans le champ Contenu, saisissez le contenu JSON que vous souhaitez intégrer au corps de la demande.

   Dans l'image suivante, à titre d'exemple, le paramètre de gravité pour les vulnérabilités `{"filters": {"severity": ["critical"]}}` importées a été personnalisé pour l'intégration Tenable.io des actifs. Cette valeur importe uniquement les vulnérabilités critiques (score CVSS de 10,0).



   Si vous souhaitez entrer plusieurs paramètres, reportez-vous à la documentation pour plus d'informations sur la Tenable.io séparation de chaque valeur.

8. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Reporting sur l'intégration de vulnérabilité tenable

Affichez les rapports sur les vulnérabilités et les éléments vulnérables sur les Réponse aux vulnérabilités tableaux de bord.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à suivre la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en visualisant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Reportez-vous à la rubrique Réponse aux vulnérabilités Espaces de travailet Exploration de l'Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Versions précédentes de Réponse aux vulnérabilités

Le tableau de bord de vue d'ensemble de Vulnerability Response (Gestion des vulnérabilités) fournit une vue d'ensemble des vulnérabilités et des éléments vulnérables, ce qui aide l'administrateur de vulnérabilité à identifier rapidement les zones de préoccupation. Le tableau de bord de rattrapage de Vulnerability Response (Vulnerability Remediation) permet à un spécialiste de la remédiation de se concentrer sur les tâches de remédiation et les éléments vulnérables qu'il possède.

Consultez Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités pour plus d'informations.

Rôle requis : propriétaire du rattrapage.

Des rôles granulaires et de profil sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.

Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pour afficher le tableau de bord, accédez à **Réponse aux vulnérabilités** > **Aperçu du rattrapage**.

Graphique d'état de l'exécution de l'intégration pour Tenable Vulnerability Integration

Le module État de l'exécution de l'intégration Tenable vous fournit une vue graphique de l'état des exécutions d'intégration Tenable.

Dans le diagramme, pointez sur n'importe quelle partie du graphique pour afficher un résumé des données spécifiques à cette partie. Si vous cliquez sur une partie du graphique à barres, une liste s'ouvre pour fournir des informations plus détaillées.

Rôle requis : administrateur de vulnérabilité.

Des rôles granulaires et de profil sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

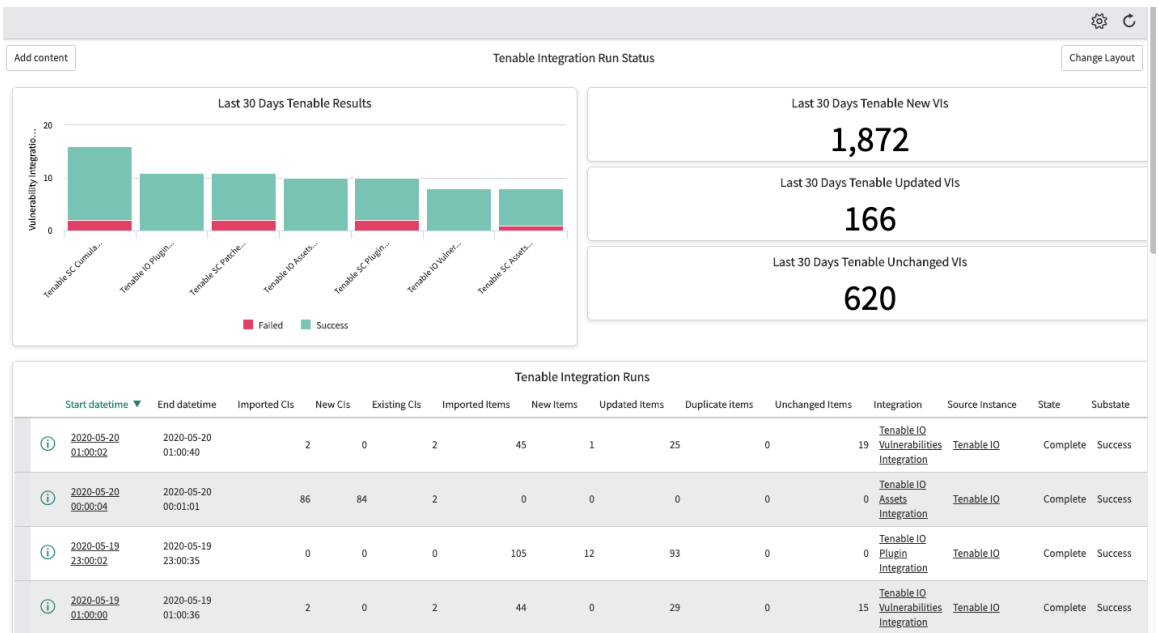
Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pour afficher les données, accédez à **Tout** > **Intégration de vulnérabilité tenable** > **État de l'exécution de l'intégration**.

À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

État d'exécution



Rapports sur les graphiques d'état de l'exécution de l'intégration Tenable

Nom	Description
Résultats Tenable au cours des 30 derniers jours	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Chaque exécution est affichée sous forme de barre dans le graphique.
Nouveaux VI Tenable au cours des 30 derniers jours	Nombre de nouveaux éléments vulnérables importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour Tenable au cours des 30 derniers jours	Nombre d'éléments vulnérables mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI inchangés Tenable au cours des 30 derniers jours	Nombre d'éléments vulnérables en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Exécutions de l'intégration Tenable	L'exécution de l'intégration enregistre dans une liste.

Traduction automatique

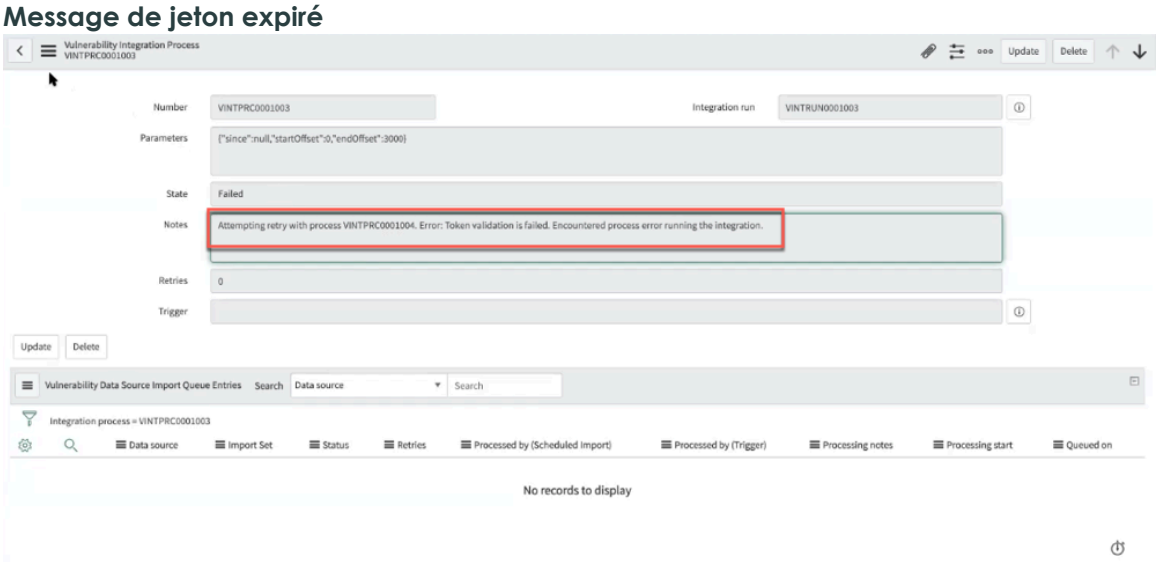
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
	Remarque : V16.1 : Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection de la *sn_vul_detection* table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, après la fin de l'exécution de l'intégration.

Expiration de la validation du jeton

Si l'exécution d'une intégration de Tenable.sc échoue pour une raison quelconque, le jeton d'authentification pour Tenable.sc expire automatiquement et un message s'affiche sur l'enregistrement du processus d'intégration de vulnérabilité.

Message de jeton expiré



Un nouveau jeton est automatiquement généré pour le prochain processus d'intégration. Tous les processus d'intégration, qu'ils aient échoué ou réussi, sont affichés dans l'onglet Processus d'intégration de vulnérabilité de l'enregistrement Processus d'intégration de vulnérabilité.

Lancer une nouvelle analyse pour l'intégration Tenable.sc

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans la plateforme Tenable. Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Tenable.sc produit à partir de votre Now Platform® instance.

Avant de commencer

Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Remarque : Tenable.sc Ne prend pas en charge le lancement d'une nouvelle analyse sur les ordinateurs basés sur un agent.

Vérifiez que votre scanner est activé avant de commencer. Accédez à la **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche
Pour lancer une nouvelle analyse à partir des espaces de travail, reportez-vous à la section Analyser Tenable.io à nouveau et Tenable.sc les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail.

Suivez les étapes ci-dessous pour lancer une nouvelle analyse dans l'environnement classique.

Pour aider à réduire les frais généraux et le volume impliqués par les analyses complètes planifiées, les responsables des rattrapages, les spécialistes informatiques, les analystes de vulnérabilité ou les gestionnaires de vulnérabilités peuvent lancer de nouvelles analyses ciblées sur demande pour des vulnérabilités spécifiques sur des actifs (éléments de configuration) dans leurs environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de remédiation (RT), d'entrée tierce (TPE) ou d'éléments détectés à partir de votre Now Platform instance.

Les nouvelles analyses permettent à vos propriétaires de rattrapage et à vos analystes de vulnérabilité de vérifier que vos activités de rattrapage, vos correctifs et vos autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

À titre d'exemple, l'ensemble de votre environnement est analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été effectuée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines la prochaine analyse planifiée pour vérifier qu'elle a été corrigée. Pour vérifier que votre correctif corrige avec succès une vulnérabilité critique détectée lors d'une analyse précédente, vous pouvez lancer une nouvelle analyse ciblée à partir de votre Now Platform recherche Tenable.sc d'éléments vulnérables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous demandez une nouvelle analyse à partir de votre Now Platform® instance, la sélection des informations d'identification Intégration de Réponse aux vulnérabilités à Tenable est facultative. L'intégration ServiceNow® Tenable.sc des informations d'identification de numérisation importe et met à jour les informations d'identification du scanner à partir Tenable.sc du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable.

Notez que ces données importées n'incluent pas les mots de passe Tenable ni d'autres informations sensibles sur le compte Tenable. L'intégration ServiceNow® Tenable.sc des informations d'identification de numérisation est activée (`active`) automatiquement à partir de l'assistant de configuration de votre instance lorsque vous configurez les Tenable.sc intégrations de vulnérabilités (Tenable.sc intégrations de vulnérabilités ouvertes et fixes).

Notez les informations suivantes au sujet des informations d'identification que vous importez afin que vos utilisateurs puissent les afficher selon leurs besoins à partir de votre Now Platform instance :

- Les informations d'identification créées avec le Tenable.sc rôle d'utilisateur administrateur sont disponibles pour les utilisateurs de toutes vos organisations.
- Les informations d'identification créées avec le rôle d'utilisateur de l'organisation Tenable.sc ne sont disponibles que pour les utilisateurs de cette organisation. Ces informations d'identification ne sont pas importées dans le référentiel Now Platform pour les utilisateurs extérieurs à l'organisation du créateur, sauf si elles sont partagées avec le compte de l'utilisateur utilisé pour se connecter à l'instance.

Consultez le site web de la Tenable.sc documentation pour plus d'informations.

Consultez Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration pour plus d'informations sur la configuration de l'application Tenable.sc . Pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation, naviguez vers **Tout** > **Intégration de vulnérabilité tenable** > **Intégrations** > **Intégration des informations d'identification Tenable.sc Scan**.

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Vous ne pouvez lancer de nouvelles analyses que pour les VI dont Tenable.sc la source est la source. Verify Tenable.sc s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le Créateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue Liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône **Personnaliser la liste** (icône Engrenage) et utilisez la zone de sélection pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** pour la tâche de rattrapage ou les enregistrements d'entrées de tiers, respectivement, que vous souhaitez utiliser pour la nouvelle analyse.

   En fonction de votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

   - Sur un enregistrement de VI unique, le VI doit provenir du Tenable.sc produit et se trouver dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent provenir du produit Tenable.sc et être dans un état autre que **Fermé**.
   - Sur un enregistrement RT, la tâche de rattrapage peut être dans n'importe quel état autre que **Fermé** et tous les VI associés doivent provenir du Tenable.sc produit.
   - Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du produit dans un Tenable.sc état autre que **Fermé**.

4. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**. Vous êtes invité à choisir les informations d'identification du scanner pour y accéder. Il s'agit des informations d'identification importées par l'intégration des informations d'identification Tenable.sc de numérisation.
5. Dans la boîte de dialogue, sélectionnez les filtres et les types d'informations d'identification souhaités.
6. Cliquez sur **Demander l'analyse**.

   Un message s'affiche pour indiquer que votre analyse est en cours de traitement. L'état de toutes les nouvelles analyses peut être consulté à tout moment sous les listes relatives à l'analyse sur les enregistrements VI, RT, TPE que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le champ État de l'enregistrement d'analyse parent est marqué comme terminé lorsque toutes les analyses enfants sont terminées avec succès. L'enfant analyse les données d'importation. L'enregistrement d'analyse parent est un conteneur pour les analyses enfants.

Votre Now Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine correctement ou jusqu'à l'expiration de la période de suivi définie, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de votre Now Platform® nouvelle analyse a cessé, et non à la date à laquelle la nouvelle analyse elle-même s'est arrêtée. Tous les VI qui sont passés ou passeront à **l'état Fermé/Fixe** sont importés avec la prochaine importation planifiée de l'intégration des vulnérabilités Tenable.sc Fixe.

Lancer une nouvelle analyse pour l'intégration Tenable.io

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans la plateforme Tenable. Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Tenable.io produit à partir de votre Now Platform® instance.

Avant de commencer

Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Vérifiez que votre scanner est activé avant de commencer. Accédez à la **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.

Pourquoi et quand exécuter cette tâche

- Consultez et Analyser à nouveau les enregistrements et les tâches de rattrapage dans Vulnerability Manager Workspace pour Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT lancer une nouvelle analyse dans les espaces de travail Vulnerability Response.
- Suivez les étapes ci-dessous pour lancer une nouvelle analyse dans l'environnement classique.

Remarque : Tenable.io Ne prend pas en charge le lancement d'une nouvelle analyse sur les ordinateurs basés sur un agent.

Pour aider à réduire les frais généraux et le volume impliqués par les analyses complètes planifiées, en tant que propriétaire du rattrapage, spécialiste informatique, analyste de vulnérabilité ou gestionnaire de vulnérabilité, vous pouvez lancer de nouvelles analyses ciblées sur demande. Vous pouvez rechercher des vulnérabilités spécifiques sur les actifs (éléments de configuration) de vos environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de rattrapage (VUL), d'entrée tierce (TPE) ou d'éléments détectés (SDI) à partir de votre Now Platform instance. Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, vos correctifs et vos autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous demandez une nouvelle analyse à partir de votre Now Platform® instance, la sélection des informations d'identification Intégration de Réponse aux vulnérabilités à Tenable est facultative. L'intégration ServiceNow® Tenable.io des informations d'identification de numérisation importe et met à jour les informations d'identification du scanner à partir Tenable.io du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable.

Notez que ces données importées n'incluent pas les mots de passe Tenable ni d'autres informations sensibles sur le compte Tenable.

Les informations suivantes décrivent les informations d'identification que vous importez afin que vos utilisateurs puissent les afficher selon leurs besoins à partir de votre Now Platform instance :

- Les informations d'identification créées avec le Tenable.io rôle d'utilisateur administrateur sont disponibles pour les utilisateurs de toutes vos organisations.
- Les informations d'identification créées avec le rôle d'utilisateur de l'organisation Tenable.io ne sont disponibles que pour les utilisateurs de cette organisation. Ces informations d'identification ne sont pas importées dans le référentiel Now Platform pour les utilisateurs extérieurs à l'organisation du créateur, sauf si elles sont partagées avec le compte de l'utilisateur utilisé pour se connecter à l'instance.

  Consultez le site web de la Tenable.io documentation pour plus d'informations.

- L'intégration Tenable.io du modèle et l'intégration des informations d'identification Tenable.io de numérisation doivent être activées avant de lancer de nouvelles analyses. Pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation, naviguez vers **Intégration de vulnérabilité tenable** > **Intégrations** > **Intégration des informations d'identification Tenable.io Scan**.

  Par défaut, les intégrations d'informations d'identification de modèle et d'analyse sont désactivées. Lorsque vous saisissez vos informations d'identification pour Tenable.io, toutes les Tenable.io intégrations sont automatiquement activées. Pour activer ou désactiver manuellement ces intégrations :

  1. Accédez à la **Tout** > **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.
  2. Dans la liste qui s'affiche, localisez les enregistrements d'intégration Tenable.io souhaités.
  3. Ouvrez chaque enregistrement et cochez la case **Actif** pour activer l'intégration.
  4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.
  5. Revenez à l'assistant de configuration pour poursuivre la configuration avec Tenable Vulnerability IntegrationRéponse aux vulnérabilités.

Pour plus d'informations sur la configuration des Tenable.io produits and, reportez-vous Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration à la section .Tenable.sc

Supposons que l'ensemble de votre environnement soit analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été effectuée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines la prochaine analyse planifiée pour vérifier qu'elle a été corrigée. Pour vérifier que votre correctif corrige avec succès une vulnérabilité critique détectée lors d'une analyse précédente, vous pouvez

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

lancer une nouvelle analyse ciblée à partir de votre Now Platform recherche Tenable.io d'éléments vulnérables.

Vous pouvez afficher les résultats mis à jour sur les enregistrements à partir desquels vous avez initié les analyses après la prochaine importation planifiée de l'intégration des vulnérabilités corrigées.

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Si vous utilisez le Tenable.io scanner, vous ne pouvez lancer de nouvelles analyses que pour les VI dont Tenable.io la source est la source. Verify Tenable.io s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le Créateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue Liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône **Personnaliser la liste** (icône Engrenage) et utilisez la zone de sélection pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** pour les enregistrements que vous souhaitez utiliser pour la nouvelle analyse.

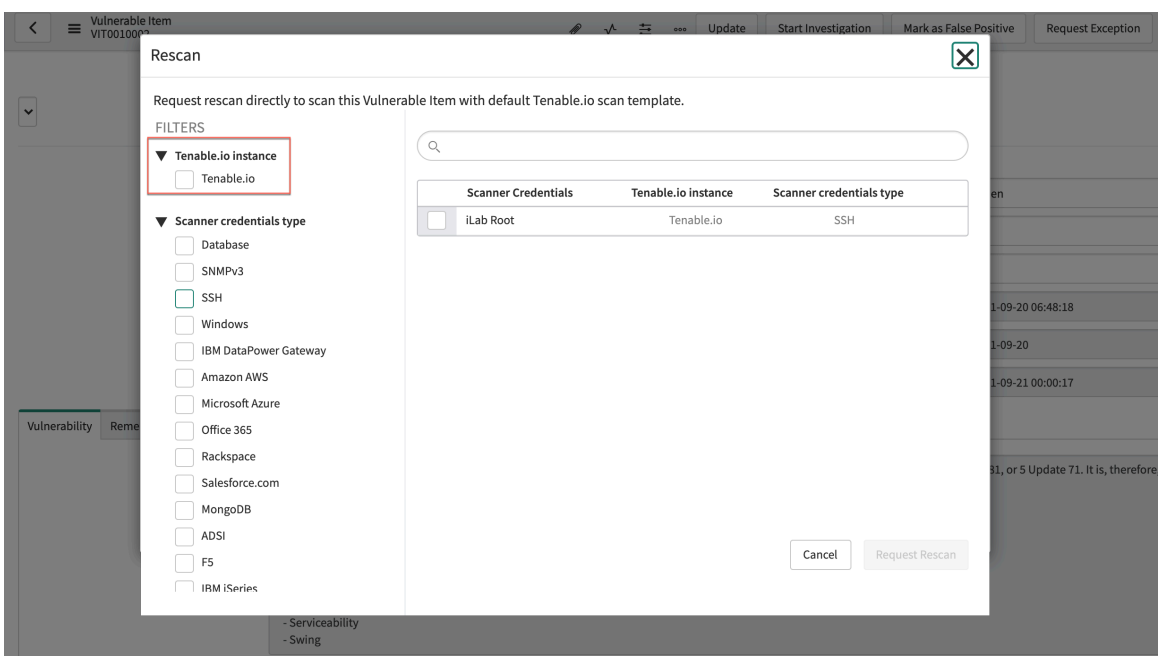
   En fonction de votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sur un seul enregistrement de VI, le VI doit être dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent provenir du Tenable.io produit et se trouver dans un état autre que **Fermé**.
- Pour les enregistrements de tâches de **rattrapage** , seules les tâches de rattrapage d'un état autre que Fermé sont prises en charge. Tous les VI associés doivent être dans un état autre que **Fermé** et être utilisés Tenable.io comme source.
- Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du produit dans un Tenable.io état autre que **Fermé**.
- Sur les enregistrements d'éléments détectés, l'enregistrement doit avoir au moins un enregistrement de VI associé du produit dans un Tenable.io état autre que **Fermé**.
- Dans la liste Éléments vulnérables, vous pouvez sélectionner les éléments vulnérables individuels que vous souhaitez analyser à nouveau. Utilisez le menu Actions sur les lignes sélectionnées en bas à gauche de l'écran pour lancer la nouvelle analyse. Vous êtes invité à saisir vos informations d'identification.

4. Dans l'angle supérieur droit d'un enregistrement, cliquez sur **Analyser à nouveau**. Vous êtes invité à choisir l'instance ou les instances pour la nouvelle analyse et les informations d'identification du scanner que vous souhaitez utiliser pour accéder au scanner. Les informations d'identification affichées sont celles importées par l'intégration des informations d'identification de numérisation Tenable.io .
5. Dans la boîte de dialogue, sélectionnez l'instance et/ou les instances et les types d'informations d'identification que vous souhaitez utiliser.

   L'image suivante montre une instance d'intégration `Tenable.io` . Si vous avez plusieurs Tenable.io instances, elles sont toutes affichées sous la section `Tenable.io` du formulaire.



Champ	Description
Instance Tenable.io	Choisissez une Tenable.io instance d'intégration à partir de laquelle vous souhaitez lancer la nouvelle analyse. Toutes vos instances d'intégration s'affichent Tenable.io . Si un VI existe dans plusieurs instances d'intégration, vous pouvez

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	utiliser ce filtre pour limiter ou développer les instances que vous souhaitez analyser. **Remarque :** Si vous choisissez d'analyser à nouveau les VI à partir d'un enregistrement de tâche de rattrapage pour une seule instance d'intégration, seuls les VI actifs associés à cette tâche de rattrapage, pour cette instance, à l'aide des informations d'identification que vous sélectionnez sont analysés.
Filtre de type d'informations d'identification du scanner	Utilisez ce filtre pour afficher les informations d'identification par type.
Volet avec les informations d'identification du scanner, Tenable.io l'instance, le type d'informations d'identification du scanner	Il s'agit des informations d'identification du scanner disponibles importées à partir des Tenable.io produits. Choisissez une ou plusieurs informations d'identification à utiliser pour l'analyse.

6. Cliquez sur **Demander une nouvelle analyse**.

   Un message s'affiche indiquant que votre analyse est en cours de traitement et qu'un enregistrement d'analyse parent a été créé. L'état de toutes les analyses enfants peut être consulté à tout moment sous les listes connexes Analyse des enregistrements VI, Tâche de rattrapage, TPE et SDI que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

   Le champ État de l'enregistrement d'analyse parent est marqué comme terminé lorsque toutes les analyses enfants sont terminées avec succès. L'enfant analyse les données d'importation. Chaque analyse prend en charge une combinaison unique d'instance d'intégration, de TPE, d'adresse IP et d'ID réseau. Vous pouvez voir plusieurs analyses enfants sur un enregistrement d'analyse parent. Par exemple, le nombre maximum d'adresses IP qu'une analyse enfant peut prendre en charge est de 1 000. S'il existe 1 002 adresses IP pour un élément vulnérable, deux analyses enfants sont créées et répertoriées sur la liste connexe Analyses pour prendre en charge la demande. L'enregistrement d'analyse parent est un conteneur pour les analyses enfants et son état reflète l'état des analyses enfants.

   Votre Now Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine correctement ou jusqu'à l'expiration de la période de suivi définie, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de votre Now Platform® nouvelle analyse a cessé, et non à la date à laquelle la nouvelle analyse elle-même s'est arrêtée. Tous les VI qui sont passés ou passeront à **l'état Fermé/Fixe** sont importés avec la prochaine importation planifiée de l'intégration Tenable.io des vulnérabilités corrigées.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour les analyses présentant des erreurs, vous pouvez vérifier les analyses enfants sur l'enregistrement d'analyse parent. Affichez l'erreur dans la charge utile de réponse de l'analyse enfant.

Vous pouvez afficher les résultats mis à jour sur les enregistrements à partir desquels vous avez initié les analyses après la prochaine importation planifiée de l'intégration des vulnérabilités corrigées.

Mettre à jour les éléments de configuration avec l'identificateur de partition de réseau pour le Tenable Vulnerability Integration

Créez des éléments de configuration (CI) uniques pour les actifs de votre environnement qui partagent des adresses IP. Identifiez les actifs distincts dans votre environnement et mettez automatiquement à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous donner plus de détails sur vos vulnérabilités.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Par défaut dans l'application, l'adresse Réponse aux vulnérabilités IP est l'un des moyens d'identifier vos actifs. Dans certains cas, les actifs peuvent partager des adresses IP, mais ils sont stockés en tant que CI unique dans votre CMDB.

Par exemple, comme le montrent les tables suivantes, plusieurs actifs (CI) de votre environnement peuvent partager des adresses IP, mais ont des ID de réseau et de référentiel uniques. Toutefois, par défaut, ces ressources sont généralement identifiées et stockées comme un seul CI `(CI 1)` lors de la recherche d'adresse IP.

Recherche d'adresses IP et création de CI par défaut

Source	Adresse IP	Network_id	Élément de configuration
Tenable.io: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	Adresse IP	Repository_id	Élément de configuration
Tenable.sc: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Vous pouvez créer des CI individuels pour les actifs qui ont la même adresse IP afin de pouvoir les identifier en tant qu'actifs distincts. À partir d'une importation de données actualisée, vous pouvez mettre à jour vos CI existants avec une plus grande granularité incluant l'identificateur de partition de réseau [network_partition_identifier] en exécutant la tâche planifiée. *`Update existing discovered items with network partition identifier`*

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette tâche planifiée est désactivée par défaut. Activez cette fonctionnalité pour les intégrations Actifs et Vulnérabilités fixes et ouvertes pour les Tenable.io et Tenable.sc les produits dans l'assistant de configuration afin d'afficher cet identificateur dans vos enregistrements.

Lorsqu'elle est activée, cette tâche planifiée ajoute l'identificateur de partition de réseau [network_partition_identifier] aux enregistrements de CI existants à partir des données importées. Les CI existants créés par l'IRE sont également mis à jour. La tâche planifiée crée également des CI qui incluent l'identificateur de partition de réseau à partir de la prochaine importation. Vous pouvez également lancer la tâche à la demande pour mettre à jour vos données existantes.

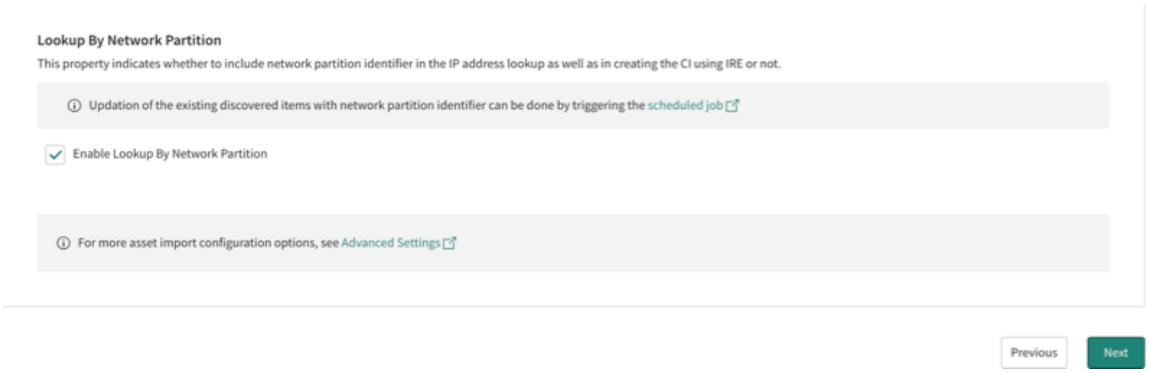
Lorsque vous effectuez une mise à niveau à partir de la version 14.0 et de Réponse aux vulnérabilités la version 2.2 de Tenable Vulnerability Integration, les modèles de classe CI CMDB (1.0.21.) sont pris en charge. Les modèles de classe ont l'identificateur de partition de réseau [network_partition_identifier] dans les règles d'identification Identification et rapprochement (IRE).

Option	Description
Exécutez les travaux planifiés sur demande.	Mettez à jour vos éléments détectés existants. Les CI de vos données Tenable existantes sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau. Les éléments détectés, les éléments vulnérables et les enregistrements de détection sont tous mis à jour avec les nouveaux CI.
Attendez les importations de données fraîches des intégrations avec les prochains travaux planifiés.	Créez des CI pour chaque nouvel actif à l'aide de l'identificateur de partition de réseau en commençant par la tâche planifiée suivante. Les enregistrements de CI, d'élément vulnérable et de détection sont tous mis à jour pour inclure la nouvelle granularité. De nouveaux CI sont créés lorsqu'aucune correspondance exacte n'est trouvée.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
2. Sélectionnez Tenable.io Intégrations ou Tenable.sc Intégrations.
3. **Modifiez** l'intégration requise.
4. Sélectionner **Configuration de l'importation d'actifs**.
5. Sélectionner **Activer la recherche par partition de réseau** case à cocher de la **Activer la recherche par partition de réseau** section.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Suivant**.

Les identificateurs de partition de réseau NETWORK_ID et les _ID REPOSITORY sont inclus et mettent à jour les CI existants ou créent des CI avec la tâche planifiée suivante.

Attribut d'identificateur de partition de réseau inclus dans la recherche d'adresses IP et la création de CI

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Éléments CI : actifs avec identificateur de partition de réseau
Tenable.io: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Source	Adresse IP	REPOSITORY_ID	CI pour les actifs sans identificateur de partition de réseau	Éléments CI : actifs avec identificateur de partition de réseau
Tenable.sc: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Avec la tâche planifiée suivante, les règles de recherche d'identification CI Adresse IP et Adresse IP incomplète incluent automatiquement l'attribut d'identificateur de partition de réseau pour une importation de données à partir des intégrations Actifs et Vulnérabilités fixes et ouvertes pour les Tenable.io produits et Tenable.sc .

Après avoir activé la propriété système et enregistré les enregistrements, vous pouvez également mettre à jour vos éléments détectés existants avec des CI qui incluent l'identificateur de partition de réseau en lançant les travaux planifiés sur demande.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer les modifications pour l'intégration de vulnérabilité Tenable

Configurez les modifications facultatives et rationalisez certaines des données spécifiquement pour l'intégration d'importation des vulnérabilités Tenable dans l'intégration des vulnérabilités ServiceNow® Tenable.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Cet ensemble de tâches nécessite du codage et des connaissances avancées sur le Now Platformfichier .

Suivez ces étapes pour créer des importations séparées par domaine pour les intégrations de vulnérabilités Tenable. L'exemple suivant concerne l'intégration des vulnérabilités ouvertes Tenable.io, mais ce contenu est applicable aux autres intégrations Tenable.

Procédure

1. Créez un domaine.
2. Pour chaque domaine que vous créez, créez un utilisateur et affectez-le à ce domaine.

   Considérez cet utilisateur comme un espace réservé run_as pour le domaine dans Tenable.io.

3. Intégration des vulnérabilités ouvertes.
   L'utilisateur est l'équivalent de la VR. Utilisateur système dans le domaine global et doit disposer des rôles suivants : sn_vul.tenable_configure_integration, import_admin et sn_vul.vulnerability_write. Cet utilisateur doit accéder aux sources de données, aux cartes de transformation et aux données de vulnérabilité.

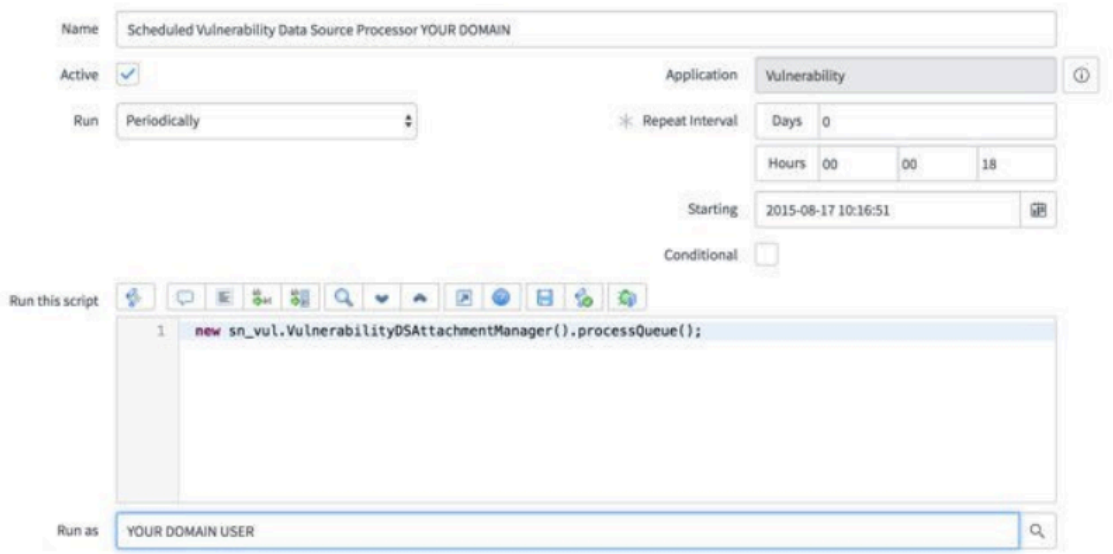
   Remarque : Considérez cet utilisateur comme spécifique à ce rôle. L'utilisateur ne doit pas avoir d'autre but

4. Dans chaque domaine, créez une tâche planifiée en copiant le processeur de source de données de vulnérabilité planifiée qui se trouve sous **Définition du système** > **Travaux planifiés**.
5. Ajoutez le domaine au nom pour identifier la tâche planifiée.
6. Remplacez l'utilisateur run_as par l'utilisateur que vous avez créé à l'étape précédente.

   Remarque : Modifiez l'action d'interface utilisateur suivante afin que l'intégration s'exécute dans le domaine de l'utilisateur run_as.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Modifiez l'action d'interface utilisateur Exécuter maintenant dans l'intégration des vulnérabilités ouvertes Tenable.io pour ajouter ce bloc de code en haut du fichier.
//sys_id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){current.run_as = gs.getUserID();}

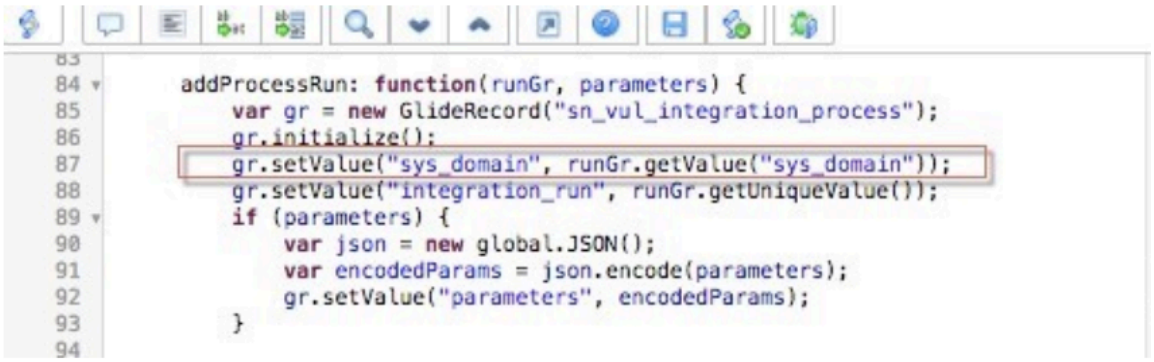
Remarque : Modifiez les includes de script suivants afin que l'intégration s'exécute dans le domaine de l'utilisateur run_as.

8. Modifiez la méthode d'include de script VulnerabilityIntegrationUtils addIntegrationRun pour ajouter le code en surbrillance.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Modifiez la méthode d'include de script VulnerabilityIntegrationUtils addProcessRun pour ajouter le code en surbrillance.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Modifier la méthode d'include de script DataSourceVulnReportRefreshProcessor _processFromDataSourceGroups pour modifier ce code d'origine : Code _processFromDataSourcesGroups d'origine en Code _processFromDataSourcesGroups modifié.
11. Modifiez la méthode d'include de script VulnerabilityDSAttachmentManager, queueItem pour ajouter les blocs de code en surbrillance suivants, queueItem, _getNext _processQueueEntry fonction.

    Vous êtes prêt pour les importations de détections d'hôtes séparées par domaine.

    Désactiver les calculateurs avant l'importation

    Suivez ces étapes pour désactiver le calculateur par défaut s'il n'est pas utilisé. Si vous n'utilisez pas de calculateurs de vulnérabilité, il est préférable de désactiver les calculateurs par défaut en plus de tous les autres que vous avez définis. Les calculateurs de vulnérabilité s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est consulté et peuvent avoir un impact sur les performances de l'instance.

    Rôle requis : sn_vul.vulnerability_admin.

12. Accédez à la **Tout** > **Vulnérabilité** > **Administration** > **Calculateurs de vulnérabilités**.
13. Ouvrez le groupe Impact de vulnérabilité.
14. Ouvrez le calculateur de score et d'impact basé sur le service.
15. Désélectionnez le champ Actif pour désactiver le calculateur.
16. Cliquez sur Mettre à jour.

    Vous avez désactivé le calculateur par défaut.

    Désactiver les règles métier basées sur la notification avant l'importation initiale

    Suivez ces étapes pour désactiver la désactivation des règles métier liées aux notifications avant l'importation initiale de l'enregistrement. Lors de l'importation initiale des enregistrements, certaines règles métier liées aux notifications peuvent générer de nombreuses notifications, ce qui a un impact sur les performances. Ces règles métier doivent être modifiées pour les désactiver lors de l'importation.

    Le rôle requis est sn_vul.vulnerability_admin.

17. Accédez à la **Tout** > **Définition du système** > **Règles métier**.
18. Recherchez les notifications de CI affectés.
19. Ouvrez la règle métier et insérez la condition suivante : *`current.sys_class_name != "sn_vul_vulnerable_item"`*.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

20. Cliquez sur **Mettre à jour**.
21. Répétez cette procédure pour les règles métier suivantes :
    - Notifications des centres de coûts affectés
    - Notifications des groupes affectés
    - Notifications d'emplacements affectés

    Remarque : Une fois l'importation d'enregistrement initiale terminée, vous pouvez réactiver ces règles métier. Cependant, envisagez de les laisser handicapés. Elles peuvent générer un grand nombre de notifications et avoir un impact sur les performances de votre instance.

    Modifier une date de début initiale

    Procédez comme suit pour modifier une date de début initiale. Lors de l'installation à l'aide de l'Assistant de configuration, vous définissez une date de début initiale pour les intégrations Tenable. Vous pouvez réinitialiser cette date de début dans l'Assistant de configuration ou à partir de l'intégration principale, comme indiqué dans les étapes suivantes.

22. Accédez à la **Tout** > **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.
23. Cliquez sur n'importe quelle intégration.
24. Cliquez sur Détails de l'intégration.
25. Définissez le champ Heure de début sur une valeur passée, de sorte que toutes les vulnérabilités analysées et détectées depuis cette heure soient détectées.

    Si vous avez configuré Tenable à l'aide de l'assistant de configuration, le champ Heure de début est pré-rempli, initialement jusqu'à trois mois avant la date d'aujourd'hui, puis jusqu'à la date d'aujourd'hui. Remarque : Envisagez de définir la valeur à un maximum d'un mois dans le passé. Cela permet d'éviter qu'une grande quantité de données ne dépasse les limites de débit de l'API de Tenable et de déclencher des délais d'exécution.

26. Cliquez sur **Envoyer** ou **Mettre à jour**.
27. Facultatif : Cliquez sur **Exécuter maintenant** pour l'exécuter immédiatement.

Présentation de l'intégration Atlassian Jira avec Réponse aux vulnérabilités

L'intégration Atlassian Jira avec Réponse aux vulnérabilités vous permet de tirer parti de différents outils de suivi des problèmes et de gestion agile pour suivre les efforts de remédiation des vulnérabilités.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Vue d'ensemble

ServiceNow® Réponse aux vulnérabilités est intégré à Atlassian Jira pour créer des problèmes correspondant à des vulnérabilités et synchroniser l'entité du problème dans Jira et l'entité de l'élément de vulnérabilité de Réponse aux vulnérabilités manière bidirectionnelle pour refléter les dernières mises à jour. Les gestionnaires de vulnérabilité exigent que les éléments

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de vulnérabilité présents dans ServiceNow Réponse aux vulnérabilités soient créés et affectés aux utilisateurs de rattrapage (développeurs en cas de) dans leur système d'enregistrement Réponse aux vulnérabilités des applicationset outil de gestion des problèmes préféré, tel que Atlassian Jira. Toute progression effectuée sur les vulnérabilités dans l'outil de gestion des problèmes doit être mise à jour pour ServiceNow Réponse aux vulnérabilités que les gestionnaires de vulnérabilité puissent les voir. En outre, toutes les mises à jour effectuées par les gestionnaires de vulnérabilité pour Réponse aux vulnérabilités les éléments de vulnérabilité doivent également être transmises à l'outil de gestion des problèmes afin qu'elles soient visibles par les utilisateurs du rattrapage.

Versions disponibles

Version	Notes de publication
Réponse aux vulnérabilités	Notes de version de Vulnerability Response Integration
Vulnerability Response et Configuration Compliance pour le conteneur	Notes de version de Container Vulnerability Response
Spoke Jira	Notes de version du spoke Jira

Jira Intégrations de vulnérabilité

Pour afficher l'intégration de Jira vulnérabilité, accédez à **Tout** > **Agile Management pour VR** > **Configurer les outils Agile** .

Les intégrations suivantes sont incluses dans le système de base. Ces intégrations ne sont pas toutes actives par défaut.

Après l'exécution initiale, chaque jour, des travaux planifiés sont enchaînés pour exécuter automatiquement les intégrations dans l'ordre. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Préparation de l'intégration Jira Réponse aux vulnérabilités

Une intégration réussie Jira de Vulnerability nécessite la planification et l'exécution de tâches préalables à l'intégration. Préparez l'intégration en effectuant ces tâches. L'intégration Jira Réponse aux vulnérabilités suppose que vous connaissez le produit et l'API Jira .

Composants installés avec l'intégration Agile et Réponse aux vulnérabilitésJira l'intégration pour Vulnerability Response

Plusieurs types de composants sont installés avec l'activation des modules d'extension Agile Integration for Vulnerability Response et Jira Integration for Vulnerability Response, notamment les tables et les rôles des utilisateurs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles installés

Titre du rôle [name]	Description
Administrateur de l'outil Agile [sn_vul_agile.agile_tool_admin]	Vous permet de créer une règle de configuration pour Gestion Agile afin de créer ou mettre à jour des problèmes. Créez des configurations de règles pour Agile Management.
Administrateur JIRA [sn_vul_jira.admin]	Vous permet de sélectionner l'outil Agile pour créer des problèmes pour la table d'entité sélectionnée.

Tables installées

Table	Description
Configuration de l'outil Agile [sn_vul_agile_tool_rule_config]	Contient des règles de configuration pour créer des problèmes sur la plateforme Agile.
Mappage du champ de l'outil Agile [sn_vul_agile_tool_field_mapping]	Contient le mappage de champs de la règle de configuration.
Mappage de l'état de l'outil Agile [sn_vul_agile_tool_state_mapping]	Contient le mappage de l'état du problème Jira avec l'état de l'élément vulnérable de l'application, de l'élément vulnérable du conteneur, de la tâche de rattrapage de l'application et de la tâche de rattrapage du conteneur.
Manifeste de l'outil Agile [sn_vul_agile_tool_manifest]	Contient la charge utile pour la création de problèmes.
Ressource de données de l'outil Agile [sn_vul_agile_tool_data_resource]	Contient les informations sur le problème Jira créé.
Administrateur JIRA [sn_vul_jira.admin]	Vous permet de sélectionner l'outil Agile pour créer des problèmes pour la table d'entité sélectionnée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer l'intégration de Vulnerability Response avec Jira

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit s'intègre Jira correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Rôle requis : admin.

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que l'application Vulnerability Response est installée et activée.	• L'intégration Jira pour Vulnerability Response nécessite l'application Vulnerability Response. • Pour la version la plus récente de Jira Integration for Vulnerability Response, vérifiez que vous avez installé la version la plus récente de Vulnerability Response. Consultez KB0856498 la matrice de compatibilité de Vulnerability Response et les changements de schéma de mise en production . • Si l'application n'est pas installée et activée, consultez Installer Vulnerability Response .
Vérifiez que le module d'extension Integration Hub est installé.	• Le spoke Jira nécessite le concentrateur d'intégration. • Consultez KB1112383 pour l'installation du concentrateur d'intégration. • Pour plus d'informations, consultez Calendriers juridiques - Vue d'ensemble d'IntegrationHub .
Vérifiez que la dernière version de Jira Rayon est installée.	Consultez KB0792632 pour l'installation du spoke Jira.
Vérifiez que l'intégration de Vulnerability Response avec Agile Management est installée.	L'intégration de Vulnerability Response avec Atlassian Jira nécessite cette intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer l'intégration Jira Réponse aux vulnérabilités .
2. Accédez au ServiceNow Store.
3. Dans le ServiceNow Store, recherchez l'intégration à Jira l'applicationRéponse aux vulnérabilités.
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **Dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Votre application est automatiquement installée sur votre instance.

Configurer les règles dans la configuration de l'outil Agile

Jira Les problèmes sont créés sur la Jira plateforme si les enregistrements créés dans l'élément vulnérable de l'application, l'élément vulnérable du conteneur, la tâche de rattrapage de l'application et la tâche de rattrapage du conteneur correspondent aux règles créées dans la configuration de l'outil Agile.

Avant de commencer

Rôles requis : sn_vul.app_read_all, sn_vul_container.read_all, sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin.

Procédure

1. Accédez à la **Tout** > **Agile Management pour VR** > **Configurer les outils Agile**.
2. Pour créer une règle de configuration dans la configuration de l'outil Agile, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire.

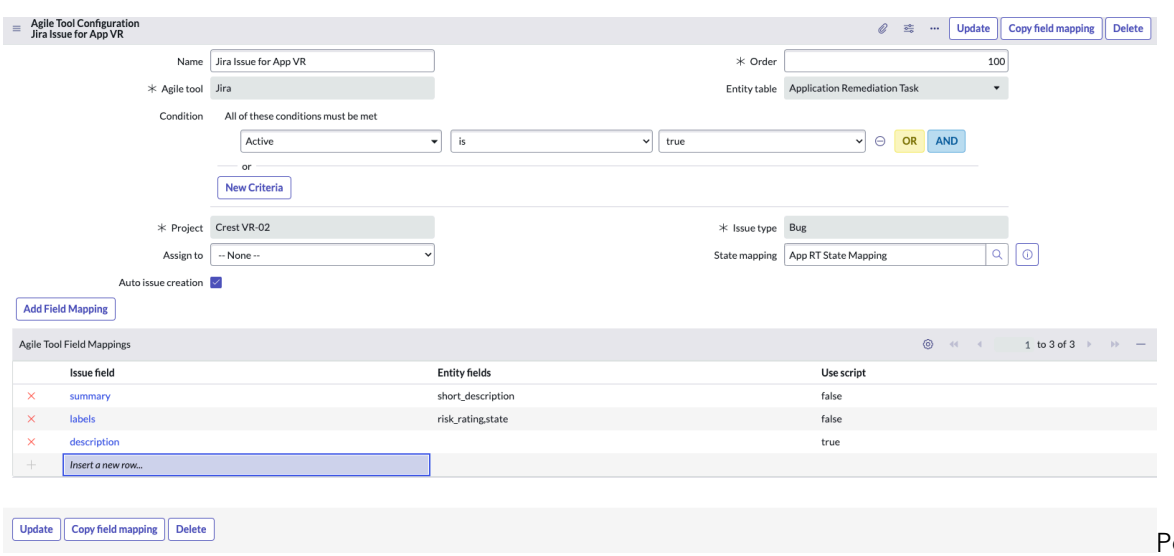
Formulaire de configuration de l'outil Agile

Champ	Description
Nom	Nom de la configuration de l'outil Agile.
Ordre	Ordre de la configuration de l'outil Agile.
Outil Agile	L'outil Agile pour créer des problèmes sur la plateforme Agile spécifique.
Table d'entité	Table sur laquelle la règle de configuration doit être appliquée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Condition	Condition de filtre sur la table d'entité sélectionnée pour créer des problèmes sur la plateforme Agile.
Création automatique de problème	La règle de configuration sera interrogée lorsqu'un nouvel enregistrement est créé dans la table d'entité sélectionnée, uniquement si la case à cocher est sélectionnée. **Remarque :** L'utilisateur doit utiliser l'action de liste pour créer des problèmes pour les enregistrements d'entité existants.
Projet	Le projet dans lequel le problème Jira sera créé.
Type de problème	Type de problème à créer dans un projet particulier.
Affecter à	Délégataire auquel le problème doit être affecté lors de la création du problème. Pour conserver les problèmes créés comme non affectés, sélectionnez « Aucun ».
Mappage de l'état	Les mappages d'état existants à partir de la table de mappage de l'état de l'outil Agile ou créez un nouveau mappage d'état entre l'état du problème dans la plateforme Agile et les états de la table d'entité ServiceNow .



Par défaut, lorsque l'application est installée, la tâche de rattrapage de l'application et la tâche de rattrapage du conteneur sont affichées dans le champ Table d'entité du formulaire de configuration de l'outil Agile.

4. Pour ajouter l'élément vulnérable d'application et l'élément vulnérable de conteneur dans la liste de choix Table d'entités, accédez à **Propriétés système> sn_vul_agile.tablesToShow** et ajoutez tout dans le champ Valeur.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de propriété système

Champ	Description
Choix	Valeurs séparées par des virgules pour une liste de choix.
Valeur	Définissez la valeur souhaitée pour la propriété. Toutes les valeurs de propriété sont stockées sous forme de chaînes. Lors de la récupération des propriétés via la méthode gs.getProperty(), traitez les résultats comme des chaînes. Par exemple, une propriété true|false renvoie « true » ou « false » (chaînes), et non l'équivalent booléen.

5. Sélectionnez l'enregistrement de mappage d'état existant ou créez un nouveau mappage d'état dans le mappage d'état de l'outil Agile.

Formulaire de mappage de l'état de l'outil Agile

Champ	Description
Nom	Insérez le nom unique du mappage d'état.
Outil Agile	Sélectionnez l'outil agile.
Table d'entité	Sélectionnez la table source sur laquelle le mappage d'état sera créé.
Projet	Sélectionnez le projet dans lequel l'état sera mappé.
État de l'entité ServiceNow	Sélectionnez l'état que vous souhaitez mapper avec l'état de l'outil agile.
État de l'outil Agile	Sélectionnez l'état que vous souhaitez mapper à partir des états des éléments de vulnérabilité.

6. Cliquez sur **Enregistrer et extraire les projets** pour extraire les projets dans la règle de configuration du champ Projet et valider les informations d'identification de l'outil Agile.

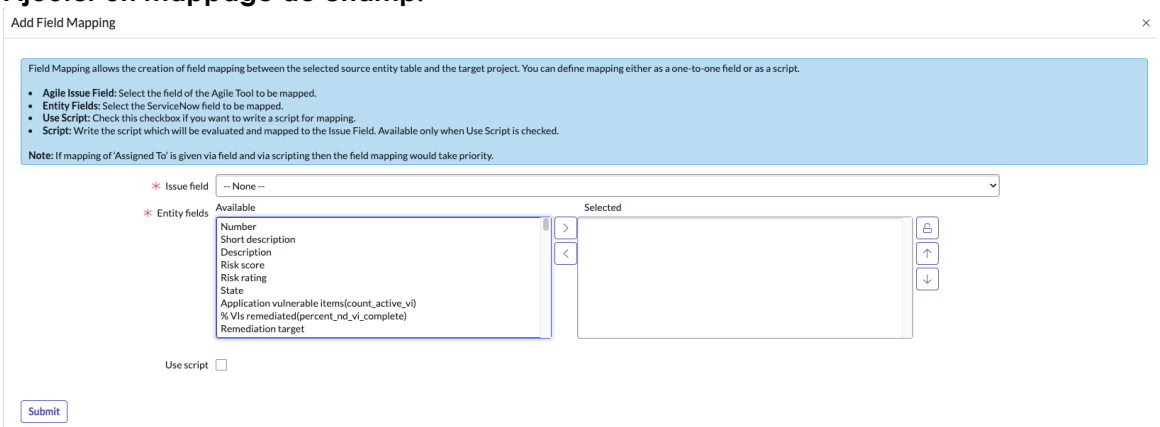
   Conseil : Vous pouvez définir la propriété système **projectsPageSize** pour extraire un nombre particulier de projets par page.

7. Accédez aux **propriétés système> sn_vul_jira.projectsPageSize** et ajoutez le nombre de projets à extraire par page dans le champ Valeur pour Jira Cloud.
8. Sélectionnez le projet, le type de problème et Affecter à dans la règle de configuration une fois les projets extraits.

   Le mappage de champs par défaut est renseigné dans la liste incorporée des mappages de champs d'outils Agile. Par défaut, les champs Résumé et Description des problèmes sont mappés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Pour mapper d'autres champs de problèmes avec les ServiceNow champs, cliquez sur **Ajouter un mappage de champ.**



Remarque :

- Vous devez mapper uniquement les champs de type chaîne et choix.
- Assurez-vous que tous les champs de problèmes obligatoires de l'outil Agile sont correctement mappés avec le champ d'entité.

Formulaire de mappage de l'état de l'outil Agile

Champ	Description
Champ du problème	Contient les champs de problème du projet et du type de problème actuellement sélectionnés dans la règle de configuration.
Champs d'entité	Contient les champs de la table d'entité sélectionnée dans la règle de configuration.
Utiliser le script	Sélectionnez cette option pour utiliser le script pour le mappage des champs de problème avec les champs d'entité.
Script	Script pour mapper le champ Problème avec les champs d'entité.

10. Cliquez sur **Envoyer** dans le modal Glide pour soumettre l'enregistrement de mappage de champs dans la table Mappages de champs de l'outil Agile.

Remarque : Si vous ne mappez pas les champs obligatoires, aucun problème ne sera créé pour cette règle de configuration.

Les champs obligatoires sont affichés en haut dans le formulaire de configuration de l'outil Agile.
Tous les mappages de champs pour une règle de configuration particulière sont affichés dans la liste incorporée de la table Mappage de champs de l'outil Agile dans la table Configuration de l'outil Agile.

11. Cliquez avec le bouton droit de la souris sur l'en-tête pour enregistrer vos modifications. L'enregistrement sauvegardé est visible dans la table Configuration de l'outil Agile. Si un enregistrement est créé dans l'élément vulnérable de l'application, l'élément vulnérable du conteneur, la tâche de rattrapage de l'application et la tâche de rattrapage

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

du conteneur correspond à une règle de configuration, le problème est créé pour l'enregistrement en fonction du mappage dans la règle de configuration.

12. Accédez aux **propriétés système** > **sn_vul_jira.cloudBulkSize** et définissez le nombre de problèmes à créer par lot dans le champ Valeur.

    Remarque : Le nombre maximum de tickets pouvant être créés par lot dans le cloud Jira est de 50).

    Vous pouvez définir la taille du lot pour créer des problèmes sur le serveur Jira.

13. Accédez aux **propriétés système** > **sn_vul_jira.onPremBulkIssue** et définissez le nombre de problèmes à créer par lot dans le champ **Valeur** .
    Vous pouvez également définir le nombre d'erreurs dans le champ Valeur de la propriété système pour traiter les enregistrements de la table de manifestes afin de créer des problèmes Jira jusqu'à un nombre d'erreurs spécifique.

14. Accédez aux **propriétés système** > **sn_vul_agile. ManifestErrorCount** et définissez le nombre maximal de fois où le manifeste avec erreur doit être traité.

Créer un problème Agile manuellement à l'aide de l'action de liste

Lorsqu'une action de liste : Créer un problème Jira est déclenchée, les enregistrements qui correspondent aux critères de configuration de la règle doivent être pris en compte pour « Créer un problème Jira » et ces enregistrements doivent être ingérés dans la table sn_vul_agile_tool_manifest avec le mappage sélectionné dans la règle de configuration.

Avant de commencer

Rôle requis : sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste** > **Tâches de remédiation/Éléments vulnérables de l'application/Éléments vulnérables du conteneur**.
2. Sélectionnez plusieurs enregistrements pour créer des problèmes Jira, puis cliquez sur **Créer un problème Jira**.
   Les enregistrements sélectionnés doivent tenir compte du mappage de champ et du mappage d'état de l'outil Agile associé.
   Les enregistrements sélectionnés qui répondent à la condition de la règle de configuration doivent être éligibles pour la création de problèmes Jira et ces enregistrements doivent être ajoutés à la *sn_vul_agile_tool_manifest* table.

Créer un problème Agile manuellement à l'aide de l'action de formulaire

Créez manuellement un problème Agile à l'aide d'une action de formulaire. Si l'enregistrement correspond à une condition de règle de configuration, une fenêtre contextuelle est renseignée avec les valeurs sélectionnées dans la règle de configuration. Si elle ne correspond à aucun critère, l'utilisateur est autorisé à sélectionner des valeurs pour les champs prédéfinis.

Avant de commencer

Assurez-vous que tous les champs de problèmes obligatoires de l'outil Agile sont correctement mappés avec le champ d'entité.

Rôles requis : sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste** > **Tâches de remédiation/Éléments vulnérables de l'application/Éléments vulnérables du conteneur**.
2. Sélectionnez n'importe quel enregistrement pour créer un problème Agile manuellement.
3. Sélectionnez **Créer un problème Agile**.
4. Insérez des détails valides pour les champs mentionnés.

   Si l'enregistrement satisfait à la condition d'une règle de configuration, les champs ci-dessous doivent être renseignés avec la valeur configurée et l'utilisateur peut modifier les valeurs de champ.

Champ	Description
Projet	Sélectionnez le projet dans lequel le problème Jira sera créé.
Type de problème	Sélectionnez le type de problème à créer dans un projet particulier.
Affecter à	Sélectionnez le délégataire auquel le problème doit être affecté lors de la création du problème.
Mappage de champs	Sélectionnez les champs Type de problème de l'outil Agile et insérez les valeurs directes pour le champ sélectionné.

5. Sélectionnez **Créer un problème Agile** pour soumettre l'enregistrement.
   Après avoir soumis l'enregistrement, l'entrée d'enregistrement est créée dans sn_vul_agile_tool_manifest table.

Synchroniser manuellement l'état du Jira problème

Mettez à jour l'état de l'enregistrement unique en cliquant sur le bouton **Synchroniser l'état Agile** du menu contextuel du formulaire et mettez à jour les états de plusieurs enregistrements en cliquant sur l'action de liste **Synchronisez l'état Agile** de l'élément vulnérable de l'application, de l'élément vulnérable du conteneur et de la table Tâche de rattrapage dans l'espace de travail du gestionnaire de vulnérabilité.

Avant de commencer

Rôles requis : sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Pourquoi et quand exécuter cette tâche

L'état est synchronisé à partir de ServiceNow l'outil Agile si l'état de l'entité est fermé ServiceNow ou si une entité est rouverte (c'est-à-dire si l'état est Ouvert). Tous les autres états seront reflétés de l'outil Agile vers ServiceNow. L'utilisateur n'est pas autorisé à synchroniser l'état des enregistrements dont la règle configurée associée n'a pas de mappage d'état ou les problèmes qui sont directement créés à partir de l'action de formulaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste** > **Tâches de remédiation/Éléments vulnérables de l'application/Éléments vulnérables du conteneur**.
2. Sélectionnez plusieurs enregistrements pour créer des tickets Jira, puis cliquez sur **Synchroniser le statut Agile**.
   Les états des enregistrements pour lesquels des problèmes sont déjà créés sont mis à jour si l'enregistrement n'est pas à l'état Fermé et si le mappage d'état existe pour les enregistrements sélectionnés dans la règle de configuration.
3. Ouvrez un enregistrement et **l'état de synchronisation Agile** est visible dans le menu contextuel du formulaire si les conditions suivantes sont remplies.
   - Un problème est créé pour l'enregistrement et l'enregistrement n'est pas à l'état Fermé
   - Le mappage de l'état existe pour l'enregistrement
4. Cliquez sur **Synchroniser l'état Agile** pour synchroniser l'état Agile avec l'état mappé.
   Vous pouvez définir la propriété système pour définir la taille du lot pour l'extraction de l'état du problème à partir de Jira.
5. Accédez à la **propriété système** > **sn_vul_jira.bulkIssueStatusSize**.
   - Pour Jira Server, le nombre maximum de problèmes à renvoyer (50 par défaut). La valeur maximale autorisée est dictée par la propriété Jira « jira.search.views.default.max ». Si vous spécifiez une valeur supérieure à ce nombre, les résultats de votre recherche seront tronqués).
   - Si le problème est créé à partir d'une action de formulaire ou si la règle configurée n'a pas de mappage d'état, ces enregistrements ne sont pas pris en compte pour la synchronisation d'état.

Configurer le planificateur pour créer automatiquement des problèmes

Configurez le planificateur pour qu'il s'exécute et crée automatiquement les Jira problèmes pour les enregistrements qui ont été créés dans la table sn_vul_agile_tool_manifest.

Avant de commencer

Rôle requis : admin ou schedule_admin.

Pourquoi et quand exécuter cette tâche

Tous les enregistrements de l'élément vulnérable de l'application, de l'élément vulnérable du conteneur, de la tâche de rattrapage de l'application et du rattrapage du conteneur créés dans la table sn_vul_agile_manifest sont pris en compte pour Jira la création du problème.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Travaux planifiés** > **Créer des problèmes Jira**.
2. Vous pouvez modifier les champs Exécution, Fuseau horaire et Heure dans le script planifié.

Formulaire Exécution de script planifiée

Champ	Description
Exécuter	Intervalle de temps à utiliser pour l'exécution de la tâche planifiée :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Quotidien : s'exécute tous les jours, à une heure précise. ◦ Hebdomadaire : s'exécute toutes les semaines, à une heure et un jour définis. ◦ Mensuel : s'exécute tous les mois, à une heure et un jour désignés du mois. ◦ Périodique : s'exécute sur un intervalle de répétition désigné. ◦ Once (Une fois) : s'exécute pour une seule occurrence. ◦ Sur demande : s'exécute immédiatement sur demande. ◦ Calendrier d'entreprise : début d'entrée : s'exécute sur les dates de début d'entrée du calendrier d'entreprise que vous sélectionnez dans le champ. Une tâche planifiée s'exécute pour la date de début de chaque entrée business que vous avez définie pour le calendrier professionnel. Par exemple, si le calendrier d'entreprise représente une année fiscale et que la date de début de chaque entrée est un mois fiscal, alors la tâche planifiée s'exécute le premier jour de chaque mois. ◦ Calendrier d'entreprise : fin de l'entrée : s'exécute pour la date de fin du calendrier d'entreprise que vous sélectionnez dans le champ. Cette sélection s'exécute de la même façon que Calendrier d'entreprise : début de l'entrée, mais en fonction des dates de fin des entrées du calendrier d'entreprise associées. **Remarque :** Lorsque vous sélectionnez Calendrier d'entreprise : début de l'entrée ou Calendrier d'entreprise : fin de l'entrée, vous pouvez appliquer un facteur de décalage pour planifier la tâche à exécuter avant ou après la période du calendrier d'entreprise sélectionné. Pour en savoir plus, reportez-vous aux champs Type de décalage et Décalage. Pour en savoir plus sur la création et l'utilisation des calendriers d'entreprise et la définition d'entrées de calendrier d'entreprise, consultez Créer un calendrier

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d'entreprise et Définir des entrées de calendrier d'entreprise .
Jour	Jour où la tâche planifiée doit s'exécuter. ◦ Si le champ Exécution est défini sur Hebdomadaire, sélectionnez le jour de la semaine. Choisissez mercredi, par exemple. ◦ Si le champ Exécution est défini sur Mensuel, sélectionnez le jour du mois. Par exemple, sélectionnez 25 pour le 25e jour du mois. Ce champ n'apparaît que si vous sélectionnez Mensuel ou Hebdomadaire dans le champ Exécution.
Intervalle de répétition	Durée de l'intervalle de répétition pour chaque exécution de tâche planifiée. Entrez la durée en nombre de jours, d'heures ou de minutes. Par exemple : ◦ Pour exécuter la tâche prévue tous les quatre jours, saisissez 04 dans le champ Jours. ◦ Pour l'exécuter toutes les 26 heures, entrez 26 dans le champ Heures. ◦ Si elle doit se répéter à un intervalle de 13 heures 30 minutes et 25 secondes, saisissez 13 dans le champ Heures, puis 30 et 25 dans les deux champs non libellés suivants.
Heure	Heure de la journée à laquelle la tâche planifiée doit s'exécuter, indiquée en heures, minutes et secondes dans un format de 24 heures. La sélection que vous effectuez dans le champ Fuseau horaire détermine le fuseau horaire de cette entrée.
Fuseau horaire	Fuseau horaire à utiliser avec l'entrée du champ Heure lorsque vous spécifiez l'heure à laquelle la tâche planifiée doit être exécutée. Sélectionnez une entrée de fuseau horaire : ◦ **Aucun** : utilisez le fuseau horaire par défaut pour l'utilisateur connecté qui crée la tâche planifiée. Par exemple, la tâche planifiée s'exécute à 16 h 45, heure US/Pacific, s'il s'agit du fuseau horaire

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	affecté à l'utilisateur et que vous entrez 16:45 dans le champ Heure. ◦ **Utiliser le fuseau horaire du système** : utilisez le fuseau horaire du système par défaut spécifié pour l'instance dans laquelle il s'exécute. Par exemple, la tâche prévue s'exécute à 22 h 15, heure de Londres, si Europe/London est le fuseau horaire du système par défaut pour l'instance, et que vous entrez 22:15 dans le champ Heure. ◦ Fuseau horaire actuel. ◦ Par exemple, la tâche planifiée s'exécute à 13 h 30 (heure de l'Est des États-Unis) si vous sélectionnez États-Unis/Est et saisissez 13 h 30 dans le champ Heure.
run_as	Par défaut, la valeur du champ run_ en tant que doit être vide. L'utilisateur peut définir la valeur en tant que valeur d'utilisateur de domaine pour créer un problème pour un domaine spécifique.

Configurer le planificateur pour mettre à jour automatiquement les problèmes

Configurez le planificateur pour mettre à jour automatiquement les Jira problèmes pour les enregistrements qui ont été ajoutés à la table sn_vul_agile_tool_manifest.

Avant de commencer
Rôle requis : admin ou schedule_admin.

Pourquoi et quand exécuter cette tâche
Tous les enregistrements de l'élément vulnérable de l'application, de l'élément vulnérable du conteneur, de la tâche de rattrapage de l'application et du rattrapage du conteneur créés dans la table sn_vul_agile_manifest sont pris en compte pour Jira la mise à jour du problème. Si l'enregistrement est fermé et que des commentaires sont ajoutés, ces valeurs doivent également être mises à jour pour le problème associé Jira .

Remarque :

- La tâche planifiée « mettre à jour les problèmes » ne met pas à jour l'état Jira si le workflow du projet de problème agile choisi empêche un utilisateur de modifier directement l'état à partir d'un autre état.
- Si vous fermez un enregistrement d'entité avec des commentaires supplémentaires, seul le dernier commentaire est pris en compte au moment de la mise à jour et, pour la prochaine mise à jour, tous les commentaires sont ajoutés au Jira.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Travaux planifiés** > **Mettre à jour les problèmes Jira**.
2. Vous pouvez modifier les champs **Exécution**, **Fuseau horaire** et **Heure** dans le script planifié.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Exécution de script planifiée

Champ	Description
Exécuter	Intervalle de temps à utiliser pour l'exécution de la tâche planifiée : ◦ Quotidien : s'exécute quotidiennement à l'heure désignée. ◦ Hebdomadaire : S'exécute toutes les semaines, à une heure et un jour désignés. ◦ Mensuel : s'exécute tous les mois, à une heure et un jour désignés du mois. ◦ Périodiquement : s'exécute selon l'intervalle de répétition désigné. ◦ Une fois : s'exécute pour une seule occurrence uniquement. ◦ Sur demande : s'exécute immédiatement sur demande. ◦ Calendrier d'entreprise : début d'entrée : s'exécute aux dates de début d'entrée du calendrier d'entreprise que vous sélectionnez dans le champ. Une tâche planifiée s'exécute pour la date de début de chaque entrée business que vous avez définie pour le calendrier professionnel. Par exemple, si le calendrier d'entreprise représente une année fiscale et que la date de début de chaque entrée est un mois fiscal, alors la tâche planifiée s'exécute le premier jour de chaque mois. ◦ Calendrier d'entreprise : fin de l'entrée : s'exécute pour la date de fin du calendrier d'entreprise que vous sélectionnez dans le champ. Cette sélection s'exécute de la même façon que Calendrier d'entreprise : début de l'entrée, mais en fonction des dates de fin des entrées du calendrier d'entreprise associées.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Lorsque vous sélectionnez Calendrier d'entreprise : début de l'entrée ou Calendrier d'entreprise : fin de l'entrée, vous pouvez appliquer un facteur de décalage pour planifier la tâche à exécuter avant ou après la période du calendrier d'entreprise sélectionné. Pour en savoir plus, reportez-vous aux champs Type de décalage et Décalage. Pour en savoir plus sur la création et l'utilisation des calendriers d'entreprise et la définition d'entrées de calendrier d'entreprise, consultez et Créer un calendrier d'entreprise Définir des entrées de calendrier d'entreprise .
Jour	Jour où la tâche planifiée doit s'exécuter. ◦ Si le champ Exécution est défini sur Hebdomadaire, sélectionnez le jour de la semaine. Choisissez mercredi, par exemple. ◦ Si le champ Exécution est défini sur Mensuel, sélectionnez le jour du mois. Par exemple, sélectionnez 25 pour le 25e jour du mois. Ce champ n'apparaît que si vous sélectionnez Mensuel ou Hebdomadaire dans le champ Exécution.
Intervalle de répétition	Durée de l'intervalle de répétition pour chaque exécution de tâche planifiée. Entrez la durée en nombre de jours, d'heures ou de minutes. Par exemple : ◦ Pour exécuter la tâche prévue tous les quatre jours, saisissez 04 dans le champ Jours. ◦ Pour l'exécuter toutes les 26 heures, entrez 26 dans le champ Heures. ◦ Si elle doit se répéter à un intervalle de 13 heures 30 minutes et 25 secondes, saisissez 13 dans le champ Heures, puis 30 et 25 dans les deux champs non libellés suivants.
Heure	Heure de la journée à laquelle la tâche planifiée doit s'exécuter, indiquée en

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	heures, minutes et secondes dans un format de 24 heures. La sélection que vous effectuez dans le champ Fuseau horaire détermine le fuseau horaire de cette entrée.
Fuseau horaire	Fuseau horaire à utiliser avec l'entrée du champ Heure lorsque vous spécifiez l'heure à laquelle la tâche planifiée doit être exécutée. Sélectionnez une entrée de fuseau horaire : ◦ Aucun : utilisez le fuseau horaire par défaut pour l'utilisateur connecté qui crée la tâche planifiée. Par exemple, la tâche planifiée s'exécute à 16h45. Heure des États-Unis/Pacifique s'il s'agit du fuseau horaire affecté par l'utilisateur et que vous saisissez 16:45 dans le champ Heure. ◦ Utiliser le fuseau horaire du système : utilisez le fuseau horaire du système par défaut spécifié pour l'instance dans laquelle il s'exécute. Par exemple, la tâche planifiée s'exécute à 22 h 15, heure de Londres, si Europe/Londres est le fuseau horaire système par défaut pour l'instance, et vous saisissez 22 h 15 dans le champ Heure. ◦ Fuseau horaire actuel. ◦ Par exemple, la tâche planifiée s'exécute à 13 h 30 (heure de l'Est des États-Unis) si vous sélectionnez États-Unis/Est et saisissez 13 h 30 dans le champ Heure.
run_as	Par défaut, la valeur **du champ run_ en tant que** est vide. Vous pouvez définir la valeur d'un utilisateur de domaine afin de créer un problème pour un domaine spécifique.

Configurer le planificateur pour synchroniser l'état Jira avec ServiceNow® automatiquement

Configurez le planificateur pour synchroniser l'état des problèmes avec l'élément de vulnérabilité de l'application Jira , les éléments de vulnérabilité du conteneur et les tâches de la table sn_vul_agile_manifest.

Avant de commencer

Rôle requis : schedule_admin ou admin

Pourquoi et quand exécuter cette tâche

Le planificateur s'exécute automatiquement selon la planification configurée. L'état des enregistrements créés dans la table Élément vulnérable de l'application, Élément vulnérable du conteneur, Tâche de rattrapage de l'application et Tâche de rattrapage du conteneur pour lesquels des problèmes Jira créés sont mis à jour en fonction de l'état actuel du

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

problème dans la Jira plateforme en fonction du mappage d'état indiqué dans la règle de configuration.

Tous les enregistrements de l'élément vulnérable de l'application, de l'élément vulnérable du conteneur, de la tâche de rattrapage de l'application et du rattrapage du conteneur créés dans la table sn_vul_agile_manifest sont pris en compte pour Jira la création du problème.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Travaux planifiés** > **État de la synchronisation**.
2. Vous pouvez modifier les champs Exécution, Fuseau horaire et Heure dans le script planifié.

Formulaire Exécution de script planifiée

Champ	Description
Exécuter	Intervalle de temps à utiliser pour l'exécution de la tâche planifiée : ◦ Quotidien : s'exécute quotidiennement à l'heure désignée. ◦ Hebdomadaire : S'exécute toutes les semaines, à une heure et un jour désignés. ◦ Mensuel : s'exécute tous les mois, à une heure et un jour désignés du mois. ◦ Périodiquement : s'exécute selon l'intervalle de répétition désigné. ◦ Une fois : s'exécute pour une seule occurrence uniquement. ◦ Sur demande : s'exécute immédiatement sur demande. ◦ Calendrier d'entreprise : début d'entrée : s'exécute aux dates de début d'entrée du calendrier d'entreprise que vous sélectionnez dans le champ. Une tâche planifiée s'exécute pour la date de début de chaque entrée business que vous avez définie pour le calendrier professionnel. Par exemple, si le calendrier d'entreprise représente une année fiscale et que la date de début de chaque entrée est un mois fiscal, alors la tâche planifiée s'exécute le premier jour de chaque mois. ◦ Calendrier d'entreprise : fin de l'entrée : s'exécute pour la date de fin du calendrier d'entreprise que vous sélectionnez dans le champ. Cette sélection s'exécute de la même façon que Calendrier d'entreprise : début de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	l'entrée, mais en fonction des dates de fin des entrées du calendrier d'entreprise associées. **Remarque :** Lorsque vous sélectionnez Calendrier d'entreprise : début de l'entrée ou Calendrier d'entreprise : fin de l'entrée, vous pouvez appliquer un facteur de décalage pour planifier la tâche à exécuter avant ou après la période du calendrier d'entreprise sélectionné. Pour en savoir plus, reportez-vous aux champs Type de décalage et Décalage. Pour en savoir plus sur la création et l'utilisation des calendriers d'entreprise et la définition d'entrées de calendrier d'entreprise, consultez Créer un calendrier d'entreprise et Définir des entrées de calendrier d'entreprise .
Jour	Jour où la tâche planifiée doit s'exécuter. ◦ Si le champ Exécution est défini sur Hebdomadaire, sélectionnez le jour de la semaine. Choisissez mercredi, par exemple. ◦ Si le champ Exécution est défini sur Mensuel, sélectionnez le jour du mois. Par exemple, sélectionnez 25 pour le 25e jour du mois. Ce champ n'apparaît que si vous sélectionnez Mensuel ou Hebdomadaire dans le champ Exécution.
Intervalle de répétition	Durée de l'intervalle de répétition pour chaque exécution de tâche planifiée. Entrez la durée en nombre de jours, d'heures ou de minutes. Par exemple : ◦ Pour exécuter la tâche prévue tous les quatre jours, saisissez 04 dans le champ Jours. ◦ Pour l'exécuter toutes les 26 heures, entrez 26 dans le champ Heures. ◦ Si elle doit se répéter à un intervalle de 13 heures 30 minutes et 25 secondes, saisissez 13 dans le champ Heures, puis 30 et 25 dans les deux champs non libellés suivants.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure	Heure de la journée à laquelle la tâche planifiée doit s'exécuter, indiquée en heures, minutes et secondes dans un format de 24 heures. La sélection que vous effectuez dans le champ Fuseau horaire détermine le fuseau horaire de cette entrée.
Fuseau horaire	Fuseau horaire à utiliser avec l'entrée du champ Heure lorsque vous spécifiez l'heure à laquelle la tâche planifiée doit être exécutée. Sélectionnez une entrée de fuseau horaire : ◦ -Aucun- : utilisez le fuseau horaire par défaut de l'utilisateur connecté qui crée la tâche planifiée. Par exemple, la tâche planifiée s'exécute à 16 h 45, heure US/Pacific, s'il s'agit du fuseau horaire affecté à l'utilisateur et que vous entrez 16:45 dans le champ Heure. ◦ Utiliser le fuseau horaire du système : utilisez le fuseau horaire du système par défaut spécifié pour l'instance dans laquelle il s'exécute. Par exemple, la tâche planifiée s'exécute à 22 h 15, heure de Londres, si Europe/Londres est le fuseau horaire système par défaut pour l'instance, et vous saisissez 22 h 15 dans le champ Heure. ◦ Fuseau horaire actuel. ◦ Par exemple, la tâche planifiée s'exécute à 13 h 30 (heure de l'Est des États-Unis) si vous sélectionnez États-Unis/Est et saisissez 13 h 30 dans le champ Heure.
run_as	Par défaut, la valeur du champ run_ en tant que est vide. Vous pouvez définir la valeur comme la valeur de l'utilisateur du domaine requis afin de créer un problème pour un domaine spécifique.

Traduction automatique

Créer manuellement une intégration de vulnérabilité

Les intégrations de vulnérabilité permettent aux clients et aux fournisseurs d'enrichir les données de vulnérabilité sur leur instance en récupérant des données provenant de systèmes et de fournisseurs externes. Cette capacité peut simplifier le cycle de vie de la correction des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Pour obtenir des instructions détaillées sur la création d'intégrations, reportez-vous à Définir une nouvelle intégration de vulnérabilité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir une nouvelle intégration de vulnérabilité

Une intégration de vulnérabilité extrait les données de rapport d'un système tiers, généralement pour récupérer les données de vulnérabilité, et traite ces données de rapport à l'aide de sources de données ou d'un processeur personnalisé.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Administration** > **Intégrations**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs nécessaires.

Intégration de vulnérabilité

Champ	Description
Nom	Un nom descriptif pour l'intégration.
Actif	Indique si l'intégration est active. Si vous ne souhaitez pas qu'il s'exécute pendant une période spécifique, vous pouvez configurer les paramètres que vous souhaitez utiliser et désactiver la tâche.
Exécuter	Fréquence à laquelle vous souhaitez que l'intégration s'exécute : Quotidienne, Hebdomadaire, Périodique, et ainsi de suite. Comme indiqué, les champs suivants s'affichent ou non en fonction du paramètre que vous avez défini dans ce champ.
Jour	Le jour où vous souhaitez que l'intégration s'exécute. ◦ Si vous avez sélectionné **Hebdomadaire** dans le champ **Exécuter** , ce champ affiche les jours de la semaine. ◦ Si vous avez sélectionné **Mensuel** dans le champ **Exécuter** , ce champ affiche les jours du mois.
Heure	Heure à laquelle vous souhaitez que l'intégration démarre. Ce champ s'affiche uniquement si vous avez sélectionné **Quotidien**, **Hebdomadaire** ou **Mensuel** dans le champ **Exécuter** .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	[Lecture seule] Nom de l'application pour laquelle cette intégration a été créée.
Intervalle de répétition	Si vous avez sélectionné **Périodiquement** dans le champ **Exécuter** , ce champ affiche le nombre de jours et d'heures avant que l'intégration ne s'exécute à nouveau.
En cours de démarrage	Si vous avez sélectionné **Périodiquement** dans le champ **Exécuter** , ce champ affiche les dates et heures à utiliser comme point de départ pour les mises à jour périodiques.
Conditionnel	Sélectionnez ce champ si vous souhaitez ajouter des paramètres conditionnels.
Condition	Si vous avez coché la case **Conditionnel** , entrez les conditions ici.
Détails de l'intégration	
Script d'intégration	Sélectionnez l'include de script qui étend VulnerabilityIntegrationBase à exécuter lors de l'exécution de l'intégration. Ce script définit comment récupérer des données à partir d'un système tiers.
Script de l'instanciateur d'intégration	Entrez un script qui définit la façon de construire l'include de script sélectionné pour le **script d'intégration**. Pour plus d'informations, consultez Champs de script de l'instanciateur d'intégration. **Remarque :** Les scripts nécessitent à la fois ServiceNow une Réponse aux vulnérabilités expertise.
Stratégie de processeur de rapport	Sélectionnez la stratégie que vous souhaitez utiliser pour gérer les données retournées par le script d'intégration lors de l'exécution de l'intégration. ◦ Sélectionnez **Pièce jointe de source de données** si vous souhaitez traiter les données à l'aide d'une source de données. ◦ Sélectionnez **Processeur de rapport personnalisé** pour sélectionner un processeur personnalisé.
Script de processeur de rapport	Si vous avez sélectionné **Processeur de rapport personnalisé** dans le champ **Stratégie de processeur de rapport** , sélectionnez l'include de script qui étend l'include de script

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	VulnerabilityReportProcessorBase à exécuter lors de l'exécution de l'intégration. Ce script définit la manière de traiter les données renvoyées par le script d'intégration.
Script de l'instanciateur de processeur	Entrez un script qui définit la façon de construire l'include de script sélectionné pour le **processeur de rapports**.

4. Cliquez sur **Envoyer**.

Information associée

- Script d'intégration de vulnérabilité
- Stratégies de processeur de rapport
- Champs de script de l'instanciateur d'intégration
- Exécuter manuellement une intégration de vulnérabilité

Script d'intégration de vulnérabilité

Sur le formulaire d'intégration de vulnérabilité, le script d'intégration fait référence à un include de script qui étend l'include de script VulnerabilityIntegrationBase.

La fonctionnalité contenue dans ce script est appelée par VulnerabilityIntegrationController pour gérer les moyens par lesquels les données sont récupérées à partir d'une source de données externe. Chaque sous-classe de VulnerabilityIntegrationBase a accès à des informations contextuelles sur le processus d'appel. Ces informations sont disponibles par le biais des variables membres suivantes :

- integrationGr — GlideRecord de l'enregistrement d'intégration de vulnérabilité dont l'exécution a été demandée.
- integrationProcessGr — GlideRecord qui fournit des informations contextuelles sur le processus actuel d'une intégration.

Le processus de vulnérabilité contient des paramètres spéciaux à utiliser dans une intégration, généralement à des fins de pagination. Chaque exécution d'une intégration de vulnérabilité (appelée exécution d'intégration de vulnérabilité) comporte au moins un processus d'intégration de vulnérabilité associé. Pour les intégrations multi-appels, il existe un ou plusieurs enregistrements de processus d'intégration de vulnérabilité pour chaque exécution d'intégration de vulnérabilité.

L'include de script doit fournir une implémentation pour la méthode `retrieveData()` et renvoyer un objet traité par le script de processeur de rapports. L'objet renvoyé par retrieveData est un objet simple avec des propriétés pour le contenu, le contentType et l'extension.

Voici une capture d'écran de VulnerabilityIntegrationBase.retrieveData() :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Base d'intégration de vulnérabilité.retrieveData()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

La logique de `la fonction retrieveData()` dépend de l'interface requise pour récupérer les données. Par exemple, si la source des données extraites dispose d'une API REST, le corps de cette méthode peut appeler le point de terminaison REST, probablement via RESTMessageV2. La réponse de l'appel peut ensuite être analysée ou mise dans une pièce jointe, et les détails peuvent être utilisés pour construire l'objet de retour.

Intégrations à appel unique

Les scripts d'intégration à appel unique (page unique) sont les types d'intégration les plus simples. Ils nécessitent un appel, souvent à une source de données externe, pour récupérer les données. Seul retrieveData() doit être implémenté pour les intégrations d'une seule page/d'un seul appel.

Voici un exemple illustrant un script d'intégration d'appel unique simple. Il crée un RESTMessageV2 et l'exécute. Il renvoie ensuite un objet utilisant le corps de la réponse comme contenu, ainsi qu'un contentType et une extension supposés.

Script d'intégration d'appel unique

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```

Intégrations de plusieurs appels

Les scripts d'intégration à appels multiples (ou à pages multiples) sont un peu plus compliqués. Ils nécessitent plusieurs appels à une source de données pour récupérer des données.

À l'instar d'une intégration à appel unique, retrieveData() doit également être implémentée pour une intégration à appels multiples. Dans le corps de retrieveData(), l'intégration utilise les méthodes hasMoreData() et setNextRunParameters() fournies par VulnerabilityIntegrationBase.

La méthode hasMoreData() accepte un seul booléen qui demande au VulnerabilityIntegrationController d'insérer plus de processus pour extraire plus de données.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lors de la transmission de true à hasMoreData(), un appel à setNextRunParameters() est effectué pour fournir un contexte au processus suivant.

La méthode setNextRunParameters() accepte un seul objet qui fournit des informations de contexte à utiliser par le prochain appel pour retrieveData(). Cet objet est utilisé pour passer l'état aux appels suivants pour retrieveData(). Un exemple de cas d'utilisation consiste à transmettre un objet qui indique le numéro et la taille de page actuels à un service Web.

Pour les intégrations d'appels multiples, chaque appel à retrieveData() vérifie d'abord les paramètres du processus actuel. La méthode _getProcessParameters() est fournie à tous VulnerabilityIntegrationBase pour faciliter l'obtention des paramètres définis par le processus précédent. S'il n'y a pas de paramètres, cela indique qu'il s'agit du premier processus.

Vous trouverez ci-dessous une capture d'écran d'un exemple de script d'intégration d'appels multiples. Dans le prolongement de l'exemple d'intégration d'appel unique, ce script illustre les appels vers un point de terminaison REST doté d'une prise en charge de base de la pagination. Il montre comment obtenir une seule page de données, reconnaître qu'il y a plus de données à récupérer, puis indiquer au processus suivant quelle page récupérer.

Script d'intégration de plusieurs appels

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

Les pièces jointes telles que retrieveData() renvoient des valeurs

Parfois, il est préférable de renvoyer une pièce jointe à partir de retrieveData(). La logique de création et/ou de récupération d'une pièce jointe est propre à l'implémentation, mais une fois que la pièce jointe est connue, ses informations peuvent être renvoyées.

Pour fournir une pièce jointe, retrieveData() renvoie un objet comme :

```
{
        contents: "attachment-sys-id",
        contentType: "sys_attachment"
}
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suit un exemple qui s'étend sur l'exemple précédent, mais qui enregistre le corps de la réponse du message REST dans l'enregistrement du processus d'intégration. Il renvoie ensuite cet identificateur de pièce jointe comme contenu de l'objet return.

Renvoyer la pièce jointe à partir de retrieveData

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

Stratégies de processeur de rapport

Le champ **Stratégie de processeur de rapport** du formulaire Intégration de vulnérabilité est utilisé pour sélectionner la méthode de traitement des données retournées par le script d'intégration de vulnérabilité lorsque le processus d'intégration de vulnérabilité est exécuté.

La valeur par défaut est **Pièce jointe de source de données**. Cette méthode est l'implémentation de base de référence qui prend les données récupérées et les transmet à une source de données pour qu'elles soient importées dans le système. La sélection **d'un processeur de rapport personnalisé** vous permet de sélectionner un script de processeur personnalisé pour le traitement des données.

Utiliser la stratégie de processeur de rapport de pièce jointe de source de données

La stratégie de processeur de rapport de pièce jointe de source de données est utilisée pour transmettre les données récupérées par le script d'intégration aux sources de données configurées.

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Administration** > **Intégrations** et créez une nouvelle intégration.
2. Dans le champ **Stratégie de processeur de rapport** , sélectionnez **Pièce jointe de source de données**.
3. Cliquez avec le bouton droit dans l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
4. Dans la liste connexe **Sources de données d'intégration de vulnérabilité** , cliquez sur **Nouveau**.
5. Définissez la source de données à utiliser.
6. Cliquez sur **Envoyer**.
7. Répétez les étapes 4 à 6 si vous avez besoin de sources de données supplémentaires. Assurez-vous de spécifier l'ordre dans lequel les multiples sources de données envoient des informations dans le champ **Ordre** .
8. Cliquez sur **Mettre à jour**.

À propos des scripts de processeur de rapport personnalisés

Sur le formulaire d'intégration de vulnérabilité, le processeur de rapport est une référence à un include de script qui étend l'include de script VulnerabilityReportProcessorBase. La fonctionnalité contenue dans ce script est appelée par VulnerabilityIntegrationController et définit les moyens par lesquels les données retournées par le script d'intégration sont traitées.

Chaque sous-classe de VulnerabilityReportProcessorBase a accès à des informations contextuelles sur le processus appelant. Ces informations sont disponibles par le biais des variables membres suivantes :

- integrationGr — GlideRecord de l'enregistrement d'intégration de vulnérabilité dont l'exécution a été demandée.
- integrationProcessGr — GlideRecord du processus de vulnérabilité qui fournit des informations contextuelles pour le processus actuel d'une intégration.

Le script include doit fournir une implémentation pour la méthode `processReport()`. L'objet passé à processReport() est l'objet renvoyé par retrieveData, et en tant que tel, est un objet simple avec des propriétés pour le contenu, le contentType et l'extension. La logique réelle dans processReport() est spécifique à l'implémentation et dépend des données du rapport fournies.

Voici une capture d'écran de VulnerabilityReportProcessorBase.processReport() :

Script de processeur de rapport personnalisé

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de script de l'instanciateur d'intégration

Le formulaire d'intégration de vulnérabilité contient le script de l'instanciateur d'intégration et, lorsque la stratégie de **processeur de rapport personnalisé** est sélectionnée, le script de l'instanciateur de processeur. Ces champs sont utilisés pour fournir la logique permettant d'instancier l'objet défini par les champs de référence du script include, le script d'intégration et le processeur de rapports, respectivement.

Lorsque l'include de script est sélectionné, les deux champs sont préremplis avec un appel de constructeur sans argument. Souvent, cela suffit, mais il peut arriver que plus de logique soit nécessaire pour instancier l'objet de script.

L'enregistrement integrationProcessGr est exposé aux champs de script de l'usine afin que les informations spécifiques au processus puissent être utilisées, selon les besoins.

Exécuter manuellement une intégration de vulnérabilité

Une intégration de vulnérabilité est configurée pour s'exécuter sur une base planifiée. Toutefois, vous pouvez les exécuter manuellement en cas de besoin.

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Administration** > **Intégrations**.
2. Ouvrez l'intégration que vous souhaitez exécuter.
3. Cliquez sur **Exécuter maintenant**.

Ingestion manuelle des vulnérabilités

Ingérer manuellement les vulnérabilités dans l'application Réponse aux vulnérabilités afin de pouvoir les corriger rapidement sans avoir à attendre les résultats du scanner.

Les scanners tiers permettent Rapid7 notamment d'importer des données Réponse aux vulnérabilités de vulnérabilité et de traiter les données pour générer un rapport sur les résultats. Avec l'intégration de l'ingestion manuelle, vous pouvez ingérer de manière proactive les vulnérabilités et les corriger au lieu d'attendre que les analyseurs signalent les actifs à risque. L'ingestion manuelle des vulnérabilités protège efficacement les actifs contre les menaces inconnues telles que les exploits zero-day.

Ingestion manuelle des vulnérabilités

Vous pouvez importer les données de vulnérabilité en chargeant un modèle dans les formats de fichier suivants :

- Excel
- Valeur séparée par des virgules (CSV)

Pour accéder au modèle et le télécharger, accédez à **Tout** > **Réponse aux vulnérabilités** > **Ingestion manuelle d'élément de vulnérabilité** > **Interface utilisateur, charger le fichier**.

Veillez à suivre ces points clés lors du remplissage des enregistrements dans le modèle :

- Ne faites pas d'erreurs de frappe dans les enregistrements de la colonne Gravité/État. En cas d'erreur de frappe, l'enregistrement est ignoré.
- Ne modifiez pas les noms de colonnes.
- Ne placez pas les noms de colonnes dans une ligne à l'exception de la première ligne.
- Ne modifiez pas l'ordre des feuilles dans le modèle Excel. Les données relatives aux vulnérabilités doivent toujours être présentes dans la deuxième feuille.
- Ne placez pas les détails des vulnérabilités dans une feuille, à l'exception de la feuille Entrées de détections manuelles.
- N'utilisez aucun caractère, à l'exception des caractères alphanumériques et spéciaux tels que le tiret (-), le point (.), plus (+), le trait de soulignement (_), l'espace, les crochets '(' ')' et le symbole arobase (@) pour le nom du fichier.

Pour obtenir des instructions sur la façon de renseigner les données du modèle, reportez-vous à la section Modèle pour l'ingestion manuelle des vulnérabilités.

Intégrations des ingestions manuelles

L'intégration est déclenchée lorsqu'un fichier est téléchargé. En fonction du type de fichier chargé, l'intégration correspondante est déclenchée.

Pour afficher les intégrations, accédez à **Tout** > **Réponse aux vulnérabilités** > **Ingestion manuelle d'élément de vulnérabilité** > **Intégrations**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les intégrations d'ingestion manuelle du système de base suivantes sont disponibles par défaut.

Intégrations

Type d'intégration	Description
Intégration de l'intégration Excel de l'ingestion manuelle	Récupère les données en récupérant le dernier fichier Excel chargé à partir de la table File d'attente push d'ingestion de vulnérabilité et copie la pièce jointe dans l'exécution d'intégration respective.
Intégration CSV de l'ingestion manuelle	Récupère les données en récupérant le dernier fichier CSV chargé à partir de la table File d'attente push d'ingestion de vulnérabilité et copie la pièce jointe dans l'exécution d'intégration respective.

L'intégration tierce de l'ingestion manuelle crée une instance d'intégration, par défaut, avec les deux paramètres d'instance d'intégration suivants :

- max_input_records : définit le nombre d'enregistrements qui peuvent être créés dans le modèle. Si vous ajoutez plus d'enregistrements que ce qui est spécifié dans ce paramètre, les enregistrements supplémentaires sont ignorés. Nombre d'enregistrements pouvant être mis à jour dans la colonne Valeur. Le nombre recommandé de créations d'enregistrements dans le modèle est 1 000. Tout ce qui dépasse cette valeur peut poser des problèmes de performances.
- insert_fixed : Importe les détections de vulnérabilité corrigées.

Pour afficher les paramètres d'instance d'intégration, accédez à **Tout** > **Réponse aux vulnérabilités** > **Ingestion manuelle d'élément de vulnérabilité** > **Intégrations** et cliquez sur l'instance source de n'importe quelle intégration. Vous pouvez également accéder à **Tout** > **Réponse aux vulnérabilités** > **Instances d'intégration** et cliquez sur **Ingestion manuelle**.

Ingérer des vulnérabilités manuellement

Ingérer manuellement les vulnérabilités en chargeant un modèle avec les données de vulnérabilités.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Interface utilisateur, charger le fichier**.
2. Cliquez sur les liens Excel ou CSV et téléchargez le modèle au format respectif.
3. Dans le modèle, entrez les données de vulnérabilité dans les enregistrements.
   Pour obtenir des instructions sur la façon de renseigner les données du modèle, reportez-vous à la section Modèle pour l'ingestion manuelle des vulnérabilités.
4. Cliquez sur **Importer le fichier** et chargez le modèle mis à jour.
5. Cliquez sur **Envoyer**.
   La page Files d'attente push d'intégration de vulnérabilité s'affiche. Vous pouvez afficher la liste des instances d'intégration, l'état des exécutions de l'intégration et les notes de journal une fois l'exécution de l'intégration terminée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Une fois le fichier chargé, accédez à **Tout** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Intégrations**. Vérifiez que l'exécution de l'intégration est correcte.

Vérifier l'exécution de l'intégration manuelle

Vérifiez que l'exécution de l'intégration est correcte. Affichez le nombre de détections individuelles et les éléments vulnérables (VI) créés ou mis à jour en raison de l'exécution de l'intégration.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Intégrations**.
2. Cliquez sur le nom de l'intégration en fonction du type de fichier chargé.
3. Cliquez sur l'onglet **Exécutions de l'intégration de vulnérabilité** .
4. Cliquez sur le numéro d'exécution de l'intégration.
5. Cliquez sur l'onglet **Éléments** .
6. Passez en revue les informations de l'onglet **Éléments** .

Onglet Éléments

Onglet/Champ	Description
Onglet Éléments	Affiche le nombre total de VI importés. Vous pouvez afficher le nombre total de détections importées en ajoutant les nombres répertoriés dans l'onglet Détections.
Nouveaux éléments	Affiche le nombre d'éléments vulnérables créés à partir de cette exécution d'intégration.
Éléments importés	Affiche la somme de tous les champs de cette section.
Éléments en double	Affiche les éléments en double. Ce champ n'est plus renseigné.
Éléments mis à jour	Affiche le nombre de fois où les éléments vulnérables sont mis à jour au cours de l'exécution de cette intégration. Cette valeur n'est pas le nombre d'éléments vulnérables uniques qui sont mis à jour. Si, par exemple, un élément vulnérable est mis à jour deux fois au cours de l'exécution de l'intégration, il est compté deux fois et affiché sous la forme `de 2` éléments mis à jour.
Éléments inchangés	Affiche les éléments vulnérables trouvés pendant l'exécution de l'intégration qui

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet/Champ	Description
	existent dans la base de données, mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

Que faire ensuite

Après avoir vérifié que l'exécution de l'intégration est réussie, accédez à **Tout** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Historique des fichiers chargés**. Vérifiez s'il existe des enregistrements ayant échoué à partir des notes.

Configurer les détections manuelles de fermeture automatique

Activez la fermeture automatique des détections manuelles pour fermer automatiquement les détections manuelles périmées.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Interface utilisateur, charger le fichier**.
2. Cliquez sur **Modifier la configuration de fermeture automatique**.
3. Cliquez sur l'onglet **Détections manuelles** .
4. Assurez-vous que la case **Fermer automatiquement les détections manuelles** est cochée.
5. Dans le champ **Dernières détections manuelles trouvées (en jours),** entrez le nombre de jours après lesquels les détections manuelles doivent être fermées.
   La valeur par défaut est de 90 jours. Vous pouvez entrer n'importe quelle valeur positive pour le nombre de jours.

Vérifier l'état du chargement

Vérifiez si l'exécution de l'intégration de vulnérabilité a réussi, partiellement réussi ou échoué.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Historique des fichiers chargés**.
2. Dans la table Files d'attente push de l'intégration de vulnérabilité, vérifiez l'heure du chargement et l'état du chargement, respectivement dans les colonnes Créé et État.
3. Facultatif : Dans le champ **Notes** , affichez le motif de l'échec.

Modèle pour l'ingestion manuelle des vulnérabilités

Le modèle fournit des colonnes qui doivent être remplies avec les données de vulnérabilité et d'élément de configuration (CI). Une fois le modèle renseigné et chargé, les données sont traitées.

Instructions pour remplir le modèle

Pour entrer les détails dans le modèle, suivez les instructions fournies dans la table suivante.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Instructions pour le modèle

Colonne	Obligatoire/ Facultatif ?	Longueur de la chaîne (max)/ valeurs valides	Description
ID de l'actif	Facultatif	255	Identificateur unique universel (UUID) ou ID d'actif. Il peut s'agir de la valeur générée par un scanner.
Saisissez des informations dans au moins une des cinq colonnes suivantes :			
Adresse MAC	Obligatoire	24	Informations sur l'hôte ou l'actif. La combinaison de toutes les valeurs fournies doit être unique pour un actif.
FQDN	Obligatoire	255	
NETBIOS	Obligatoire	255	
Adresse IP	Obligatoire	255	
Nom d'hôte	Obligatoire	255	
Les colonnes restantes ne dépendent pas les unes des autres.			
ID de la vulnérabilité	Obligatoire	255	Représente une vulnérabilité dans la base de données de vulnérabilité nationale (NVD) ou un ID renvoyé par un scanner tiers.
Résumé de la vulnérabilité	Facultatif	512	Brève description de la vulnérabilité. Il est ajouté à la base de données uniquement lorsque l'ID de vulnérabilité n'est pas disponible.
Sévérité	Facultatif	Critique, Élevé, Moyen, Faible, Aucun	Gravité de la vulnérabilité. Il est ajouté à la base de données uniquement lorsque l'ID de vulnérabilité n'est pas disponible. Si l'enregistrement est vide, il est considéré par défaut comme critique.
Port	Facultatif	Non applicable	Port à partir duquel la vulnérabilité est détectée. La valeur doit être un nombre entier valide. S'il existe une entrée non valide, l'enregistrement est ignoré.
Protocole	Facultatif	40	Type de protocole réseau utilisé.
Preuve	Facultatif	4 000	Représente l'emplacement ou le chemin d'accès du système de la vulnérabilité.
État	Facultatif	ouvert, fixe	État de la détection. Si l'enregistrement est vide, il est considéré comme ouvert par défaut.

Traduction automatique

Réponse aux vulnérabilités Vue d'ensemble du rattrapage

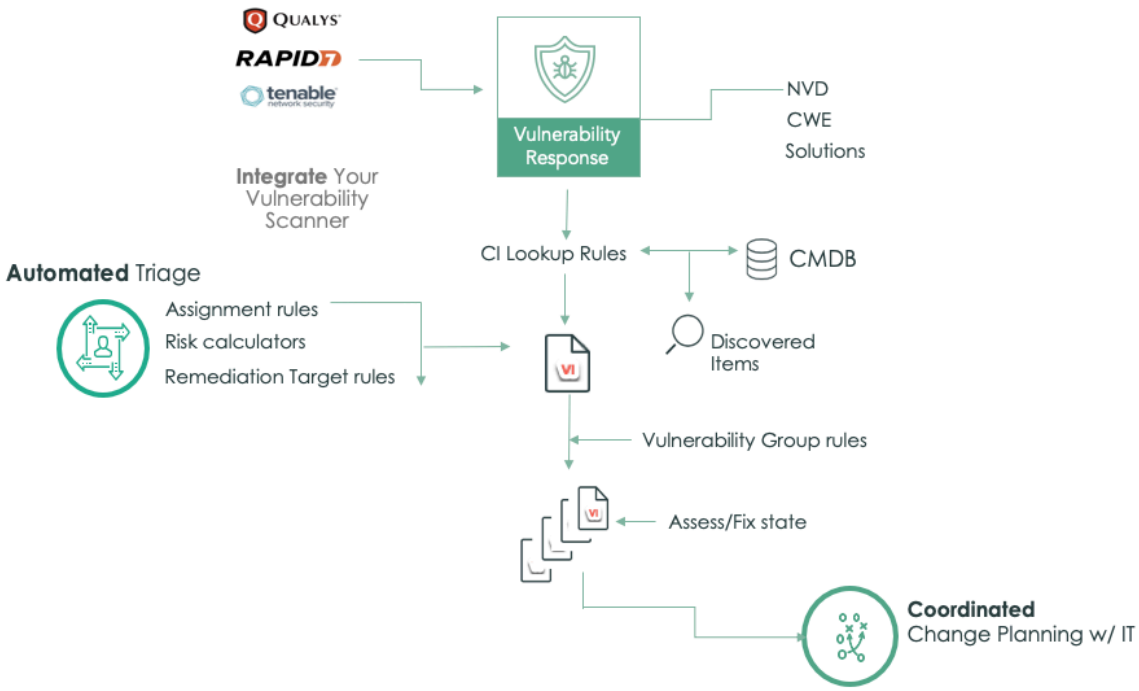
Réponse aux vulnérabilités Le rattrapage est un processus en plusieurs étapes qui consiste à vérifier l'achèvement de l'importation, à trier les nouvelles vulnérabilités et à surveiller

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

la progression jusqu'à son achèvement. Abordé de cette manière, le rattrapage devient gérable, opportun et, à bien des égards, automatisé.

Comprendre votre posture de sécurité sur l'ensemble des actifs de l'entreprise vous aide à identifier les vulnérabilités les plus critiques à corriger. Ce processus de rattrapage nécessite l'installation et la configuration d'une intégration tierce telle que Réponse aux vulnérabilités celle-ci Qualys Vulnerability Integration .

Flux de processus d'intégration de Vulnerability Response



Vérifier que les importations d'intégration tierce se déroulent correctement

La première phase de ce processus consiste à s'assurer que tout fonctionne correctement. Réponse aux vulnérabilités est prédéfini pour télécharger les vulnérabilités de la base de données de vulnérabilité nationale (NVD) et de la faiblesse d'énumération commune (CWE). Les importations tierces vous fournissent les données dont vous avez besoin pour créer des éléments vulnérables et des tâches de rattrapage. La réussite d'un rattrapage dépend de l'importation cohérente et réussie des vulnérabilités et des éléments vulnérables.

Pendant l'importation, les règles de recherche de CI associent les actifs tiers aux actifs dans le Base de données de gestion des configurations (CMDB). Tous les actifs sont stockés dans le module Éléments détectés. Les informations sur les CI sont essentielles à la mise en œuvre de la solution.

Remarque : Une fois qu'une intégration tierce a été installée et configurée, il existe quelques cas où une importation peut échouer, par exemple, si le fournisseur tiers limite ses appels d'API. Lorsque les importations échouent, elles doivent faire l'objet d'une attention rapide.

Des rapports d'exécution d'état d'intégration pour les intégrations tierces prises en charge sont fournis avec les applications pour vous donner une vue d'ensemble graphique de vos importations. Utilisez ce rapport, ou créez le vôtre, pour déterminer facilement si votre dernière importation a réussi. Pour en savoir plus sur les intégrations prises en charge, reportez-vous à la section Intégrations de Réponse aux vulnérabilités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Examiner et trier les vulnérabilités et les éléments vulnérables

La phase suivante du rattrapage consiste à examiner les nouvelles vulnérabilités et les nouveaux éléments vulnérables. Un élément vulnérable (VI) est une combinaison détectée de vulnérabilité et d'élément de configuration (CI). Au fur et à mesure que des éléments vulnérables sont formés, diverses règles sont exécutées pour affecter des éléments vulnérables, déterminer le risque qu'ils posent et définir des cibles de rattrapage. Ajustez toutes les règles, si nécessaire, pour vous assurer que les éléments vulnérables ont été triés avec succès.

Surveiller l'avancement des rattrapages de vulnérabilité existants

La dernière phase du rattrapage consiste à suivre vos progrès.

- Examinez l'état des importations pour les implémentations de correctifs qui ne se sont pas affichées et effectuez un suivi avec les opérations informatiques.
- Suivez l'évolution des obligations de conformité réglementaire et assurez-vous de leur respect.
- Examinez l'état des éléments différés et révisez ou implémentez des correctifs.
- Surveillez les tableaux de bord Gestion des vulnérabilités. Pour examiner les tendances, afficher des rapports en temps réel et utiliser des mesures qui suivent les taux d'atteinte de vos objectifs de rattrapage, vous préférez peut-être surveiller vos processus avec l'application Analyse des performances pour Vulnerability Response .
- Fermeture des détections obsolètes dans Réponse aux vulnérabilités.

Vérifier la bonne exécution des importations d'intégration Réponse aux vulnérabilités

Le moyen le plus simple de déterminer si vos importations ont réussi est d'utiliser un tableau de bord État d'exécution de l'intégration. Le tableau de bord État de l'exécution de l'intégration fournit un exemple de vue graphique de l'état des exécutions d'intégration tierce.

Les Qualys intégrations de vulnérabilité et Rapid7 disposent d'un tableau de bord d'état d'exécution de l'intégration. Consultez Qualys Graphique d'état de l'exécution de l'intégration ou Intégration des vulnérabilités Rapid7 Exécuter le graphique d'état pour obtenir des informations détaillées sur le contenu des graphiques.

Remarque : Les graphiques, pour les intégrations non fournies par ServiceNow®, peuvent être créés à partir de rapports dans un tableau de bord, mais peuvent nécessiter ServiceNow une expertise. Pour plus d'informations sur la création de rapports et de tableaux de bord, voir Prise en main des rapports et des tableaux de bord .

Afficher les Réponse aux vulnérabilités données de détection des éléments vulnérables

Les données complètes collectées par vos intégrations de scanners Réponse aux vulnérabilités tiers avec sont affichées dans les onglets Détections et Détections initiales des enregistrements d'éléments vulnérables (VIT). Il est également affiché dans les enregistrements de détection de la liste de détection des éléments vulnérables de votre Now Platform® instance.

Avant de commencer

Les intégrations tierces récupèrent les données de détection des éléments vulnérables. Les détections sont des occurrences distinctes de vulnérabilités telles que signalées par les scanners. Les données de détection sont couplées à des éléments vulnérables et l'état de VI est mis à jour en fonction de l'état des détections. Si aucun VI n'est trouvé, un nouveau VI est créé. Les détections ne sont ouvertes ou fermées que par des données trouvées directement par un scanner.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis :

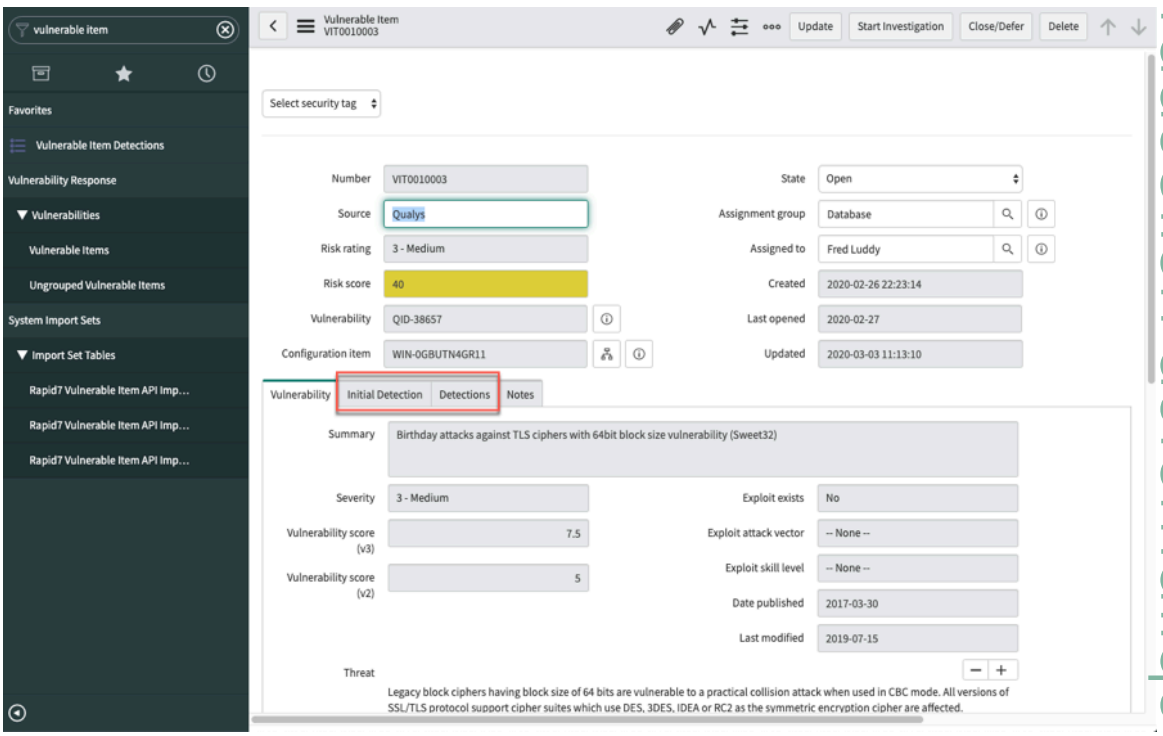
- sn_vuln.admin lance les exécutions d'intégration et affiche les données de détection des éléments vulnérables.
- sn_vul.remediation_owner se voit affecter des éléments vulnérables créés à partir des détections d'éléments vulnérables et affiche les données sur les enregistrements de VI.

Procédure

1. Pour afficher les données de détection des éléments vulnérables, accédez à un enregistrement d'élément vulnérable et ouvrez-le.

   L'enregistrement s'affiche avec les onglets Détections initiales et Détections.

   Remarque : Les données précédemment affichées dans l'onglet Détails de la configuration s'affichent avec d'autres données de détection dans les onglets Détection initiale et Détections.

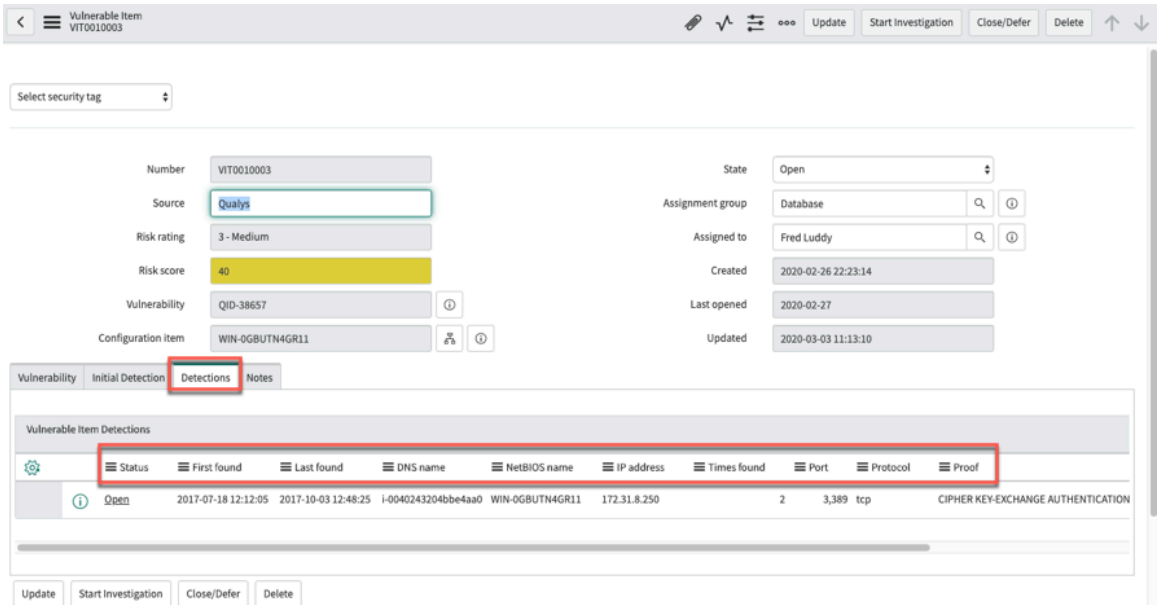


2. Cliquez sur l'onglet **Détections** .

   Lorsqu'un élément vulnérable est créé à partir des résultats d'une analyse tierce, les données de l'analyse sont affichées sur l'enregistrement de détection, comme illustré dans la figure suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Chaque ligne de la section Détection des éléments vulnérables représente les données d'une détection distincte. Dans la colonne Premier trouvé, la date à laquelle l'élément vulnérable est détecté pour la première fois par le scanner s'affiche. Dans la colonne Dernier trouvé, la date de la détection la plus récente s'affiche. Le champ Source affiche le scanner qui a récupéré les données.

Remarque : Pour Qualys, avec les détections d'éléments vulnérables, les champs suivants sont déconseillés sur l'enregistrement de VI et ne sont plus renseignés :

- Qualys sévérité
- Dernière mise à jour par source

De même, pour Qualys, comme le montre la figure précédente, lorsqu'un VI est créé à partir d'une analyse, la valeur de l'analyse des résultats s'affiche dans la colonne Preuve de l'enregistrement de détection. Toutefois, cette valeur n'est pas affichée dans la partie supérieure de l'enregistrement VI.

Pour Rapid7, lorsqu'un VI est créé à partir d'une analyse, la valeur Preuve de l'analyse peut être affichée à la fois dans la colonne Preuve de l'enregistrement de détection et dans la partie supérieure de l'enregistrement de VI, mais pas par défaut. Pour afficher cette valeur dans la partie supérieure de l'enregistrement VI, sélectionnez le champ Preuve dans la mise en page du formulaire.

3. Facultatif : Pour configurer la mise en page de l'onglet Détections sur l'enregistrement, procédez comme suit.

   a. Les colonnes suivantes s'affichent par défaut dans l'onglet Détections.

   - Statut
   - Premier trouvé (données)
   - Dernier trouvé (date)
   - Nom DNS
   - Nom du BIOS net
   - Adresse IP

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Durées trouvées
- Port
- Protocole
- Preuve
- SSL

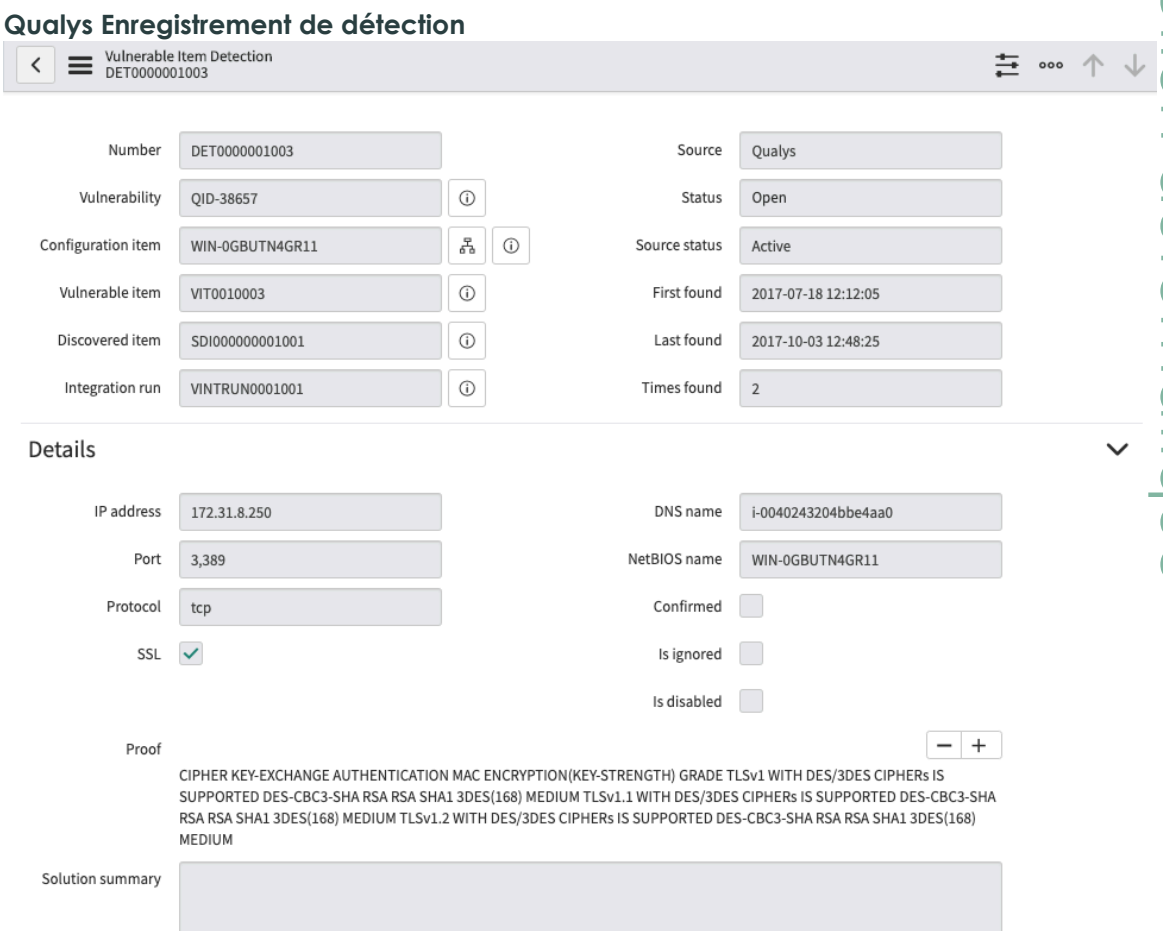
Remarque :

Remarque : s'il n'y a pas de valeur dans une colonne, les données de ce champ n'ont pas été détectées par le scanner.

b. Cliquez sur l'icône Engrenage (icône) pour personnaliser votre vue.

c. Sélectionnez les colonnes de la zone de sélection pour afficher des données spécifiques, puis cliquez sur **OK**.

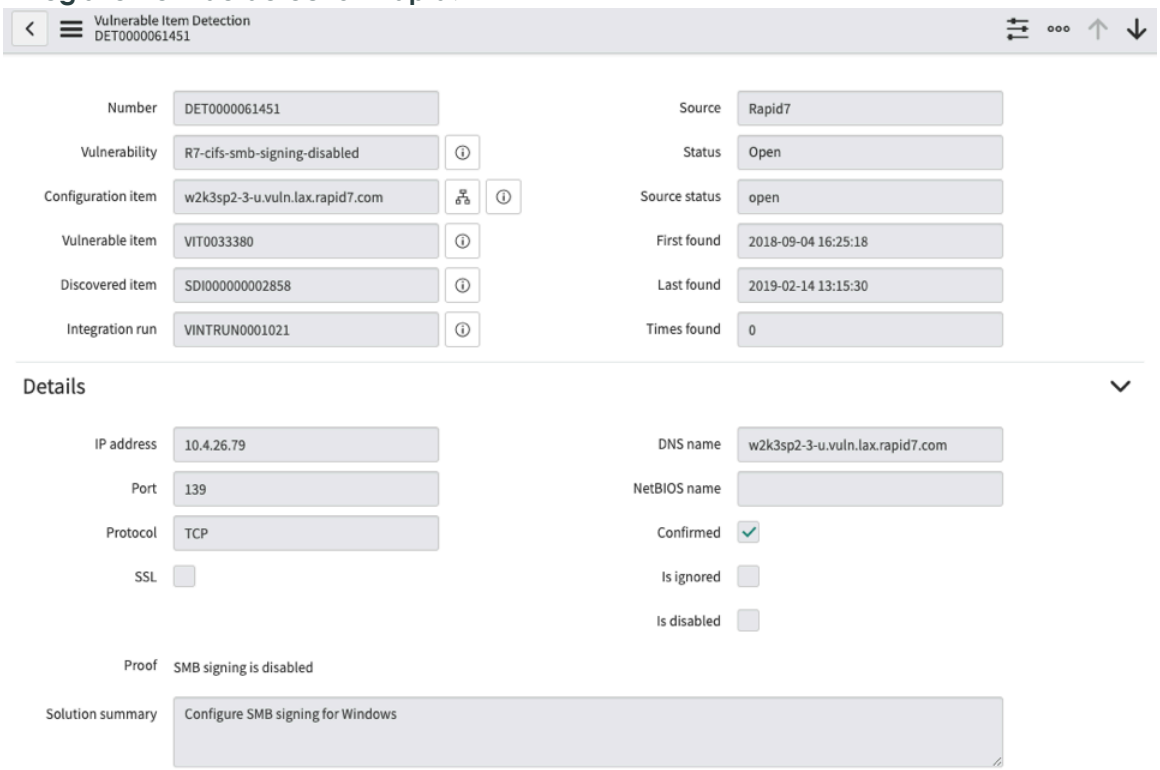
4. Avec l'onglet Détections sélectionné, dans la colonne État, cliquez sur un élément pour ouvrir l'enregistrement de détection et afficher les détails associés à cet élément vulnérable, y compris un résumé de la solution (intégration Rapid7 InsightVM uniquement).



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

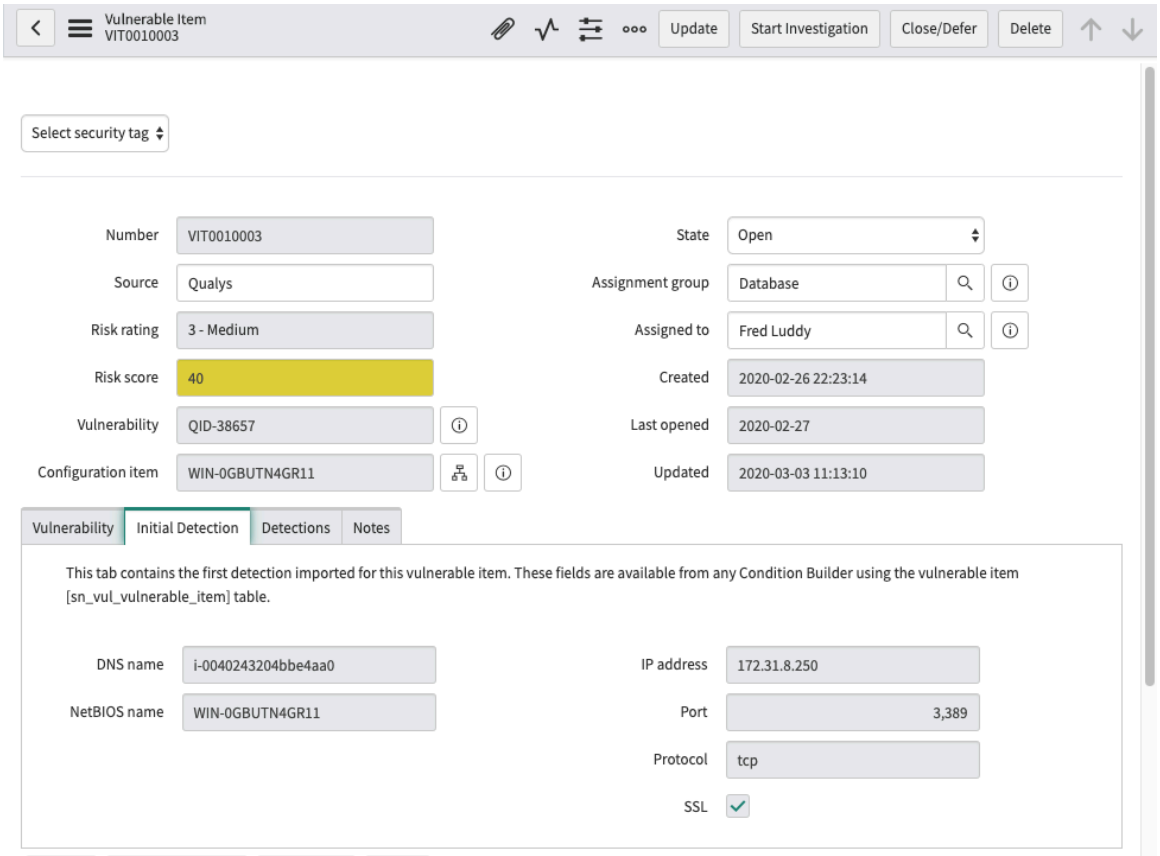
Enregistrement de détection Rapid7



5. Revenez à l'enregistrement et sélectionnez l'onglet Détection initiale.

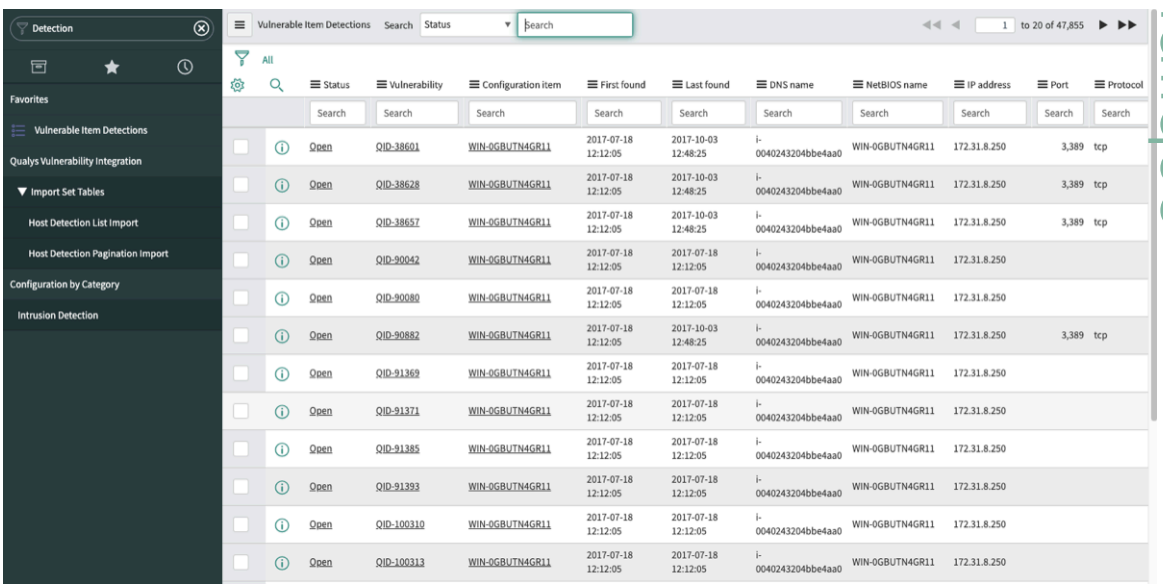
L'onglet Détections initiales affiche les données importées du scanner tiers lors de la première occurrence de la détection. Ces informations de l'onglet de détection initiale ne changent pas au fur et à mesure que les données de détection sont mises à jour.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Facultatif : Naviguez vers Détections d'éléments vulnérables pour afficher la liste de détection des éléments vulnérables.

   (Optional) La liste de détection des éléments vulnérables s'affiche. Chaque ligne de la liste Détection des éléments vulnérables représente une détection distincte. Les colonnes affichent les mêmes données que l'enregistrement VI.



   Les détections ne sont ouvertes ou fermées que par les données trouvées par un scanner, elles ne sont pas déroulantes à partir des VI. Au fur et à mesure que les détections sont importées, elles sont utilisées pour créer des VI et mettre à jour les états des VI. Si toutes les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

détections sont fermées pour un élément vulnérable, cet élément vulnérable sera fermé. Sur l'enregistrement VI, l'état est `Fermé` et le Sous-état est `Fixe`.

Remarque : Les erreurs sont consignées lorsque :

- Traitement des pièces jointes récupérées à partir de l'analyseur.
- Création ou mise à jour de détections ou d'éléments vulnérables.

Pour plus d'informations sur la gestion des erreurs de détection, reportez-vous à la section Gestion des erreurs pour les détections.

Lorsque tous les VI sont fermés pour une tâche de rattrapage, la tâche de rattrapage est fermée.

Les VI fermés avec un sous-état **Fixe** ou **Périmé** sont rouverts si une nouvelle détection est créée et les VI peuvent être mis en correspondance avec la nouvelle vulnérabilité.

Les éléments vulnérables définis sur **Résolu** dans votre instance, mais pas sur **Fermé/Résolu** par les exécutions d'intégration suivantes, sont rouverts s'ils sont détectés lors des nouvelles analyses.

Lorsque tous les VI sont fermés pour une tâche de rattrapage, l'enregistrement est fermé.

Les éléments vulnérables définis sur « Résolu » dans votre instance, mais qui ne sont pas passés à l'état « Fermé/Résolu » par les exécutions d'intégration suivantes, sont rouverts s'ils sont détectés lors des nouvelles analyses.

Pour Rapid7 les détections, une option est désormais disponible sur la page de configuration Rapid7 de votre instance pour rouvrir les VI résolus par âge. Si cette option est activée, les VI définis sur **Résolu** , mais qui ne sont pas ensuite transférés à **l'état Fermé/ Corrigé** par les analyses suivantes, reviennent à **l'état Ouvert** après le nombre de jours que vous entrez.

Pour Qualys les détections, si le scanner continue de trouver des VI qui ont été définis sur « Résolu » mais qui ne sont pas passés à **l'état Fermé/Fixe** par les analyses suivantes, ces VI reviennent à **l'état Ouvert** lorsque la dernière date de recherche est postérieure à la date de résolution.

Que faire ensuite

Pour afficher plus de données, notamment le nombre d'éléments et de détections, vous pouvez Vérifier Réponse aux vulnérabilités les données de détection d'éléments vulnérables sur les enregistrements d'exécution de l'intégration (VINTRUN).

Vérifier Réponse aux vulnérabilités les données de détection d'éléments vulnérables sur les enregistrements d'exécution de l'intégration (VINTRUN)

À partir des enregistrements d'exécution de l'intégration dans votre Now Platform® instance, vous pouvez localiser les données de détection d'éléments vulnérables d'intégration tierce en fonction de la date et de l'heure des analyses. Vérifiez que l'analyse a été effectuée avec succès, affichez le nombre (nombres) de détections individuelles, ainsi que tous les éléments vulnérables (VI) créés ou mis à jour directement à la suite des analyses.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vuln.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il est préférable d'avoir les informations d'exécution de l'intégration, soit la date et l'heure de l'analyse, soit le numéro d'enregistrement d'exécution de l'intégration (VINTRUN#) à partir de l'élément vulnérable ou des enregistrements de détection pour vous aider à localiser des enregistrements spécifiques dans les listes suivantes.

Procédure

1. Choisissez-en un pour continuer.

Intégration	Description
Accédez à la **Rapid7 Vulnerability Integration** > **Administration** > **Intégrations**	Dans la liste Intégrations Rapid7, choisissez l'intégration pour laquelle vous souhaitez afficher les résultats de l'analyse de détection. **a.** Entrepôt de données Rapid7 : ▪ Intégration des éléments vulnérables Rapid7 ▪ Intégration de la résolution des éléments vulnérables Rapid7 ▪ Intégration complète des éléments vulnérables Rapid7 **b.** Intégration de résolution des éléments vulnérables Rapid7 (InsightVM) ▪ Intégration d'éléments vulnérables Rapid7 : API ▪ Intégration complète des éléments vulnérables Rapid7 : API
Accédez à la **Qualys** > **Intégration de vulnérabilité Qualys** > **Intégrations principales**	Dans la liste Intégrations Qualys, choisissez parmi : ◦ Intégration de la détection d'hôte Qualys ◦ Intégration complète de la détection d'hôte Qualys
Accédez à la **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**	Dans la liste Intégrations Tenable, choisissez l'intégration pour laquelle vous souhaitez afficher les résultats de l'analyse de détection.
Accédez à la **Intégration de vulnérabilité Microsoft TVM** > **Administration** > **Intégrations**	Dans la liste Intégrations Microsoft TVM, choisissez l'intégration pour laquelle vous souhaitez afficher les résultats de l'analyse de détection.

2. En bas de la page qui s'affiche, cliquez sur l'onglet**Exécutions de l'intégration de vulnérabilité**.

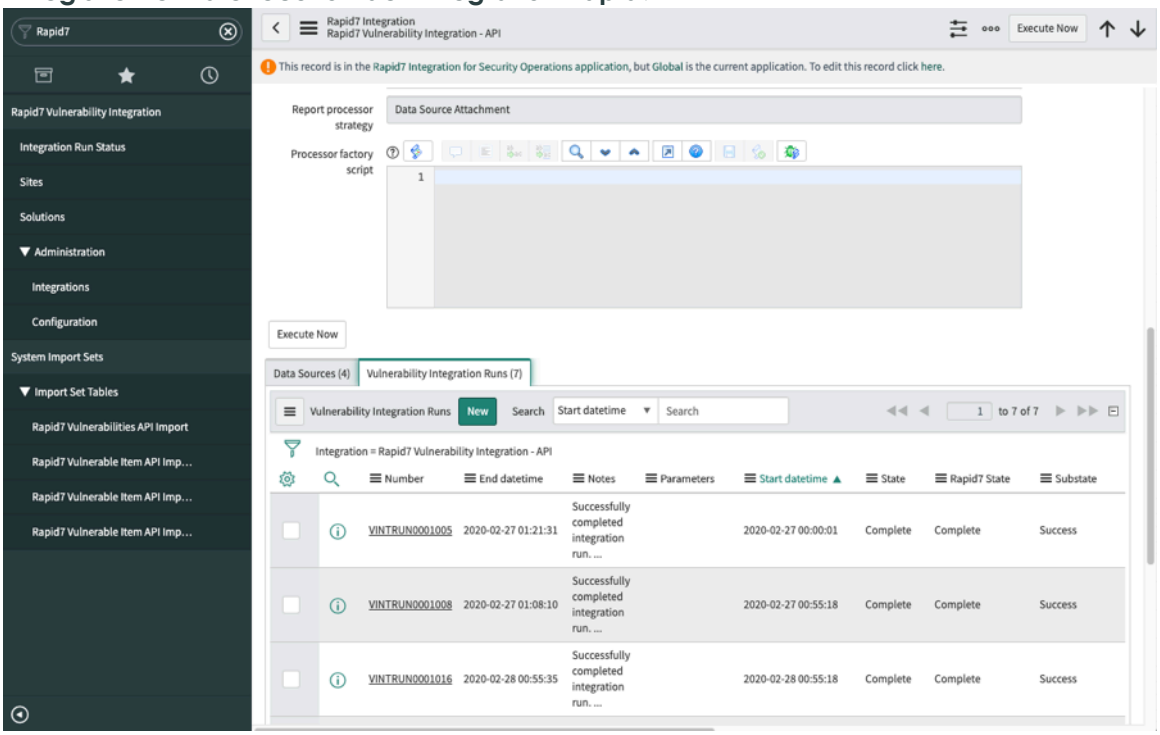
3. Cliquez sur un élément dans la colonne Nombre ou Source d'importation pour ouvrir un enregistrement.

L'enregistrement d'exécution de l'intégration s'affiche.

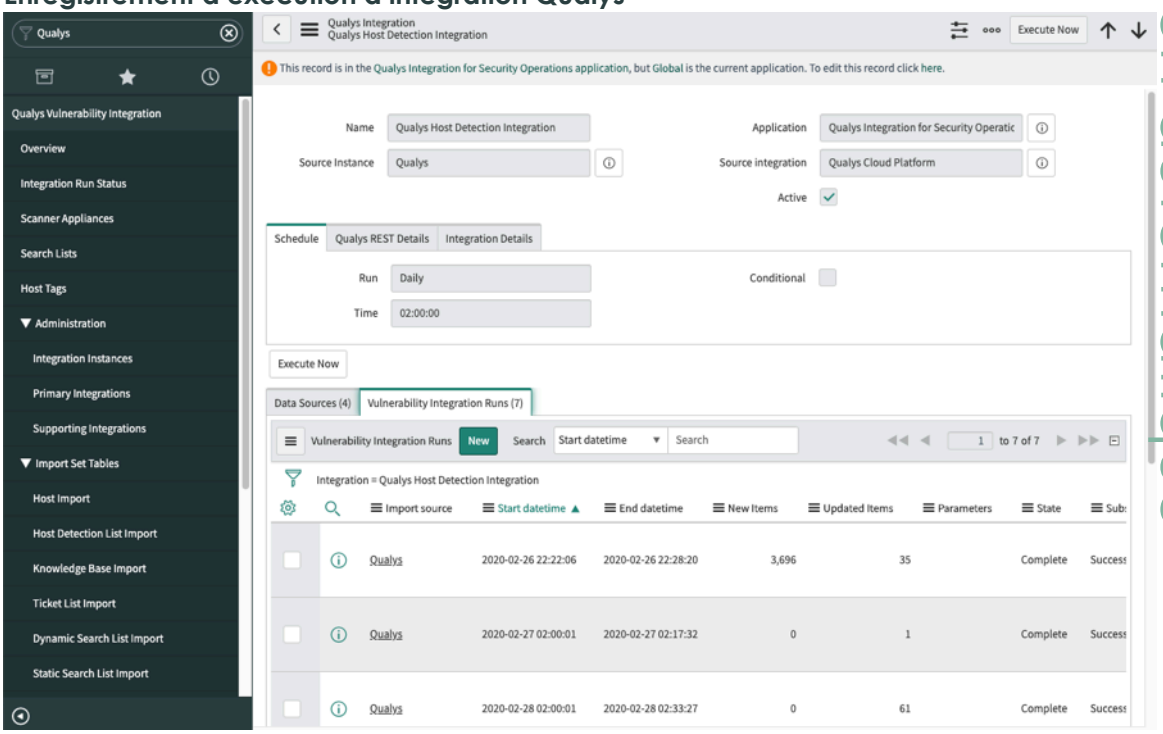
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrement d'exécution de l'intégration Rapid7



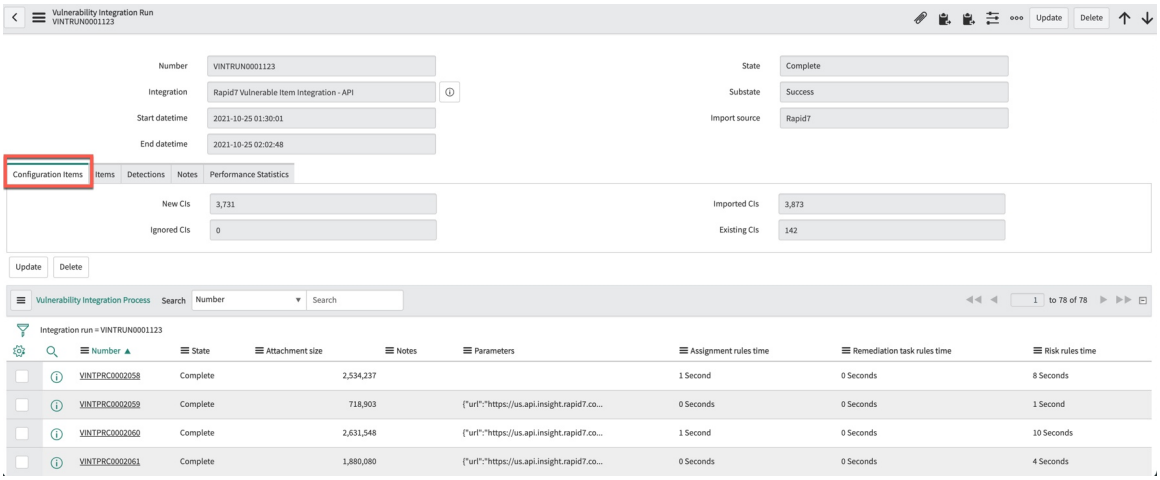
Enregistrement d'exécution d'intégration Qualys



L'enregistrement d'exécution de l'intégration s'affiche. Vous pouvez vérifier dans le champ État que l'intégration s'est correctement exécutée. Sélectionnez l'onglet **Éléments de configuration** .

Traduction automatique

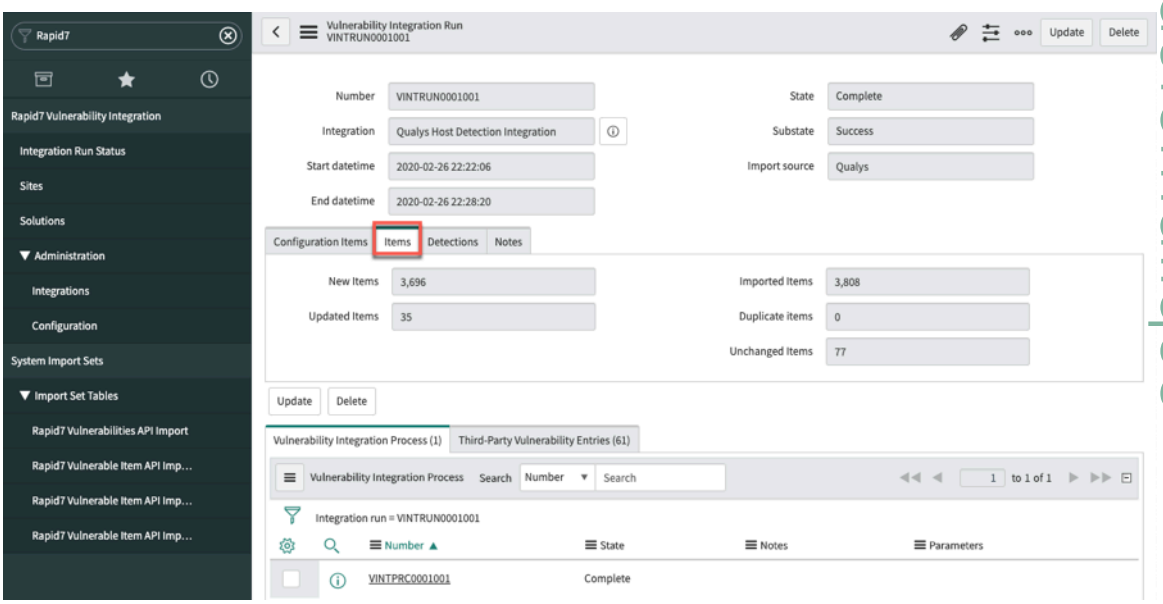
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'onglet Éléments de configuration affiche les informations suivantes :

- L'onglet Éléments de configuration affiche le nombre total d'éléments de configuration importés.
- Le champ Nouveaux CI affiche le nombre de CI créés dans le cadre de cette exécution d'intégration.
- Le champ CI importés affiche la somme de tous les CI de cette section.
- La valeur du champ CI ignorés est toujours de 0 pour les Réponse aux vulnérabilités intégrations.
- Le champ CI existants affiche le nombre total de CI déjà existants.

Cliquez sur l'onglet **Éléments** .



L'onglet Éléments affiche les informations suivantes :

- L'onglet Éléments affiche le nombre total de VI importés. Vous pouvez afficher le nombre total de détections importées en ajoutant les nombres répertoriés dans l'onglet Détections.
- Le champ Nouveaux éléments affiche le nombre d'éléments vulnérables créés à partir de cette exécution d'intégration.
- Le champ Éléments importés affiche la somme de tous les champs de cette section.

Traduction automatique

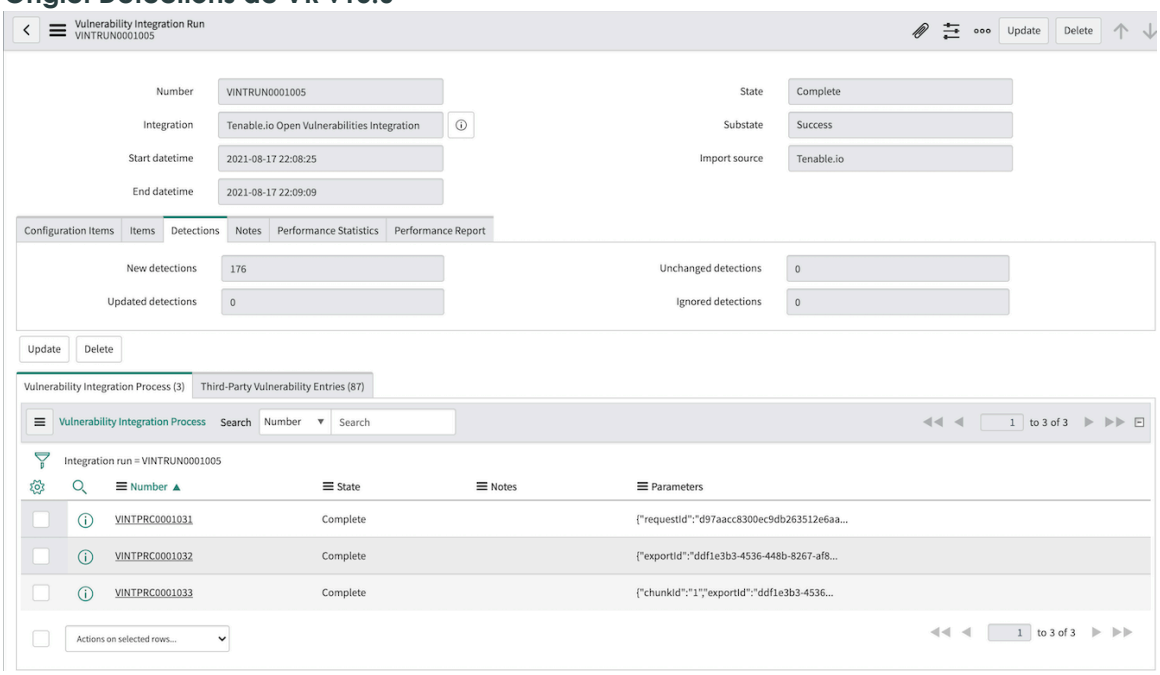
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le champ Éléments en double n'est plus renseigné.
- Le champ Éléments mis à jour affiche le nombre de fois où des éléments vulnérables sont mis à jour au cours de cette exécution d'intégration. Cette valeur n'est pas le nombre d'éléments vulnérables uniques qui sont mis à jour. Si, par exemple, un élément vulnérable est mis à jour deux fois au cours de l'exécution de l'intégration, il est compté deux fois et affiché sous la forme `de 2` éléments mis à jour.
- Le champ Éléments inchangés affiche les éléments vulnérables trouvés pendant l'exécution de l'intégration qui existent déjà dans la base de données, mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

4. Cliquez sur l'onglet **Détections** .

Cet onglet s'affiche uniquement si l'exécution de l'intégration comporte des détections. Vous pouvez vérifier le nombre total de détections importées en ajoutant les nombres répertoriés.

Onglet Détections de VR v15.0



Remarque : Avant la version 15.0, il n'existait aucun champ pour les détections ignorées.

L'onglet Détections affiche les informations suivantes :

- À partir de la version 15, un nouveau champ Détections ignorées a été ajouté pour suivre les détections, qui étaient auparavant ignorées. Avec cette implémentation, le nombre de détections importées et le nombre suivi sur les enregistrements d'exécution de l'intégration deviennent cohérents. Cette fonctionnalité a été implémentée pour tous les scanners, Qualys Vulnerability IntegrationIntégration des vulnérabilités Rapid7c'est-à-dire , , Tenable Vulnerability Integration et Microsoft TVM.
- Le champ Nouvelles détections affiche les nouvelles détections créées au cours de cette exécution d'intégration.
- Le champ Détections non modifiées affiche les détections trouvées pendant l'exécution de l'intégration qui existent déjà dans la base de données, mais qui n'ont pas été mises à jour, car aucune des valeurs de champ pertinentes n'a changé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le champ Détections mises à jour affiche le nombre de fois où les détections sont mises à jour au cours de cette exécution d'intégration. Cette valeur n'est pas le nombre de détections uniques mises à jour. Si, par exemple, une détection est mise à jour deux fois dans le cadre de l'exécution de l'intégration, elle est comptée deux fois et affichée comme 2 détections mises à jour.

  Remarque : Les détections qui ne sont pas affichées dans ces nombres sont des détections à l'état Fermé (Fixe), car les enregistrements fixes sont utilisés pour mettre à jour les VI existants. Si vous souhaitez améliorer la visibilité de ces enregistrements de détection, vous pouvez afficher les VI fermés créés lorsqu'il n'existe aucun VI correspondant à l'état ouvert. Pour plus d'informations sur les vulnérabilités à l'état fixe que vous pouvez activer dans l'Assistant de configuration pour l'intégration Qualys, reportez-vous à la section Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration.

5. Cliquez sur un élément dans la colonne Nombre ou Source d'importation pour ouvrir un enregistrement.

Affichage des données de correctifs et planification des correctifs dans Réponse aux vulnérabilités

À partir de la version 16.1 de Réponse aux vulnérabilités, vous pouvez planifier des correctifs et afficher les données de correctifs ainsi que les informations sur la solution et d'autres vulnérabilités dans les enregistrements dans l'environnement classique et les Réponse aux vulnérabilités espaces de travail de votre Now Platform instance.

Rôles requis

Les utilisateurs ont besoin de rôles spécifiques à l'intégration d'orchestration de correctifs que vous utilisez pour importer vos correctifs afin d'afficher les données et de planifier les correctifs. Consultez les intégrations prises en charge pour plus d'informations.

- Présentation de l'intégration de l'orchestration des correctifs HCL BigFix avec Réponse aux vulnérabilités et Présentation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités.
- Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord dans l'environnement classique.
- Affichez les données des tableaux de résultats dans le Réponse aux vulnérabilités Espaces de travail.

Planification des correctifs

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- Mise à jour de correctif (VPU)
- Tâche de rattrapage (RT)
- Élément détecté (SDI)

Appliquer des correctifs aux données dans l'environnement classique

Depuis l'environnement classique de l'application Réponse aux vulnérabilités :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour afficher les enregistrements de mise à jour de correctifs, naviguez vers **Tout** > **Réponse aux vulnérabilités** > **Correctifs**.
- Pour afficher les solutions, accédez à **Tout** > **Réponse aux vulnérabilités** > **Solutions**.
- Pour afficher les VI qui vous sont affectés et qui ont des correctifs, accédez à **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Affecté à moi avec correctifs**.
- Pour afficher les tâches de rattrapage, accédez à **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Affecté à moi avec correctifs**
- Pour afficher les enregistrements d'éléments détectés, accédez à **Tout** > **Security Operations** > **Éléments détectés**.

Déploiement des données et de l'état des correctifs pour l'orchestration des correctifs dans Réponse aux vulnérabilités

À partir de la version 16.1, les données et les états des correctifs sont déployés vers la mise à jour des Réponse aux vulnérabilités correctifs et d'autres enregistrements dans l'application Réponse aux vulnérabilités .

Enregistrements de mise à jour de correctif dans les espaces de travail de l'environnement classique dans Réponse aux vulnérabilités

Les informations sur les correctifs, les solutions de vulnérabilité et les vulnérabilités sont toutes connectées dans l'application Réponse aux vulnérabilités .

Les données de correctif et les données et l'état de déploiement de correctif sont affichés sur les enregistrements de votre instance. Les enregistrements de correctifs sont inclus dans la fonctionnalité d'orchestration de correctifs de cette intégration avec Réponse aux vulnérabilités. Affichez les enregistrements de correctifs (VPU) dans les espaces de travail Vulnerability Response à partir de la vue Liste de l'espace de travail de remédiation informatique. Les enregistrements de mise à jour de correctif dans la vue classique et dans les espaces de travail Vulnerability Response incluent les données suivantes :

- Données et informations sur les solutions de vulnérabilité provenant des fournisseurs de correctifs importées par l'application Gestion des solutions de vulnérabilité.
- État du rattrapage à la source qui inclut le nombre total d'appareils présentant une vulnérabilité qui peut être corrigée par un correctif, ainsi que tous les appareils pour lesquels des mises à jour sont manquantes.
- État du rattrapage qui inclut le % de VI rattrapés et le total des VI pour lesquels un correctif est préféré.
- Appareils associés, éléments vulnérables, déploiements de correctifs et demandes de correctifs sur les liens connexes des enregistrements dans la vue de classe. Ces données sont affichées sous forme d'onglets sur les enregistrements dans les espaces de travail Vulnerability Response.
- Demandes de correctifs que les propriétaires de rattrapage ont soumises pour approbation.

Rôles requis

Les utilisateurs ont besoin de rôles spécifiques à l'intégration d'orchestration de correctifs que vous utilisez pour afficher les données et planifier les correctifs. Consultez les intégrations prises en charge pour plus d'informations.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

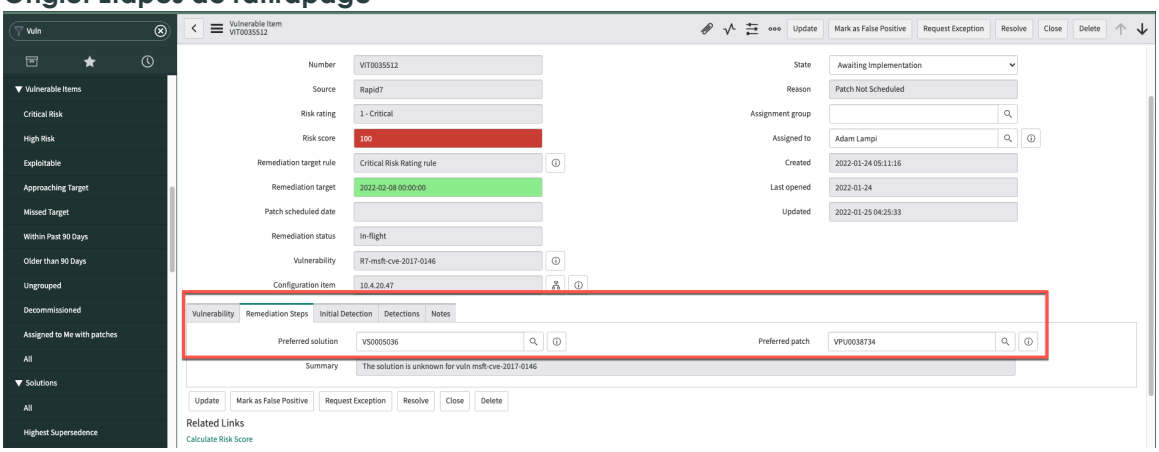
- Présentation de l'intégration de l'orchestration des correctifs HCL BigFix avec Réponse aux vulnérabilités et Présentation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités.
- Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord dans l'environnement classique.
- Affichez les données des tableaux de résultats dans le Réponse aux vulnérabilités Espaces de travail.

Déploiement des données et de l'état des correctifs

Pour afficher les éléments vulnérables qui ont des correctifs et qui vous sont affectés dans l'environnement classique, accédez à **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Mes affectations avec correctifs**.

Si un enregistrement d'élément vulnérable est renseigné avec un correctif préféré, il passe automatiquement à **l'état En attente d'implémentation** uniquement si l'état du VI n'est pas **Fermé**, **Résolu**, **Différé** ou **En cours de révision**. Pour explorer les données afin d'afficher la solution préférée et d'autres données, cliquez sur l'onglet **Rattrapage** de l'enregistrement de VI.

Onglet Étapes de rattrapage



Un VI avec un correctif préféré passe à **l'état En attente d'implémentation** dans les cas suivants :

- Si le déploiement d'un correctif est planifié sur un CI qui fait partie d'une importation de collection et que le CI est associé à un VI, la raison pour laquelle le VI est **En attente d'implémentation** est **Correctif planifié**.
- Si le déploiement d'un correctif est planifié sur un CI qui fait partie d'une importation de collection, si le CI est associé à un VI et si la date cible de rattrapage (échéance) est ultérieure à la date de délai de rattrapage (TTR), l'état du VI est En **attente d'implémentation** avec pour motif **correctif planifié (date cible manquante).**
- Si le déploiement d'un correctif n'est pas planifié sur un CI qui fait partie d'une importation de collection, l'état du VI est En **attente d'implémentation**, avec pour raison **Correctif non planifié**.

Cliquez sur l'icône **d'informations sur le correctif préféré** pour ouvrir les mises à jour de correctifs et afficher les informations suivantes sur les liens connexes :

Éléments vulnérables

Éléments vulnérables associés à ce correctif.

Appareils associés

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appareils avec mises à jour et ceux qui n'ont pas de mises à jour.

Déploiements de correctifs

Déploiements planifiés pour ce correctif sur des ordinateurs individuels (actifs) ou sur des groupes de ressources.

Demandes de correctifs

Une liste des demandes de correctif qui ont été envoyées pour approbation avant leur déploiement planifié.

Correctifs potentiels

Correctifs susceptibles de corriger une vulnérabilité.

Cliquez sur l'icône **d'informations sur le correctif préféré** pour ouvrir l'enregistrement et afficher les informations répertoriées précédemment, en plus des données de mise à jour de correctif suivantes :

État du rattrapage de la source

Nombre total d'appareils qui nécessitent ce correctif et tous les appareils qui n'ont pas besoin du correctif.

État du rattrapage

État (VI totaux, % rattrapés, VI différés) des VI qui possèdent ce correctif préféré.

Correctifs et solutions préférés

Lorsqu'une vulnérabilité importée correspond à un actif de votre Base de données de gestion des configurations (CMDB), un élément vulnérable (VI) est créé dans Réponse aux vulnérabilités. Si l'élément de configuration (CI) associé à ce VI est également importé d'un fournisseur de correctif tiers et qu'il manque un correctif pour la même vulnérabilité, un correctif préféré est répertorié et déployé sur vos solutions. Ces informations vous permettent de savoir qu'un actif (CI) dispose d'un correctif provenant d'un correctif disponible qui correspond le mieux à sa vulnérabilité.

Affichage des correctifs sans solutions

Après une importation, si aucune donnée de solution de vulnérabilité n'est disponible, le champ **Solution de vulnérabilité** de l'enregistrement de mise à jour de correctif est laissé vide. Pour en savoir plus sur l'affichage des informations relatives à ces types de correctifs, reportez-vous à la section Afficher les correctifs sans solution dans Réponse aux vulnérabilités.

Afficher les correctifs sans solution dans Réponse aux vulnérabilités

À partir de la version 16.0 de , pour les correctifs qui n'ont pas de solution après une importation, le système recherche ensuite les ID de correctifs dans les données de Réponse aux vulnérabilitésréférence de vulnérabilité afin que vous puissiez afficher ces correctifs sur les enregistrements de vulnérabilité.

Correctifs sans solutions

Rôle requis : sn_vul.vulnerability_admin.

Les données importées des applications d'orchestration de correctifs et de solutions de vulnérabilité, ainsi que des intégrations de scanner de correctifs, sont traitées, connectées et affichées dans l'application sur les Réponse aux vulnérabilités enregistrements de mise à jour de correctifs.

Lorsqu'une solution existe pour une vulnérabilité, les informations connexes sont corrélées dans votre instance et sont déployées à partir des correctifs, vers les solutions de vulnérabilité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

et vers les vulnérabilités. Pour afficher ces informations, accédez à **Tout** > **Réponse aux vulnérabilités** > **Correctifs** > **Tout**.

Après une importation, si aucune donnée de solution de vulnérabilité n'est disponible, le champ **Solution de vulnérabilité** de l'enregistrement de mise à jour de correctif est laissé vide. Pour que vous puissiez voir les informations de solution connexes pour ces correctifs, une propriété système, [**sn_vul_patch_orch.no_solution_patch_rollup**], est activée par défaut dans votre instance. Cette propriété recherche les ID de bulletins et les ID d'articles dans les données de référence de vulnérabilité à partir des importations de scanner. Si une correspondance est trouvée, les données associées sont renseignées dans la table des correctifs potentiels, et ces informations sont affichées dans les listes connexes des enregistrements de vulnérabilité.

Si vous avez un grand nombre de vulnérabilités ou si la tâche planifiée de déploiement prend beaucoup de temps, vous préférerez peut-être désactiver cette propriété système pour éviter d'éventuels problèmes de performances. Toutefois, notez que si vous désactivez cette propriété système, les données de solution importées ne sont ni recherchées, ni déployées vers vos vulnérabilités sans solution.

En tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin, procédez comme suit pour désactiver la propriété système :

1. Accédez à la **sys.properties.list**.
2. Localisez **sn_vul_patch_orch.no_solution_patch_rollup** et cliquez dessus pour ouvrir l'enregistrement.
3. Dans le champ Valeur, tapez `false`.
4. Cliquez sur **Mettre à jour**.

Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord

À partir de la version 16.1, vous pouvez afficher les données de mise à jour des correctifs dans l'environnement classique sur les tableaux de bord inclus dans l'application Réponse aux vulnérabilités .

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à suivre la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en visualisant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Voir Espace de travail du gestionnaire de vulnérabilités et Exploration de l'Espace de travail de remédiation IT pour plus d'informations.

Vous pouvez également afficher ces données sur les tableaux de bord CISO et Gestion de la vulnérabilité (PA) si vous disposez d'un abonnement à Analyse des performances.

Vous pouvez également afficher les données de correctifs dans l'environnement classique. Pour plus d'informations sur les rôles requis et sur la façon d'afficher les données sur les Réponse aux vulnérabilités tableaux de bord dans l'environnement classique qui sont inclus dans l'application et ceux qui nécessitent un abonnement distinct, reportez-vous Réponse aux vulnérabilités à la section Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.

Afficher une solution

Affichez toutes les solutions, les solutions avec la priorité la plus élevée et les solutions associées aux éléments vulnérables pour éclairer vos activités de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul.read, sn_vul.vulnerability_admin ou sn_vul.remediation_owner
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

En tant qu'analyste de vulnérabilité ou propriétaire du rattrapage, vous pouvez afficher différents ensembles de solutions liés aux éléments vulnérables.

Remarque : Les enregistrements de solutions sont en lecture seule, sauf sous **Notes** dans la section **Notes internes** ou solutions créées par l'utilisateur.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Solutions**.
2. Choisissez une liste de solutions.

   Remarque : Vous pouvez filtrer une liste de solutions à l'aide de caractères génériques pour le nom du produit.

3. Pour passer en revue, cliquez sur chaque élément.
4. Facultatif : Saisissez des notes sous l'onglet **Notes** et cliquez avec le bouton droit sur **Enregistrer** pour rester sur la page ou cliquez sur **Mettre à jour** pour enregistrer et revenir à la liste **des solutions de vulnérabilité** .

   Remarque : Si vous ne disposez que du rôle sn_vul.read, vous ne serez pas en mesure d'effectuer cette étape.

Créer une solution de vulnérabilité

Créez une solution de vulnérabilité afin de pouvoir suivre les solutions de vulnérabilité qui ne sont pas couvertes par le contenu de solution tiers.

Avant de commencer

Rôle requis : admin, sn_vul.vulnerability_admin ou sn_vul.admin (obsolète), ou vulnerability.write
Gestion des solutions pour vulnérabilités est une fonctionnalité disponible dans l'application Réponse aux vulnérabilités . Gestion des solutions pour vulnérabilités Nécessite un abonnement distinct.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer une solution à partir de n'importe quelle liste de solutions. Vous devez installer l'application Gestion des solutions en matière de vulnérabilité avant de pouvoir créer une solution.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Solutions**.
2. Choisissez une liste de solutions : **Tous**, **Priorité la plus élevée** ou **Avec éléments vulnérables**.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs modifiables du formulaire comme il convient.
   Vous pouvez laisser tous les champs inutilisés vides. Pour plus d'informations sur les champs individuels, reportez-vous à la section Champs du formulaire Solution.
5. Cliquez avec le bouton droit sur **Enregistrer** dans l'en-tête.
   L'enregistrement de solution est ajouté et apparaît par défaut dans les listes **Tout** et **Remplacement le plus élevé** .
6. Les listes connexes s'affichent.

   Vous pouvez associer cette solution aux listes connexes suivantes : **Éléments vulnérables**, **Vulnérabilités tierces**, **CVE**, **Solutions de remplacement** et **Solutions précédentes**. Choisissez une vulnérabilité ou une solution, puis cliquez sur **Soumettre**.

Remarque :

Gestion des solutions pour vulnérabilités Associe automatiquement les éléments vulnérables et les tâches de rattrapage aux solutions lorsque les enregistrements de vulnérabilité sont associés manuellement aux solutions.

Les éléments vulnérables réaffectés manuellement à une autre solution ne sont pas automatiquement mis à jour avec les changements de solution au niveau de la vulnérabilité.

Si vous souhaitez exclure la relation entre une vulnérabilité tierce et une solution parce qu'elle n'est pas pertinente pour le CI que vous corrigez ou parce qu'elle n'est pas préoccupante dans votre environnement, reportez-vous à la section Exclure manuellement les solutions des enregistrements tiers ou inversement.

Exclure manuellement les solutions des enregistrements tiers ou inversement

Excluez la relation entre une vulnérabilité tierce et une solution, car elle n'est pas pertinente pour le CI que vous corrigez ou parce qu'elle ne constitue pas un problème dans votre environnement. Excluez manuellement les solutions à l'aide d'une vulnérabilité tierce ou d'un enregistrement de solution.

Avant de commencer

Rôle requis :

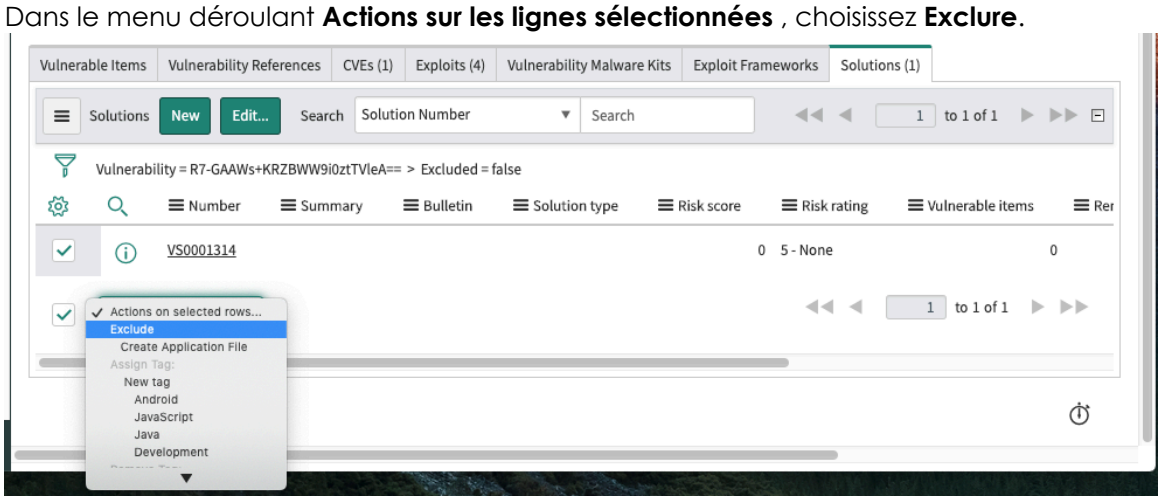
- sn_vul.write
- sn_vul.remediation_owner

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** ou **Réponse aux vulnérabilités** > **Toutes les solutions**
2. Ouvrez un enregistrement de vulnérabilité ou de solution tierce.
   a. Pour un enregistrement de tiers : sélectionnez l'onglet **Solutions** connexes.
   b. Pour un enregistrement de solution : Sélectionnez l'onglet **connexe des vulnérabilités tierces** .
3. Cochez la case en regard de chaque enregistrement de vulnérabilité ou de solution que vous souhaitez exclure.
4. Dans le menu déroulant **Actions sur les lignes sélectionnées** , choisissez **Exclure**.



L'enregistrement du tiers ou de la solution n'apparaît plus dans l'onglet connexe.

Les relations de vulnérabilité tierce avec les solutions sont également exclues lorsque les solutions sont mises à jour ou si la tâche nocturne est activée.

Les relations des vulnérabilités tierces avec les solutions sont exclues pendant la tâche planifiée nocturne.

L'exclusion des vulnérabilités tierces signifie que la solution n'est plus un facteur d'évaluation d'une solution privilégiée. Impacts de l'exclusion :

- Tous les éléments sont pris en compte pour les solutions, car la vulnérabilité tierce, les éléments vulnérables (VI) et les éléments de configuration (CI) attachés à la vulnérabilité tierce ne sont plus pris en compte dans la solution.
- Détermination de la solution préférée pour la vulnérabilité tierce et, par extension, de la solution préférée de tous les VI attachés et des tâches de remédiation contenant l'élément vulnérable.

Triage automatique des vulnérabilités

L'examen et le triage des nouvelles vulnérabilités sont nécessaires pour garantir une correction réussie. Transformez les importations de vulnérabilités en tâches de remédiation grâce à l'affectation automatisée des éléments vulnérables (VI), au calcul du risque, aux cibles de remédiation et au regroupement des VI.

En commençant par les vulnérabilités importées, rapprochez les actifs introuvables dans la CMDB, classez les résultats par ordre de priorité, traduisez-les en activités de rattrapage qui sont automatiquement affectées, orchestrez le processus de rattrapage et confirmez son achèvement par une analyse de validation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les nouveaux éléments vulnérables sont généralement triés en tâches de rattrapage lors de leur importation, en fonction des règles de tâches de rattrapage. Parfois, les éléments vulnérables ne peuvent pas être regroupés ou ne contiennent pas d'élément de configuration reconnu.

Voici une vue d'ensemble du processus de triage des vulnérabilités :

- Connectez-vous à votre instance Réponse aux vulnérabilités.
- Validez le fait que vos règles (recherche de CI, affectation) pour l'élément vulnérable fonctionnent comme prévu. Pour plus d'informations sur la révision des règles de recherche de CI, reportez-vous à la section Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces. Pour en savoir plus sur les règles d'affectation, reportez-vous à la section Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

  Remarque : En raison du volume important d'importations de données, il convient d'être prudent avec l'affectation automatisée des éléments vulnérables.

- Vérifiez que vos cibles de rattrapage sont correctes. Reportez-vous à la rubrique Réponse aux vulnérabilités Règles de cibles de rattrapage pour en savoir plus sur le fonctionnement et la révision des règles de cibles de rattrapage.
- Affichez les éléments vulnérables non groupés.
  - En examinant les éléments vulnérables non groupés, envisagez de réviser vos règles de groupe et d'effectuer une nouvelle analyse. Consultez Créer ou modifier Réponse aux vulnérabilités des règles de tâche de rattrapage pour plus d'informations.
  - Regroupez manuellement les éléments vulnérables. Créer manuellement une tâche de rattrapage dans Réponse aux vulnérabilités pour plus d'informations.
  - Révisez les scores de risque pour les éléments vulnérables dans vos tâches de rattrapage. Consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité pour plus d'informations.
  - Fermez les éléments vulnérables plus anciens qui n'ont pas été détectés récemment par vos intégrations tierces. Consultez Fermeture automatique des éléments vulnérables et des détections pour plus d'informations.
- Afficher et reclasser des éléments de configuration sans correspondance.
- Recherchez ce qui doit être fait pour la correction.

  Cette étape peut inclure :

  - Déterminez ce qu'il faut traiter maintenant et ce que vous pouvez différer. Cette détermination est souvent basée sur le score de risque, les systèmes affectés et les correctifs avec des fenêtres de changement.

    Remarque : Les règles de cibles de rattrapage appartiennent aux éléments vulnérables. Ces règles sont exécutées lorsque l'élément vulnérable est importé. Ces règles ont été créées précédemment dans l'assistant de configuration.

  - Actualisez les éléments vulnérables, si nécessaire, et Afficher l'état de la cible de rattrapage d'un Réponse aux vulnérabilités élément vulnérable.
  - Créez une **demande de changement** et affectez la tâche de rattrapage à un groupe d'affectation (Opérations informatiques) pour le rattrapage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si la vulnérabilité constitue un incident de sécurité et que le module d'extension Réponse aux incidents de sécurité (com.snc.security_incident) est activé, vous pouvez créer des enregistrements d'incident de sécurité à partir des tâches de rattrapage.

- Après avoir soumis une ou plusieurs demandes de changement, passez l'état du groupe à En cours d'examen.

Modifier les éléments vulnérables en bloc dans Réponse aux vulnérabilités

Modifiez les éléments vulnérables en bloc pour gagner du temps en sélectionnant des champs et en exécutant une tâche de modification en bloc asynchrone en arrière-plan.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Important : La fonctionnalité de modification en bloc est disponible pour les éléments vulnérables de l'hôte dans le Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez L'utilisation de la modification en bloc dans Espace de travail du gestionnaire de vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Vulnérabilités** > **Éléments vulnérables**.
2. Sélectionnez les éléments vulnérables en effectuant l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Seuls les éléments sélectionnés** dans le #unique_122_Connect_42_entry-be-record-selection champ.
   - Appliquez des filtres si vous souhaitez utiliser l'option **Tous les éléments vulnérables qui correspondent au filtre** dans le #unique_122_Connect_42_entry-be-record-selection champ.
3. Sélectionnez le bouton **Modifier en bloc** .
4. Renseignez les champs de la fenêtre modale de modification en bloc.

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ Uniquement les éléments vulnérables sélectionnés ◦ Tous les éléments vulnérables qui correspondent au filtre ◦ Tâche de rattrapage ◦ Entrée de vulnérabilité
État	Changement de **l'état** dans l'élément vulnérable. Les choix possibles sont les suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Ne pas mettre à jour ◦ Ouvrir ◦ En cours d'examen ◦ En attente d'implémentation ◦ Différé **Remarque :** ▪ Lorsque vous sélectionnez cette option, les champs Motif, Description brève, Jusqu'à et Informations supplémentaires s'affichent. ▪ Lorsque vous différez les VIT, une tâche de rattrapage est créée et cette tâche est envoyée pour approbation. ◦ Fermé **Remarque :** ▪ Lorsque vous sélectionnez cette option pour marquer les enregistrements comme faux positifs, les champs Motif, Description brève, Jusqu'à et Informations supplémentaires s'affichent. ▪ Lorsque vous marquez les enregistrements comme faux positifs, une tâche de rattrapage est créée et cette tâche est envoyée pour approbation. ◦ Résolu
Solution privilégiée	Solution ciblée pour le rattrapage de tous les éléments vulnérables sélectionnés pour une modification en bloc. Sélectionnez le changement pour le champ **Solution privilégiée** dans l'élément vulnérable (VIT). Les choix proviennent d'une liste de recherche des solutions préférées disponibles pour les VIT sélectionnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ◦ L'ensemble des solutions privilégiées disponibles est une intersection de toutes les solutions potentielles des vulnérabilités dans tous les VIT sélectionnés. ◦ Lors de la sélection de **Sélection d'enregistrement** > **Entrée de vulnérabilité** pour une modification en bloc, tous les VIT pour la vulnérabilité sont définis sur la solution préférée sélectionnée. **Remarque :** Cette opération ne définit pas la **solution privilégiée** au niveau de l'entrée de vulnérabilité. La définition de la **solution privilégiée** au niveau d'entrée de vulnérabilité définira la **solution privilégiée** pour tous les nouveaux VIT à l'avenir. La modification en bloc ne modifie que l'ensemble actuel des VIT. ◦ Les vulnérabilités distinctes par rapport aux critères de sélection sont limitées à 500. S'il existe plus de 500 vulnérabilités distinctes, un message d'avertissement s'affiche vous demandant de sélectionner des VIT avec différents critères pour définir la **solution privilégiée**. ◦ Le nombre total de solutions pouvant être affichées dans la liste de recherche est limité à 170. S'il y a plus de 170 solutions, un message d'avertissement s'affiche. La valeur mise à jour est affichée dans la vue de liste Élément vulnérable.
Correctif préféré	Correctif ciblé pour corriger tous les éléments de vulnérabilité sélectionnés pour la modification en bloc. **Remarque :** ◦ Vous devez installer Patch Orchestration pour afficher la liste des correctifs préférés. ◦ L'ensemble des correctifs préférés disponibles est une intersection de tous les correctifs potentiels pour tous les VIT sélectionnés. ◦ Les vulnérabilités distinctes par rapport aux critères de sélection sont limitées à 500. S'il existe plus de 500 vulnérabilités distinctes, un message d'avertissement s'affiche vous demandant de sélectionner des VIT avec différents critères pour définir le **correctif préféré**. ◦ Le nombre total de correctifs pouvant être affichés dans la liste de recherche est limité à 170. S'il y a plus de 170 correctifs, un message d'avertissement s'affiche.
Motif	Motif du report des enregistrements :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre Motif de fermeture des enregistrements : ◦ Faux positif **Remarque :** ▪ Lorsque vous sélectionnez cette option, les champs Brève description, Jusqu'à et Informations supplémentaires s'affichent. ▪ Une tâche de rattrapage est créée lorsque vous marquez les enregistrements comme faux positifs et que cette tâche est envoyée pour approbation. ◦ Annulé ◦ Fixe **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé ou Fermé.
Description brève	Brève note décrivant la raison du report et des demandes de Fermé-Faux positif. Ces informations sont reflétées dans le champ Description de la tâche de rattrapage créée pour les demandes de report et les demandes de faux positifs fermés. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé et Fermé : faux positif.
Jusqu'à	Date à laquelle l'enregistrement demeure différé. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé.
Information supplémentaire	Toute autre information nécessaire. Ces informations sont reflétées dans le champ Informations supplémentaires de l'onglet Vue d'ensemble. Si votre demande de report est approuvée, ces informations supplémentaires apparaissent sous forme de notes de report à la fois dans VIT et dans la tâche de rattrapage. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé et Fermé : faux positif.
Annuler l'affectation	Tous les éléments sélectionnés ne sont plus affectés au groupe d'affectation et au propriétaire du rattrapage. Pour plus d'informations sur la façon dont un propriétaire de rattrapage peut supprimer les affectations des éléments vulnérables, consultez

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Supprimer les affectations des éléments vulnérables pour vous ou vos groupes. **Remarque :** ◦ Ce champ s'affiche lorsque vous sélectionnez l'état Ne pas mettre à jour. ◦ Lorsque vous annulez l'affectation d'enregistrements, une tâche de rattrapage est créée et cette tâche est envoyée pour approbation.
Groupe d'affectation	Groupe d'affectation pour le VIT. Sélectionnez manuellement ou utilisez les recommandations d'affectation si cette option est activée. **Remarque :** Ce champ est désactivé lorsque vous cochez la case **Annuler l'affectation** .
Notes de travail	Texte que vous saisissez pour décrire les changements.

5. Sélectionnez **OK**.
   Une tâche asynchrone de modification en bloc met à jour les enregistrements sélectionnés. Le numéro de tâche accompagné d'un lien s'affiche sur la page Éléments vulnérables où vous pouvez afficher son état. Une tâche de rattrapage est créée avec les éléments vulnérables sélectionnés lorsque vous différez, annulez l'affectation ou fermez (faux positifs) éléments vulnérables en bloc. Et cette tâche de rattrapage est envoyée pour approbation.

Éléments vulnérables dégroupés Réponse aux vulnérabilités

Les éléments vulnérables sont automatiquement affectés à une tâche de rattrapage lorsqu'ils sont importés. Cependant, parfois, si un élément vulnérable (VI) est créé manuellement, par exemple, le VI peut devenir orphelin. Le module **Élément vulnérable dissocié répertorie** les éléments vulnérables sans groupe.

Remarque : Les processus automatisés d'intégration ne créent pas d'orphelins, ce cas d'utilisation devrait donc être de petite taille.

La dissociation se produit si un élément vulnérable a été créé sans vulnérabilité, ou s'il n'existe aucune règle de tâche de rattrapage qui affecte le VI à un groupe.

Dans ce cas, passez en revue la liste des éléments vulnérables dissociés en accédant à **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Dégroupés**.

Après examen, vos choix sont les suivants :

- Vous pouvez Créer ou modifier Réponse aux vulnérabilités des règles de tâche de rattrapage intercepter tous les éléments qui apparaissent sur cette liste.
- Vous pouvez Créer manuellement une tâche de rattrapage dans Réponse aux vulnérabilités ajouter manuellement des éléments de cette liste au groupe ou définir une condition qui correspond à ces éléments.
- Vous pouvez ouvrir une tâche de rattrapage existante et ajouter tous les éléments vulnérables pertinents au groupe , à condition que l'état soit Ouvert ou En cours d'examen.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les éléments vulnérables ajoutés manuellement ne sont pas automatiquement supprimés des tâches de rattrapage par les règles de tâche de rattrapage ou les conditions de groupe.

Pour en savoir plus sur le comportement des tâches de rattrapage et des règles de tâche, reportez-vous à Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage.

Afficher les éléments vulnérables dégroupés Réponse aux vulnérabilités

Les éléments vulnérables qui ne sont pas affectés à un groupe sont placés dans une liste visible.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Vulnérabilités** > **Éléments vulnérables dégroupés**.
2. Examinez les éléments vulnérables dans la liste.
3. Cliquez sur chaque élément vulnérable pour afficher et déterminer comment l'inclure dans un groupe.

Ajouter manuellement un élément vulnérable à une tâche de rattrapage

Si un élément vulnérable n'est pas groupé, vous pouvez l'ajouter à une tâche de rattrapage.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Enregistrez le numéro vulnérable.
2. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
3. Choisissez une tâche de rattrapage (VUL) pour votre élément vulnérable.
4. Sélectionnez **Modifier** en bas à droite.
5. Saisissez le numéro de **l'élément vulnérable** dans le champ de recherche pour la collecte.
6. Sélectionnez l'élément vulnérable dans la collection et ajoutez-le à la liste.
7. Cliquez sur **Enregistrer**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Supprimer les affectations des éléments vulnérables

Réaffectez les enregistrements d'éléments vulnérables dans les Réponse aux vulnérabilités applications et Réponse aux vulnérabilités des applications

Avant de commencer

Rôle requis : sn_vul.remediation_owner

Pourquoi et quand exécuter cette tâche

Si vous déterminez que les éléments vulnérables (VIT) ne sont pas dans votre champ d'application pour le rattrapage, ou si vous pensez que les enregistrements ont été affectés de manière incorrecte à vous ou à vos groupes, vous pouvez vous supprimer ou supprimer vos groupes des champs Affecté à et **Groupe d'affectation** sur les enregistrements d'éléments vulnérables et de tâches de rattrapage.

Le bouton **Annuler l'affectation** s'affiche sur les enregistrements suivants dont l'état n'est pas Fermé ou Résolu :

- Tâches de remédiation (VUL) dans l'environnement classique et les Réponse aux vulnérabilités espaces de travail. Si une tâche de rattrapage est mise à jour avec cette fonctionnalité, les champs **Affecté à** et**Groupe d'affectation** de tous ses VIT associés sont également effacés.
- Éléments vulnérables (VIT) dans l'environnement classique et les Réponse aux vulnérabilités espaces de travail.
- Éléments vulnérables de l'application (AVIT).
- Éléments vulnérables du conteneur (CVIT).

Important : Vous pouvez annuler l'affectation des éléments vulnérables d'hôte en bloc dans le Espace de travail du gestionnaire de vulnérabilitésfichier . Pour plus d'informations, consultez L'utilisation de la modification en bloc dans Espace de travail du gestionnaire de vulnérabilités.

Procédure

1. Dans l'environnement classique ou dans IT Remediation Owner Workspace, accédez à un enregistrement d'élément vulnérable (VIT) qui vous est affecté et qui est dans un état autre que Fermé ou Résolu.
2. Pour effacer les champs **Affecté à** et **Groupe d'affectation** , en haut de l'enregistrement, sélectionnez **Annuler l'affectation**.
3. Facultatif : Vous pouvez également accéder à un AVIT qui vous est affecté, à vous ou à vos groupes, et cliquer sur **Annuler l'affectation** pour effacer les champs d'affectation.
4. Dans la boîte de dialogue Annuler l'affectation, fournissez des notes de travail et sélectionnez **Soumettre**.
5. Facultatif : Si vous souhaitez effacer les champs d'affectation de plusieurs VIT d'une liste, sélectionnez les VIT souhaités, puis sélectionnez **Modifier en bloc**.

   a. Dans la boîte de dialogue Modification en bloc de l'élément vulnérable, sélectionnez **Uniquement les éléments vulnérables sélectionnés** dans le champ **Sélection d'enregistrement** , cochez la case **Annuler l'affectation** , puis sélectionnez **OK**.
   Pour plus d'informations sur les modifications en bloc, consultez Modifier en bloc les éléments vulnérables de Vulnerability Response.

   b. Sélectionnez l'ID de tâche de rattrapage qui s'affiche dans la notification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Affichez les informations suivantes :
   - Les notes de travail que vous avez fournies sont affichées dans la section Notes.
   - Dans l'onglet **Approbation de changement d'état** , l'enregistrement d'approbation de changement d'état affiche l'état En cours de révision, qui permet de suivre le workflow d'approbation.
   - Dans l'onglet **Approbations demandées** , votre demande de suppression de vous-même ou de votre groupe d'affectation s'affiche à l'état Demandé.

Résultats

La demande est approuvée à l'aide d'un workflow d'approbation à un niveau par défaut. Pour plus d'informations, consultez Approuver les demandes dans les espaces de travail du gestionnaire de vulnérabilités.

- Si votre demande est approuvée, l'enregistrement d'approbation de changement d'état et l'enregistrement d'approbation demandé passent à l'état Approuvé. Vous et vos groupes êtes supprimés des champs Affecté à et **Groupe d'affectation**. `Non affecté` s'affiche dans le champ **Type d'affectation** , et la tâche de rattrapage et les VIT sont affichés dans la liste du module Non affecté pour Conformité de la configuration.

  Les notifications indiquant que les enregistrements ne sont pas affectés sont envoyées automatiquement aux gestionnaires de vulnérabilités ou aux analystes du groupe de notification Annuler l'affectation. Pour configurer le marqueur d'approbation, les notifications et le groupe d'affectation par défaut, consultez Suppression des affectations des éléments vulnérables et des tâches de rattrapage.

- Si votre demande est rejetée, l'état de l'enregistrement d'approbation de changement et de l'enregistrement de l'approbation demandée passe à l'état Rejeté.

Remarque : En tant qu'administrateur de vulnérabilité, vous pouvez définir la *`sn_vul.unassign_vr.approval_required`* propriété système sur **false** pour désactiver le processus d'approbation.

Que faire ensuite

Accédez aux modules non affectés pour les Réponse aux vulnérabilités applications et Réponse aux vulnérabilités des applications Réponse aux vulnérabilités pour conteneurs , surveillez tous les enregistrements non affectés pour détecter les éléments qui pourraient entrer dans votre champ d'application et réaffectez-les à vous-même.

Approuver ou rejeter une demande de désaffectation dans Réponse aux vulnérabilités

Approuvez les demandes de suppression des éléments vulnérables d'un groupe d'affectation ou d'un utilisateur individuel dans l'application Réponse aux vulnérabilités .

Avant de commencer

Rôle requis : pour les approbations non affectées, un approbateur est requis dans le groupe Approbateur – Niveau 1.

- sn_vul.unassign_approver pour les AVIT et les VIT
- sn_vul_container.unassign_approver pour les CVIT

Pourquoi et quand exécuter cette tâche

Par défaut, une configuration d'approbation est fournie et un groupe d'approbation de désaffectation est créé. Les utilisateurs du groupe Annuler l'affectation de l'approbateur - niveau 1 peuvent approuver la demande. Ce groupe contient un rôle d'approbateur de désaffectation, sn_vul.unassign_approver, par défaut. Vous pouvez modifier ou créer un nouveau groupe et mettre à jour la configuration de l'approbation. Pour configurer

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

une règle d'approbation, sélectionnez l'une des règles d'approbation suivantes dans le module Règles d'approbation et accédez à la configuration de l'approbation dans l'onglet **Configurations d'approbation** :

- *Vulnerable item field change request* pour un élément vulnérable.
- *Vulnerability field change request* pour une tâche de rattrapage.
- *Application vulnerability field change request* pour un élément vulnérable de l'application (AVIT).
- *Approval for container management* pour un élément vulnérable de conteneur (CVIT).

Pour plus d'informations sur les règles d'approbation et les configurations, reportez-vous à Configurations du workflow d'approbation pour la demande de désaffectation.

Important : Vous pouvez approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilitésfichier . Pour plus d'informations, consultez Approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Mes approbations** pour les VIT et les AVIT. Vous pouvez également accéder à **Tout** > **Conteneur Vulnerability Response** > **Mes approbations** pour les CVIT.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande en ajoutant les commentaires appropriés.

Fermeture automatique des éléments vulnérables et des détections

Vous pouvez fermer automatiquement les détections périmées et les éléments vulnérables (VI) associés aux CI mis hors service à l'aide du module Configuration de fermeture automatique.

Pour configurer l'option de fermeture automatique, accédez à **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Configuration de fermeture automatique**. Vous pouvez fermer automatiquement les détections et les VI obsolètes dans les scénarios suivants :

- Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités
- Fermer automatiquement les éléments vulnérables associés aux CI mis hors service

Pour plus d'informations sur l'utilisation d'éléments de configuration mis hors service, reportez-vous à la section Utilisation d'éléments de configuration mis hors service.

Utilisation d'éléments de configuration mis hors service

Les éléments de configuration (CI) mis hors service passent à l'état Mis hors service, Archivé ou Supprimé dans le Base de données de gestion des configurations (CMDB). Réponse aux vulnérabilités contient des éléments vulnérables (VI) qui sont constitués de CI. Lorsque l'état d'un CI est mis à jour sur Mis hors service, les VI associés sont fermés avec le sous-état « CI désactivé ».

Si la CMDB définit l'état d'étape du cycle de vie d'un CI sur Mis hors service, vous pouvez choisir de fermer automatiquement les VI associés. Pour en savoir plus sur la fermeture automatique des VI associés, reportez-vous à la section Fermer automatiquement les éléments vulnérables associés aux CI mis hors service.

Le CI mis hors service est éventuellement archivé ou définitivement supprimé du CMDBfichier .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Impact de la mise hors service des CI :

- **Impact sur les éléments détectés :** Lorsque le CI est mis hors service, l'élément détecté (DI) connexe est marqué comme « CI désactivé ».
- **Impact sur les éléments vulnérables :** Lorsque l'état d'un élément de données est mis à jour sur « CI désactivé », le VI associé est fermé et la section Notes est automatiquement mise à jour.

> **Remarque :** L'état d'un élément de données est automatiquement mis à jour sur « CI désactivé » chaque fois que l'état du cycle de vie d'un CI est mis à jour. D'autre part, l'état d'un VI est mis à jour sur Fermé uniquement lorsque l'option **Fermer automatiquement les VI liés aux CI hors service** est activée. Pour en savoir plus sur la fermeture automatique des VI associés, reportez-vous à la section Fermer automatiquement les éléments vulnérables associés aux CI mis hors service.

La tâche *Close detections/VIs for decommissioned CIs* planifiée est exécutée quotidiennement pour les DI mis à jour. Si l'option de configuration de fermeture automatique est activée pour les CI mis hors service, elle identifie le DI contenant un CI désactivé et ferme le VI associé avec le sous-état « CI désactivé ». Si tous les VI d'une tâche de rattrapage sont fermés et que leur sous-état est CI désactivé, la tâche de rattrapage est également fermée avec le sous-état « Annulé ». Pour afficher les VI mis hors service, accédez à **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Désactivé**.

> **Remarque :** Si un CI revient à l'état d'origine depuis l'état « Hors service », l'entrée « Éléments détectés » est également mise à jour. Les VI sont automatiquement ouverts lorsque les données sont à nouveau ingérées à partir du scanner.

Fermer automatiquement les éléments vulnérables associés aux CI mis hors service

Si l'état Base de données de gestion des configurations (CMDB) de l'étape du cycle de vie d'un élément de configuration (CI) passe à Mis hors service, vous pouvez choisir de fermer automatiquement les éléments vulnérables (VI) et les détections associés.

Avant de commencer
Rôle requis : sn_vul.admin

Pourquoi et quand exécuter cette tâche
À partir de la version 22.0 de Réponse aux vulnérabilités, pour fermer automatiquement les VI et détections associés, vous devez activer la propriété *sn_vul_cmn.auto_close_vis_linked_retired_cis* système pour fermer automatiquement les VI associés aux CI mis hors service. Pour activer l'option, définissez le champ Valeur sur « 1 ». Inversement, pour désactiver l'option, définissez le champ Valeur sur « 0 ».

Lors d'une mise à niveau, si la propriété *sn_vul_cmn.auto_close_vis_linked_retired_cis* système est sélectionnée dans la version 21.0 de Réponse aux vulnérabilités, la valeur reste « 1 ». Lorsque cette option est activée, les VI et détections nouveaux ou existants signalés pour le même CI sont automatiquement créés ou mis à jour avec l'état « Fermé ». Cette valeur est basée sur l'ID d'actif dans la charge utile du scanner et sur l'état de l'entrée Éléments détectés. Pour plus d'informations sur l'impact des CI mis hors service, consultez Utilisation d'éléments de configuration mis hors service

.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'état d'un élément de données est défini sur « CI désactivé » chaque fois que l'état du cycle de vie d'un CI est mis à jour. D'autre part, l'état d'un VI est mis à jour sur Fermé uniquement lorsque l'option **Fermer automatiquement les VI liés aux CI hors service** est activée.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Configuration de fermeture automatique** > **Cycle de vie de l'élément de configuration**.
2. Pour fermer automatiquement les éléments vulnérables associés aux CI hors service, cochez la case **Fermer automatiquement les éléments vulnérables liés aux CI hors service** .
3. Sélectionnez **Mettre à jour**.

Remarque : Si un CI est déjà mis hors service avant que l'option **Fermer automatiquement les VI liés aux CI hors service** soit activée, les VI sont créés uniquement pour les nouvelles détections à partir des scanners. L'état de ces VI est Fermé et le sous-état est CI désactivé.

Vous ne pouvez pas rouvrir manuellement les VI dont l'état est CI désactivé à l'aide des options **Rouvrir** ou **Modifier en bloc** .

Les VI fermés avec un sous-état Fixe ou Périmé sont rouverts si une nouvelle détection est créée et les VI peuvent être mis en correspondance avec la nouvelle vulnérabilité. Consultez États des détections, des tâches de rattrapage et des éléments vulnérables pour plus d'informations.

Fermeture des détections obsolètes dans Réponse aux vulnérabilités

Le module Fermer automatiquement les détections périmées vous aide à nettoyer automatiquement les détections vulnérables anciennes et périmées qui n'ont pas été trouvées récemment par vos intégrations tierces. Le déplacement de ces détections vers Fermé réduit le nombre d'éléments vulnérables actifs et de tâches de rattrapage dans votre Now Platform instance et vous aide à rapprocher les actifs dans votre CMDB.

Vue d'ensemble et termes clés

Afin de déployer plus précisément les données de détection sur vos éléments vulnérables, le module Fermer automatiquement les détections périmées vous aide à nettoyer les détections d'éléments vulnérables anciennes et périmées qui n'ont pas été trouvées récemment par vos intégrations tierces. Pour plus d'informations sur cette fonctionnalité, consultez le cas d'utilisation ci-dessous et l'article Fermer automatiquement les détections obsolètes [KB 0958638].

Dans les versions précédentes de Réponse aux vulnérabilités, le module Éléments vulnérables à fermeture automatique faisait automatiquement passer les éléments vulnérables qui n'ont pas été récemment trouvés ou mis à jour par vos intégrations de scanners tiers vers le module Fermé - Périmé.

Avant d'activer la fonctionnalité Fermer automatiquement les détections périmées, passez en revue les termes suivants, la façon dont les états se déploient jusqu'aux éléments vulnérables et aux tâches de rattrapage, ainsi que les prérequis pour vos intégrations tierces qui importent les données de détection.

Pour activer cette fonctionnalité, reportez-vous à la section Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités.

Termes clés

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détections périmées

Fait référence aux détections associées à des éléments vulnérables dans votre Now Platform® instance qui vieillissent et n'ont pas été trouvées, mises à jour ou détectées par les analyses d'intégration tierces pendant une période prolongée.

Dernières détections trouvées

Cette option de recherche utilise une date et une heure fournies par l'analyseur tiers. Ce terme désigne la date et l'heure les plus récentes ou les plus récentes auxquelles les détections ont été retrouvées par le scanner.

Derniers actifs numérisés

Cette option de recherche utilise une date et une heure fournies par l'analyseur tiers. Ce terme désigne la date et l'heure les plus récentes auxquelles un actif a été analysé pour la dernière fois par un scanner tiers.

Cas d'utilisation

Parfois, des actifs (éléments de configuration) peuvent être mis hors service dans votre environnement ou purgés par des scanners tiers, et leurs détections associées ne sont pas mises à jour par les détections d'éléments vulnérables. Par conséquent, les détections et leurs éléments vulnérables associés ne sont pas mis à jour dans l'application Réponse aux vulnérabilités et deviennent inactifs (périmés).

Pour fermer ces détections vieillies qui ont des données d'éléments vulnérables inchangées et réduire ensuite le nombre de VI actifs et de tâches de remédiation (RT), activez Fermer automatiquement les détections obsolètes. Cette fonctionnalité ferme automatiquement les détections d'éléments vulnérables qui ne sont pas récemment trouvées ou mises à jour par vos intégrations de scanners tiers en fonction des critères de recherche et de l'âge en nombre de jours que vous définissez.

À titre d'exemple, supposons qu'un élément de configuration particulier (CI) possède plusieurs ID d'actif et que l'un de ces ID n'a pas été importé lors d'une détection à partir d'un scanner tiers au cours des 90 derniers jours. Cette fonctionnalité ferme automatiquement cette détection qui n'a pas de nouvelles données de vulnérabilité afin que l'élément vulnérable associé puisse être fermé.

Étant donné qu'un VI peut être associé à plusieurs détections, cette fonctionnalité ne fait passer d'une détection à l'autre que les détections jugées périmées par les paramètres que vous définissez. Par exemple, si quatre détections sont associées à un VI et que deux d'entre elles ont expiré (c'est-à-dire qu'aucune nouvelle donnée de vulnérabilité n'a été importée au cours des 90 derniers jours), cette fonctionnalité ferme uniquement les détections périmées. Pour pouvoir fermer le VI, vous devez d'abord corriger les deux autres détections ouvertes.

Déploiement des états de détection vers les VI

Pour différencier les détections fermées automatiquement des détections fermées par des scanners tiers, une nouvelle valeur a été ajoutée pour le champ État, Périmé. Les valeurs possibles pour ce champ sont Ouvert, Fermé et Périmé. Périmé indique qu'une détection a été fermée par la fonctionnalité de détection de fermeture automatique.

Priorité de l'état : Ouvert > Fermé > périmé.

1. Si des détections sont ouvertes, l'état du VI associé reste Ouvert.
2. Si aucune détection n'est ouverte, certaines sont fermées et d'autres périmées, l'état de VI associé passe à Fermé - Fixe.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Si toutes les détections sont périmées, l'état du VI associé passe à Fermé - Périmé.

   À partir de Réponse aux vulnérabilités la version 20.0, si la détection est périmée et que son VI associé est à l'état Fermé, l'état du VI ne passe pas à Fermé - Périmé. Cela permet d'éviter que le VI ne se rouvre lorsqu'une nouvelle détection est identifiée, afin d'éviter de passer par l'ensemble du processus de demande et d'approbation de faux positif. Pour inverser ce comportement, décochez la case **Ignorer les détections obsolètes pour les VI fermés** dans le formulaire Configuration de fermeture automatique. Pour plus d'informations, consultez Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités.

Déploiement des états des VI sur les tâches de remédiation (VUL)

Priorité de l'état : Ouvert > Fermé : Fixe > Fermé : périmé.

1. Si des VI dans une tâche de rattrapage sont ouverts, l'état de vulnérabilité n'est pas modifié.
2. Si au moins un VI est Fermé - Fixe et que les autres sont Fermé - Périmé, l'état de la vulnérabilité passe à Fermé - Fixe.
3. Si tous les VI d'une VUL sont Fermé - Périmé, l'état de la VUL passe à Fermé - Annulé.

Détections de fermeture automatique et exigences d'intégration tierce

Les utilisateurs de Microsoft TVM et les détections obsolètes de fermeture automatique

Élément de liste de vérification	Description
Intégration de vulnérabilité Microsoft TVM	Avec Microsoft TVM Vulnerability Integration, si vous sélectionnez **Dernières détections trouvées** pour baser votre recherche, cette fonctionnalité nécessite une exécution réussie de l'intégration des vulnérabilités des machines Microsoft TVM (importation complète) au cours des sept derniers jours. Cette intégration s'exécute chaque semaine. Si la fermeture automatique des détections périmées est activée et **configurée pour les détections détectées en dernier**, que l'intégration des vulnérabilités des ordinateurs Microsoft TVM est désactivée ou qu'aucune importation de données n'est effectuée avec succès au cours des sept derniers jours, la tâche planifiée de fermeture des détections s'exécute toujours quotidiennement, mais certaines détections périmées peuvent ne pas être fermées comme prévu. Si vous sélectionnez **Derniers actifs numérisés** pour baser votre recherche, il n'est pas nécessaire d'exécuter l'intégration des vulnérabilités des ordinateurs Microsoft TVM. Pour activer cette intégration :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément de liste de vérification	Description
	1. Accédez à la **Intégration de vulnérabilité Microsoft TVM** > **Administration** > **Intégration**. 2. Recherchez et activez **l'intégration des vulnérabilités des machines Microsoft TVM (importation complète).**
(Facultatif) Déployez plusieurs instances d'intégrations Microsoft TVM dans votre environnement.	Vous pouvez éventuellement déployer plusieurs instances d'intégrations dans votre environnement. La fermeture automatique des détections obsolètes n'est pas spécifique à une instance et est activée ou désactivée dans votre environnement. Les détections périmées sont automatiquement transférées vers l'état périmé sur les instances qui ont terminé avec succès les exécutions d'intégration. Si la fermeture automatique des détections périmées est activée et que vous désactivez les intégrations qui s'exécutent chaque semaine dans une instance, la tâche planifiée de fermeture des détections s'exécute toujours quotidiennement, mais certaines détections peuvent ne pas passer automatiquement à l'état périmé comme prévu.

Qualys utilisateurs et fermer automatiquement les éléments vulnérables périmés

- Toutes les intégrations tierces activées Qualys qui récupèrent les données de détection peuvent s'exécuter avec ce module. Aucune application spécifique Qualys n'est requise.
- Vous pouvez éventuellement déployer plusieurs instances d'intégrations Qualys dans votre environnement.
- La fermeture automatique des détections obsolètes n'est pas spécifique à une instance et est activée ou désactivée dans votre environnement. Les détections périmées sont automatiquement transitionnées vers l'état périmé sur toutes les instances.

Rapid7 utilisateurs et fermer automatiquement les détections obsolètes

Élément de liste de vérification	Description
L'intégration Rapid7 de vulnérabilité	Si vous sélectionnez **Dernières détections trouvées** pour baser votre recherche, cette fonctionnalité nécessite une exécution réussie de l'une des Rapid7 intégrations complètes d'éléments vulnérables au cours des sept derniers jours. Ces intégrations complètes s'exécutent chaque semaine : • Pour Rapid7 Nexpose l'entrepôt de données, une exécution réussie à partir de l'intégration Rapid7 complète des éléments vulnérables est requise. • Pour Rapid7 InsightVM, une exécution réussie de l'intégration Rapid7 complète des éléments vulnérables - API est requise. Si l'option Fermer automatiquement les détections périmées est activée et **configurée pour les dernières détections**,

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément de liste de vérification	Description
	et que les Rapid7 intégrations complètes des éléments vulnérables sont désactivées, ou qu'aucune importation de données n'est effectuée avec succès au cours des sept derniers jours, la tâche planifiée de fermeture des détections s'exécute toujours quotidiennement, mais certaines détections périmées peuvent ne pas être fermées comme prévu. Si vous sélectionnez **Derniers actifs numérisés** pour baser votre recherche, aucune exécution d'intégration complète Rapid7 n'est requise. Pour activer ces intégrations : **1.** Accédez à la **Rapid7 Vulnerability Integration** > **Administration** > **Intégration**. **2.** Localisez et activez l'intégration complète des Rapid7 éléments vulnérables dont vous avez besoin. **Remarque :** En plus de ces intégrations qui s'exécutent de manière Rapid7 Nexpose hebdomadaire et Rapid7 InsightVM qui ont chacune des intégrations de VI qui s'exécutent quotidiennement, l'intégration d'éléments vulnérables Rapid7 et l'intégration d'éléments vulnérables Rapid7 - API. Si les intégrations quotidiennes et hebdomadaires Rapid7 sont activées, une seule intégration s'exécute à la fois. Si l'un de ces travaux d'intégration est en cours d'exécution, le travail de l'autre intégration est ignoré jusqu'à la tâche planifiée suivante.
(Facultatif) Déployez plusieurs instances d'intégrations Rapid7 dans votre environnement.	En option, vous pouvez déployer plusieurs instances d'intégrations complètes dans votre environnement. La fermeture automatique des détections obsolètes n'est pas spécifique à une instance et est activée ou désactivée dans votre environnement. Les détections périmées sont automatiquement transférées vers l'état périmé sur les instances qui ont terminé avec succès les exécutions d'intégration. Si l'option Fermer automatiquement les détections périmées est activée et que vous désactivez les intégrations qui s'exécutent chaque semaine dans une instance, la tâche planifiée de fermeture des détections s'exécute toujours quotidiennement, mais certaines détections peuvent ne pas passer automatiquement à l'état Périmé comme prévu.

Utilisateurs de l'intégration de vulnérabilité Tenable et fermeture automatique des éléments vulnérables périmés

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Toutes les intégrations activées à partir de Tenable Vulnerability Integration qui récupèrent les données de détection peuvent s'exécuter avec ce module. Aucune intégration de vulnérabilité Tenable spécifique n'est requise.
- Vous pouvez éventuellement déployer plusieurs instances de Tenable Vulnerability Integration dans votre environnement.
- La fermeture automatique des détections obsolètes n'est pas spécifique à une instance et est activée ou désactivée dans votre environnement. Les détections périmées sont automatiquement transitionnées vers **l'état périmé** sur toutes les instances.

Après avoir vérifié que vos intégrations sont correctement configurées, reportez-vous à la rubrique Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités pour activer la fonctionnalité.

Mettre à niveau les informations de Fermer automatiquement les éléments vulnérables périmés vers Fermer automatiquement les détections obsolètes

Pour le module Fermer automatiquement les éléments vulnérables périmés, si vous avez précédemment utilisé l'option Fermer automatiquement les éléments vulnérables périmés :

- La valeur du nombre de jours que vous avez saisi pour l'option **Derniers actifs numérisés** dans Fermer automatiquement les éléments vulnérables périmés est conservée automatiquement pour les **derniers actifs numérisés** dans Fermer automatiquement les détections obsolètes.
- La valeur du nombre de jours que vous avez saisis pour l'option **Derniers éléments vulnérables trouvés** dans Fermer automatiquement les éléments vulnérables périmés est conservée automatiquement pour **les détections détectées pour la dernière fois** dans Fermer automatiquement les détections périmées.
- Les détections ouvertes existantes avec éléments vulnérables comme Fermé - Périmé passeront à l'état Périmé selon les paramètres de configuration de fermeture automatique lorsque la tâche planifiée s'exécutera après la *`Auto-Close Stale Detections`* mise à niveau.

Informations sur le déploiement

- Si un élément vulnérable était Fermé - Périmé avant la mise à niveau, et que toutes ses détections sont marquées comme Périmées après la mise à niveau, l'état du VI reste Fermé - Périmé.
- Si un élément vulnérable était Fermé - Périmé avant la mise à niveau, et que seules certaines de ses détections sont marquées comme Périmées après la mise à niveau et que les autres ont été fermées par l'analyseur, l'élément vulnérable passe à l'état Fermé - Corrigé selon la logique de déploiement.

Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités

Activez Fermer automatiquement les détections périmées pour fermer automatiquement les détections vulnérables périmées qui n'ont pas été trouvées récemment par vos intégrations tierces.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vuln.admin (déconseillé), ou un gestionnaire des vulnérabilités avec le rôle granulaire sn_vul.manage_auto_close_stale_vi.

Pour plus d'informations sur cette fonctionnalité, les termes clés et toute configuration qui peut être requise pour vos intégrations tierces qui importent des données de détection,

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

reportez-vous à la section Fermeture des détections obsolètes dans Réponse aux vulnérabilités pour plus d'informations.

Remarque : Les informations fournies dans la procédure suivante ne s'appliquent qu'aux versions antérieures à la version 22.0 de Réponse aux vulnérabilités. À partir de la version 22.0 de Réponse aux vulnérabilités, vous pouvez configurer des options de recherche supplémentaires. VoirCréer des règles de fermeture automatique pour plus d'informations.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Configuration de fermeture automatique** > **Détections périmées**.
   Le formulaire Configuration périmée de fermeture automatique s'affiche.
2. Renseignez les champs.
3. Pour le champ **Fermer automatiquement les détections obsolètes en fonction d'un** champ, choisissez une option pour votre recherche.

   Les deux recherches correspondent à l'âge des détections anciennes et périmées en nombre de jours jusqu'à une date fournie par votre scanner.

   Remarque : À partir de la version 22.0 de Réponse aux vulnérabilités, les options **Dernières détections trouvées** et **Derniers actifs analysés** sont créées sous forme de liste.

   - **Dernières détections trouvées**. Cette option recherche la date la plus récente ou la plus récente à laquelle les détections ont été retrouvées par le scanner.

     Remarque : Pour Rapid7 les utilisateurs de TVM et Microsoft TVM, un message d'avertissement s'affiche lorsqu'ils ont besoin d'informations de détection actuelles.

     Si vous sélectionnez **Dernières détections trouvées** pour baser votre recherche, cette fonctionnalité nécessite une exécution réussie de l'une des intégrations complètes d'éléments vulnérables au cours des Rapid7 sept derniers jours.

     Si vous sélectionnez **Dernières détections trouvées** pour baser votre recherche, cette fonctionnalité nécessite une exécution réussie de l'intégration des vulnérabilités des machines Microsoft TVM (importation complète) au cours des sept derniers jours.

   - **Derniers actifs analysés**. Cette option recherche la date la plus récente à laquelle un actif a été analysé pour la dernière fois par un scanner tiers.
4. Microsoft Pour Rapid7 les utilisateurs et TVM uniquement, vérifiez que toutes les intégrations requises sont activées.
   Voir Présentation de Intégration des vulnérabilités Rapid7 et Présentation de l'intégration des vulnérabilités de Microsoft Threat and Vulnerability Management pour plus d'informations.
5. Pour activer le module, cochez la case Actif pour le sélectionner.
6. Dans le champ **Dernières détections trouvées (en jours),** entrez l'âge des détections anciennes et périmées en nombre de jours.

   La valeur par défaut est de 90 jours. Vous pouvez entrer n'importe quelle valeur positive pour le nombre de jours. Cette valeur est utilisée pour correspondre à une date fournie par votre scanner. Avec 90 et **Dernières détections trouvées** affichées, toutes les détections introuvables au cours des 90 derniers jours sont automatiquement fermées. Avec 90 et

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Derniers actifs scannés affichés, toutes les détections associées à des actifs non scannés au cours des 90 derniers jours sont automatiquement fermées.

Remarque :

Il existe une relation entre le **champ Dernières détections trouvées/Dernière numérisation des actifs (il y a jours)** pour cette fonctionnalité et le champ **Importer depuis** sur l'API Rapid 7 Comprehensive Vulnerable Item Integration et Microsoft TVM Machine Vulnerabilities Integration.

Pour ces intégrations, le champ **Importer depuis** des pages de configuration est vide par défaut.

Si vous ne saisissez pas de valeur ou si le champ n'a pas de valeur, les données relatives au nombre de jours configurés dans le champ **Dernières détections trouvées/Dernière numérisation des actifs (il y a x jours) sont utilisées** .

Par exemple, si le nombre de jours défini dans le formulaire de configuration de fermeture automatique est `de 90` et que le champ **Importer depuis** est vide sur les pages de configuration de l'intégration, la première exécution de l'intégration importe les données des 90 derniers jours. Les champs **Importer depuis** pour l'API Rapid7 Intégration complète des éléments vulnérables - API et l'intégration Vulnérabilités des ordinateurs Microsoft TVM sont modifiables, de sorte que vous pouvez également fournir les valeurs que vous souhaitez. La valeur 90 jours est fournie par défaut si le champ reste vide afin que la fonctionnalité de fermeture automatique ne ferme pas les faux positifs.

Cette relation entre ces champs s'applique uniquement à la première exécution d'intégration. Par la suite, la modification du champ **Dernières détections trouvées/ Dernière numérisation des actifs (il y a quelques jours)** sur le formulaire Fermer automatiquement les détections vulnérables périmées n'affecte pas le champ **Importer depuis** sur les pages de configuration de l'intégration. Le champ est remplacé par l'heure de début de la première exécution afin que les exécutions d'intégration suivantes importent uniquement les informations delta.

7. Facultatif : Cochez la case **Ignorer les détections périmées des VI différés** pour ignorer les détections périmées mappées sur des VI différés ou sur des VI actuellement en cours d'examen en vue d'un report.

   (Optional) Si vous laissez cette option désactivée, toutes les détections qui correspondent à vos critères seront fermées et mappées aux VI différés ou aux VI en cours d'examen en vue d'un report. Les VI différés ou les VI en cours de révision qui correspondent à ces détections sont également automatiquement fermés en fonction de la logique de déploiement. Pour plus d'informations sur la logique de déploiement, reportez-vous à la section Fermeture des détections obsolètes dans Réponse aux vulnérabilités.

   Si vous activez cette option, toutes les détections qui correspondent à vos critères, à savoir le mappage aux VI différés ou aux VI en cours d'examen en vue d'un report, sont ignorées pendant la fermeture automatique.

8. Facultatif : Décochez la case **Ignorer les détections obsolètes pour les VI fermés** .

   (Optional) Par défaut, cette case est cochée afin que le VI fermé ne soit pas rouvert lorsqu'une nouvelle détection liée à ce VI fermé est identifiée. Pour plus d'informations sur la logique de déploiement, reportez-vous à la section Fermeture des détections obsolètes dans Réponse aux vulnérabilités.

9. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La tâche planifiée *Auto-Close Stale Detections* s'exécute quotidiennement. La tâche détermine si vous avez sélectionné la date à laquelle les détections ont été détectées pour la dernière fois ou la date à laquelle les actifs ont été analysés pour la dernière fois. Il fait ensuite passer les détections correspondantes à l'état Périmé. Il est important de noter que la fonctionnalité de fermeture automatique de la détection obsolète ne ferme les détections obsolètes que pour les instances d'intégration actives. Les éléments vulnérables et les détections associés aux instances d'intégration actives sont fermés. À partir de Réponse aux vulnérabilités la version 22.0, la tâche planifiée a été modifiée pour prendre en compte la table commune [sn_vul_cmn_auto_close_rule].

Une fois les détections marquées comme périmées, si le scanner signale avoir à nouveau détecté cette détection, le champ État des détections passe à Ouvert. Les éléments vulnérables correspondants à la détection sont également rouverts.

De plus, si la détection est marquée comme périmée et que le scanner détecte qu'elle est fixe, la détection passe à l'état Fermé. L'état s'étend également aux VI.

Créer des règles de fermeture automatique

Utilisez des règles de fermeture automatique pour fermer automatiquement les détections plus anciennes en fonction des conditions de filtre que vous définissez.

Avant de commencer

Rôle requis : sn_vul.manage_auto_close_stale_vi

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles de fermeture automatique**.

   Le système de base fournit les règles de fermeture automatique suivantes :

   - **Derniers actifs analysés** : les détections associées à des actifs qui n'ont pas été analysés au cours des 90 derniers jours passent à **l'état Périmé** .
   - **Dernières détections manuelles trouvées** : détections manuelles introuvables au cours des 90 derniers jours. Si vous activez **le dernier enregistrement de détections trouvé** , cette fonctionnalité nécessite une exécution d'intégration réussie des intégrations complètes des éléments vulnérables et de l'intégration des vulnérabilités des machines Microsoft TVM (importation complète) au cours des Rapid7 sept derniers jours.
   - **Dernières détections trouvées** : détections qui n'ont pas été trouvées au cours des 90 derniers jours.
2. Sélectionnez **Nouveau** pour créer une règle de fermeture automatique.
3. Renseignez les champs du formulaire.

Champ	Valeur
Nom	Nom de la règle de fermeture automatique.
Actif	Option permettant d'activer la règle. Si elle est activée, elle ferme automatiquement toutes les détections qui correspondent à ses critères de filtrage.
Ignorer les éléments différés	Si cette option est sélectionnée, toutes les détections mappées sur les états **En cours de révision** ou **Différé** sont ignorées et ne sont pas fermées. Si vous désactivez cette

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
	option, toutes les détections qui correspondent à vos critères sont fermées.
Ordre d'exécution	Valeur unique pour l'exécution de la règle de fermeture automatique. Cette valeur détermine l'ordre d'exécution. La valeur par défaut est 100.
Description	Description de la règle de fermeture automatique.
Condition	Conditions de filtre utilisées pour identifier les détections qui doivent être fermées.

4. Sélectionnez **Soumettre**.

La tâche planifiée *Auto-Close Stale Detections* s'exécute quotidiennement. Il identifie les détections en fonction des conditions spécifiées et fait passer celles qui correspondent à l'état **Périmé** . La tâche gère les scénarios suivants :

- Si toutes les détections au sein d'un élément vulnérable (VIT) sont marquées comme périmées, le VIT est fermé avec le sous-état défini sur « Périmé ».
- Si au moins une détection reste ouverte dans un VIT, tandis que d'autres sont à l'état Périmé, le VIT reste ouvert.
- Dans les cas où des détections présentent à la fois des états « Fermé » et « Périmé » dans un VIT, le VIT est fermé avec le sous-état défini sur « Fixe ».

Lorsque vous effectuez une mise à niveau vers la dernière version de Réponse aux vulnérabilités, les conditions définies dans vos règles de fermeture automatique sont également mises à jour en conséquence. En outre, si les règles sont associées à différents domaines, elles sont créées spécifiquement au sein de ces domaines.

Reclassifier le matériel non classé

Reclasser le matériel non classé en mettant à jour les règles de recherche de CI.

Avant de commencer

Rôle requis : sn_sec_cmn.admin

Pourquoi et quand exécuter cette tâche

La table Carte d'importation d'hôte [sn_sec_cmn_src_cmdb_map] affiche les variables entrantes de la charge utile et leurs affectations correspondantes dans la table Éléments détectés. Parfois, des différences dans les conventions de dénomination entre le scanner et Discovery peuvent conduire à ce que le matériel ne soit pas classifié. Lors de la création d'un CI matériel non classé, assurez-vous que le nom dans la charge utile contient uniquement le nom de l'hôte. Par la suite, lorsque Découverte identifie l'actif, il peut être reclassé dans la classe CI appropriée. Si nécessaire, un script peut être écrit pour générer une valeur dérivée qui s'aligne sur le nom du CI dans Détection et dans Base de données de gestion des configurations (CMDB).

Si le moteur Identification et rapprochement (IRE) est activé, l'option de reclassification des éléments détectés n'est pas prise en charge.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Mappages d'importations d'hôtes**.
2. Sélectionnez une source.
3. Dans la liste Champ cible, sélectionnez **Nom**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La case à cocher **Utiliser un script** devient visible.

Remarque :

- Le script n'est disponible que si Nom est sélectionné dans la liste **Champ** cible.
- Pour ajouter un script pour d'autres options dans la liste Champ Cible, vous devez désactiver la politique d'interface utilisateur en :
  - Désactivation de l'option « Définir l'utilisation d'un script faux ».
  - Désactivation de l'option « Afficher ou masquer le script d'utilisation ».
  - Suppression de la condition « le champ cible est nom » dans « Afficher ou masquer la politique de script »
- La table Cartes d'importation d'hôte est mise à jour avec deux nouvelles colonnes : Script et Script d'utilisation.

4. Cochez la case **Utiliser un script** .
   Le champ **Script** affiche le script par défaut, mais vous pouvez en créer un personnalisé. Dans ce champ, vous pouvez spécifier les valeurs source et dérivées à aligner avec la convention de dénomination de la base de données. La valeur générée par le script est stockée dans sourcePayload['DERIVED'][rule.source_field]. Assurez-vous que les règles de recherche de CI sont ajustées pour utiliser la charge utile source, les valeurs dérivées et les valeurs d'attributs ciblés lors de l'archivage des tables correspondantes.
5. Pour appliquer le script à des enregistrements en double plus anciens, procédez comme suit :

   a. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments détectés**.

   b. Sélectionnez les enregistrements en double.

   c. Dans la liste Action sur les lignes sélectionnées, sélectionnez **Réappliquer les règles de recherche de CI**.
   Il affiche une correspondance avec un actif existant.

6. Pour appliquer le script de Tenable.io, procédez comme suit :

   a. Accédez à la **Réponse aux vulnérabilités Mappages d'importation d'hôtes**.

   b. Sélectionnez le script pour la ligne avec NetBIOS, HOSTNAMES et le nom FQDNS comme champ **Source** .

   c. Mettre à jour le script pour chaque élément.

   Remarque : Pour Tenable.io, le scanner renvoie un tableau pour NetBIOS, HOSTNAMES et FQDNS name, pour lesquels le script ne fonctionne pas comme prévu.

   Étant donné que la carte d'importation d'hôte contient Tenable.io**netbios_name** dans le champ **Source** , vous devez écrire un script. Lors de la recherche, un autre champ source, **NETBIOS** , est utilisé, qui contient un tableau de valeurs. Une nouvelle ligne est donc ajoutée dans la table, et la même logique doit être écrite en boucle dans le script. Il en va de même pour **les noms de domaine complets et les noms d'hôte.**

7. Pour appliquer le script de Rapid7, procédez comme suit :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Tout** > **Réponse aux vulnérabilités Mappages d'importation d'hôtes**.

b. Pour Rapid7 les lignes avec FQDN et HostName, mettez à jour la méthode de recherche sur Script.

Remarque : Pour Rapid7, la méthode de recherche de CI est définie sur Correspondance de champ pour le nom de domaine complet et le nom d'hôte, ce qui permet de l'empêcher d'utiliser le script.

Créer manuellement une tâche de rattrapage dans Réponse aux vulnérabilités

La création manuelle d'une tâche de rattrapage est effectuée lorsque vous souhaitez regrouper des éléments vulnérables selon un critère autre que les critères des règles de tâche de rattrapage. Par exemple, vous pouvez créer des tâches pour un gestionnaire particulier ou pour de nouveaux exploits actifs, tels qu'un rançongiciel, qui incluent différentes vulnérabilités. Vous pouvez également l'utiliser pour regrouper des éléments vulnérables non groupés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.

   Les règles de tâche de rattrapage fonctionnent de la même manière que les règles de groupe de vulnérabilité auparavant, et elles sont toujours à votre disposition. Toutefois, vous préférerez peut-être laisser les règles de tâche de rattrapage inactives le temps de vous habituer aux fonctionnalités disponibles pour vos gestionnaires de sécurité et vos équipes informatiques dans les espaces de travail.

2. Sélectionnez l'une des catégories de tâches pour ouvrir la liste.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire comme il convient.
   Pour en savoir plus sur des champs spécifiques, reportez-vous à la section Champs du formulaire de tâche de rattrapage.
5. Cliquez sur **Envoyer**.
   Lorsque la tâche est créée, à l'aide du type de filtre **Condition** ou **Groupe de filtres** , la liste connexe **Élément vulnérable** recherche et affiche tous les éléments vulnérables correspondants.

   Vous pouvez utiliser le lien connexe, Analyser à **nouveau pour les vulnérabilités** pour déclencher manuellement une ServiceNow® analyse lancée. Pour en savoir plus sur la configuration d'un scanner de vulnérabilité, reportez-vous à la section Configurer et gérer Qualys les scanners et analyses de vulnérabilité.

   Pour une intégration de vulnérabilité Qualys, un scanner par défaut est préinstallé dans le module **Scanners de vulnérabilité** . Ce scanner est désactivé par défaut. Cochez les cases **Actif** et **Par défaut** pour activer le scanner Qualys afin qu'il utilise le lien connexe **Analyser les vulnérabilités** sur la tâche de rattrapage et les formulaires d'élément vulnérable.

   Le lien **connexe État de mise à jour** affiche la date et l'heure de la dernière mise à jour. Il déploie les informations des VI dans la tâche de rattrapage. Consultez Champs du formulaire de tâche de rattrapage pour plus d'informations. Lorsqu'une tâche est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

formée en fonction d'une vulnérabilité spécifique, cette vulnérabilité est répertoriée sur le formulaire de tâche de rattrapage.

Si vous ouvrez un élément vulnérable associé, toutes les entrées de tâche de rattrapage associées apparaissent sous l'onglet de liste connexe **Tâche de rattrapage** .

Ajouter des utilisateurs au groupe Vulnerability Response

Lorsque la fonctionnalité Fermer/Différer est utilisée pour différer ou fermer un élément vulnérable sans nécessiter d'analyse, le Réponse aux vulnérabilités groupe est notifié pour approuver ou rejeter la demande. Vous pouvez affecter les utilisateurs appropriés.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Groupes**.
2. Ouvrir le Réponse aux vulnérabilités groupe.
3. Cliquez sur la liste connexe **Membres du groupe** , puis cliquez sur **Modifier**.
4. Sélectionnez un ou plusieurs noms dans la liste **Collection** .
5. Cliquez sur **Ajouter**.
6. Cliquez sur **Enregistrer**.

Information associée

Créer un utilisateur

Gérer manuellement les éléments vulnérables individuels

Les éléments vulnérables représentent un élément de configuration (CI) avec une vulnérabilité donnée. Les éléments vulnérables sont importés à partir de sources tierces ou à l'aide des informations NVD SAM (lien) pour comparer les entrées de vulnérabilité aux enregistrements logiciels récupérés à partir du module Logiciel Gestion des actifs .

Les éléments vulnérables sont contenus dans les tâches de rattrapage définies par les règles de vulnérabilité. En règle générale, les tâches de rattrapage sont l'emplacement où les groupes d'éléments vulnérables sont affectés et traités.

Les éléments vulnérables peuvent être visualisés et modifiés en bloc à partir du module **Éléments vulnérables** . Les enregistrements d'éléments vulnérables affichent des informations issues de la vulnérabilité dans l'onglet **Vulnérabilité** . Cet onglet peut indiquer s'il existe des exploits publics ou actifs. En outre, il indique s'il peut être corrigé via un correctif, un changement de configuration ou une combinaison des deux. Si des adresses IP sont trouvées lors de la déduplication, elles apparaissent dans une liste connexe.

Si un CI est supprimé de la CMDB, tous les éléments vulnérables associés le sont également.

Lorsqu'un élément vulnérable est ajouté à une tâche de rattrapage, le groupe apparaît dans la liste des éléments vulnérables des **tâches de rattrapage** .

Lorsqu'une tâche affectant un élément vulnérable est créée, la tâche apparaît dans la liste connexe des **éléments vulnérables Tâches affectées** .

Les éléments vulnérables peuvent être créés manuellement. Vous pouvez créer des incidents de sécurité ou des demandes de changement et les fermer ou les différer manuellement. Les règles de tâche de rattrapage peuvent être appliquées aux éléments vulnérables créés manuellement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les tâches de rattrapage et les règles de tâche de rattrapage ont été améliorées pour prendre en charge la fonctionnalité de tâche. Les éléments vulnérables ne peuvent pas être liés en tant que tâche parente.

Créer des Réponse aux vulnérabilités éléments vulnérables

Plusieurs méthodes créent des éléments vulnérables (VI). Le plus souvent, une intégration à un scanner de vulnérabilité est installée et configurée pour importer les résultats tous les soirs. Dans certains cas, comme des vulnérabilités de sécurité physique, vous préférez peut-être ajouter manuellement des enregistrements d'éléments vulnérables.

Avant de commencer
Rôle requis : sn_vul.vulnerability_write

Pourquoi et quand exécuter cette tâche
Les VI que vous créez manuellement et les VI créés automatiquement sont automatiquement ajoutés et supprimés des tâches de rattrapage par les règles de tâche de rattrapage et les conditions de groupe.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Sélectionnez une catégorie pour ouvrir la liste.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire comme il convient.
   Pour en savoir plus sur les champs des éléments vulnérables, Réponse aux vulnérabilités Champs du formulaire d'élément vulnérablereportez-vous à .
5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.

   Les règles de tâche de rattrapage évaluent l'élément vulnérable et l'ajoutent à une tâche existante ou créent une nouvelle tâche. Si l'évaluation échoue, l'élément vulnérable est ajouté à la liste **des éléments vulnérables non groupés** .

   Lorsque vous enregistrez un nouvel élément vulnérable, tous les calculateurs activés s'exécutent.

   Remarque : Un seul calculateur par **champ cible** peut être actif à la fois. Lorsque vous en activez un, tous les autres avec le même **champ Cible** sont désactivés.

6. Vous pouvez cliquer sur l'une des listes connexes pour afficher des informations supplémentaires.

   Vous pouvez utiliser le lien connexe, Rechercher les **vulnérabilités** , pour déclencher manuellement une ServiceNow® analyse initiée. Pour en savoir plus sur la configuration d'un scanner de vulnérabilité, reportez-vous à la section Configurer et gérer Qualys les scanners et analyses de vulnérabilité.

   Pour une intégration de vulnérabilité Qualys, un scanner par défaut est préinstallé dans le module **Scanners de vulnérabilité** . Ce scanner est désactivé par défaut. Cochez les cases **Actif** et **Par défaut** pour activer le scanner Qualys afin qu'il utilise le lien connexe **Analyser les vulnérabilités** sur la tâche de rattrapage et les formulaires d'élément vulnérable.

   Les options de modification et de correction suivantes sont disponibles à partir de la barre d'en-tête :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Mettre à jour : enregistre les mises à jour du formulaire.
- Créer un incident de sécurité : crée un incident de sécurité.
- Fermer : ferme l'élément. Si tous les éléments de son groupe sont fermés, la tâche de rattrapage se ferme automatiquement.
- Demande d'exception : soumet une demande de report d'un élément.
- Résoudre : résout l'élément.
- Supprimer : supprime l'élément vulnérable.

Information associée

Modifier les éléments vulnérables en bloc dans Réponse aux vulnérabilités

Différer un élément vulnérable

Si vous déterminez que le problème associé à un élément vulnérable (VIT) présente un risque faible et peut être différé immédiatement sans analyse supplémentaire, vous pouvez utiliser la fonctionnalité **Différer** .

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Une tâche planifiée s'exécute tous les jours pour vérifier les éléments vulnérables différés qui ont atteint leur date de réouverture. Le jour où le report du VI doit expirer, l'enregistrement est rouvert.

À partir de la Réponse aux vulnérabilités version 20.0, avant de rouvrir un VI différé, la tâche planifiée `Vérifier l'expiration du report des éléments vulnérables et des groupes` vérifie si une règle d'exception est applicable sur un VI différé et met à jour les champs **Motif** et **Jusqu'à** conformément à la règle d'exception. L'état du VI reste Reporté jusqu'à la dernière date d'expiration.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Ouvrez un élément vulnérable.
3. Cliquez sur **Demander une exception**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Jusqu'à	Sélectionnez la date à laquelle l'état Différé expire et à laquelle la tâche de rattrapage est réactivée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : À partir de la version 18.0 de Réponse aux vulnérabilités (VR), si un élément vulnérable différé est fermé et rouvert par un scanner avant l'expiration de la fenêtre d'exception, l'état du VIT revient à l'état différé honorant la fenêtre d'exception active. Pour activer cette fonctionnalité, définissez la valeur de la propriété système sn_vul.auto_defer_vit_in_active_exception_window sur vrai. De plus, la date de fin différée persiste même après la fermeture de l'élément vulnérable ou l'expiration de l'exception. Le rôle requis est sn_vul.manage_exception_configuration pour la lecture et l'écriture. Une fois l'enregistrement soumis, si des notifications par e-mail sont définies, les membres du groupe reçoivent un e-mail lorsque la Réponse aux vulnérabilités date d'expiration est inférieure à une semaine. Lorsque la date de report expire, l'élément vulnérable est remis en état Ouvert et une deuxième notification par e-mail est envoyée.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Faux positif ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

Traduction automatique

5. Cliquez sur **Envoyer**.
   Le groupe est marqué **comme En cours de révision**. Un lien **connexe Rouvrir** s'affiche. La date et le motif de réouverture apparaissent dans les notes de travail sous l'onglet **Approbations de changement d'état** .

Demander une extension pour un élément vulnérable différé

Demandez une extension pour un élément vulnérable différé avant qu'il n'atteigne sa date de report jusqu'à l'échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche
Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités.

Procédure
1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Ouvrez un élément vulnérable différé.
3. Sélectionnez **Demande d'extension**.

> **Remarque :** Le bouton Demande d'extension n'est visible que lorsque l'état de l'élément vulnérable est Différé.

4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle l'élément vulnérable différé doit être prolongé pour le rattrapage.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Un e-mail est déclenché lors de l'envoi de la demande et de l'action ultérieure de l'approbateur.

> **Remarque :**
> ◦ La demande passe par deux niveaux d'approbation.
> ◦ Si une règle d'exception différée est à nouveau étendue, le nombre de reports prolongés augmente dans le back-end.

6. Une fois la demande approuvée, les notes Jusqu'à, Motif et Report sont mises à jour.

Actualiser Réponse aux vulnérabilités les éléments vulnérables
Le lien connexe **Mettre à jour l'état** permet d'inspecter les éléments vulnérables pour voir s'il existe d'autres éléments vulnérables qui appartiennent à une tâche de rattrapage. Utilisez-la si une mise à jour est justifiée en dehors de la tâche planifiée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_write ou, sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Le lien connexe **Mettre à jour le statut** est uniquement modifiable sur le formulaire de tâche de rattrapage dans les états **Ouvert** ou **En cours d'examen** , à l'aide d'un groupe de filtres ou lorsque le type de filtre est Condition. Cette inspection est effectuée quel que soit l'état de la case à cocher **Actualiser automatiquement les éléments vulnérables** .

À partir de la version 22.0 de , le bouton **Mettre à jour l'état** est disponible dans la vue d'enregistrement pour les tâches de Réponse aux vulnérabilitésrattrapage dans et Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Ouvrez n'importe quel enregistrement à l'état **Ouvert** ou **En cours d'examen** .
3. Cliquez sur le lien **Mettre à jour le statut** .
   De nouveaux éléments vulnérables apparaissent sous l'onglet **Éléments vulnérables** .

Identifier et escalader les problèmes de sécurité dans les logiciels tiers

Vous pouvez afficher les vulnérabilités logicielles renvoyées par des entrées tierces pour déterminer la correction. Utilisez ces informations pour faire correspondre les entrées de logiciel vulnérables à un modèle de détection de logiciels Gestion des actifs .

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Bibliothèques** > **Tierce partie**.
   Une liste des logiciels vulnérables téléchargés s'affiche.
2. Cliquez sur un enregistrement logiciel pour afficher les informations sur les vulnérabilités.
3. Cliquez sur les listes connexes suivantes pour obtenir plus d'informations sur l'identification des vulnérabilités.

Liste connexe	Description
Éléments vulnérables	Répertorie tous les éléments vulnérables, qui consistent en des appariements d'un élément de configuration potentiellement vulnérable et d'un logiciel. Pour obtenir plus

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Description
	d'informations sur un appairage, cliquez sur l'icône d'informations ( ). **Remarque :** Si le logiciel est supprimé, tous les éléments vulnérables associés sont fermés et supprimés de la liste connexe des **éléments vulnérables** .
Entrées de vulnérabilité	Répertorie les entrées de vulnérabilité pour l'enregistrement logiciel sélectionné. Cliquez sur un enregistrement pour en afficher les détails.

Si des vulnérabilités ont été identifiées et que des éléments vulnérables ont été créés, vous pouvez Résoudre les tâches de rattrapage, selon les besoins.

Identifier et escalader les problèmes de sécurité à l'aide de NVD

Lorsque les enregistrements de l'identificateur commun de vulnérabilité et d'exposition (CVE-ID) sont téléchargés à partir de la Base de données de vulnérabilité nationale (NVD), ils sont comparés aux logiciels de votre réseau d'entreprise tels qu'identifiés par le modèle de détection des actifs logiciels. Lorsqu'un CVE-ID correspond à un logiciel ou à un élément de configuration vulnérable de votre réseau, un élément vulnérable est créé. Vous utilisez les informations de l'enregistrement CVE-ID pour décider s'il convient d'escalader l'élément vulnérable à des fins de correction.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Bibliothèques** > **NVD**.
   Une liste des CVE-ID qui ont été téléchargés à partir du NVD s'affiche. Les mises à jour à partir du NVD peuvent être effectuées à la demande et par exécutions planifiées à partir des enregistrements d'intégration de la base de données des vulnérabilités nationale NIST situés à **Tout** > **Administration** > **Intégrations**.
2. Cliquez sur un enregistrement CVE pour afficher les informations suivantes :
   - un résumé pour le CVE-ID.
   - une référence à une entrée Common Weakness Enumeration (CWE), le cas échéant.
   - le score de vulnérabilité du CVE-ID sur le système commun de notation des vulnérabilités (CVSS). Pour plus d'informations sur le CVSS, consultez le site Web de la Base de données nationale sur les vulnérabilités .
3. Cliquez sur les listes connexes pour plus d'informations sur les vulnérabilités.

   Références de vulnérabilité

   Nom, description et URL de la vulnérabilité donnée et où elle est référencée.

   Exploite

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails.

Faiblesses

Liste des faiblesses de CWE.

4. Cliquez sur les listes connexes suivantes pour obtenir plus d'informations sur l'identification des vulnérabilités.

Liste connexe	Description
Éléments vulnérables	Répertorie tous les éléments vulnérables, qui consistent en des appariements d'un élément de configuration potentiellement vulnérable et d'un logiciel. Pour obtenir plus d'informations sur un appairage, cliquez sur l'icône d'informations ( ). **Remarque :** Si le logiciel est supprimé, tous les éléments vulnérables associés sont fermés et supprimés de la liste connexe des **éléments vulnérables** .
Entrées de vulnérabilité	Répertorie les entrées de vulnérabilité pour l'enregistrement logiciel sélectionné. Cliquez sur un enregistrement pour en afficher les détails.

Si des vulnérabilités ont été identifiées et que des éléments vulnérables ont été créés, vous pouvez Résoudre les tâches de rattrapage, selon les besoins.

Identifier et escalader les problèmes de sécurité à l'aide de CWE

Consultez la bibliothèque des enregistrements Common Weakness Enumeration (CWE) de la Base de données de vulnérabilité nationale (NVD) pour comprendre comment ils sont liés aux enregistrements Common Vulnerability and Exposure (CVE). Utilisez ensuite ces informations pour faire correspondre les entrées de logiciel vulnérables à un modèle de détection de logiciels Gestion des actifs .

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Bibliothèques** > **CWE**.
   Une liste des logiciels vulnérables téléchargés s'affiche.
2. Cliquez sur un enregistrement logiciel CWE pour afficher les informations de vulnérabilité.
3. Cliquez sur les listes connexes suivantes pour obtenir plus d'informations sur l'identification des vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Description
Éléments vulnérables	Répertorie tous les éléments vulnérables, qui consistent en des appariements d'un élément de configuration potentiellement vulnérable et d'un logiciel. Pour obtenir plus d'informations sur un appairage, cliquez sur l'icône d'informations ( ). **Remarque :** Si le logiciel est supprimé, tous les éléments vulnérables associés sont fermés et supprimés de la liste connexe des **éléments vulnérables** .
Entrées de vulnérabilité	Répertorie les entrées de vulnérabilité pour l'enregistrement logiciel sélectionné. Cliquez sur un enregistrement pour en afficher les détails.

Si des vulnérabilités ont été identifiées et que des éléments vulnérables ont été créés, vous pouvez Résoudre les tâches de rattrapage, selon les besoins.

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

Lorsqu'un élément vulnérable a presque atteint (ou dépassé) sa date cible de rattrapage, telle que définie par une règle de cible de rattrapage, l'enregistrement d'élément vulnérable est mis à jour avec un état. Ces informations peuvent aider l'analyste à surveiller de manière proactive les activités de rattrapage à venir.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_admin
- sn_vul.read_remediation_target_rules [lecture seule]

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Une tâche planifiée appelée **Évaluer les cibles de rattrapage** s'exécute une fois par jour pour comparer la date actuelle à la date de rattrapage de l'élément vulnérable spécifiée dans la règle de cible de rattrapage associée. Lorsque la date actuelle tombe dans le nombre de jours avant que le rattrapage ne soit échu, un état de rattrapage est ajouté à l'enregistrement d'élément vulnérable.

Pour en savoir plus sur les règles de cibles de rattrapage, reportez-vous à Réponse aux vulnérabilités Règles de cibles de rattrapage.

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Éléments vulnérables**.
2. Cliquez sur l'élément vulnérable que vous souhaitez examiner.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si la date de rattrapage de l'élément vulnérable se situe dans la plage des conditions définies dans la règle de la cible de rattrapage, l'onglet État de la **cible de rattrapage** est visible.

3. Cliquez sur l'onglet **État de la cible de rattrapage** .
4. Cliquez sur l'enregistrement de l'état de la cible de rattrapage pour l'examiner.

> **Remarque :** Pour afficher le nombre d'éléments vulnérables qui approchent de la cible, en cours et qui ont dépassé la cible, reportez-vous à Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.

Information associée

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

Utilisation de CI sans correspondance

En tant que responsable et analyste des vulnérabilités, vous pouvez afficher et reclasser les éléments de configuration (CI) sans correspondance, rapprocher les éléments détectés sans correspondance, réappliquer des règles de recherche de CI sur les éléments détectés sélectionnés et dédupliquer les CI existants.

Afficher et reclasser des éléments de configuration sans correspondance

Les éléments de configuration (CI) qui ne se trouvent pas dans le Base de données de gestion des configurations (CMDB) sont placés dans une liste consultable des éléments détectés. Cette liste offre un moyen pratique de reclasser les CI sans correspondance.

Avant de commencer

Rôle requis :
sn_vul.read (minimum pour afficher les CI sans correspondance)

et

ITIL ou actif (à reclasser)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

En tant qu'analyste de vulnérabilité, vous pouvez afficher les CI sans correspondance.

L'action reclassifier n'est disponible que sur *sn_sec_cmn_unmatched_ci* les CI de classe, lorsque vous disposez du rôle itil ou actif. Une fois qu'un CI a été reclassé, il ne peut pas l'être à l'aide de l'interface utilisateur. Vous pouvez reclasser, à partir du formulaire CI ou de la vue de liste CI, en modifiant la valeur de la **classe** . Pour en savoir plus, consultez Reclassifier un CI .

Procédure

1. Accédez à la **Tout** > **Security Operations** > **CMDB** > **Éléments détectés**.
2. Pour passer en revue, cliquez sur chaque élément.
3. Pour apporter des corrections aux informations contenues dans les champs du formulaire **Élément détecté** , modifiez cette page et cliquez avec le bouton droit sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Toutes les données ajoutées ou laissées dans ces champs sont transférées vers **l'élément de configuration** résultant lorsqu'il est reclassé.

4. Si tout semble correct, cliquez sur **Reclasser**.
5. Dans la liste de choix, sélectionnez un **nom de classe** et cliquez sur **Soumettre**.
   La **classed'élément détecté** est mise à jour, le champ **État** est changé en Reclassé et toutes les données se trouvent dans la CMDB.

Rapprocher les éléments détectés sans correspondance

Créez une tâche planifiée pour rapprocher les éléments détectés sans correspondance.

Avant de commencer

Rôles requis : admin

Pourquoi et quand exécuter cette tâche

Un élément vulnérable (VI) se compose d'une vulnérabilité et d'un élément de configuration (CI). Lorsqu'un VI est créé, le CI qui y est ajouté au moment de la création peut être obsolète. Les informations de CI sans correspondance ne sont pas rapprochées si les informations contenues dans la CMDB changent. Pour le rapprochement, appliquez des règles de recherche d'éléments de configuration (CI) sur les éléments qui sont dans un état sans correspondance lorsque la CMDB est mise à jour avec les derniers CI.

Vous pouvez exécuter une demande de tâche planifiée afin de réappliquer la règle de correspondance CI pour les éléments détectés dans un état sans correspondance. Si le CI change après réapplication des règles de recherche, les éléments détectés sont mis à jour avec le nouveau CI. Les détections impactées et les éléments vulnérables sont également mis à jour. Pour plus de détails, voir Changements de CI pour les éléments détectés.

Procédure

1. Accédez à la **Tout** > **Security Operations > rapprocher les éléments détectés sans correspondance**.
2. Sur la page Tâches en arrière-plan, cliquez sur **Créer une tâche de rapprochement**.
3. Renseignez les champs du formulaire.

Remarque : Vous ne pouvez modifier que le champ **Paramètres** .

Formulaire de tâche en arrière-plan

Champ	Description
Numéro	Numéro de tâche unique.
Créé par	Utilisateur qui a créé la tâche.
Paramètres	Paramètres permettant de rapprocher les éléments détectés sans correspondance : ◦ limit : nombre maximal d'éléments détectés à rapprocher. Si vous ne saisissez pas de valeur, 10 000 éléments détectés sont rapprochés. ◦ firstDiscovereditem : premier élément détecté qui doit être rapproché. Si vous ne saisissez pas de valeur, le processus de rapprochement commence à partir du premier élément détecté.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
État	État actuel de la tâche en arrière-plan.
Description d'état	Description de l'état actuel de la tâche en arrière-plan.
Type de tâche	Type d'emploi. La valeur est **Rapprocher les éléments détectés sans correspondance**.
Démarré à	Heure de début de la tâche.
Heure de fin	Heure à laquelle la tâche a été terminée.
Durée de la tâche	Temps total nécessaire à l'achèvement de la tâche.
Sous-état	Sous-état de l'état sélectionné.
Notes	Nombre d'enregistrements qui ont été traités.

4. Cliquez sur **Envoyer**.

Remarque :

- Pour arrêter l'exécution de la tâche, cliquez sur **Annuler**.
- Vous ne pouvez pas rapprocher les CI sans correspondance ni réappliquer des règles de recherche de CI pendant que vous importez des hôtes ou des éléments vulnérables.

Réappliquer des règles de recherche de CI sur les éléments détectés sélectionnés

Réappliquez les règles de recherche d'éléments de configuration (CI) sur les éléments détectés sélectionnés à partir des actions de sélection de la vue de liste des éléments détectés. Si le CI change après que vous avez réappliqué les règles, les éléments détectés sont mis à jour avec le nouveau CI et les détections impactées. Les éléments vulnérables sont également mis à jour.

Avant de commencer

Rôles requis : admin

Pourquoi et quand exécuter cette tâche

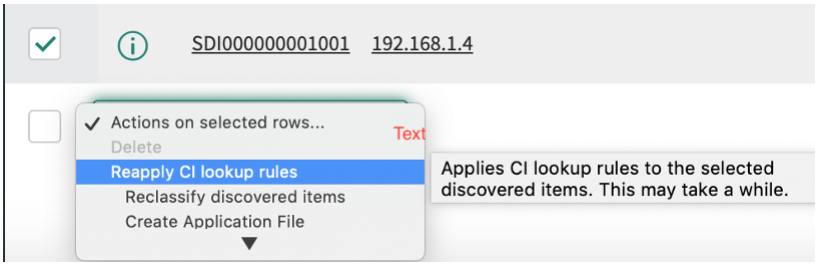
Pour plus d'informations, consultez Changements de CI pour les éléments détectés.

Pour plus d'informations sur les concepts de correspondance CI et CMDB, de recherche d'éléments détectés, d'identification basée sur des règles et d'autres informations détaillées sur le fonctionnement de la correspondance CI, consultez l'article Correspondance CI dans Vulnerability Response [KB0998706] dans la base de connaissances HI.

Procédure

1. Accédez à la **Tout** > **Opérations de sécurité** > **CMDB** > **Éléments détectés**.
2. Sélectionnez les éléments détectés requis et cliquez sur **Action sur les lignes sélectionnées**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans la liste, sélectionnez **Réappliquer les règles de recherche de CI**.

   Les règles sont réappliquées sur ces éléments détectés.

4. Cliquez sur **Afficher l'état** dans le message.

   L'état s'affiche sur le formulaire de tâche en arrière-plan.

   Remarque : Dans le champ **Notes** , les `éléments détectés n'ont pas pu être traités en raison d'une` exception attribut avec une valeur non nulle qui indique qu'une erreur ou une exception se produit lors de la réapplication d'une règle de recherche de CI. Consultez les journaux système pour en savoir plus.

Étapes pour empêcher les enregistrements en double ou orphelins après l'exécution de Réponse aux vulnérabilités règles de recherche de CI

Prenez des mesures pour empêcher les enregistrements en double ou orphelins résultant de la mise en correspondance (éléments de configuration (CI) dans le CMDBfichier .

L'importation de données de vulnérabilité peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas soigneusement construites. La logique utilisée pour itérer et effectuer une correspondance au sein de la CMDB peut entraîner de longs délais de traitement. Des tests et un débogage approfondis des scripts de traitement dans les règles permettent d'atténuer le risque de problèmes ultérieurs au cours du processus.

Empêcher les enregistrements en double ou orphelins

- Utilisez de petits sous-ensembles de données spécifiques à la règle de recherche de CI testée.
  - Définissez toutes les règles de recherche de CI, autres que celle testée, sur Inactive.
  - Analysez les CI importés pour vous assurer que vous observez le comportement attendu et que la correspondance se produit correctement.
- Examiner les CI correspondants
  - Examinez le nombre de CI correspondants par rapport aux CI sans correspondance. Assurez-vous que le pourcentage est acceptable. Ne vous contentez pas de regarder la première page, c'est probablement la première insérée.
  - Recherchez manuellement certains CI.
  - Vérifiez s'il existe des problèmes de nom ou de champ (tels que la recherche d'un domaine spécifique).

    Si cela vous semble approprié, ajoutez des règles de correspondance supplémentaires.
- Examiner les CI sans correspondance
  - Accédez à la table CI sans correspondance.
  - Grouper par classe d'élément de configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

    - Examinez toutes les classes qui ne semblent pas correctes (certificats, cartes réseau, images).
        - Déterminez pourquoi ils ne correspondaient pas au CI approprié ?
        - La classe doit-elle être exclue ?
        - La classe doit-elle être élevée à une classe connexe ?
- Examinez les états du CI tels que **Mis hors service**.
- Supprimer les données de test
    - Une fois que vous commencez à observer le comportement correct ou attendu dans la correspondance CI, recommencez.
    - Recommencer par : Suppression des données utilisées pour les tests : (voir la section **Suppression des données des tables**)
        - Éléments détectés
        - Éléments vulnérables
        - Tâches de rattrapage
    - Réexécution manuelle de toutes les règles de correspondance des CI.

Pour plus d'informations sur les règles de recherche de CI et Qualys, consultez l'article KB0750656 .

Pour plus d'informations sur les règles de recherche de CI et Rapid7, consultez le KB0818096 .

Suppression des données des tables

Parfois, vous avez importé des données et vous vous rendez compte que quelque chose ne va pas. Si quelque chose ne va pas dans un environnement de développement ou de performance, vous pouvez vous retirer d'un meilleur environnement, mais ce n'est pas toujours une option.

Remarque : La réalisation de ces actions nécessite une ServiceNow expertise.

Il existe quatre options pour supprimer les données des tables :

- Utilisation de **Supprimer tous les enregistrements** sur **la configuration de table**.
- Configurez le **nettoyeur de table** en accédant à **Purges automatiques** (sys_auto_flush.list) et en créant un nouvel enregistrement **de vidage automatique** .
- Tronquez la gs.truncateTable à l'aide d'un script en arrière-plan.

  L'utilisation *truncateTable* nécessite de désactiver la case à cocher Enregistrement pour la restauration dans les scripts en arrière-plan. Dans le cas contraire, une copie de la table et des tables en cascade connexes est créée, prend trop de temps et risque d'échouer.

  Remarque : Ne jamais utiliser *truncateTable* dans un environnement de production. Consultez votre représentant du support avant d'exécuter des suppressions importantes dans des environnements de production ou partagés.

Déduplication d'éléments de configuration existants

Chaque fois que des éléments de configuration (CI) sont mis à jour via une tâche de déduplication, les éléments détectés (DI) associés à ces CI sont également mis à jour. Les éléments vulnérables (VI) et les détections sont également mis à jour avec le CI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations, consultez Changements de CI pour les éléments détectés.

Information associée

Corriger une tâche de déduplication

Résoudre les tâches de rattrapage

La flexibilité inhérente à vous permet de corriger les vulnérabilités de la manière qui Réponse aux vulnérabilités convient le mieux à votre organisation de sécurité.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche

Une fois que vous êtes informé qu'une demande de changement est résolue, passez l'état de la tâche de rattrapage sur Résolu et attendez la prochaine analyse. Les nouvelles analyses sont déclenchées automatiquement par le calendrier d'importation tierce configuré dans l'assistant de configuration.

Remarque :

Si la synchronisation d'état est activée, les tâches de rattrapage passent automatiquement à l'état Résolu après l'implémentation d'une demande de changement associée à une tâche de rattrapage (VUL) et à l'état Réviser. Consultez Gestion des changements pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de rattrapage** > **Mes affectations**.
2. Cliquez sur un enregistrement à l'état Ouvert.

   L'état Ouvert indique que l'enregistrement n'a pas encore été traité. Le formulaire s'affiche :

   - Informations sur la tâche de rattrapage
   - Détails de la configuration des groupes
   - Notes
   - Éléments vulnérables associés
   - SLA de tâche
   - Demandes de changement
3. Effectuez votre analyse du groupe.
4. Lorsque vous êtes prêt à commencer à travailler sur l'enregistrement, choisissez l'une des options suivantes.

Option	Description
Si l'élément vulnérable présente un risque pour votre environnement informatique, créez un enregistrement CHG et escaladez le problème à l'équipe Gestion des changements .	Affectez le groupe au groupe ou à la personne approprié, puis cliquez sur **Créer un changement**.
Si l'élément vulnérable pose un risque de sécurité potentiel pour votre organisation, créez un enregistrement d'incident de sé-	Cliquez sur **Créer un incident de sécurité**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
curité et escaladez le problème à l'équipe Réponse aux incidents de sécurité .	Ce bouton n'est affiché que lorsque Réponse aux incidents de sécurité est activé. Un calcul d'impact sur l'entreprise est appliqué, l'incident est affecté et l'incident de sécurité est créé.

Une fois que vous avez créé une demande de changement, l'enregistrement approprié apparaît dans la liste connexe **Demandes de changement** sur le formulaire Groupe de vulnérabilité.

5. Si vous déterminez que le problème présente un risque faible et qu'il peut être reporté, cliquez sur **Demande d'exception**.
   Pour en savoir plus sur le report d'une tâche de rattrapage, reportez-vous à Différer une tâche de rattrapage.
6. Si vous déterminez que le problème peut être fermé immédiatement sans autre analyse, cliquez sur **Fermer**.
   Pour en savoir plus sur la fermeture d'une tâche de rattrapage, reportez-vous à Fermer une tâche de rattrapage. À partir de la version 23.0 de , le bouton **Fermer** a été supprimé pour une tâche de Réponse aux vulnérabilitéscorrection.

   Une tâche planifiée d'intégration tierce met à jour et analyse automatiquement les enregistrements à un intervalle défini. Les éléments vulnérables sont analysés à la date et à l'heure planifiées suivantes. Vous pouvez également lancer manuellement une analyse des vulnérabilités à l'aide du lien **connexe Rechercher les vulnérabilités** .

   Si l'analyse détecte à nouveau la vulnérabilité sur l'élément de configuration et ne le marque pas comme Corrigé, l'élément vulnérable revient à l'état En cours d'examen. Contactez les opérations informatiques pour rouvrir la demande de changement.

   Si l'analyse ne trouve pas la vulnérabilité et renvoie que l'élément vulnérable a été marqué comme Corrigé, l'élément vulnérable passe à l'état Fermé-Fixe et est fermé pendant l'importation.

   Ce n'est que lorsque tous les éléments vulnérables d'une tâche sont à l'état Fermé-Résolu que la tâche de rattrapage se ferme automatiquement. Les tâches de rattrapage avec des éléments vulnérables à l'état Fermé autre que Fixe doivent être fermées manuellement.

Différer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage (VUL) n'est pas une priorité et qu'il peut être différé immédiatement sans analyse supplémentaire, vous pouvez utiliser la fonctionnalité **Demande d'exception** .

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche

Vous pouvez différer une tâche de rattrapage à partir d'un enregistrement de tâche de rattrapage dans les Réponse aux vulnérabilités espaces de travail. Une fois que vous avez soumis la demande, elle est envoyée pour approbation. Consultez Demander une exception dans le Espace de travail de remédiation IT.

Une tâche planifiée s'exécute tous les jours pour vérifier les tâches de rattrapage différées qui ont atteint leur date de réouverture. Le jour où le report de la tâche doit expirer, la tâche est rouverte.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre dans leurs enregistrements respectifs sur leurs enregistrements respectifs lorsque la synchronisation d'état est activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement les tâches de rattrapage des états Fermé ou Différé.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Ouvrez un enregistrement.
3. Cliquez sur **Demander une exception**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Jusqu'à	Sélectionnez la date à laquelle l'état Différer expire et à laquelle la tâche de rattrapage est réactivée. Une fois l'enregistrement soumis, si des notifications par e-mail sont définies, les membres du groupe reçoivent un e-mail lorsque la Réponse aux vulnérabilités date d'expiration est inférieure à une semaine. Lorsque la date de report expire, la tâche de rattrapage est redéfinie sur **Ouvert** et une deuxième notification par e-mail est envoyée.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Faux positif ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

5. Cliquez sur **Envoyer**.
   Le groupe est marqué comme En cours de révision. Un lien **connexe Rouvrir** s'affiche. La date et le motif de réouverture apparaissent dans les notes de travail sous l'onglet **Approbations de changement d'état** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander une extension pour une tâche de rattrapage différée

Demandez une prolongation pour une tâche de rattrapage différée (VUL) avant qu'elle n'atteigne sa date de report jusqu'à l'échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Ouvrez une tâche de rattrapage différée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date à laquelle l'état Différer expire et à laquelle la tâche de rattrapage est réactivée.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les changements de la tâche de rattrapage sont également étendus aux éléments vulnérables, qui font partie de la tâche de rattrapage. Toutefois, les éléments vulnérables doivent être dans l'état Différé et leur date actuelle jusqu'à ce que les données précèdent la date de fin de mise à jour. Un e-mail est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

également déclenché lors de la soumission de la demande et de l'action ultérieure de l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une tâche de rattrapage différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

Fermer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage peut être fermé immédiatement sans autre analyse, vous pouvez utiliser la fonctionnalité **Fermer** . À partir de la version 23.0 de , le bouton **Fermer** a été supprimé pour une tâche de Réponse aux vulnérabilitésrattrapage et la fermeture d'une tâche de rattrapage est pilotée par le scanner.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Dans les Réponse aux vulnérabilités espaces de travail, une tâche de rattrapage passe par les mêmes états qu'une tâche de rattrapage antérieure dans les versions précédentes de Réponse aux vulnérabilités. Lorsque tous les éléments vulnérables (VIT) d'une tâche de rattrapage sont fermés, la tâche de rattrapage passe à l'état Inactif.

Important : Vous pouvez déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre dans leurs enregistrements respectifs sur leurs enregistrements respectifs lorsque la synchronisation d'état est activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement les tâches de rattrapage des états `Fermé` ou `Différé` .

Procédure

1. Ouvrez l'enregistrement pour lequel vous souhaitez demander une révision.
2. Sélectionnez le bouton **Fermer/Différer** .
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
État	Sélectionnez un état. Les choix possibles sont les suivants : ◦ Différé ◦ Fermé
Jusqu'à	Disponible uniquement dans la fenêtre contextuelle **État différer** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Sélectionnez la date à laquelle l'état **Différer** expire et à laquelle la tâche de rattrapage est réactivée. Une fois l'enregistrement soumis, si des notifications par e-mail sont définies, les membres du groupe reçoivent un e-mail lorsque la Réponse aux vulnérabilités date d'expiration est inférieure à une semaine. Lorsque la date de report expire, l'élément vulnérable est remis en **état Ouvert** et une deuxième notification par e-mail est envoyée.
Motif	Entrez le motif de la fermeture du problème.
Information supplémentaire	Saisissez toute autre information pertinente.

4. Sélectionnez **Soumettre**.
   La tâche de rattrapage est **marquée comme fermée**.

Identification des éléments vulnérables en double à partir de plusieurs scanners

Si vous utilisez plusieurs analyseurs sur le même actif pour détecter les vulnérabilités, plusieurs éléments vulnérables (VI) peuvent être créés. Vous pouvez identifier ces VI en double pour vous assurer que les vulnérabilités en double ne sont pas affectées aux propriétaires du rattrapage.

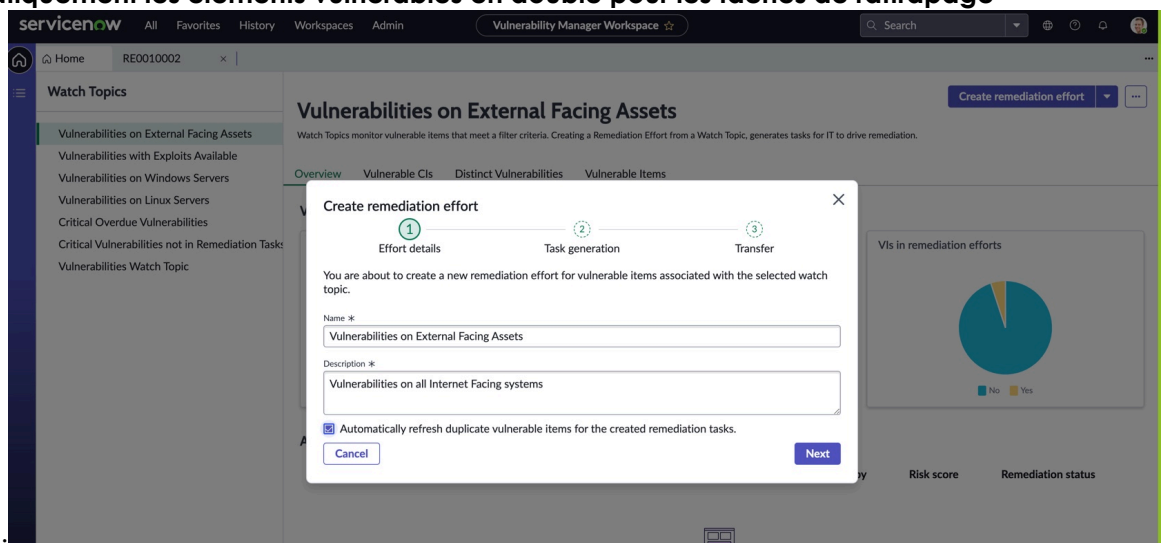
Cette résolution n'est possible que si les mêmes vulnérabilités, telles que les mêmes vulnérabilités et expositions communes (CVE) sont détectées. La combinaison de vulnérabilité dépend des scanners utilisés. Par exemple, Qualys et Tenable ont leur propre type de vulnérabilité, c'est-à-dire des entrées tierces (TPE), et d'autres scanners tels que Microsoft Defender for Endpoint détectent les vulnérabilités basées sur les CVE.

À partir de la version 17.1, lors de la création d'un effort de rattrapage, vous pouvez actualiser automatiquement les éléments vulnérables en double sur les tâches de rattrapage créées. Pour actualiser automatiquement les éléments vulnérables en double, vous devez sélectionner l'option **Actualiser**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

automatiquement les éléments vulnérables en double pour les tâches de rattrapage créées .



Afficher les VI en double : identifiez les éléments vulnérables en double signalés par plusieurs scanners dans le système. Vous pouvez marquer le VI en double comme Résolu. Pour en savoir plus, reportez-vous Résolvez automatiquement les vulnérabilités en doubleà . Les entrées en double ne sont affichées que lorsque la combinaison de vulnérabilités est créée à l'aide de CVE. Pour plus d'informations, consultez États de la tâche de rattrapage et des éléments vulnérables de Vulnerability Response.

Des doublons potentiels sont identifiés pour les combinaisons de vulnérabilités suivantes :

Combinaison de scanners	Type de vulnérabilité
Scanner 1 et Scanner 2	CVE
Scanner 1 et Scanner 2	CVE et TPE

Résolvez automatiquement les vulnérabilités en double

À partir de Réponse aux vulnérabilités (VR) v17.1, vous pouvez résoudre automatiquement toutes les vulnérabilités en double sur un actif.

Lorsqu'un actif est analysé avec plusieurs scanners, il est possible d'identifier la même vulnérabilité sous forme de doublons par les différents scanners. Par exemple, si les scanners Qualys et Microsoft identifient la même vulnérabilité, vous pouvez choisir de résoudre automatiquement la vulnérabilité en double.

Exemple de scénario

VR crée un enregistrement, VI1, pour la vulnérabilité 1 à partir du scanner Microsoft Defender for Endpoint. Un deuxième enregistrement, VI2, est créé à partir de l'analyseur Qualys pour la même vulnérabilité. L'équipe de rattrapage applique les correctifs susceptibles de résoudre les enregistrements VI1 et VI2. Si vous configurez le calendrier d'analyse Qualys au-delà d'une journée, à ce moment-là, Microsoft Defender fournit les informations de vulnérabilité corrigées et VR ferme l'enregistrement VI1 comme Fermé/Corrigé.

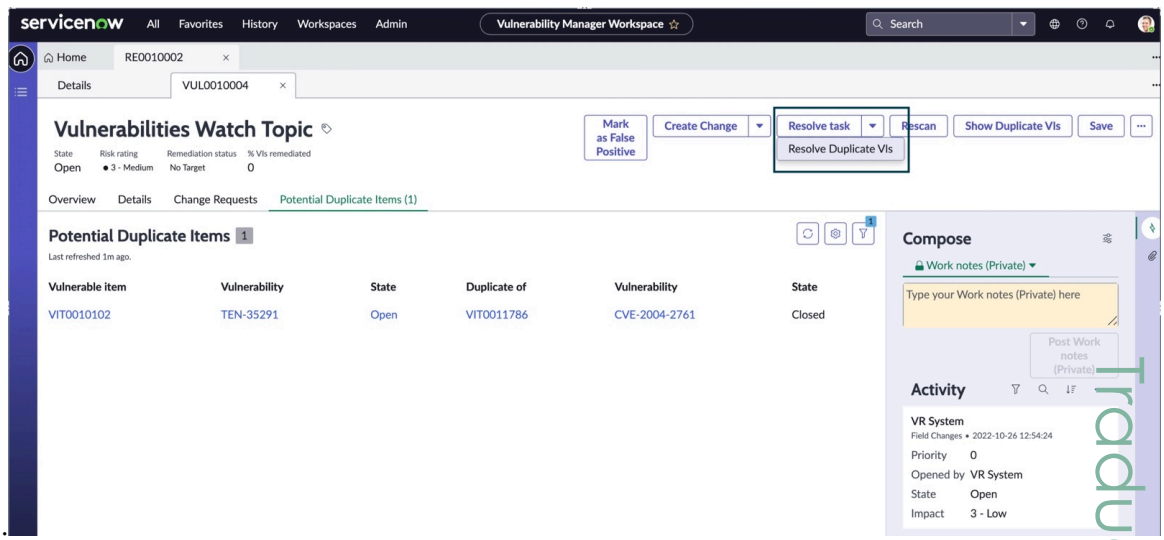
Dans ce scénario, l'enregistrement VI2 est toujours à l'état Ouvert et VR attend les résultats de l'analyse Qualys. Dans ce cas, les enregistrements de VI du deuxième scanner restent à l'état Ouvert même si le correctif est appliqué et que le VI est confirmé comme corrigé par l'autre scanner.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour remédier à cette situation, vous pouvez envisager de résoudre l'enregistrement de vulnérabilité en double à condition que la vulnérabilité soit fermée par le premier scanner.

Résolvez les vulnérabilités de la manière suivante :

- Sur demande : sélectionnez l'action d'interface utilisateur **Résoudre les VI en double** sur la tâche de rattrapage.



- Automatisé : activez la propriété système `sn_vul.auto_resolve_duplicate_vit` pour résoudre automatiquement les éléments vulnérables en double. La tâche planifiée quotidienne « Actualiser et résoudre les VIT en double sur la tâche de rattrapage » actualise automatiquement les éléments en double.

Les VI en double sont alors marqués comme résolus.

Remarque : L'enregistrement d'élément de vulnérabilité résolu est rouvert si le scanner l'identifie comme **Non réparé**.

Créer et modifier un groupe de classification

Créez des groupes afin que les règles sous-jacentes de ce groupe puissent classer les enregistrements de table en fonction des conditions. Les règles peuvent être utilisées pour sélectionner n'importe quel champ dans la table correspondante.

Avant de commencer

Rôle requis : sn_vul.manage_classification_rule

Procédure

1. Accédez à la table Propriétés système.
2. Dans la *sn_sec_cmn.classificationTables* propriété système, ajoutez le nom de la table pour laquelle vous souhaitez créer le groupe de classification.
3. Créez une nouvelle règle métier en ajoutant l'extrait de code suivant à la règle métier sur la table définie dans le groupe :

```
var classificationCalc = nouveau sn_vul.
CalculateurVulnérabilité(actuel,vrai,faux,'sn_vul_classification_group','sn_vul_classi
classificationCalc.calculer() ;
```

Remarque : Des règles métier sont fournies pour exécuter la classification pendant l'ingestion pour les tables Éléments détectés et Entrée de vulnérabilité. Pour les autres tables, vous devez ajouter les règles métier afin d'avoir les règles de classification sur l'ingestion.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles de classification**.
5. Dans le menu contextuel Groupes de classification, cliquez sur **Nouveau**.
6. Renseignez les champs du formulaire.

Formulaire Groupe de classification de vulnérabilité

Champ	Description
Nom	Nom du nouveau groupe de classification.
Actif	Option permettant d'activer le groupe.
Description	Description du nouveau groupe de classification.
Table	Table sur laquelle les règles sont exécutées. **Remarque :** Le système de base de Vulnerability Response comprend des groupes de classification pour les éléments détectés et les vulnérabilités.

Créer et modifier une règle de classification

Créez des règles pour classer automatiquement les vulnérabilités entrantes aux équipes appropriées pour la correction.

Avant de commencer

Rôle requis : sn_vul.manage_classification_rule

Pourquoi et quand exécuter cette tâche

Lorsqu'elles sont créées, ces règles classent les vulnérabilités comme appartenant à une plateforme ou à une application. Vous pouvez configurer ces règles pour remplacer la valeur d'un champ spécifique dans l'entrée de vulnérabilité.
Utilisez ces règles pour déplacer le calcul en amont vers la table Entrée des vulnérabilités tierces afin d'activer la réutilisation du contenu.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles de classification**.
2. Pour afficher un groupe de classification, cliquez sur ce groupe.
3. Dans le menu contextuel Règles de classification, cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire.

Formulaire Règle de classification de vulnérabilité

Champ	Description
Nom	Nom de la nouvelle règle de classification.
Actif	Option permettant d'activer la règle.
Description	Description de la nouvelle règle de classification.
Ordre d'exécution	Ordre dans lequel la règle doit être exécutée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Vue avancée	Option permettant d'afficher des champs supplémentaires sur les sections à onglets.
Quand cette condition est remplie	
Type de condition	Type de condition pour la règle. Les choix sont les suivants : ◦ **Filtre** : conditions de filtre de base permettant de déterminer s'il faut utiliser la règle ou non. ◦ **Groupe de filtres** : ensemble de plusieurs conditions utilisées ensemble. La règle est évaluée en fonction des conditions définies dans le groupe de filtres. ◦ **Script** : condition de script utilisée pour déterminer quand appliquer cette règle. Ce champ s'affiche uniquement lorsque l'option **Vue avancée** est sélectionnée.
Condition	Condition de la règle. Définissez les conditions en fonction de la colonne sélectionnée dans la colonne d'entrée de vulnérabilité requise. Vous pouvez ajouter plusieurs conditions pour affiner la règle. Ce champ s'affiche uniquement lorsque **l'option Filtre** est sélectionnée dans le champ **Type de condition** . **Remarque :** Lors de la définition de plusieurs conditions ou modèles, vous pouvez sélectionner uniquement parmi une table parente et une table enfant. Vous ne pouvez pas effectuer votre sélection parmi deux tables enfants ou plus.
Groupe de filtres	Groupe de filtres. Le groupe est défini lorsqu'un ensemble de conditions est utilisé de manière répétée à plusieurs endroits. Cliquez sur la recherche à l'aide de l'icône de liste ( ) pour sélectionner le groupe de filtres. Pour plus d'informations, consultez Créer et définir des groupes de filtres dans Security Operations. Ce champ s'affiche uniquement lorsque le **groupe de filtres** est sélectionné dans le champ **Type de condition** .
Script	Script évalué pour déterminer quand appliquer cette règle. Vous pouvez écrire votre code et définir la réponse sur vrai ou faux. Ce champ s'affiche uniquement

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	lorsqu'un script est sélectionné dans le champ **Type de condition**
Définir ces valeurs	
Classification	Classification de la règle. Pour sélectionner une option, cliquez sur l'icône d'ampoule (icône). La liste affiche les options de plateforme et d'application. Vous pouvez également entrer votre propre classification qui n'est pas dans la liste.
Type de classification	Type de classification. Ce champ affiche la liste filtrée des types de classification en fonction de la valeur que vous avez sélectionnée pour le champ **Classification** .
Type de valeur	Type de la valeur affectée à l'aide de cette règle. Les choix sont les suivants : ◦ **Modèle** : sélectionnez un modèle. Vous pouvez utiliser un modèle requis. ◦ **Script** : sélectionnez un script préexistant ou écrivez votre propre script personnalisé. Ce champ s'affiche uniquement lorsque l'option **Vue avancée** est sélectionnée.
Modèle	Autre condition pour la règle en dehors des champs **Classification** et **Type de classification** . Sélectionnez une combinaison de champs et de valeurs que vous souhaitez définir lors de l'évaluation de la règle. Ce champ s'affiche uniquement lorsque **le modèle** est sélectionné dans le champ Type de **valeur** .
Valeur de script	Script pour définir des valeurs sur l'enregistrement actuel. Ce champ définit les valeurs à définir sur les champs dans les entrées de vulnérabilité. Ce champ s'affiche uniquement lorsque **l'option Script** est sélectionnée dans le champ Type de **valeur** .

Traduction automatique

5. Pour créer la nouvelle règle, cliquez sur **Soumettre**.

Example:
Utilisez des règles de classification VR pour ajouter la logique aux tables en amont telles que Vulnérabilité et Éléments détectés et la calculer. Vous pouvez réutiliser la sortie plusieurs fois, ce qui améliore les performances des règles telles que les règles d'affectation. Par exemple, classez l'entrée tierce (TPE) comme Java et réutilisez la sortie dans les règles d'affectation plusieurs fois. Exemple de règle d'affectation :

```
VI.TPE.Classfication Type
          | IS | Java
```

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer une règle à une vulnérabilité existante

Lorsque vous modifiez une règle de classification, réexécutez toutes les règles actives sur toutes les entrées de vulnérabilité. Vous pouvez également moderniser les vulnérabilités existantes en appliquant les règles de classification nouvellement créées aux vulnérabilités existantes.

Avant de commencer
Rôle requis : sn_vul.manage_classification_rule

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Administration** > **Règles de classification de vulnérabilité**.
2. Pour sélectionner une règle, cochez la case en regard de la règle.
3. Cliquez sur **Appliquer les changements**.
4. Cliquez sur **Réappliquer**.

Désactiver ou supprimer une règle de classification

Désactivez ou supprimez une règle de classification si elle n'est plus nécessaire ou pertinente.

Avant de commencer
Rôle requis : sn_vul.manage_classification_rule

Pourquoi et quand exécuter cette tâche
Lorsqu'une règle de classification est désactivée ou supprimée, les données qui ont été renseignées dans les champs **Classification** et **Classification_type** par cette règle supprimée sont conservées dans leurs tables respectives.

Si vous souhaitez effacer ces données, créez une règle avec des valeurs vides dans les champs **Classification** et **Classification_type** et réappliquez le groupe. Une fois que cette nouvelle règle est réappliquée, les changements sont reflétés sur tous les enregistrements auxquels cette règle s'applique, en fonction des conditions de la règle.

Procédure

1. Accédez à la **Tout** > **Vulnérabilité** > **Administration** > **Règles de classification de vulnérabilité**.
2. Pour sélectionner la règle que vous souhaitez supprimer, cochez la case en regard de la règle.
3. Pour supprimer la règle, effectuez l'une des opérations suivantes :
   - Dans la liste Action sur les lignes sélectionnées, cliquez sur **Supprimer**.
   - Sélectionnez la règle et cliquez sur le bouton **Supprimer** .
4. Cliquez sur **Appliquer les changements**.

> **Remarque :** Si vous ne cliquez pas sur ce bouton, la règle continue de résider dans le système. Les vulnérabilités référencées par la règle continuent de les référencer.

Créer une règle d'exclusion

Créez une règle pour filtrer ou exclure les détections afin qu'elles ne soient pas converties en éléments vulnérables (VIT) pendant l'ingestion.

Avant de commencer
Rôle requis : administrateur de vulnérabilité

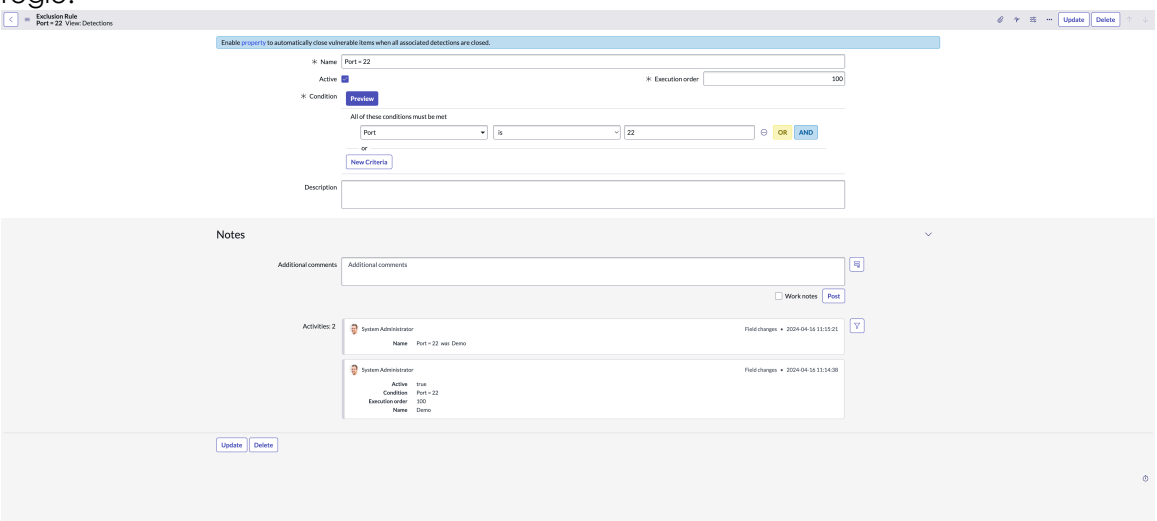
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Règles d'exclusion**.
2. Sur la page d'enregistrement Règle d'exclusion, sélectionnez **Nouveau** pour créer une règle.



Un message indiquant « Activer la propriété pour fermer automatiquement les éléments vulnérables lorsque toutes les détections associées sont fermées » s'affiche. Par défaut, la propriété est inactive. Pour l'activer, sélectionnez le lien de la propriété et entrez la valeur sur Vrai dans le champ **Valeur** .

3. Renseignez les champs du formulaire.

Formulaire Règle d'exclusion

Champ	Description
Nom	Nom de la règle d'exclusion.
Actif	Option permettant d'activer la règle d'exclusion.
Ordre d'exécution	Ordre unique pour chaque règle d'exclusion.
Condition	Conditions de filtre pour les détections qui peuvent être définies lors de leur traitement. **Remarque :** Vous ne pouvez pas sélectionner la règle d'exclusion ou les conditions de champ d'élément de vulnérabilité.
Description	Description de la règle d'exclusion.

4. Sélectionnez **Soumettre**.
L'activité est enregistrée dans le système.

Remarque : Une fois qu'une règle d'exclusion est créée, elle prend effet sur les détections à partir de l'ingestion suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion des changements Tâches pour Réponse aux vulnérabilités

À partir des tâches de rattrapage (RT), créez des demandes de changement, associez des RT à des demandes de changement existantes ou divisez les tâches de rattrapage en nouvelles tâches avec des sous-ensembles d'éléments vulnérables (VI).

Créez et gérez les demandes de changement directement à partir d'une tâche de rattrapage si un processus manuel et contrôlé, quel qu'il soit, est requis pour la modification ou la suppression des éléments de configuration (CI) pris en charge dans votre CMDB. La création et la gestion des demandes de changement directement à partir d'un enregistrement vous aident à examiner et à résoudre rapidement les vulnérabilités.

Reportez-vous à la section Gestion des changements pour Réponse aux vulnérabilités pour obtenir une vue d'ensemble du fonctionnement de Change Management avec l'application Réponse aux vulnérabilités et la configuration requise pour obtenir une vue d'ensemble.

Consultez les rubriques suivantes pour savoir comment créer des demandes de changement, associer des tâches de rattrapage à des demandes de changement existantes et diviser des tâches de rattrapage. Pour Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage en savoir plus sur la façon dont les champs d'état des demandes de changement (CHG) résolvent automatiquement les tâches de rattrapage.

Créer une demande de changement à partir d'une tâche de rattrapage

En tant que propriétaire du rattrapage informatique, créez une demande de changement (CHG) directement à partir d'une tâche de rattrapage (VUL) pour tous les éléments vulnérables du groupe. Créez une demande de changement avec des informations pré-remplies qui incluent la solution préférée pour accélérer votre enquête sur les vulnérabilités qui nécessitent une intervention manuelle.

Avant de commencer

Rôles requis : Pour créer une demande de changement : tout utilisateur disposant du rôle itil. Le rôle sn_vul.remediation_owner est également automatiquement attribué lorsque le rôle itil est affecté à un utilisateur.

Rôle requis : pour l'approbation des demandes de changement : utilisateurs disposant de rôles itil, admin, sn_change_write change_manager.

Pourquoi et quand exécuter cette tâche

Pour en savoir plus sur la création d'une demande de changement à partir des espaces de travail, reportez-vous à la Réponse aux vulnérabilités section Créer une demande de changement dans Espace de travail de remédiation IT.

Pour créer une demande de changement à partir de l'environnement classique, suivez les étapes ci-dessous.

Vous pouvez créer, approuver, implémenter, examiner et fermer des demandes de changement directement à partir d'une tâche de rattrapage. Vous pouvez créer trois types de demandes de changement avec des informations pré-remplies à partir d'une tâche de rattrapage :

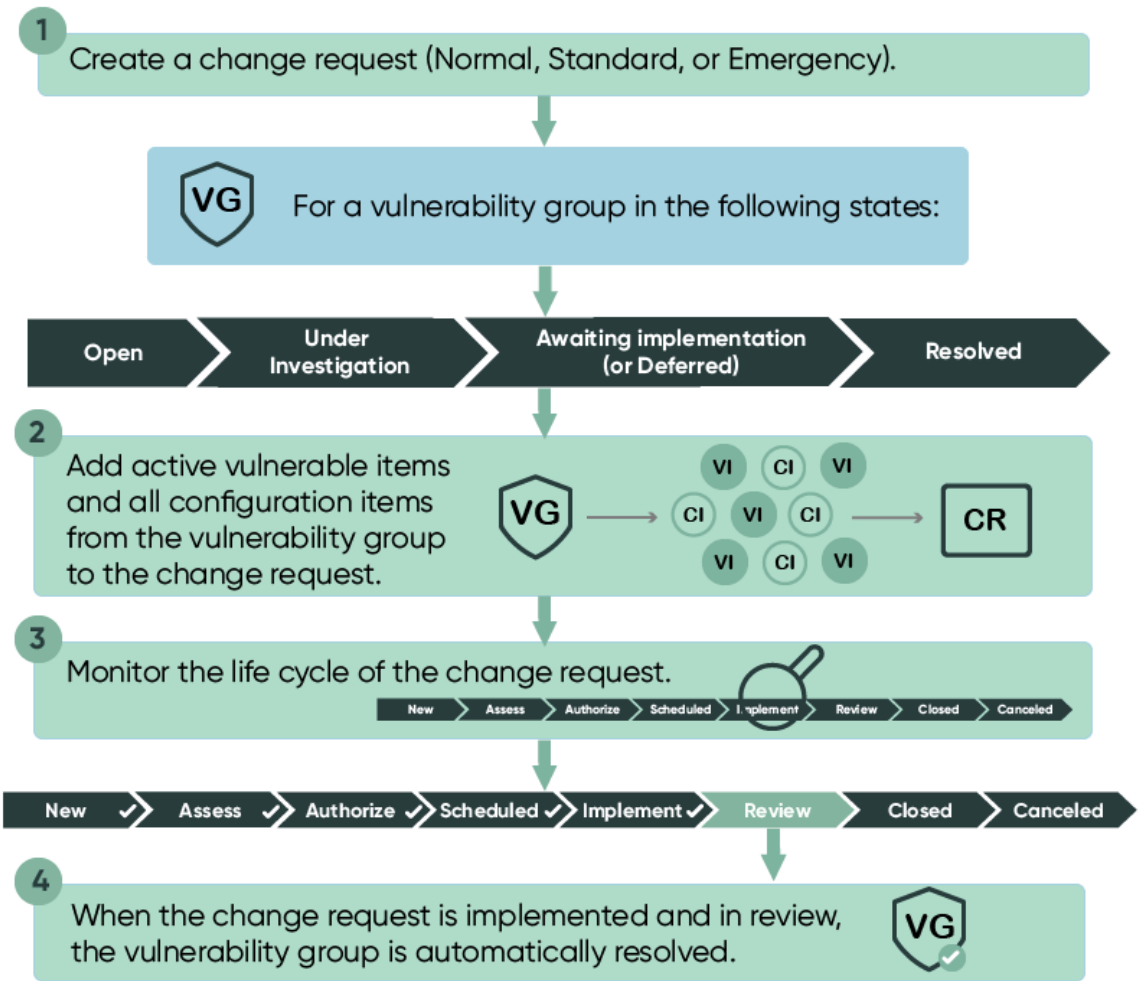
- Standard. Un changement pré-autorisé à risque faible, relativement commun et qui suit une procédure ou une instruction de travail spécifique.
- Normal. Les demandes de changement normal suivent un processus prescriptif qui requiert deux niveaux d'approbation avant d'être implémentées, examinées et fermées.
- Urgence. Un changement pour résoudre un incident majeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'image suivante illustre le flux de base pour la création d'une demande de changement à partir d'une tâche de rattrapage (VUL). Les étapes détaillées de ce flux suivent l'image.

L'enregistrement de tâche de rattrapage est appelé VUL dans les sections suivantes. Dans les versions précédentes de , les tâches de Réponse aux vulnérabilitésremédiation étaient appelées groupes de vulnérabilité (VG). Dans les images suivantes, VG = tâche de rattrapage, ou un enregistrement VUL.



Remarque : Points clés sur la création de nouvelles demandes de changement :

- Vous pouvez créer de nouvelles demandes de changement pour n'importe quelle tâche de rattrapage (VUL) dont l'état n'est pas `Fermé`.
- Vérifiez que vous disposez d'un approbateur pour les demandes de changement autres que Standard (préapprouvé) que vous créez ou associez à un VUL. Cela accélère la résolution de la vulnérabilité. Pour plus d'informations sur l'ajout d'utilisateurs, reportez-vous à la section Ajouter des utilisateurs au groupe Vulnerability Response.
- Pour qu'une tâche de rattrapage puisse être résolue, toutes les tâches d'au moins un CHG associé à la vulnérabilité doivent être terminées afin que la demande de changement puisse être implémentée et passer à l'état `Réviser` .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Pour créer une demande de changement complète à partir d'un enregistrement de tâche de rattrapage existant, accédez à **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**.
   La liste des tâches de rattrapage affectées à votre groupe d'affectation s'affiche.
2. Facultatif : Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Aperçu du rattrapage** pour afficher le tableau de bord Vue d'ensemble du rattrapage et localiser une vulnérabilité qui vous est affectée ou qui est affectée à votre groupe d'affectation.
3. Vous pouvez également cliquer sur une tâche de rattrapage dans la colonne Nombre pour ouvrir l'enregistrement et afficher les détails.
   L'enregistrement s'affiche.
4. Une fois affiché l'enregistrement VUL pour lequel vous souhaitez créer la demande de changement, cliquez sur **Créer un changement** dans le coin supérieur droit de l'enregistrement.
   Le formulaire Créer une demande de changement s'affiche.
5. Renseignez les champs.

   a. Dans la liste de choix du champ S'applique à, choisissez-en un pour continuer.

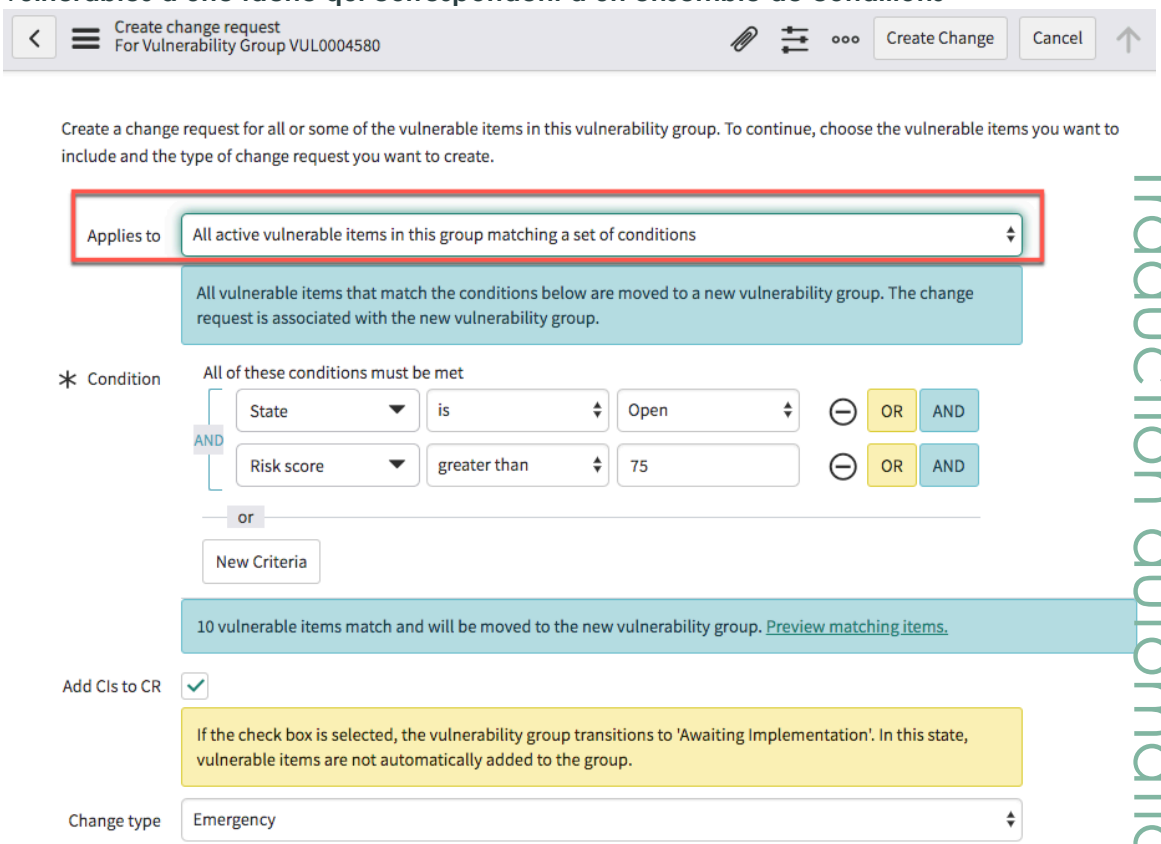
Option	Description
Tous les éléments vulnérables actifs dans ce groupe	Si cette option est sélectionnée, tous les éléments vulnérables actifs de cette tâche de rattrapage avec un état autre que Fermé sont ajoutés automatiquement à la demande de changement une fois que vous avez cliqué sur **Créer un changement**.
Tous les éléments vulnérables de ce groupe correspondant à un ensemble de conditions	S'il est sélectionné, le créateur de conditions s'affiche comme illustré dans la deuxième figure ci-dessous. Entrez des critères de filtre pour identifier les éléments vulnérables que vous souhaitez pour la nouvelle demande de changement. Un exemple de filtre peut inclure uniquement les éléments vulnérables qui correspondent à des critères de recherche spécifiques : **L'état est Ouvert** et **le score de risque est supérieur à 75**. Une fois que vous avez saisi vos conditions, un message s'affiche avec le nombre de VI qui correspondent à vos critères (`10`). Un lien (**Aperçu des éléments correspondants**) permettant d'afficher un aperçu des éléments correspondants s'affiche. Si aucun élément ne correspond à vos conditions de filtre, un message s'affiche sous le créateur de conditions qui vous demande d'ajuster votre filtre.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Une fois que vous avez cliqué sur **Créer un changement**, tous les éléments vulnérables qui correspondent à ce filtre de condition sont déplacés vers une nouvelle tâche de rattrapage. Cette demande de changement est associée à la nouvelle tâche de rattrapage.

Créer un formulaire de demande de changement pour les éléments vulnérables d'une tâche qui correspondent à un ensemble de conditions



b. Facultatif : S'il s'affiche sur le formulaire, cliquez sur le lien **Visualiser les éléments correspondants** pour obtenir une liste des éléments correspondants à vos critères de filtre.
L'aperçu de la liste des tâches de remédiation s'affiche. Vous pouvez sélectionner des éléments dans cette liste d'aperçu et effectuer des actions d'interface utilisateur sur eux, cependant, ces actions sont également effectuées sur le VUL. Par exemple, si vous supprimez un VI de la liste d'aperçu, ce VI est également supprimé de la VUL.

c. Une fois que vous avez terminé votre aperçu, fermez la fenêtre du navigateur pour renvoyer le formulaire de demande de changement.

d. Pour la case à cocher Ajouter des CI au CR, choisissez-en une pour continuer.

Option	Description
Case à cocher Ajouter des CI au CR sélectionnée	Cette valeur est sélectionnée par défaut. Si la case est cochée, tous les éléments

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	de configuration (CI) qui appartiennent aux éléments vulnérables actifs dans cette tâche de rattrapage sont ajoutés à cette demande de changement. La vulnérabilité passe automatiquement à l'état `En attente d'implémentation`.
Ajouter des CI au CR case décochée	Décochez la case si vous ne souhaitez pas que les CI des éléments vulnérables actifs de cette tâche de rattrapage soient ajoutés à la nouvelle demande de changement. Lorsqu'elle est désactivée, l'état de la demande de changement n'est pas synchronisé avec la vulnérabilité et la vulnérabilité reste dans son état actuel.

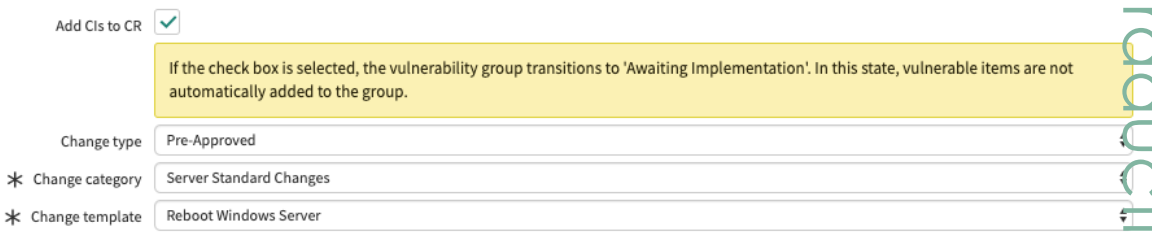
e. Dans la liste de choix du champ Type de changement, choisissez-en un pour continuer.

Type de changement	Description
Urgence	Un changement pour résoudre un incident majeur.
Normal	Type de changement utilisé pour implémenter tout changement apporté à un service qui n'est ni standard ni urgent.
Standard	Demande de changement préautorisée et à faible risque fréquemment implémentée. Les demandes de changement standard approuvées peuvent être prédéfinies dans un catalogue de modèles pour améliorer l'accès et le processus de demande d'un changement standard. Si cette option est sélectionnée, deux champs sont affichés, comme illustré dans la figure suivante. Sélectionnez-en un dans chaque liste de choix pour remplir les champs suivants : ▪ Catégorie de changement : sélectionnez une catégorie pour le changement dans votre catalogue existant, par exemple, `Matériel`, `Changements standard de serveur`, `Logiciel`. Dans cet exemple, `l'option Appliquer des correctifs aux changements standard` est sélectionnée. ▪ Modèle de changement : sélectionnez un modèle disponible pour les demandes de changement avec des tâches de prise en charge prédéfi-

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type de changement	Description
	nies dans votre catalogue. Dans cet exemple, le modèle `Microsoft Monthly Patching Cycle est` sélectionné. Pour plus d'informations sur les catégories, les modèles et les types de changement de demande de changement ITSM, consultez Types de changement .

La fonctionnalité lit automatiquement les types de demandes de changement que vous configurez dans votre catalogue dans ITSM Change Management. Par exemple, si vous changez le nom de vos demandes de changement standard dans ITSM de `Standard` à `Préapprouvé`, votre nouveau nom s'affiche automatiquement dans la liste de choix de type de changement de la Créer une demande de changement à partir de, comme illustré dans la figure suivante.



Les champs de la section Aperçu de la demande de changement du formulaire sont pré-remplis avec les informations provenant de la VUL. Si nécessaire, ces valeurs de champ peuvent être modifiées. Par exemple, examinez les valeurs des champs de la figure suivante :

Date de fin prévue

Cette date (`2019-10-10`) est la même valeur que celle affichée dans le champ Date cible de rattrapage de la VUL. Cette valeur est dérivée de la date cible de rattrapage la plus précoce à partir des éléments vulnérables qui appartiennent à la vulnérabilité. Si vous créez une demande de changement pour un problème critique qui nécessite une date de correction antérieure, vous préférez peut-être modifier cette valeur et celle du champ Priorité.

Justification

Ce champ affiche le nombre de CI ajoutés au CHG. Si vous souhaitez ajouter des informations supplémentaires, vous pouvez modifier ce texte. Par exemple, vous préférez peut-être ajouter une note dans ce champ concernant le filtre que vous avez utilisé pour créer la nouvelle vulnérabilité (par exemple, `Score de risque supérieur à 75`). Ce texte peut vous aider à localiser votre nouvelle demande de changement et votre nouveau groupe de vulnérabilité.

Plan d'implémentation

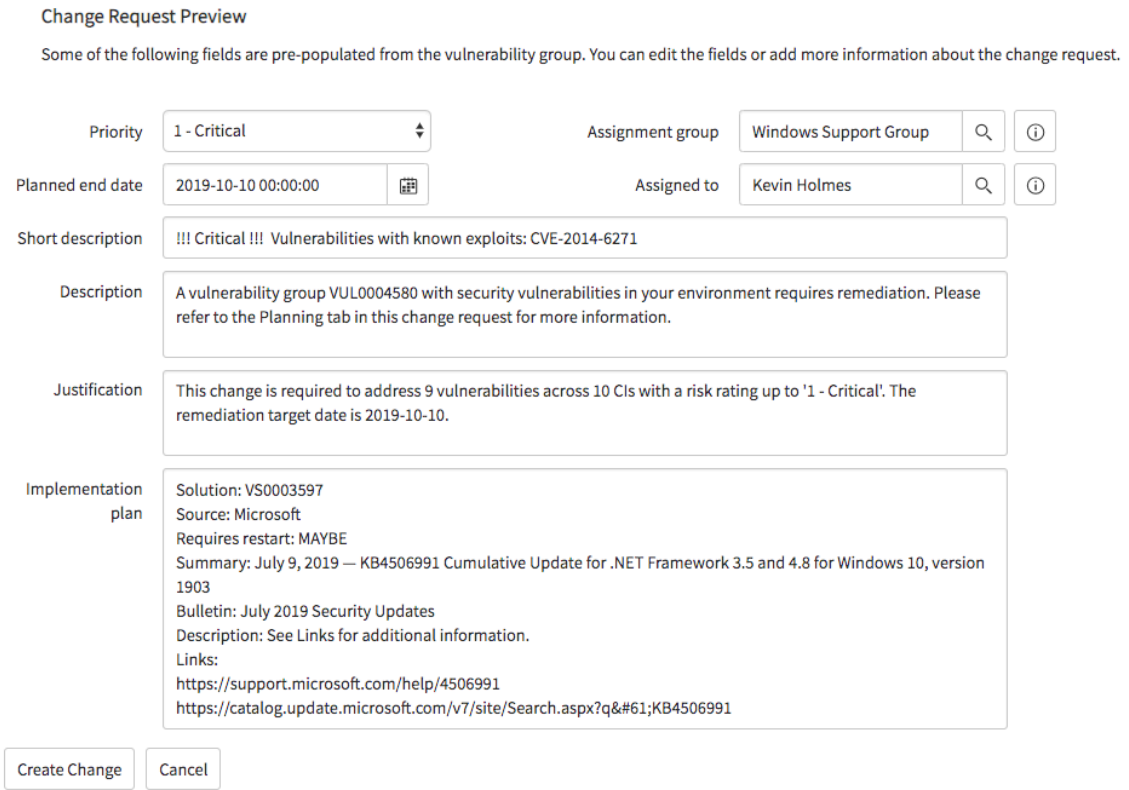
Ce champ affiche la solution préférée pour la vulnérabilité.

Groupe d'affectation et Affecté à

Modifiez ces champs pour modifier le groupe d'affectation ou réaffecter cette demande de changement à un utilisateur de l'un de vos groupes d'affectation.

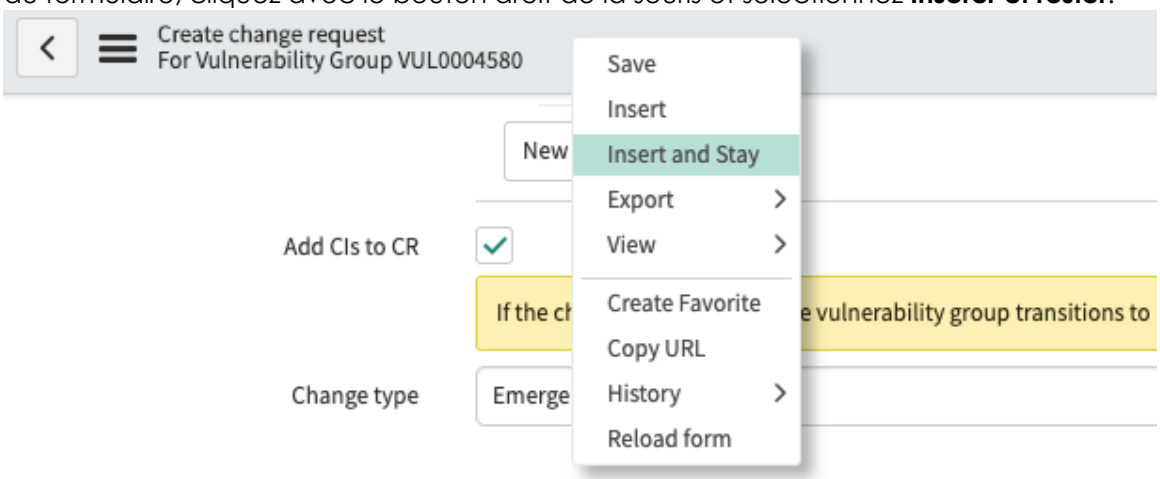
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Continuez à prévisualiser et modifier les champs selon vos besoins.

7. Pour enregistrer vos modifications et rester sur cette page, dans la bannière grise en haut du formulaire, cliquez avec le bouton droit de la souris et sélectionnez **Insérer et rester**.



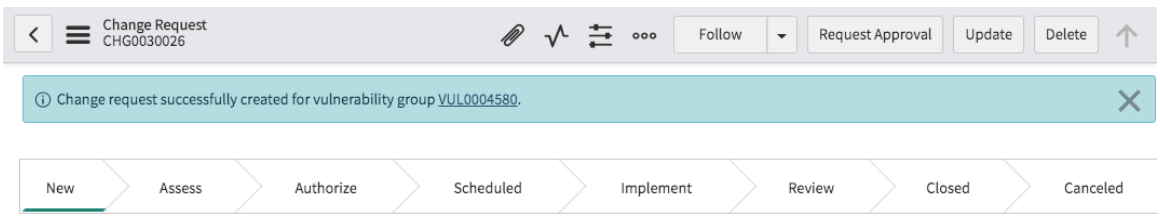
8. Une fois que vous avez terminé vos modifications, choisissez-en une pour continuer.

Option	Description
Créer un changement	Votre demande de changement est créée et la nouvelle demande de changement affiche l'état `Nouveau` . En haut, des messages s'affichent qui indiquent que la demande de changement a été créée avec succès avec le nombre d'éléments vulné-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	rables qui ont été ajoutés, comme illustré dans la figure suivante. Si la synchronisation de l'état est activée et que la vulnérabilité n'est pas déjà en `cours d'examen`, elle passe automatiquement dans `la catégorie En cours d'examen` et une note de travail est publiée.
Annuler	La demande de changement n'est pas créée et la vulnérabilité s'affiche.



Remarque :

Pour une tâche de rattrapage à l'état `Ouvert` avec les champs Groupe d'affectation et Affecté à non affectés (vides), l'utilisateur actuellement connecté est automatiquement affecté à la tâche une fois que vous avez cliqué sur **Créer un changement**. De plus, la case Ajouter des CI au CR doit être cochée. En haut de la VUL, un message de confirmation bleu s'affiche qui indique cette affectation.

Que faire ensuite

Surveillez la demande de changement et les tâches de changement pour vérifier qu'elles sont terminées et que la demande de changement est implémentée. Une fois ce CHG implémenté et passé à l'état `Révision` , si la synchronisation d'état est activée, la vulnérabilité passe automatiquement à l'état `Résolu`. Pour plus d'informations sur la synchronisation des états, reportez-vous à la section Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.

Associer une tâche de rattrapage à une demande de changement existante

En tant que propriétaire de rattrapage informatique, évitez de créer des demandes de changement (CHG) en double lorsque vous travaillez à résoudre vos tâches de rattrapage en associant une tâche de rattrapage (VUL) à une demande de changement déjà disponible dans votre instance.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : tout utilisateur ayant le rôle itil. Le rôle sn_vul.remediation_owner est également attribué automatiquement à un utilisateur lorsque le rôle itil est affecté.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

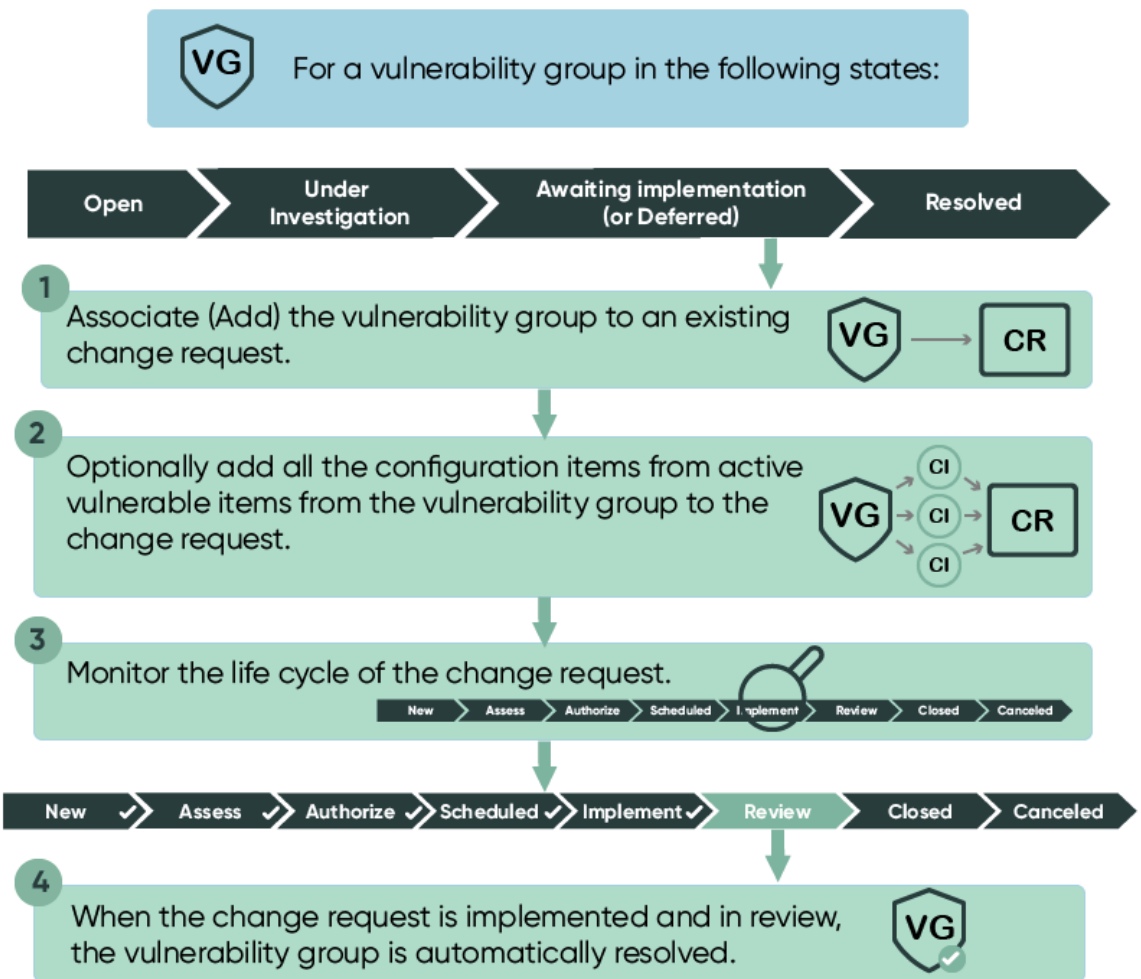
Pourquoi et quand exécuter cette tâche
Pour plus d'informations sur l'association d'une tâche de rattrapage à une demande de changement existante, reportez-vous à Créer une demande de changement dans Espace de travail de remédiation IT.

L'enregistrement de tâche de rattrapage est appelé VUL dans les sections suivantes. Dans les versions précédentes de , les tâches de Réponse aux vulnérabilitésremédiation étaient appelées groupes de vulnérabilité (VG). Dans les images suivantes, VG = tâche de rattrapage, ou un enregistrement VUL.

Pour plus d'informations sur l'association d'une tâche de rattrapage à une demande de changement existante, reportez-vous à Créer une demande de changement dans Espace de travail de remédiation IT.

En tant que propriétaire de rattrapage, vous pouvez associer des tâches de rattrapage qui vous sont affectées ou qui sont affectées à votre groupe d'affectation à des demandes de changement existantes directement à partir des enregistrements de tâches de rattrapage. L'image suivante illustre le flux de base pour associer une demande de changement à une VUL (VG) existante. Les étapes détaillées de ce flux suivent l'image.

Workflow pour associer une tâche de rattrapage à une demande de changement existante



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez associer une demande de changement existante à une vulnérabilité dans n'importe quel état (Ouvert, En cours d'examen, En attente d'implémentation, Fermé et Différé). Lorsque vous associez une demande de changement à une VUL existante, seuls les VI actifs sont ajoutés à la demande de changement.

Avant de commencer, pour éviter de créer des demandes de changement en double, vous préférez peut-être afficher toutes les demandes de changement existantes déjà associées à une vulnérabilité. Pour suivre facilement le nombre de demandes de changement liées à une VUL spécifique, reportez-vous à la colonne Nombre de CR sur la liste Tâches de rattrapage. S'il n'est pas affiché, cliquez sur l'icône des paramètres (en haut à droite. Déplacez la colonne du nombre de CR de Disponible à Sélectionné, puis cliquez sur **OK**.

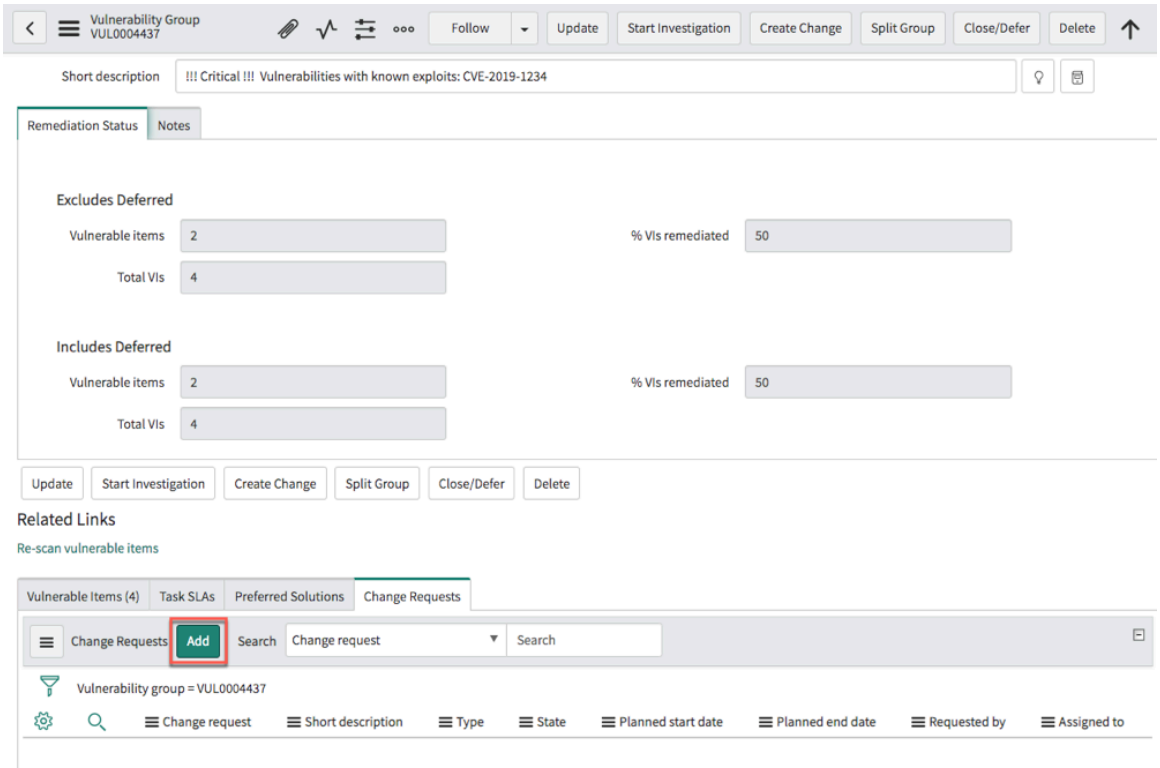
Pour remplir automatiquement la nouvelle colonne, pour les clients ayant des données existantes dans cette table, exécutez la tâche planifiée : `Remplir la nouvelle colonne du nombre de CR`.

Procédure

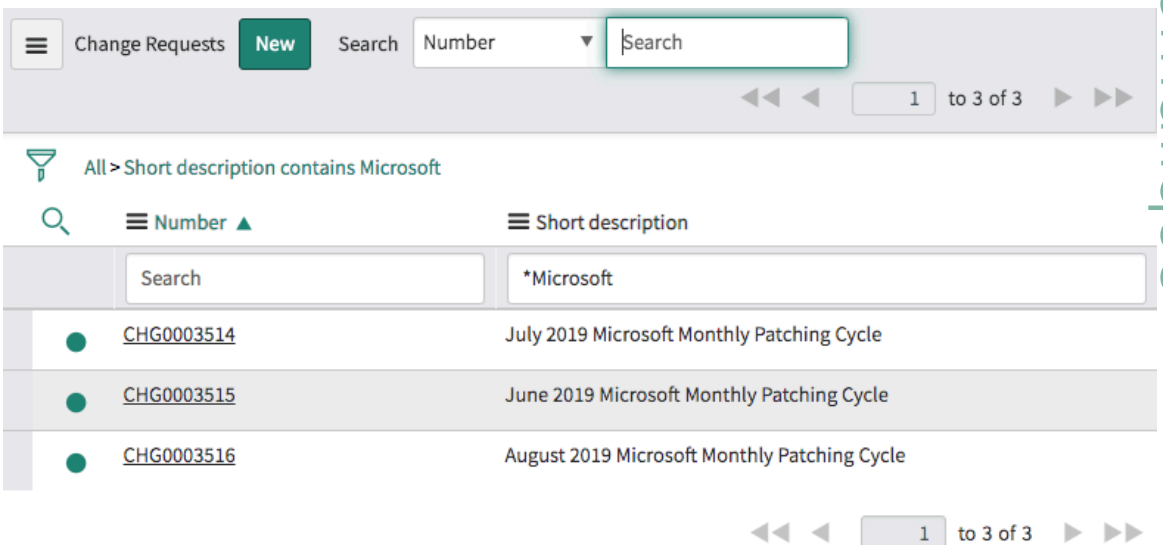
1. Pour associer une tâche de rattrapage à une demande de changement existante, accédez à **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Localisez la tâche de rattrapage avec laquelle vous travaillez.
3. Facultatif : Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Aperçu du rattrapage** pour afficher le tableau de bord Vue d'ensemble du rattrapage et localiser une vulnérabilité qui vous est affectée ou qui est affectée à votre groupe d'affectation.
4. Dans la colonne Numéro, cliquez sur un enregistrement VUL pour l'ouvrir. L'enregistrement VUL s'affiche.
5. Une fois l'enregistrement ouvert affiché, s'il n'est pas déjà affiché, faites défiler jusqu'à la liste connexe Demandes de changement et sélectionnez-la. Toutes les demandes de changement associées à la vulnérabilité sont affichées avec le bouton **Ajouter** . Dans la figure suivante, aucune demande de changement n'est déjà associée à cette vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Pour associer le VUL à un CHG existant, cliquez sur **Ajouter**.
   Le formulaire Ajouter une demande de changement existante à une tâche de rattrapage s'affiche.
7. Dans le formulaire, cliquez sur l'icône de recherche.
   Une vue de liste des demandes de changement existantes s'affiche dans une nouvelle fenêtre, comme le montre la figure suivante.



8. Sélectionnez un élément dans la liste affichée ou cliquez sur le filtre ( ) et entrez des conditions pour limiter les résultats de votre recherche.
9. Pour la case à cocher Ajouter des CI au CR, choisissez-en une pour continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Cette case à cocher s'affiche uniquement pour les demandes de changement existantes à l'état `Nouveau` .

Option	Description
Case à cocher Ajouter des CI au CR sélectionnée	Cette valeur est sélectionnée par défaut. Si la case est cochée, tous les éléments de configuration (CI) qui appartiennent aux éléments vulnérables actifs dans cette tâche de rattrapage sont ajoutés à cette demande de changement. Lorsque cette option est sélectionnée, l'état de la demande de changement est synchronisé avec la vulnérabilité virtuelle. Pour plus d'informations, consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.
Ajouter des CI au CR case décochée	Décochez la case si vous ne souhaitez pas que les CI des éléments vulnérables actifs de cette tâche de rattrapage soient ajoutés à la nouvelle demande de changement. Lorsqu'elle est désactivée, l'état de la demande de changement n'est pas synchronisé avec la vulnérabilité et la vulnérabilité reste dans son état actuel.

10. Une fois le numéro de la demande de changement affiché dans le champ Rechercher une demande de changement, cliquez sur **Soumettre**.
La VUL s'affiche. En haut de l'enregistrement, le message de confirmation bleu s'affiche et indique que la demande de changement que vous avez sélectionnée est correctement associée à la VUL.

    Remarque : Dans le cas d'une vulnérabilité vulnérable à l'état `Ouvert` avec les champs Groupe d'affectation et Affecté à non affectés (vides), l'utilisateur connecté actuel est automatiquement affecté à la vulnérabilité une fois que vous avez cliqué sur **Ajouter**. De plus, la case Ajouter des CI au CR doit être cochée. En haut de la VUL, un message de confirmation bleu s'affiche indiquant que l'utilisateur actuel est affecté.

Que faire ensuite

Passez en revue l'enregistrement VUL. Dans la colonne Demande de changement de la liste connexe Demandes de changement, cliquez sur le lien pour que le nouveau CHG affiche l'enregistrement CR. Dans l'enregistrement CHG ouvert, vous pouvez surveiller l'état de la demande de changement. Les éléments de configuration (CI) affectés et les tâches de rattrapage sont affichés dans les listes connexes CI affectés et tâches de rattrapage.

Diviser une tâche de rattrapage

En tant que propriétaire du rattrapage informatique, identifiez à partir d'une tâche de rattrapage existante (VUL) un sous-ensemble d'éléments vulnérables (VI) que vous souhaitez déplacer vers un nouveau groupe.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Remarque :

Les cas d'utilisation de fractionnement de VI à partir de VUL existants en de nouvelles tâches de rattrapage peuvent inclure les exemples suivants :

- Lorsque vous souhaitez créer une demande de changement ou des demandes de changement pour une tâche fractionnée.
- Lorsque vous réaffectez un groupe fractionné à un autre utilisateur de votre groupe d'affectation.
- Lorsque vous demandez un report ou une exception pour une tâche fractionnée, car vous savez que certaines vulnérabilités sur des éléments de configuration (CI) spécifiques ne peuvent pas être corrigées dans un délai donné.

Rôle requis : tout utilisateur disposant du rôle itil pour fractionner un VUL.

Remarque : Le rôle sn_vul.remediation_owner est également automatiquement attribué lorsque le rôle itil est affecté à un utilisateur.

Pourquoi et quand exécuter cette tâche

Pour en savoir plus sur le fractionnement des tâches de rattrapage dans les Réponse aux vulnérabilités espaces de travail, reportez-vous à la section Fractionner une tâche de rattrapage dans Espace de travail de remédiation IT.

Pour fractionner une tâche de rattrapage dans l'environnement classique ou pour les versions de Réponse aux vulnérabilités.

Vous pouvez diviser les tâches de rattrapage existantes avec plusieurs éléments vulnérables qui sont à l'état `Ouvert`, En cours d'examen ou En attente d'implémentation. En créant une nouvelle vulnérabilité avec des éléments vulnérables qui correspondent à des critères spécifiques, vous pouvez travailler avec un groupe spécifique d'éléments vulnérables sans affecter la tâche de rattrapage d'origine.

Lorsque vous spécifiez les conditions des éléments vulnérables que vous souhaitez déplacer vers une nouvelle tâche de rattrapage avec le Créateur de conditions, seuls les éléments vulnérables actifs qui correspondent à vos critères sont déplacés vers le nouveau groupe.

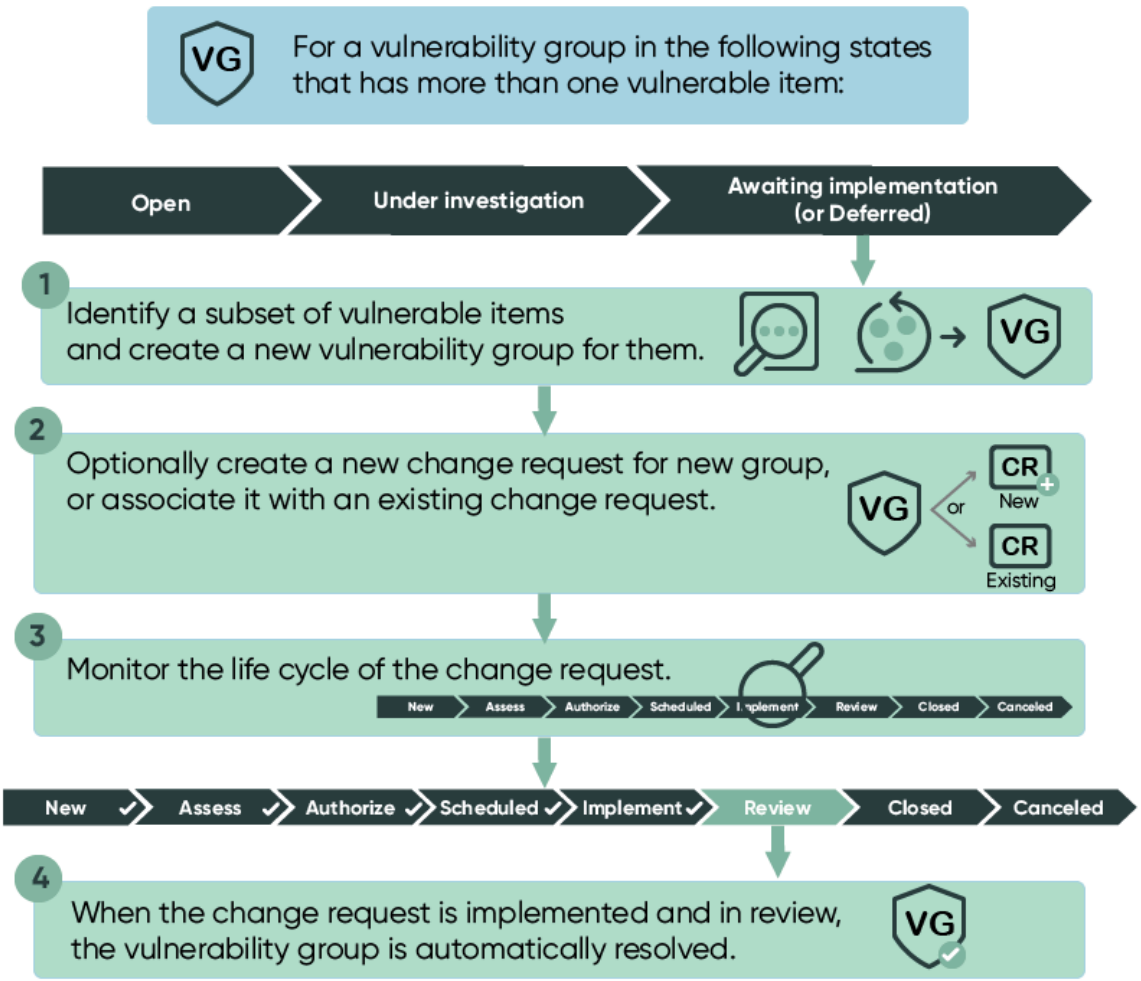
Vous n'avez pas besoin de créer des demandes de changement (CHG) lorsque vous fractionnez une VUL. Vous avez la possibilité de diviser une VUL en même temps que vous créez une demande de changement, ou vous pouvez diviser une VUL sans créer de demande de changement. L'image suivante illustre le flux de base pour fractionner un groupe de vulnérabilité. Les étapes détaillées de ce flux suivent l'image.

L'enregistrement de tâche de rattrapage est appelé VUL dans les sections suivantes. Dans les versions précédentes de , les tâches de Réponse aux vulnérabilitésremédiation étaient appelées groupes de vulnérabilité (VG). Dans les images suivantes, VG = tâche de rattrapage, ou un enregistrement VUL.

Traduction automatique

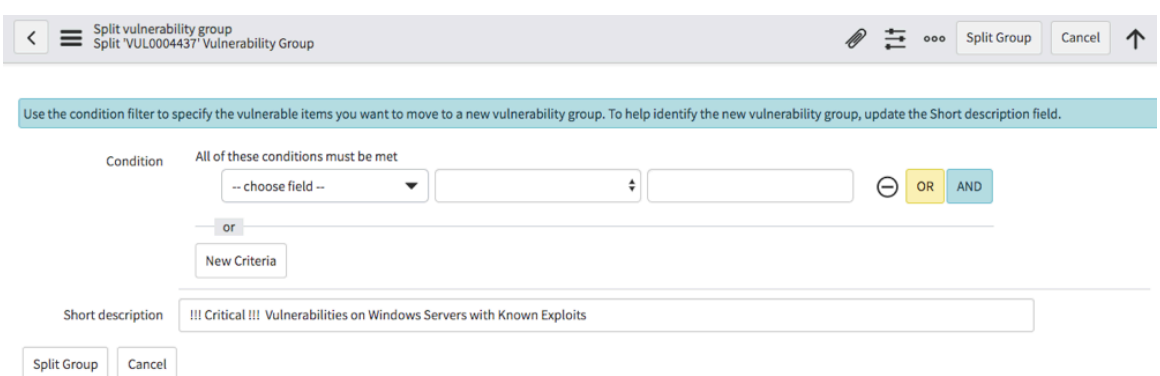
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow pour fractionner une tâche de rattrapage



Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**.
   La liste des tâches de rattrapage s'affiche.
2. Dans la colonne Nombre, cliquez sur un enregistrement pour l'ouvrir.
   L'enregistrement s'affiche.
3. Dans l'angle supérieur droit de la VUL, cliquez sur **Fractionner la tâche**.
   Le formulaire Diviser la tâche de rattrapage s'affiche.



Traduction automatique

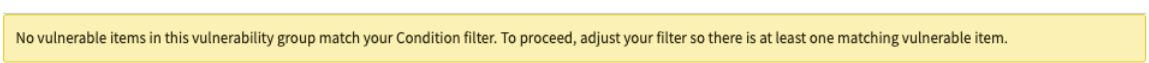
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Une fois le filtre de condition affiché, spécifiez les conditions pour les éléments vulnérables que vous souhaitez déplacer vers une nouvelle tâche.
   Par exemple, vous pouvez préférer filtrer uniquement les éléments vulnérables qui correspondent aux conditions suivantes :
   - À l'état `Ouvert` .
   - Scores de risque supérieurs à `80`.
   - Éléments de configuration qui contiennent « `WINSV` ».
   - Situé à San Diego.

   À titre d'exemple, pour les conditions, vous pouvez saisir :
   - État : est : Ouvert
   - Score de risque : est supérieur ou égal à 80
   - Élément de configuration . Nom : contient : WINSV
   - Élément de configuration . Emplacement - est - San Diego

   Si les éléments vulnérables correspondent à votre filtre une fois que vous avez entré les conditions, un message s'affiche avec le nombre d'éléments vulnérables qui correspondent.

   Remarque : Si un message indiquant qu'aucun élément vulnérable ne correspond à votre filtre s'affiche, ajustez les conditions de sorte qu'au moins un élément vulnérable corresponde à vos critères de filtre.

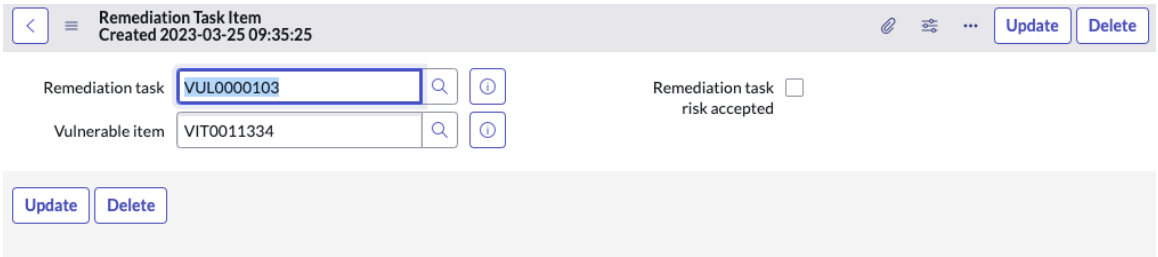
5. Facultatif : Ajustez le filtre selon vos besoins.
6. Facultatif : Pour vous aider à identifier la nouvelle vulnérabilité après sa création, vous pouvez mettre à jour le champ Brève description.
   En cas de modification, utilisez le champ Brève description comme critère de recherche pour la nouvelle vulnérabilité virtuelle afin de vous aider à la localiser après sa création, par exemple `SITUÉE À SAN DIEGO`.
7. Facultatif : Pour prévisualiser les détails des éléments vulnérables qui correspondent à vos critères de filtrage, procédez comme suit avant de cliquer sur **Fractionner la tâche** pour créer le nouveau VUL.
   Ces détails incluent les demandes de changement existantes qui sont déjà associées à ce sous-ensemble et les VUL avec ces éléments vulnérables. L'affichage de ces informations dans l'aperçu peut vous empêcher de créer des VUL en double.

   a. Dans le message de confirmation bleu du formulaire Diviser la tâche de rattrapage, cliquez sur **Prévisualiser les éléments correspondants**.
      La liste des éléments de tâche de rattrapage s'affiche dans une nouvelle fenêtre dans votre navigateur avec une liste d'éléments vulnérables qui correspondent à vos conditions.

   b. Dans la colonne Nombre, cliquez sur un élément pour ouvrir l'enregistrement.

   c. Dans l'enregistrement qui s'affiche, à droite du groupe de vulnérabilité ou des champs d'élément vulnérable, cliquez sur l'icône d'informations de l'élément vulnérable pour afficher les enregistrements.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement**.
Les informations relatives à la date cible de rattrapage s'affichent. Dans la section Listes connexes, cliquez sur une liste connexe pour afficher plus d'informations sur le VI.

8. Lorsque vous êtes prêt à créer la nouvelle VUL avec le ou les VI qui répondent à vos conditions, fermez la fenêtre d'aperçu pour revenir au formulaire de fractionnement de tâche dans l'autre fenêtre et, en haut du formulaire, cliquez sur **Fractionner la tâche**.

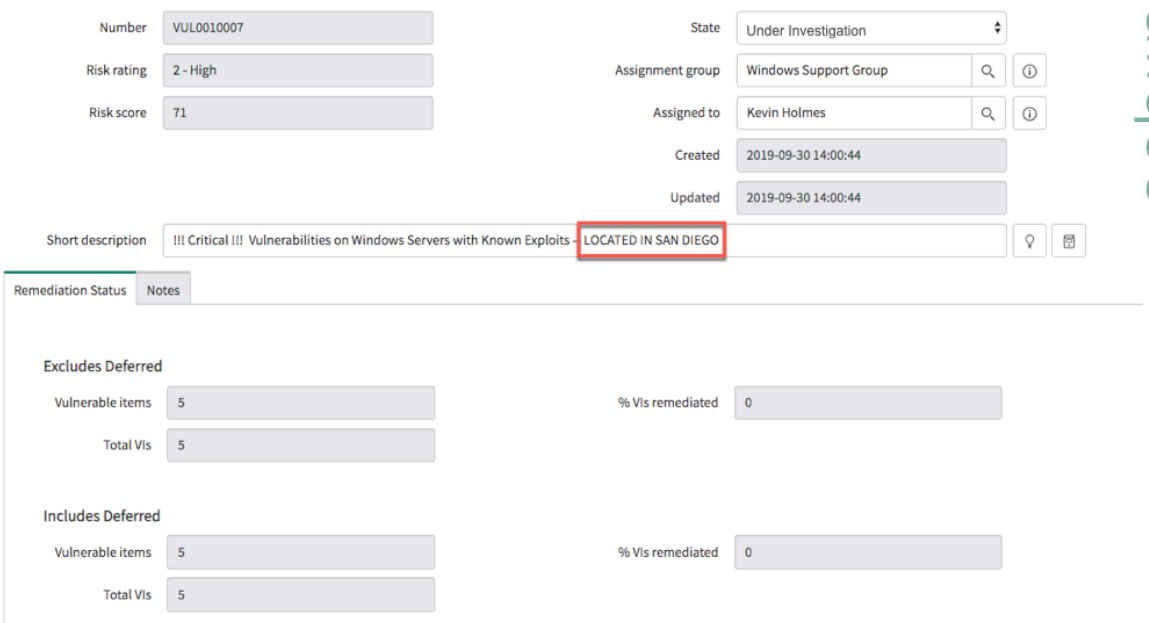
Remarque :

Pour moins de 200 VI, l'opération de fractionnement est effectuée de manière synchrone.

Au-delà de 200 VI, l'opération de division est effectuée de manière asynchrone en arrière-plan, et l'apparition des VI dans le nouveau groupe peut prendre quelques secondes.

Un message de confirmation s'affiche pour afficher tous les VI actifs qui ont été déplacés vers le nouveau groupe. Le nouveau numéro de tâche de rattrapage s'affiche également. S'il n'est pas déjà en cours d'examen, le VUL est déplacé vers En cours d'examen. Cochez le champ Brève description du texte que vous avez saisi pour le nouveau VUL dans le (`SITUÉ À SAN DIEGO`).

Des calculs cumulatifs sur le nouveau groupe sont effectués pour calculer son nouveau score de risque, sa date cible de rattrapage et d'autres valeurs de champ.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les éléments vulnérables, les solutions privilégiées et les demandes de changement sont affichés dans les listes connexes au bas de l'enregistrement. Traitez et surveillez cette nouvelle tâche comme vous le feriez pour n'importe quelle tâche de rattrapage.

9. Facultatif : Faites défiler jusqu'à la liste connexe **Notes** et cliquez dessus pour la sélectionner.
   Confirmez que le nombre d'éléments vulnérables de la tâche de rattrapage d'origine a été déplacé vers le nouveau groupe dans le flux d'activité.
10. Facultatif : Sur le nouveau VUL, pour sélectionner et diviser à nouveau les éléments vulnérables de la liste connexe des éléments vulnérables, faites défiler vers le bas de l'enregistrement du groupe de vulnérabilité et, avec les éléments vulnérables que vous souhaitez déplacer sélectionnés dans la colonne Élément vulnérable de la liste connexe des éléments vulnérables, dans la liste de choix Actions sur les lignes sélectionnées, sélectionnez **Fractionner la tâche**.
    Le formulaire Diviser la tâche de rattrapage s'affiche.
11. Pour diviser à nouveau le groupe et déplacer les éléments sélectionnés vers un nouveau groupe, cliquez sur **Fractionner la tâche**.
    Les VI sélectionnés sont déplacés vers une autre tâche de rattrapage, le message de confirmation s'affiche et le nouveau groupe s'affiche.
12. Choisissez-en un pour poursuivre votre enquête ou votre rattrapage.

Option	Description
Créer un incident de sécurité	Créer un incident de sécurité.
Créer un changement	Créez une demande de changement pour cette tâche de rattrapage.
Fractionner la tâche	Si le nouveau groupe a plusieurs éléments vulnérables, divisez à nouveau cette tâche de rattrapage pour créer un autre sous-ensemble d'éléments vulnérables.
En attente d'implémentation	Si cette option s'affiche, déplacez la tâche de l'état En cours d'examen à l'état En attente d'implémentation.
Fermer ou demander une exception	Fermez ou différez la tâche de rattrapage. Une boîte de dialogue de confirmation s'affiche avec les champs obligatoires suivants : ◦ État ◦ Motif ◦ Information supplémentaire Renseignez les champs pour fermer ou différer le groupe, puis cliquez sur **Soumettre**.
Supprimer	Supprimez cette tâche de rattrapage.
État	Déplacez l'enregistrement vers un autre état affiché dans la liste de choix et cliquez sur **Mettre à jour** pour enregistrer vos modifications apportées à l'enregistrement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Vous pouvez déplacer manuellement le nouveau VUL d'un état à l'autre au cours de son cycle de vie. Toutefois, si la synchronisation d'état est activée et que le système enregistre qu'une demande de changement associée au VUL a changé d'état, ou si vous ajoutez un CHG ou le supprimez du VUL, la synchronisation de l'état peut potentiellement remplacer votre intervention manuelle. Pour plus d'informations, consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.
Groupe d'affectation	Réaffectez la VUL à un groupe d'affectation et cliquez sur **Mettre à jour** pour enregistrer vos changements dans l'enregistrement.
Affecté à	Affectez le VUL à vous-même ou à un utilisateur spécifique dans un autre groupe d'affectation et cliquez sur **Mettre à jour** pour enregistrer vos changements dans l'enregistrement.

Que faire ensuite

Surveillez l'état de la nouvelle vulnérabilité pour accélérer sa résolution.

Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage

Il existe une relation synchronisée entre les champs d'état des tâches de rattrapage (VUL) et les champs d'état des demandes de changement (CHG) dans le Réponse aux vulnérabilités produit. Au fur et à mesure qu'une demande de changement avance dans son cycle de vie, elle déplace automatiquement l'état de toutes les tâches de rattrapage connexes.

Vue d'ensemble

L'enregistrement de tâche de rattrapage est appelé VUL dans les sections suivantes. Dans les versions précédentes de , les tâches de Réponse aux vulnérabilitésremédiation étaient appelées groupes de vulnérabilité (VG). Dans les images suivantes, VG = tâche de rattrapage, ou un enregistrement VUL.

La synchronisation d'état est activée par défaut par une propriété système (sn_vul.cr_state_synch) dans votre instance lorsque vous téléchargez l'application Réponse aux vulnérabilités .

Lorsque la synchronisation d'état est activée, le champ État CHG change automatiquement le champ État de la tâche de rattrapage dans les cas suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

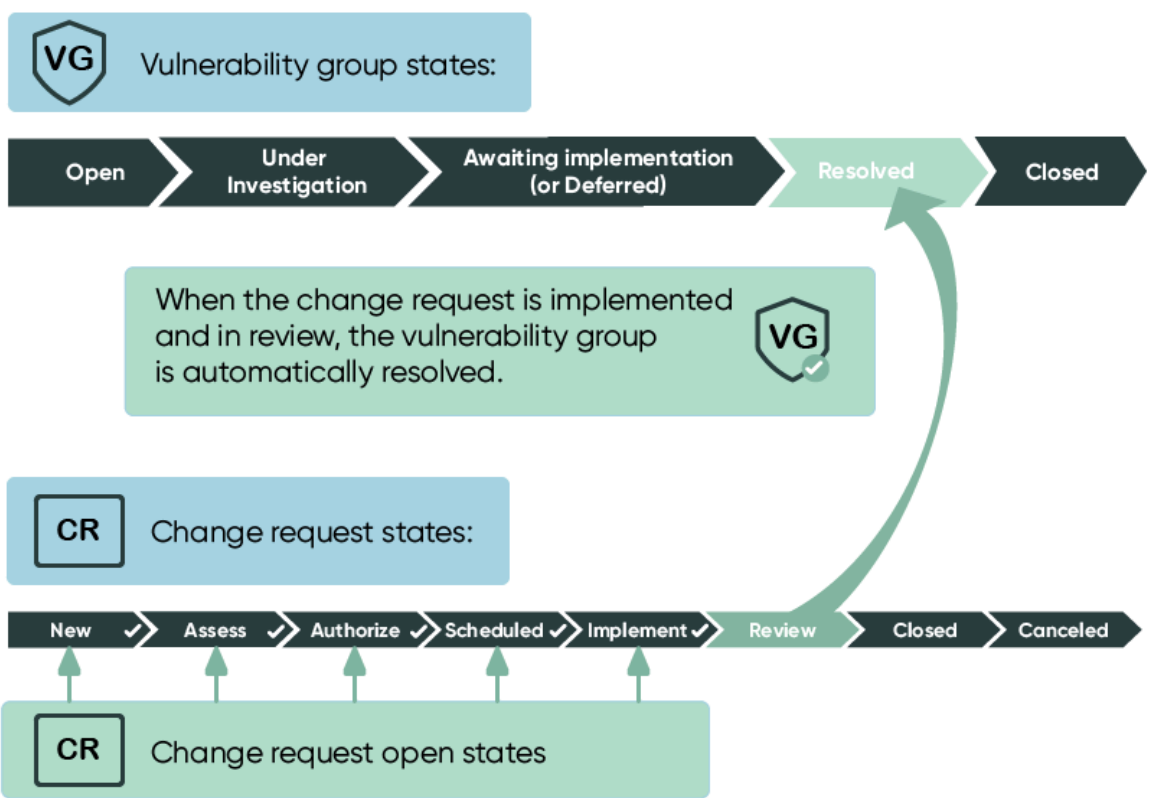
- Lorsqu'un nouveau CHG est créé pour une tâche de rattrapage (VUL), s'il n'est pas en `attente d'implémentation`, l'état VUL passe à `En attente d'implémentation`.
- Lorsqu'un CHG existant est associé à un VUL, s'il n'est pas en `attente d'implémentation`, l'état de VUL passe à `En attente d'implémentation`.
- Une fois que les tâches d'un CHG sont terminées (`implémentées`) et que le CHG est passé à l'état de `révision` , le VUL passe à l'état `Résolu`.

Pour plus d'informations et des exemples de synchronisation d'état, consultez les sections suivantes.

Remarque : Vous pouvez toujours déplacer manuellement les CHG et les VUL à travers les états de leurs cycles de vie respectifs sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'un VUL, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la vulnérabilité des états `Fermé` ou `Différé` .

Synchronisation de l'état vers l'avant

L'image suivante illustre comment les états CHG déplacent automatiquement les états VUL dans un cycle de vie vers l'avant, c'est-à-dire `d'Ouvert` à `Résolu`.



Vous pouvez créer de nouvelles demandes de changement pour n'importe quelle tâche de rattrapage dont l'état n'est pas `Fermé`. La synchronisation de l'état déplace automatiquement la vulnérabilité de manière bidirectionnelle entre les états `Ouvert`, `En cours d'examen`, `En attente d'implémentation` et `Résolu` . Ce déplacement est basé sur certaines valeurs du champ d'état de la demande de changement. La synchronisation d'état entre la demande de changement et la tâche de rattrapage est

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

invoquée automatiquement, sauf si la case à cocher (`Ajouter des CI au CR`) s'affiche sur un formulaire et que vous choisissez de la décocher.

La VUL ne passe pas à `l'état Résolu` lorsqu'un CHG est dans ses états ouverts. Tout CHG dans des états antérieurs à la `révision` dans son cycle de vie, tels que `Nouveau`, `Évaluer`, `Autoriser`, `Planifié` ou `Implémenter` , comme indiqué dans la figure précédente, est considéré comme un état ouvert pour le CHG. Les états ouverts ne déplacent pas le champ État sur la VUL, car les enquêtes ou les tâches sur le CHG ne sont pas terminées. La synchronisation d'état est invoquée lorsqu'un CHG est créé ou associé à la VUL, ou lorsque l'état d'une relation existante change sur le CHG. Les états CHG terminés sont `Examiner` et `Fermé` avec succès. Lorsqu'un CHG est fermé avec succès, ses codes fermés sont : `Successful` ou `Successful with issues`, auquel cas le VUL passe à `l'état Résolu`.

Synchronisation d'état en amont

Comme un CHG est traité au cours de son cycle de vie, il peut être annulé à un moment donné. Dans ce cas, si le CHG est `annulé` ou `fermé` (avec un code de fermeture en `échec`), le VUL revient automatiquement à `l'état En cours d'examen`. La vulnérabilité revient à `l'état En cours d'examen`, car il n'existe aucun plan actif pour corriger la vulnérabilité.

Si un VUL est à l'état `Résolu` et que vous créez un nouveau CHG ou l'associez à un CHG existant dans l'un des états ouverts initiaux, le VUL revient automatiquement à `l'état En attente d'implémentation`. Le VUL revient à cet état, car davantage de travail est maintenant affecté au CHG.

VUL avec plus d'un CHG

Si plusieurs CHG sont associés à une VUL en `attente d'implémentation` , la synchronisation de l'état est basée sur l'état du CHG au plus tôt de son cycle de vie. Par exemple, quatre CHG lui sont associés, CHG1, CHG2, CHG3 et CHG4, comme indiqué dans le tableau suivant.

Numéro CHG	État du CHG
1	Implémenter
2	Annulé
3	Fermé (code de fermeture de `En échec`)
4	Fermé (code de fermeture `réussi`)

Dans ce cas, la synchronisation de l'état entre le CHG et le VUL est basée sur CHG1, qui est dans l'état le plus ancien des quatre CHG, (`Implémenter`). Dans ce cas, le VUL reste en `attente d'implémentation`.

Dans un autre exemple, si une VUL est à l'état `Résolu` et qu'un CHG existant a été implémenté et est à l'état `Révision` , et qu'un nouveau CHG est créé, la VUL revient de `Résolu` à `En attente d'implémentation`. La synchronisation de l'état est basée sur le CHG dans l'état `Nouveau` , qui est le CHG dans l'état le plus ancien.

Numéro CHG	État du CHG
1	Revue
2	Nouveau

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

De plus, lorsque les VUL ont plus d'un CHG, l'état des VUL est automatiquement transféré dans les cas suivants :

- Lorsqu'un CHG passe à `l'état Révision`, si tous les autres CHG associés à la VUL sont à l'état `Révision` ou `Fermé` (avec un code de fermeture réussi), la VUL passe automatiquement à `l'état Résolu`. Tous les autres CHG associés qui sont annulés ou fermés sans succès sont ignorés.
- Lorsqu'un CHG passe à `l'état Annulé` ou `Fermé` (code de fermeture de `En échec`), si tous les autres CHG associés à la VUL sont dans le même état, la VUL revient automatiquement à `l'état En cours d'examen`.

Pour en savoir plus sur les états des tâches de rattrapage et sur ce que vous pouvez faire dans chaque état, reportez-vous à la section Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables.

Évaluer votre exposition aux logiciels vulnérables

Vous pouvez fournir des informations sur l'éditeur et le produit dans le module Évaluation de l'exposition pour évaluer l'exposition zero-day (jour actuel) de vos actifs à des logiciels vulnérables à l'aide de l'application Gestion des actifs logiciels pour ITSM (SAM) Foundation.

Important : Vous pouvez effectuer l'évaluation de l'exposition par logiciel et par vulnérabilités et expositions courantes (CVE) pour tirer parti des options supplémentaires de l'espace de travail d'évaluation de la vulnérabilité. Pour plus d'informations, consultez Explorer l'espace de travail de l'évaluation de la vulnérabilité.

Avant de commencer

Rôle requis : administrateur de vulnérabilité (sn_vulnerability_write)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Disposez des informations suivantes sur le logiciel vulnérable que vous souhaitez évaluer :

- Éditeur
- Version
- Produit
- Édition

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la configuration requise, reportez-vous à la section Configurer l'évaluation de l'exposition à la vulnérabilité.

Affichez le module d'évaluation de l'exposition logicielle et créez et modifiez des enregistrements d'évaluation de l'exposition sur demande pour les logiciels vulnérables de votre Now Platform® instance.

Vous gérez les activités de Vulnerability Response pour une grande opération responsable de nombreux actifs. Le centre des opérations de sécurité (SOC) de votre exploitation vous contacte au sujet d'une version de logiciel qu'il a apprise comme étant vulnérable. Vous découvrez qu'une analyse de vos actifs a été effectuée récemment et que vous n'avez pas trouvé cette vulnérabilité. L'équipe SOC a pris connaissance de cette vulnérabilité auprès d'une source fiable en dehors de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou des autres bibliothèques tierces de votre

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

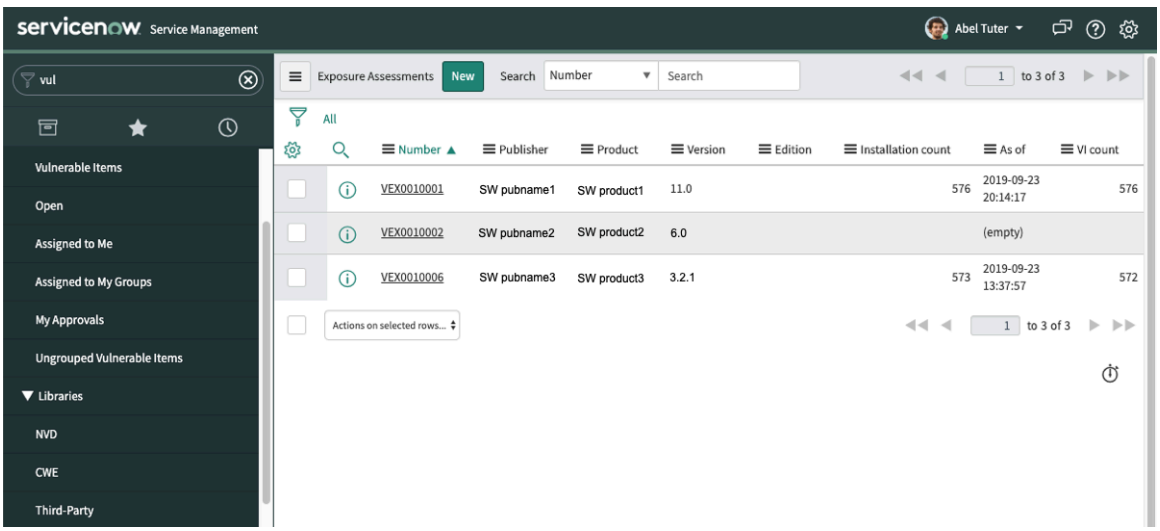
instance, et vous craignez que votre scanner de vulnérabilité n'ait pas encore ajouté le module d'extension correspondant.

Vous êtes sûr que les données de cette vulnérabilité seront mises à jour dans le NVD et importées prochainement afin que votre scanner puisse détecter cette vulnérabilité lors de la prochaine analyse, mais comme vous êtes préoccupé par l'étendue de votre exposition potentielle, vous souhaitez déterminer aujourd'hui si vous avez des actifs dans votre réseau sur lesquels ce logiciel est installé.

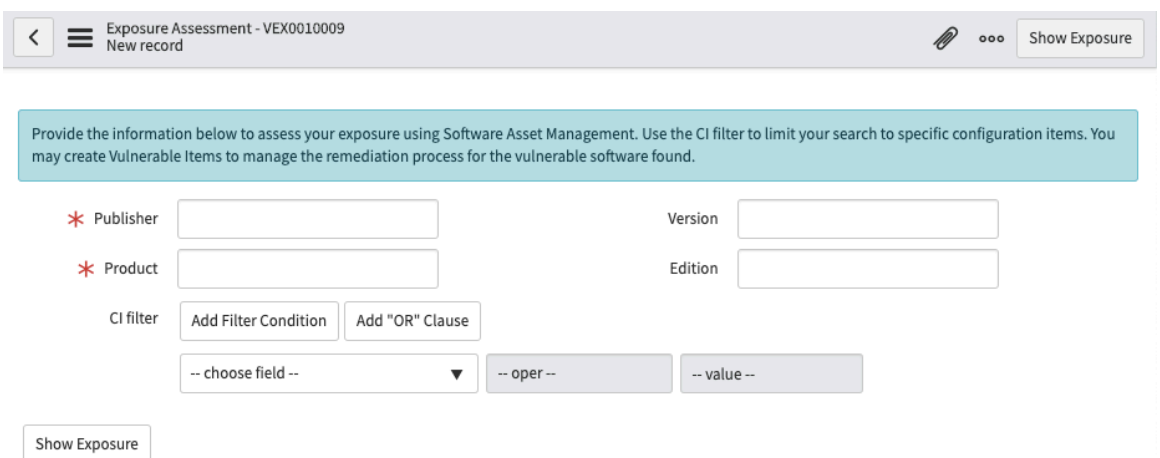
À partir de la version 23.0 de Réponse aux vulnérabilités, si vous disposez de l'abonnement Pro ou Enterprise, vous êtes redirigé vers la page **Évaluation de l'exposition** dans les espaces de travail en fonction de votre rôle lorsque vous sélectionnez le lien Évaluation de **l'exposition** dans le menu Tout. Pour plus d'informations, consultez Configurer l'évaluation de l'exposition à la vulnérabilité.

Procédure

1. Pour créer une nouvelle évaluation de l'exposition, accédez à **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Évaluation de l'exposition**.
   La liste des évaluations de l'exposition s'affiche.



2. Sélectionnez **Nouveau**.
   Le formulaire d'évaluation de l'exposition s'affiche.



3. Remplissez le formulaire.

Traduction automatique

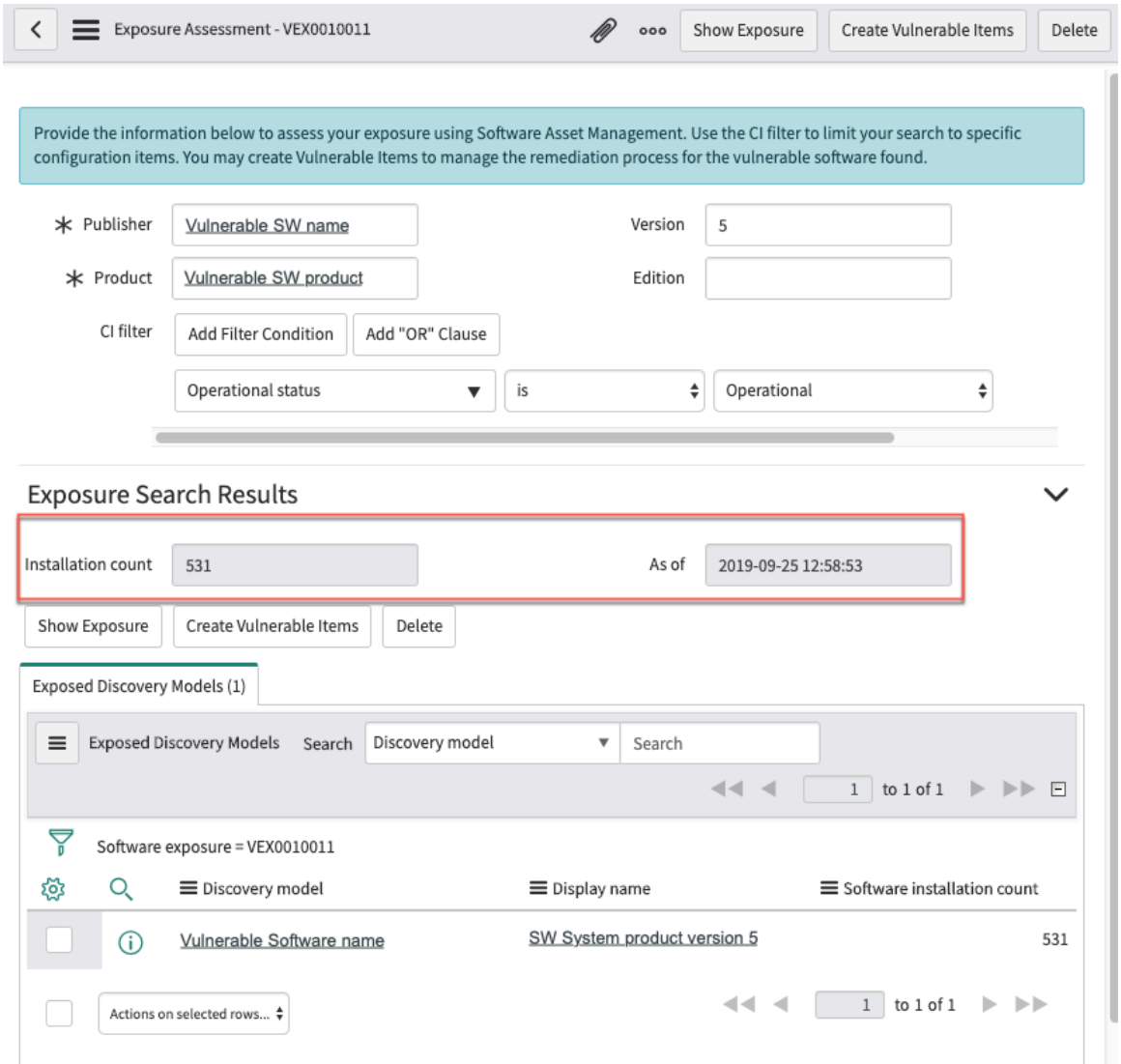
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Éditeur	Nom de l'éditeur du logiciel.
(Facultatif) Version	Saisissez le numéro de version pour vous aider à affiner la recherche sur vos actifs.
Produit	Nom du produit logiciel.
(Facultatif) Édition	Saisissez l'édition pour vous aider à affiner la recherche sur vos actifs.
Filtre de CI	Utilisez les listes de choix du filtre d'éléments de configuration (CI) pour limiter votre recherche à des éléments de configuration spécifiques (ressources). Par exemple, vous pouvez soumettre une requête uniquement pour les actifs actifs sur lesquels ce logiciel est peut-être installé : `L'état opérationnel est Opérationnel`

4. Sélectionnez **Afficher l'exposition**.
   L'enregistrement de l'évaluation de l'exposition avec votre modèle de détection et le nombre d'installations de logiciels sur vos actifs à la date spécifique s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Choisissez-en un pour continuer.

Option	Description
Afficher l'exposition	Ajoutez des conditions de filtre CI supplémentaires et sélectionnez **Afficher l'exposition** pour affiner davantage vos résultats de recherche.
Créer des éléments vulnérables	Créez des éléments vulnérables pour les éléments de configuration à partir de vos résultats de recherche. Si des éléments vulnérables sont créés avec succès, une tâche de rattrapage est créée pour tous les éléments vulnérables et affichée sur l'enregistrement d'évaluation de l'exposition.
Supprimer	Supprimez cet enregistrement et revenez à la liste des évaluations de l'exposition. Une boîte de dialogue de confirmation s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Facultatif : Créez un élément vulnérable pour votre résultat de recherche.

   Remarque : Une fois que vous avez créé des éléments vulnérables, vous ne pouvez plus modifier les critères de recherche pour cet enregistrement d'exposition.

7. Vous pouvez également modifier vos conditions de filtre et affiner davantage vos résultats de recherche.
8. Pour créer des éléments vulnérables, procédez comme suit :

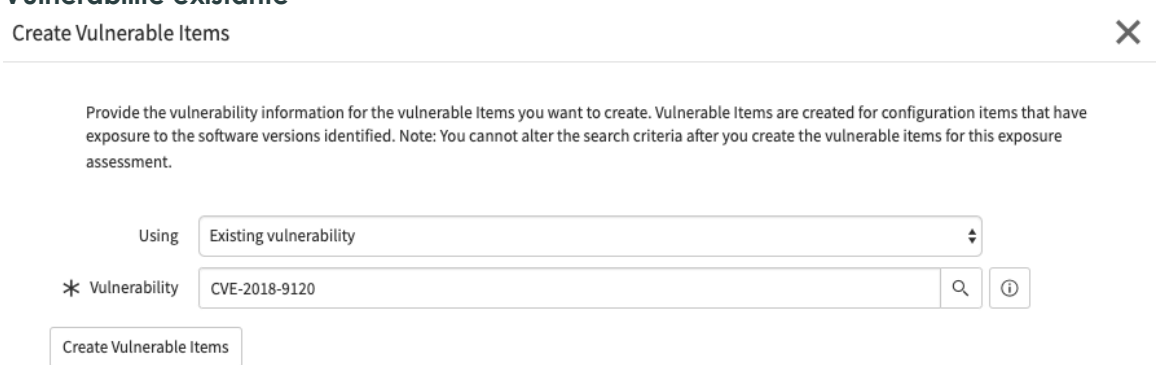
   a. Sélectionnez **Créer des éléments vulnérables**.
   La boîte de dialogue Créer des éléments vulnérables s'affiche.

   b. Renseignez les champs.

Champ	Description
Utilisant	Formez la liste de choix, choisissez-en une pour continuer. ▪ **Vulnérabilité existante**. À droite du champ Vulnérabilité, cliquez sur l'icône de recherche. Dans la liste qui s'affiche, sélectionnez le CVE-ID ou entrez des critères de recherche pour localiser le CVE-ID existant, par exemple, CVE 2018-9120. **Remarque :** Il peut s'agir d'un CVE-ID provenant d'une base de données de vulnérabilités autre que la NVD. ▪ **Nouvelle vulnérabilité**. Saisissez le CVE-ID de votre nouvelle vulnérabilité au format xxxx-xxxx, xxxx-xxxxx ou xxxx-xxxxxxx.
Résumé de la vulnérabilité (pour la nouvelle vulnérabilité uniquement)	Saisissez un résumé pour la nouvelle vulnérabilité, par exemple, `Un attaquant peut exécuter un script sur le navigateur d'un utilisateur peu méfiant`.

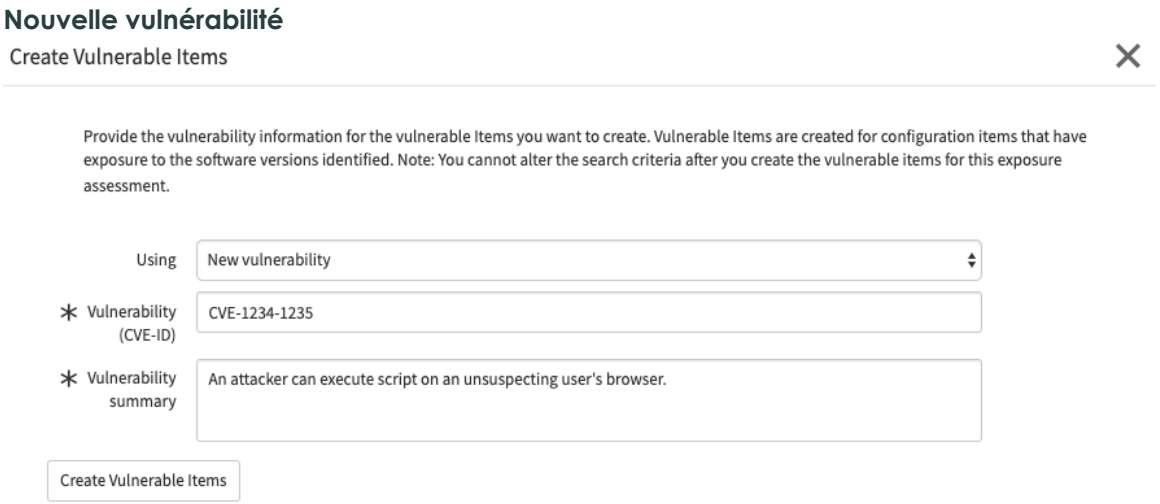
Les images suivantes montrent des exemples de formulaire rempli pour une vulnérabilité existante et une nouvelle vulnérabilité.

Vulnérabilité existante



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



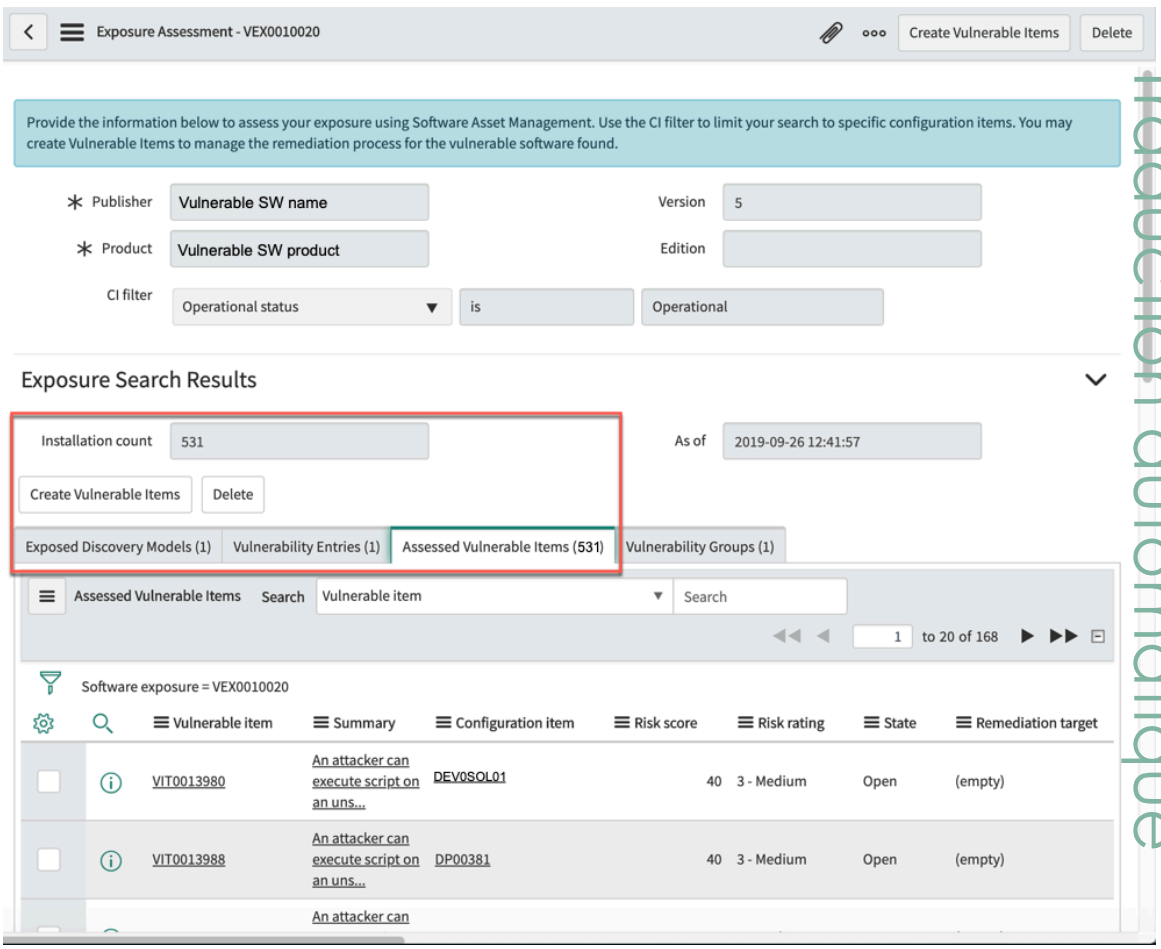
c. Sélectionnez **Créer des éléments vulnérables**.
L'enregistrement de l'évaluation de l'exposition s'affiche avec un message d'état qui indique que des éléments vulnérables sont en cours de création.

d. Après quelques secondes, en haut du formulaire, faites un clic droit dans la bannière grise pour recharger la page.
Les nouveaux éléments vulnérables sont affichés, comme le montre la figure suivante dans l'onglet Éléments vulnérables évalués (531). La nouvelle tâche de rattrapage créée pour ces éléments vulnérables s'affiche dans l'onglet Tâche de rattrapage (1).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Dans cet exemple, une tâche de rattrapage est créée en fonction des règles et conditions de groupe de la règle de la tâche de rattrapage appelée Vulnérabilité. Cette règle de groupe est la règle de tâche de rattrapage par défaut installée avec le produit Vulnerability Response dans votre Now Platform® instance. Dans cet exemple, les conditions de cette règle de regroupement ont placé tous les éléments vulnérables dans une seule tâche de rattrapage. Si vous préférez créer plusieurs tâches de rattrapage pour les éléments vulnérables qui correspondent aux résultats de recherche de votre évaluation de l'exposition, vous pouvez configurer des règles de tâche de rattrapage supplémentaires. La création d'autres tâches de rattrapage peut vous aider à éviter de créer des tâches de rattrapage avec un grand nombre d'éléments vulnérables. Pour en savoir plus sur les règles de tâche de rattrapage, reportez-vous aux rubriques Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage et Créer ou modifier Réponse aux vulnérabilités des règles de tâche de rattrapage.

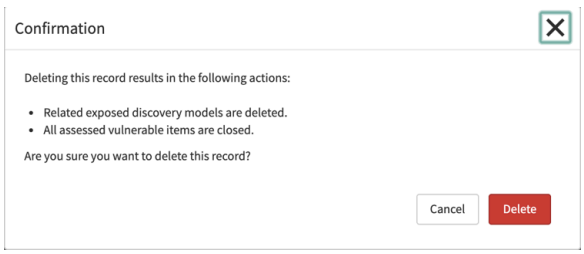


Traduction automatique

9. Choisissez-en un pour continuer.

Option	Description
Tâches de rattrapage	Après avoir sélectionné l'onglet Tâches de rattrapage, dans la colonne numérique, cliquez pour ouvrir l'enregistrement, puis examiner et affecter la tâche de rattrapage. Pour en savoir plus sur les groupes d'affectation, reportez-vous à Création de groupes .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Éléments de vulnérabilité évaluée	Après avoir sélectionné l'onglet Éléments vulnérables évalués, dans la colonne Éléments vulnérables, cliquez pour ouvrir les enregistrements et examiner et affecter des éléments vulnérables individuels.
Supprimer	Supprimer l'enregistrement de l'évaluation de l'exposition. Une boîte de dialogue de confirmation s'affiche. **Remarque :** Si vous supprimez l'enregistrement d'exposition après avoir créé des éléments de vulnérabilité, tous les éléments vulnérables que vous créez pour cet enregistrement et qui ne sont pas liés à un autre enregistrement d'exposition passent automatiquement à l'état `Fermé` . La raison de la fermeture est `Annulé`.
	

Que faire ensuite

Répondez à toute menace zero-day (jour actuel) en fonction de votre évaluation de l'exposition. Pour plus d'informations sur les tâches de rattrapage et la gestion des changements pour Réponse aux vulnérabilités, consultez et Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapageGestion des changements pour Réponse aux vulnérabilités.

Affichage des recommandations d'affectation

Un groupe d'affectation est généralement alloué à un élément vulnérable à l'aide de règles d'affectation. Ces règles sont configurées par l'administrateur de vulnérabilité pour allouer les groupes d'affectation appropriés en fonction des données reçues des scanners tiers.

Pour plus d'informations, consultez Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation. Si un groupe d'affectation correspondant n'est pas disponible ou est incorrect, vous pouvez l'utiliser Recommandations d'affectation de vulnérabilité pour afficher d'autres groupes d'affectation.

Utilisez l'action Recommandations d'affectation de vulnérabilité pour effectuer les actions suivantes :

- Demander des recommandations de groupe d'affectation pour un élément vulnérable.
- Demander des recommandations de groupe d'affectation pour plusieurs éléments vulnérables.
- Demander des recommandations de groupe d'affectation pour une tâche de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander des recommandations de groupe d'affectation pour un élément vulnérable

Demande Recommandations d'affectation de vulnérabilité afin que vous puissiez afficher les recommandations du groupe d'affectation. Vous pouvez demander des recommandations si un groupe d'affectation correspondant n'est pas disponible ou est incorrect pour un élément vulnérable (VI).

Avant de commencer
Rôle requis : sn_vul.remediation_owner

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables** et ouvrez un VI. L'élément doit être à l'état Ouvert, Différé, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur l'icône de recommandation ( ) en regard du champ **Groupe d'affectation** pour des suggestions d'affectation pour ce VI.
3. Dans la boîte de dialogue Recommandations de groupe d'affectation, sélectionnez une recommandation basée sur le score de confiance.
   Le score de confiance prédit la pertinence de la correspondance pour le VI. Pour plus d'informations, consultez Solutions d'apprentissage machine pour Réponse aux vulnérabilités.
4. Cliquez sur **Affecter**.

Résultats
Le groupe sélectionné apparaît dans le champ **Groupe d'affectation** et le type d'affectation devient Recommandation.

Demander des recommandations de groupe d'affectation pour plusieurs éléments vulnérables

Utilisez cette propriété Recommandations d'affectation de vulnérabilité pour afficher les recommandations du groupe d'affectation pour plusieurs éléments vulnérables (VI) à l'aide d'une modification en bloc. Lorsque plusieurs VI sont sélectionnés, une prédiction est effectuée sur un échantillon aléatoire des VI sélectionnés.

Avant de commencer
Rôle requis : sn_vul.remediation_owner

Pourquoi et quand exécuter cette tâche
Les recommandations et leurs scores de confiance peuvent différer légèrement d'une invocation à l'autre, en fonction des échantillons prélevés à partir des VI sélectionnés. Le score de confiance évalue si le système est convaincu que le groupe d'affectation recommandé est apte à résoudre la vulnérabilité. Utilisez la propriété système `assignment_recommendation_batchsize` pour définir la taille du lot lorsque vous demandez Recommandations d'affectation de vulnérabilité des tâches de rattrapage (VUL) et des VI à l'aide de l'option de modification en bloc. La valeur par défaut de cette propriété système est définie pour des performances de prédiction optimales.

Remarque : Si vous augmentez la valeur par défaut, le délai de réponse pour Recommandations d'affectation de vulnérabilité ces tickets peut changer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Élément vulnérable** et sélectionnez plusieurs VI.
   Les éléments doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur **Modifier en bloc**.
3. Renseignez les champs du formulaire.

Formulaire d'éléments vulnérables en bloc

Champ	Description
Sélection d'enregistrement	Enregistrements à sélectionner pour modification en bloc.
Groupe d'affectation	Groupe d'affectation à définir pour les éléments vulnérables sélectionnés. Pour afficher les groupes d'affectation recommandés, cliquez sur l'icône de recommandation (icône en regard du champ. Sélectionnez une recommandation basée sur le score de confiance et cliquez sur **Affecter**.
Notes de travail	Notes à ajouter.

4. Cliquez sur **OK**.

Résultats
Le groupe sélectionné apparaît dans le champ **Groupe d'affectation** et le type d'affectation devient Recommandation pour tous les VI sélectionnés.

Demander des recommandations de groupe d'affectation pour une tâche de rattrapage

Permet Recommandations d'affectation de vulnérabilité d'afficher les recommandations du groupe d'affectation pour une tâche de rattrapage (VUL).

Avant de commencer
Rôle requis : sn_vul.remediation_owner

Pourquoi et quand exécuter cette tâche
Utilisez la propriété système `assignment_recommendation_batchsize` pour définir la taille du lot lorsque vous demandez Recommandations d'affectation de vulnérabilité des VUL et des éléments vulnérables (VI) à l'aide de l'option de modification en bloc. La valeur par défaut de cette propriété système est définie pour des performances de prédiction optimales.

Remarque : Si vous augmentez la valeur par défaut, le délai de réponse pour Recommandations d'affectation de vulnérabilité ces tickets peut changer.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation** et sélectionnez un VUL.
   Le groupe doit être dans l'état Ouvert, En cours d'examen ou En attente d'implémentation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Cliquez sur l'icône de recommandation ( ) en regard du champ **Groupe d'affectation** pour les recommandations du groupe d'affectation pour la VUL sélectionnée.
   La boîte de dialogue Recommandations de groupe d'affectation affiche les groupes d'affectation recommandés avec le score de confiance moyen pour tous les VI de ce groupe.
3. Sélectionnez une recommandation dans la liste des groupes d'affectation en fonction du score de confiance.
   Le score de confiance prédit la pertinence de la correspondance pour la VUL sélectionnée.
4. Cliquez sur **Affecter**.
   Le groupe sélectionné apparaît dans le champ **Groupe d'affectation** .
5. Enregistrez la tâche de rattrapage avec les informations mises à jour.

Résultats
Tous les VI ayant le même groupe d'affectation que le VUL sont affectés au groupe d'affectation sélectionné. Le type d'affectation devient Recommandation pour le VUL ainsi que tous les VI modifiés.

Demande et approbation d'une exception

Vous pouvez demander à différer le rattrapage d'un élément vulnérable ou d'une tâche de rattrapage pour une période spécifiée. Par exemple, en tant que propriétaire du rattrapage, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine. Les approbateurs qui y ont accès peuvent approuver les demandes d'autres utilisateurs.

Vous pouvez demander des exceptions à partir Réponse aux vulnérabilités des espaces de travail. Consultez Demander une exception dans le Espace de travail de remédiation IT.

- Demander une exception pour un élément vulnérable
- Demander une exception pour une tâche de rattrapage
- Demander une exception en bloc

Vous pouvez également demander des exceptions de politique à l'aide de GRC : gestion de la politique et de la conformité:

- Demander une exception à l'aide de GRC : gestion de la politique et de la conformité
- Demander une exception en bloc à l'aide de GRC : gestion de la politique et de la conformité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Des notifications par e-mail sont envoyées à chaque étape de la gestion des exceptions, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'une exception est demandée, le demandeur reçoit un e-mail confirmant que la demande est émise. L'approbateur reçoit également un e-mail l'informant qu'une exception a été demandée.

À partir de la version 21.0 de Réponse aux vulnérabilités, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Demander une exception pour un élément vulnérable

Demandez une exception pour un élément vulnérable (VI) qui ne peut pas être corrigé immédiatement. Par exemple, en tant que propriétaire du rattrapage, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine.

Avant de commencer

Rôle requis : sn_vul.remediation_owner

Pourquoi et quand exécuter cette tâche

Important : Vous pouvez demander des exceptions au Gestionnaire de vulnérabilité et aux espaces de travail de remédiation informatique. Pour plus d'informations, consultez Demander des exceptions pour les tâches et les enregistrements de rattrapage auprès du Espace de travail du gestionnaire de vulnérabilités et Demander une exception dans le Espace de travail de remédiation IT.

Vous pouvez également demander des exceptions pour les VI dans l'environnement classique.

Remarque :

À partir de la version 21.0 de Réponse aux vulnérabilités, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Tout**.
2. Sélectionnez l'élément pour lequel vous souhaitez demander une exception. L'élément sélectionné doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Sur le formulaire Élément vulnérable, cliquez sur **Demande d'exception**.
4. Si Réponse aux vulnérabilités cette option est sélectionnée dans l'écran Gestion des exceptions, renseignez les champs du formulaire Demande d'exception.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée sélectionnée dans le **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Gestion des exceptions** écran. Lorsque la demande d'exception expire, le groupe revient à l'état Ouvert. **Remarque :** À partir de la version 18.0 de Réponse aux vulnérabilités (VR), si un élément vulnérable a été différé pour correction à l'aide de la fonctionnalité de gestion des exceptions, alors au cas où il serait rouvert par le scanner, la date de report définie sur la vulnérabilité persistera. Pour activer cette fonctionnalité, définissez la valeur de la propriété *sn_vul.auto_defer_vit_in_active_exception_win* système sur vrai. De plus, la date **de fin** différée persiste même après la fermeture de l'élément vulnérable ou l'expiration de l'exception. Le rôle requis est sn_vul.manage_exception_configuration pour la lecture et l'écriture.
Motif	Motif de la demande. Les choix possibles sont les suivants : ◦ Risque accepté ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Contrôle d'atténuation en place ◦ Autre Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à la section Définir le mappage de motif de politique.
Information supplémentaire	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ obligatoire doit être mis à jour par le propriétaire du rattrapage.

5. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

L'état de l'élément vulnérable passe à En cours de révision. Utilisez l'onglet **Approbation de changement d'état** pour suivre l'état de la demande d'exception.

Demander une exception pour une tâche de rattrapage

Demandez une exception pour différer une tâche de rattrapage pendant une période spécifiée si elle ne peut pas être résolue immédiatement.

Avant de commencer

Important :

Vous pouvez demander des exceptions auprès du Gestionnaire de vulnérabilité et des espaces de travail de remédiation informatique. Consultez Demander une exception dans le Espace de travail de remédiation IT.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.remediation_owner

Vous pouvez également demander des exceptions pour les tâches de rattrapage dans l'environnement classique.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de rattrapage** > **Tout**.
2. Sélectionnez le groupe pour lequel vous souhaitez demander une exception.
   La tâche sélectionnée doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Dans l'enregistrement de tâche de rattrapage (VUL), sélectionnez **Demande d'exception**.
4. Renseignez les champs du formulaire.

Formulaire Demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée d'exception définie dans la configuration.
Motif	Justification de la demande d'exception.
Information supplémentaire	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ doit être mis à jour par le propriétaire du rattrapage.

5. Cliquez sur **Demander l'approbation**.

Demander une exception en bloc

Utilisez l'option de modification en bloc pour demander une exception pour plusieurs éléments vulnérables (VIT) au lieu de sélectionner manuellement chaque élément.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vul.vulnerability_analyst

Pourquoi et quand exécuter cette tâche
Lorsque plusieurs VIT sont sélectionnés, une tâche de rattrapage (VUL) est formée avec ces éléments. Pour plus d'informations sur la modification de plusieurs VIT, reportez-vous Modifier les éléments vulnérables en bloc dans Réponse aux vulnérabilités à la section .

Important : Vous pouvez demander une exception pour :

- un VIT du Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT. Pour plus d'informations, consultez Demander une exception dans le Espace de travail de remédiation IT.
- plusieurs VIT du Espace de travail du gestionnaire de vulnérabilitésfichier . Pour plus d'informations, consultez Demander une exception en bloc dans Vulnerability Manager Workspace.

Procédure
1. Accédez à la **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Tout** et sélectionnez les éléments pour lesquels vous souhaitez demander une exception.
   Les éléments sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur **Modifier en bloc**.
3. Renseignez les champs du formulaire.

Formulaire de modification en bloc de l'élément vulnérable

Champ	Description
Sélection d'enregistrement	Enregistrements que vous avez sélectionnés pour une modification en bloc.
État	État de l'élément vulnérable. Sélectionnez l'état Différé pour demander une exception pour les éléments sélectionnés.
Motif	Sous-état de l'état que vous avez sélectionné.
Description brève	Nom de la tâche de rattrapage que vous créez.
Jusqu'à	Date de fin que vous spécifiez pour votre demande d'exception.
Information supplémentaire	Détails supplémentaires que vous souhaitez mentionner pour informer l'approbateur des raisons de votre demande.
Solution privilégiée	Solution ciblée pour la correction de tous les éléments vulnérables que vous avez sélectionnés pour une modification en bloc.
Groupe d'affectation	Groupe d'affectation pour le VI. Vous pouvez sélectionner un groupe manuellement ou utiliser les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	recommandations d'affectation si cette fonctionnalité est activée.
Notes de travail	Notes à ajouter.

4. Cliquez sur **OK**.
   Une tâche de rattrapage contenant les VI que vous avez sélectionnés est créée. Cette tâche de rattrapage est soumise pour approbation.

Demander une exception à l'aide de GRC : gestion de la politique et de la conformité

Demandez des exceptions de politique à l'aide de l'option GRC de gestion des exceptions de politique de l'application à partir de .Gestion de la politique et de la conformitéRéponse aux vulnérabilités

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions de politique, vous devez télécharger l'application GRC : gestion de la politique et de la conformité à partir du ServiceNow Store.

Rôle requis : sn_vul.remediation_owner

Vous pouvez également demander des exceptions dans l'interface utilisateur classique :

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables** (ou **Tâches de rattrapage**)>**Tous**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.
   L'élément ou le groupe sélectionné doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Sur le formulaire sélectionné, cliquez sur **Demande d'exception**.
3. Renseignez les champs du formulaire.

Formulaire Demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas sélectionnée, tous les objectifs de contrôle sont listés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date du jour. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale (jours) de l'exception** que vous avez définie pour la politique dans Policy and Compliance. Pour plus d'informations, reportez-vous à la section Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ obligatoire doit être renseigné par le propriétaire du rattrapage.

4. Cliquez sur **Envoyer**.
   Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez la configuration facultative de Gestion de la politique et de la conformité .

Demander une exception en bloc à l'aide de GRC : gestion de la politique et de la conformité

Sélectionnez un groupe d'éléments vulnérables et soumettez une exception en bloc.

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions en bloc, vous devez télécharger l'application GRC : gestion de la politique et de la conformité à partir du ServiceNow Store.

Remarque : Pour utiliser cette fonctionnalité, vous devez effectuer une mise à niveau GRC : gestion de la politique et de la conformité avant de mettre à niveau Réponse aux vulnérabilités. Si vous avez déjà effectué une mise à niveau Réponse aux vulnérabilités antérieure GRC : gestion de la politique et de la conformitéet que vous souhaitez utiliser cette fonctionnalité, vous devez effectuer à nouveau les procédures de mise à niveau dans le bon ordre.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.remediation_owner

Vous pouvez également demander des exceptions dans l'environnement classique de .Réponse aux vulnérabilités

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Tout** et sélectionnez les éléments pour lesquels vous souhaitez demander une exception. Les éléments sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur **Modifier en bloc**.
3. Renseignez les champs du formulaire.

Formulaire de modification en bloc de l'élément vulnérable

Champ	Description
Sélection d'enregistrement	Enregistrements que vous avez sélectionnés pour une modification en bloc.
État	État de l'élément vulnérable. Sélectionnez l'état Différé pour demander une exception pour les éléments sélectionnés.
Description brève	Nom de la tâche que vous créez.
Solution privilégiée	Solution que vous ciblez pour corriger tous les éléments vulnérables que vous avez sélectionnés pour la modification en bloc.
Groupe d'affectation	Groupe d'affectation pour le VI. Vous pouvez sélectionner un groupe manuellement ou utiliser les recommandations d'affectation si cette fonctionnalité est activée.
Notes de travail	Notes à ajouter.

4. Cliquez sur **OK**.
   Une tâche de rattrapage est créée avec les éléments vulnérables sélectionnés.
5. Renseignez les champs du formulaire.

Formulaire Demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas sélectionnée, tous les objectifs de contrôle sont listés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date du jour. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale (jours) de l'exception** que vous avez définie pour la politique dans GRC : gestion de la politique et de la conformité. Pour plus d'informations, reportez-vous à la section Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ obligatoire doit être renseigné par le propriétaire du rattrapage.

6. Cliquez sur **Envoyer**.
   Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez la configuration facultative de Gestion de la politique et de la conformité .

Approuver ou rejeter une demande d'exception dans Réponse aux vulnérabilités

Approuvez ou rejetez les demandes d'exception pour les éléments vulnérables ou les tâches de rattrapage qui ne peuvent pas être corrigés immédiatement. Vous devez évaluer les risques de ces demandes, puis approuver leur report jusqu'à ce qu'elles puissent être corrigées.

Important :

Vous pouvez approuver ou rejeter les demandes d'exception dans le Espace de travail du gestionnaire de vulnérabilitésfichier . Pour plus d'informations, consultez Approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer
Rôle requis : sn_vul.exception_approver
Vous pouvez également approuver les demandes d'exception dans l'environnement classique.

Remarque :

À partir de la version 21.0 de Réponse aux vulnérabilités, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Utilisation d'une règle d'exception

Vous pouvez demander une exception pour les vulnérabilités, les éléments vulnérables (VI) ou les éléments de configuration (CI) qui ne peuvent pas être corrigés ou différés immédiatement. En automatisant le processus de report des VI, vous pouvez différer les éléments vulnérables correspondants en fonction de la règle lorsque le système les identifie.

Vous pouvez effectuer les tâches suivantes pour une règle d'exception :

- Créer une règle d'exception
- Approuver une demande de règle d'exception
- Activation d'une règle d'exception
- Rouvrir une règle d'exception
- Mettre à jour une règle d'exception approuvée
- Supprimer une règle d'exception

Remarque :

À partir de la version 21.0 de Réponse aux vulnérabilités, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Créer une règle d'exception

Créez une règle pour demander automatiquement une exception pour une condition spécifique pour un groupe d'éléments vulnérables (VI), telle qu'une règle avec une condition basée sur la gravité de vulnérabilité de ces VI. Avec cette règle, vous pouvez différer automatiquement les VI nouveaux et existants s'ils correspondent à la condition de règle approuvée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

La règle s'applique à partir de la date « Valide à partir de » jusqu'à la date « Valide jusqu'à ». La tâche de rattrapage (VUL) est créée lorsque la règle est approuvée. La méthode de regroupement de cette vulnérabilité est connue sous le nom de règles d'exception. La vulnérabilité est créée à l'état Différé. Vous ne pouvez pas fermer, rouvrir ou supprimer ce VUL. Les VI nouveaux et rouverts sont différés et ajoutés à cette VUL à partir de la date de début de validité jusqu'à l'expiration du groupe à la date de fin de validité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de la règle d'exception. Ces e-mails fournissent l'état et d'autres détails d'une demande. Par exemple, lorsqu'une règle d'exception est demandée, le demandeur reçoit un e-mail qui confirme que la demande est envoyée.

Remarque : Si la règle est rejetée, vous pouvez la rouvrir à l'état Brouillon, la mettre à jour, puis la soumettre à nouveau pour approbation.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'exception**.
2. Sur la page d'enregistrement Nouvelle règle d'exception, cliquez sur **Nouveau** pour créer une règle.
3. Renseignez les champs du formulaire.

Formulaire Règle d'exception

Champ	Description
Nom	Nom de la règle d'exception.
Début de validité	Date à partir de laquelle cette règle est active pour différer les VI.
Date de fin de validité	Date à partir de laquelle la tâche de rattrapage cesse d'accepter de nouveaux VI.
Motif	Raison pour laquelle cette règle d'exception a été créée.
Groupe d'affectation	Groupe auquel la tâche de rattrapage créée pour le suivi des VI différés est affectée.
Information supplémentaire	Informations supplémentaires que le demandeur souhaite fournir à l'approbateur. Ces informations sont renseignées dans le champ de description de la tâche de rattrapage.
Condition	Condition de filtre pour les VI qui peut être définie lors du traitement des VI.
Exécuter sur les données existantes	Option qui vous permet d'exécuter cette règle sur des données existantes la première fois que cette règle est exécutée.
Étape du workflow	État d'approbation actuel de la règle d'exception.
État	État de la règle d'exception.
Ordre d'exécution	Ordre unique pour chaque règle d'exception.
Reporté jusqu'à	Date jusqu'à laquelle les VUL et VI sont reportés. À cette date, la vulnérabilité créée est fermée, tous les VI sortent du

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	groupe et les règles de groupe sont réappliquées.

4. Ajoutez le groupe d'affectation lors de la création de la règle.
5. Envoyez le formulaire pour approbation.
   L'état de la demande passe à En cours de révision. Tant que vous n'avez pas soumis la règle d'exception, elle reste à l'état Brouillon.

Approuver une demande de règle d'exception

évaluer les demandes de règles d'exception émanant des utilisateurs afin de pouvoir approuver ou rejeter ces demandes.

Avant de commencer
Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche
Les membres du groupe d'utilisateurs de niveau 1 de l'approbateur d'exception peuvent approuver les demandes de règles d'exception de niveau 1. De même, les membres du groupe d'utilisateurs de niveau 2 de l'approbateur d'exceptions peuvent approuver les demandes de règles d'exception de niveau 2. Les deux groupes d'utilisateurs héritent du rôle d'approbateur d'exception par défaut.

Remarque :

Si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas le repasser en workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et des faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande et expliquez pourquoi vous avez approuvé ou rejeté la demande.
   Après l'approbation d'une règle d'exception, une tâche de rattrapage (RT) est créée dans l'état Différé par défaut. À partir de la date de début de validité, cette règle s'exécute sur tous les VI créés, mais aussi sur ceux qui passent de l'état Fermé à l'état Ouvert. Les VI qui correspondent aux conditions définies sont ajoutés au RT et reportés pour la période spécifiée.

   Remarque : Si la règle est rejetée, vous pouvez la rouvrir à l'état Brouillon, la mettre à jour, puis la soumettre à nouveau pour approbation.

Activation d'une règle d'exception

Une règle est activée à sa date de début de validité. Après l'activation, il automatise le processus d'exception pour les éléments vulnérables (VI).

La règle d'exception suit le cycle de vie suivant :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Les nouveaux éléments vulnérables (VI) que vous créez ou rouvrez et qui remplissent la condition spécifiée sont reportés. Si vous activez l'option Exécuter sur les données existantes lors de la première exécution de la règle d'exception, tous les VI actifs et non différés qui correspondent à la condition de la règle d'exception sont déplacés vers la tâche de rattrapage (RT) nouvellement créée et son état devient Différé.
2. Si un VI nouvellement créé correspond à la condition de la règle d'exception, il est déplacé vers le RT différé qui est associé à la règle et la règle de groupe n'est pas exécutée dessus.
3. À la date de début de validité, les VI existants sont ajoutés si vous activez l'option Exécuter sur les données existantes.
4. Le RT cesse d'accepter de nouveaux VI lorsque la règle expire à la date de fin de validité. Le RT reste en vigueur jusqu'à la date « Différé jusqu'à ».
5. La règle d'exception expire à la date de fin de validité.

Demander une extension pour une règle d'exception

Demandez une prolongation pour une règle d'exception différée avant qu'elle n'atteigne sa date de report jusqu'à échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Règles d'exception**.
2. Sélectionnez une règle d'exception approuvée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle la règle d'exception doit être prolongée.
Motif	Entrez le motif du report de la règle d'exception. Les choix sont les suivants : ◦ Risque accepté ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les champs Reporté jusqu'à, Motif et Informations supplémentaires sont mis à jour sur la règle d'exception et les tâches de rattrapage et les éléments vulnérables associés. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure de l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une règle d'exception différée est à nouveau étendue, le nombre de reports prolongés augmente dans le back-end.
- À partir de la version 21.0 de Réponse aux vulnérabilités, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Rouvrir une règle d'exception

Rouvrez une règle d'exception qui a été rejetée, mais que vous souhaitez soumettre à nouveau. La réouverture de la règle la fait passer à l'état Brouillon.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Vous pouvez ensuite mettre à jour et soumettre à nouveau la règle pour approbation.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'exception**.
2. Recherchez la règle que vous souhaitez rouvrir et cliquez sur **Rouvrir**.
3. Mettez à jour le formulaire et soumettez-le à nouveau pour approbation.

Mettre à jour une règle d'exception approuvée

Annulez une règle approuvée pour pouvoir la mettre à jour. Par exemple, avant de pouvoir modifier des dates ou ajouter une condition à une règle approuvée, vous devez l'annuler afin que la tâche de rattrapage (VUL) soit supprimée et que les éléments vulnérables (VI) passent à l'état Ouvert.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Les règles de groupe sont réappliquées à ces VI. Soumettez la règle après avoir apporté les modifications afin qu'elle passe à nouveau par le processus d'approbation.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'exception**.
2. Ouvrez la règle d'exception que vous souhaitez annuler, puis cliquez sur **Annuler**.
3. Dans la boîte de dialogue Annuler la règle, cliquez sur **Annuler la règle**.
   La règle revient à l'état Brouillon et le VUL associé est supprimé. Les VI associés sont rouverts et les règles de groupe sont appliquées aux VI individuels.

Supprimer une règle d'exception

Supprimez une règle d'exception qui n'est plus requise. Par exemple, vous pouvez supprimer une règle si vous ne souhaitez pas différer un élément vulnérable (EV) pendant l'ingestion.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
La suppression d'une règle annule la tâche de rattrapage associée (VUL). Les VI associés sont rouverts et les règles de groupe sont appliquées aux VI individuels.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'exception**.
2. Ouvrez la règle d'exception que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue Supprimer la règle, cliquez sur **Supprimer la règle** pour supprimer la règle sélectionnée.
   La tâche de rattrapage associée est également supprimée. Les VI associés sont rouverts et les règles de groupe sont appliquées aux VI individuels.

Marquage et approbation d'un faux positif

Les éléments vulnérables (VI) et les tâches de remédiation (VUL) peuvent être marqués comme faux positifs. Les approbateurs ayant un accès en écriture peuvent approuver ces demandes de la part d'autres utilisateurs.

- Marquer comme faux positif
- Modification en bloc pour les faux positifs
- Approuver ou rejeter un faux positif

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de faux positif, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'un VI ou une tâche de rattrapage est marqué comme faux positif, le demandeur reçoit un e-mail de confirmation. Simultanément, l'approbateur reçoit un e-mail indiquant qu'un VI ou une tâche de rattrapage a été marqué comme faux positif.

À partir de la version 21.0 de Réponse aux vulnérabilités, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Marquer comme faux positif

Marquez un élément vulnérable (VI) ou une tâche de rattrapage (VUL) comme faux positif si l'avertissement émis par le scanner n'est pas réellement un problème. Par exemple, si un élément de configuration a été mis hors service, mais que le scanner soulève toujours un problème qui lui est lié, marquez-le comme faux positif.

Avant de commencer

Rôle requis : propriétaire de la résolution
Vous pouvez demander des faux positifs à partir Réponse aux vulnérabilités des espaces de travail. Consultez Demander un faux positif dans le Espace de travail de remédiation IT.

Vous pouvez également demander des faux positifs dans l'environnement classique :

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Éléments vulnérables (ou tâches de rattrapage)** > **Tout**.
2. Ouvrez le VI ou la VUL que vous souhaitez marquer comme faux positif et cliquez sur **Marquer comme faux positif**.
   Le VI ou le VUL doit être à l'état **Ouvert** .
3. Sur le formulaire Faux positif, saisissez les détails dans **Informations supplémentaires** et cliquez sur **Demander l'approbation**.
   La demande est envoyée pour approbation et l'état du VI ou de la VUL devient **En cours de révision**.

Modification en bloc pour les faux positifs

Utilisez la modification en bloc pour marquer plusieurs éléments vulnérables (VIT) comme faux positifs. Si plusieurs VIT sont sélectionnés, une tâche de rattrapage est formée avec ces éléments.

Important : En tant qu'administrateur ou analyste, vous pouvez utiliser la fonctionnalité de modification en bloc de Vulnerability Manager Workspace pour marquer plusieurs VIT comme faux positifs. Pour plus d'informations, consultez Modification en bloc pour les faux positifs dans Vulnerability Manager Workspace.

Avant de commencer

Rôle requis : propriétaire de la résolution
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Vous pouvez également demander des faux positifs dans l'environnement classique :

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Tout** et sélectionnez les éléments que vous souhaitez marquer comme faux positifs.
   Les éléments sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur **Modifier en bloc**.
3. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de modification en bloc de l'élément vulnérable

Champ	Description
Sélection d'enregistrement	Enregistrements à sélectionner pour modification en bloc.
État	État des éléments vulnérables. Sélectionnez Fermé pour marquer comme faux positif.
Motif	Sous-état de l'état sélectionné. Si vous avez sélectionné l'état Fermé, sélectionnez ici Faux positif pour marquer comme faux positif.
Annuler l'affectation	Soumettez une demande pour effacer les champs Affecté à et Groupe d'affectation.
Solution privilégiée	Solution ciblée pour le rattrapage de tous les éléments vulnérables sélectionnés pour la modification en bloc.
Groupe d'affectation	Groupe d'affectation pour le VI. Sélectionnez manuellement ou à l'aide des recommandations d'affectation si cette option est activée.
Notes de travail	Notes à ajouter.

4. Cliquez sur **OK**.
   Une nouvelle tâche de rattrapage contenant les VI sélectionnés est créée et cette tâche est envoyée pour approbation.

Approuver ou rejeter un faux positif

En tant qu'approbateur de faux positif, vous pouvez approuver ou rejeter les demandes de faux positif d'autres utilisateurs.

Important :

Vous pouvez approuver ou rejeter les demandes de faux positif dans le Espace de travail du gestionnaire de vulnérabilitésfichier . Pour plus d'informations, consultez Approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis : sn_vul.false_positive_approver ou sn_vul.app_false_positive_approver

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Vulnérabilités** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Remarque : Un faux positif peut être limité dans le temps. Seul l'approbateur peut définir la date de fin.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Solutions d'analyse et de génération de rapports pour Réponse aux vulnérabilités

La surveillance du rattrapage des vulnérabilités implique l'affichage des tendances, la gestion des risques et la surveillance des groupes d'affectation. Vous pouvez examiner les problèmes à risque élevé, les charges de travail des groupes d'affectation, les reports et les vulnérabilités récurrentes. Réponse aux vulnérabilités propose des outils, des rapports et des procédures pour rendre ce processus plus productif et efficace.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à suivre la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en visualisant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Consultez Espace de travail du gestionnaire de vulnérabilités et Exploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Les analystes de vulnérabilité peuvent également utiliser les tableaux de bord par défaut Réponse aux vulnérabilités à l'adresse **Tout** > **Réponse aux vulnérabilités** > **Vue d'ensemble**.

Important :

À partir de la version 19.0 de Réponse aux vulnérabilités, ce tableau de bord peut également être consulté dans l'interface utilisateur de la nouvelle expérience. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Tableaux de bord dans Vulnerability Manager Workspace et Tableaux de bord dans IT Remediation Workspace.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Réponse aux vulnérabilités Processus de rattrapage

La plupart des actions de rattrapage des vulnérabilités sont effectuées à partir de l'enregistrement de la tâche de rattrapage dans les Réponse aux vulnérabilités espaces de travail. À partir des tâches de rattrapage (RT) à l'état En cours d'examen, vous pouvez effectuer plusieurs tâches.

- Créer des demandes de changement.
- Ajoutez des notes de travail et des descriptions des vulnérabilités au sein de la tâche de rattrapage.
- Reportez la tâche de rattrapage et les éléments vulnérables qu'elle contient à une date ultérieure.
- Fermez la tâche de rattrapage.
- Suivez les nouvelles obligations de conformité réglementaire, qui sont généralement urgentes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Connectez-vous à votre instance Réponse aux vulnérabilités.
- Passez en revue votre Gestion des vulnérabilités ainsi que les tableaux de bord et rapports tiers pour localiser les zones problématiques. Par exemple, affichez les tableaux de bord qui affichent l'ancienneté des tâches de rattrapage (RT) par états ou des éléments vulnérables (VI) à risque élevé au-delà de leur date cible de rattrapage.
- Passez en revue l'état des tâches de rattrapage, par ordre de risque.
- Révisez l'ordre de priorité des tâches en ajustant vos calculateurs de score de risque si le score de risque n'est pas calculé correctement, ou en différant les VI ou les RT, selon les besoins. Consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité ou Différer une tâche de rattrapage pour plus d'informations sur ces options.
- Examinez les éléments vulnérables différés sur le point d'être rouverts et prenez des mesures supplémentaires si besoin. Si vous souhaitez initier et suivre des activités de changement sur vos actifs, vos tâches de rattrapage et leurs éléments vulnérables correspondants, reportez-vous à la rubrique Gestion des changements pour Réponse aux vulnérabilitéspour connaître les actions à entreprendre pour en savoir plus.
- Examinez les commentaires des opérations informatiques.

  Une fois que vous êtes informé qu'une demande de changement est résolue, attendez la prochaine analyse. Les analyses sont déclenchées automatiquement par le calendrier d'importation tierce configuré dans l'assistant de configuration.

- Après une analyse, si l'état est Fixe, les éléments vulnérables sont automatiquement fermés pendant l'importation. Le groupe se ferme lorsque tous les éléments vulnérables du groupe sont corrigés.
- Après l'analyse, si l'état n'est pas Fixe, le VI est automatiquement renvoyé à l'état En cours d'examen.

- Les éléments vulnérables définis sur « Résolu » dans votre instance, mais pas sur « Fermé/Résolu » par les exécutions d'intégration tierces sont rouverts s'ils sont détectés lors des nouvelles analyses.

  Pour Qualys les détections, si le scanner continue de trouver des VI qui ont été définis comme « Résolu » mais qui ne sont pas passés à « Fermé/Fixe » par les analyses suivantes, ces VI reviennent à « Ouvert » lorsque la dernière date trouvée est ultérieure à la date de résolution.

  Pour Rapid7 les détections, une option est maintenant disponible sur la page de Rapid7 configuration de votre instance pour rouvrir les VI résolus par âge. Si cette option est activée, les VI définis sur « Résolu », mais qui ne sont pas transitionnés à l'état « Fermé/Fixe » par les analyses suivantes, reviennent à l'état « Ouvert » après le nombre de jours que vous entrez.

Gestion des solutions pour vulnérabilités Progression du déploiement

Des mesures de déploiement complètes pour les tâches de rattrapage et les entrées de vulnérabilité sont incluses dans Gestion des solutions pour vulnérabilités sous **État de rattrapage** dans vulnérabilités, éléments vulnérables. Identifiez facilement la tâche de rattrapage ou la vulnérabilité qui ralentit la progression de la résolution. Explorez la façon dont la vulnérabilité est identifiée ou les aspects des actifs affectés qui peuvent être à l'origine du problème de rattrapage. Mettez à jour l'état de vos mesures à l'aide du lien connexe **Mettre à jour l'état** dans les formulaires Vulnérabilité, Solutions et Tâche de rattrapage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités

Le Réponse aux vulnérabilités tableau de bord de vue d'ensemble (Gestion de la vulnérabilité) fournit une vue d'ensemble des vulnérabilités et des éléments vulnérables, ce qui aide l'administrateur de vulnérabilité à identifier rapidement les zones de préoccupation. Le Réponse aux vulnérabilités tableau de bord de rattrapage (Rattrapage de vulnérabilité) permet à un spécialiste du rattrapage de se concentrer sur les tâches de rattrapage et les éléments vulnérables qu'il possède.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

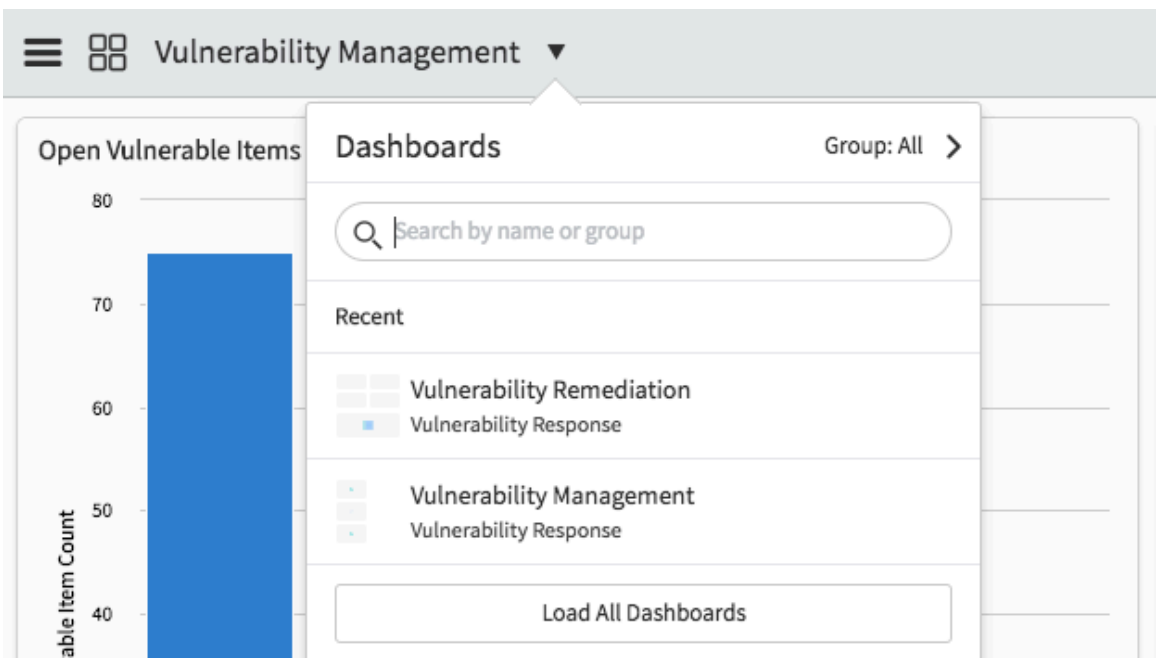
Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à suivre la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en visualisant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Reportez-vous à la rubrique Réponse aux vulnérabilités Espaces de travailet Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Les analystes de vulnérabilité peuvent également utiliser les tableaux de bord par défaut Réponse aux vulnérabilités .

Rôles requis : sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst et les utilisateurs ayant sn_vul.vulnerability_read (ou qui héritent du rôle sn_vul.vulnerability_read) et pa_viewer.

Les tableaux de bord par défaut Réponse aux vulnérabilités dans l'environnement hérité

Ces rapports sont inclus dans l'application et ne nécessitent pas d'abonnement Analyse des performances pour Réponse aux vulnérabilités distinct. Pour en ouvrir un, sélectionnez la liste de choix pour la développer et choisir un tableau de bord. Vous pouvez également saisir le nom d'un tableau de bord dans le champ de recherche.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Lorsque le pack de contenu pour Réponse aux vulnérabilités l'application Analyse des performances est installé et activé, le tableau de bord Gestion de la vulnérabilité (PA) s'affiche automatiquement dans le module de vue d'ensemble. Ce tableau de bord contient des rapports couvrant toutes les étapes du cycle de vie de la gestion des vulnérabilités.

Pour plus d'informations sur les rapports inclus dans le pack de contenu Analyse des performances pour Réponse aux vulnérabilités, consultez le tableau de bord Gestion de la vulnérabilité [PA].

Pour plus d'informations sur le tableau de bord CISO et les rapports de couverture de l'analyse, consultez le tableau de bord CISO de gestion des vulnérabilités.

Tableau de bord de gestion de la vulnérabilité

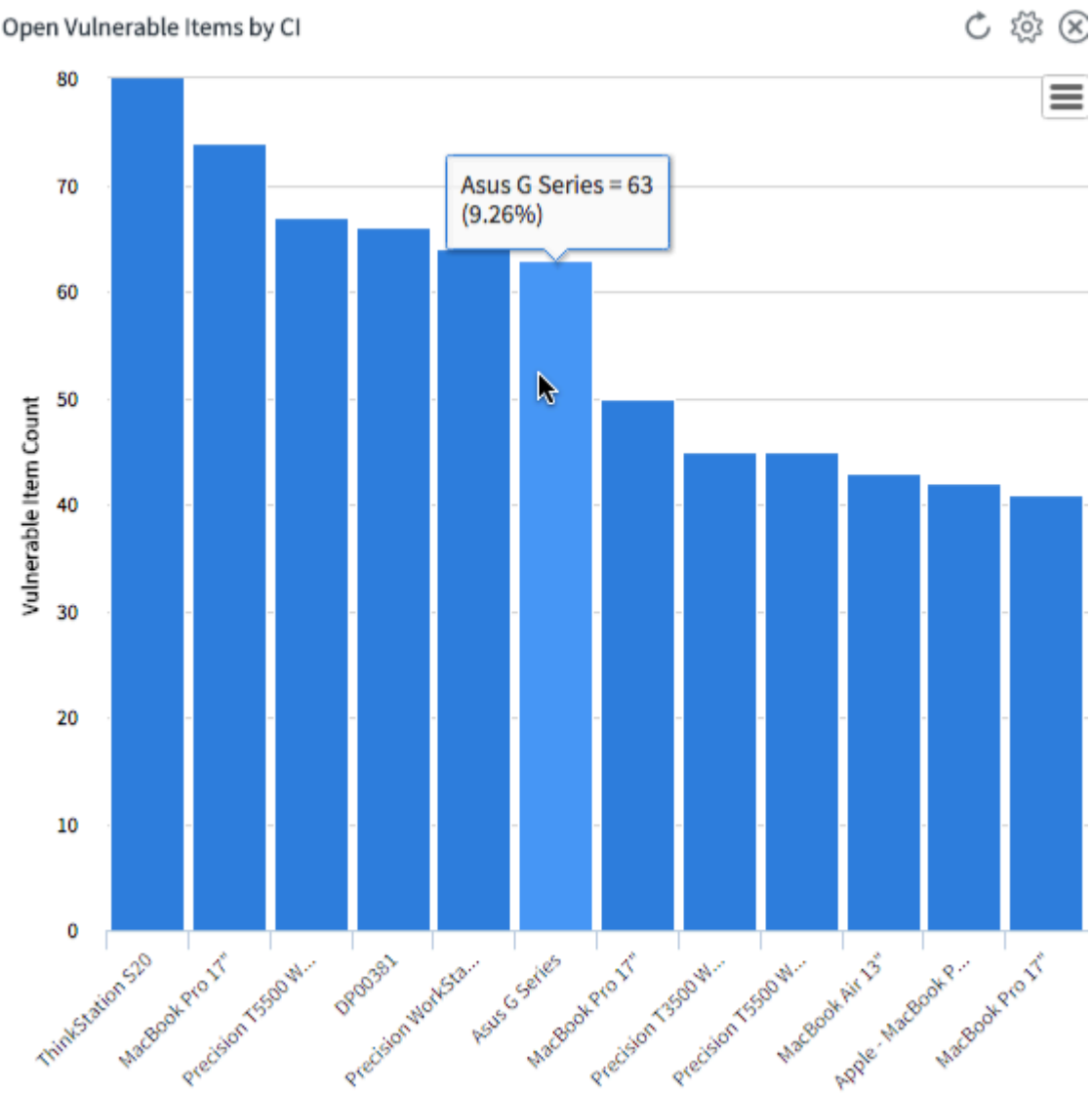
Dans chaque graphique, vous pouvez pointer sur n'importe quelle partie d'un graphique (barre, secteurs, point de données, etc.) pour afficher des données générales spécifiques à cette pièce. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

Remarque :

Si des tableaux de bord personnalisés sont nécessaires, consultez Créer et utiliser des tableaux de bord pour plus d'informations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Rapports Vue d'ensemble de la vulnérabilité

Nom	Visuel	Description
Ouvrir les éléments vulnérables par CI	Histogramme	Affiche le nombre d'éléments vulnérables ouverts enregistrés pour chaque élément de configuration (CI), du plus au moins élevé.
Éléments vulnérables par état de la cible de rattrapage	Histogramme	Affiche le nombre d'éléments vulnérables qui approchent de la cible, en cours et qui dépassent la cible. **Remarque :** Les éléments à l'état Différé, Résolu ou Fermé ne sont pas inclus.
Éléments vulnérables différés arrivant à expiration cette semaine	Graphique	Affiche le nombre d'éléments vulnérables différés planifiés pour être réactivés dans les sept jours.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports Vue d'ensemble de la vulnérabilité (suite)

Nom	Visuel	Description
Ouvrir les éléments vulnérables par vulnérabilité	Histogramme	Affiche le nombre d'éléments vulnérables ouverts pour chaque vulnérabilité, de la plus importante à la plus faible.
Vulnérabilités par modèle	Histogramme	Affiche le nombre d'éléments vulnérables enregistrés pour chaque modèle (classe CI), du plus au moins élevé.
Vulnérabilités par semaine	Graphique de tendance	Affiche le nombre d'entrées de vulnérabilité enregistrées chaque semaine.
Modèles les plus vulnérables	Couronne	Affiche les modèles (classes CI) avec les éléments les plus vulnérables.
Vulnérabilités par éditeur	Histogramme	Affiche le nombre d'éléments vulnérables enregistrés pour chaque éditeur, du plus au moins élevé.
Vulnérabilités par impact	Histogramme	Affiche le nombre d'entrées de vulnérabilité pour les types de réseaux impactés.
Éditeurs les plus vulnérables	Couronne	Affiche les éditeurs ayant les éléments les plus vulnérables.
CI les plus vulnérables	Couronne	Affiche les CI avec les éléments les plus vulnérables.
Vulnérabilités par score	Histogramme	Affiche le nombre d'entrées de vulnérabilité par scores de vulnérabilité.
Éléments vulnérables rouverts	Liste	Répertorie les éléments vulnérables rouverts et leur âge.
CI les plus vulnérables par classe	Couronne	Affiche les CI avec les éléments les plus vulnérables.
Âge de l'élément vulnérable	Liste	Répertorie le nombre de jours depuis la dernière ouverture des éléments vulnérables.
CI avec vulnérabilité par date	Liste	Répertorie les éléments de configuration qui ont été analysés au cours des 30 derniers jours.
CI pas analysés	Liste	Répertorie les éléments de configuration qui n'ont jamais été analysés pour détecter les vulnérabilités.

Tableau de bord de rattrapage de vulnérabilité

À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Le tableau de bord de rattrapage de vulnérabilité contient les onglets suivants : **Affecté à mes groupes**, **Affecté à moi** et **Demandé par moi**. Les onglets Affecté à mes groupes et Affecté à moi affichent les mêmes rapports. Le premier onglet présente les rapports par

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

groupes d'affectation auxquels vous appartenez, et le second par éléments vulnérables ou tâches de rattrapage qui vous sont affectés. L'onglet Demandé par moi signale les faux positifs et les exceptions que vous avez demandées.

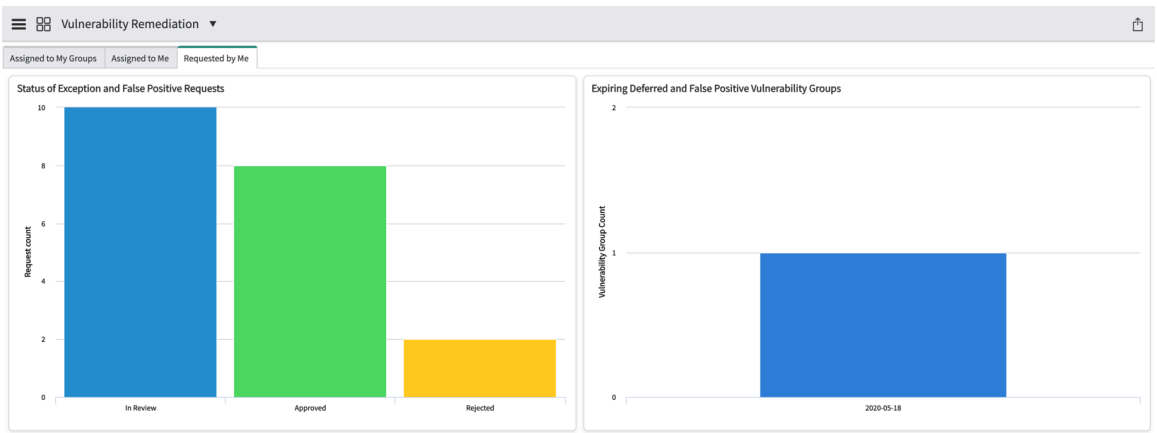
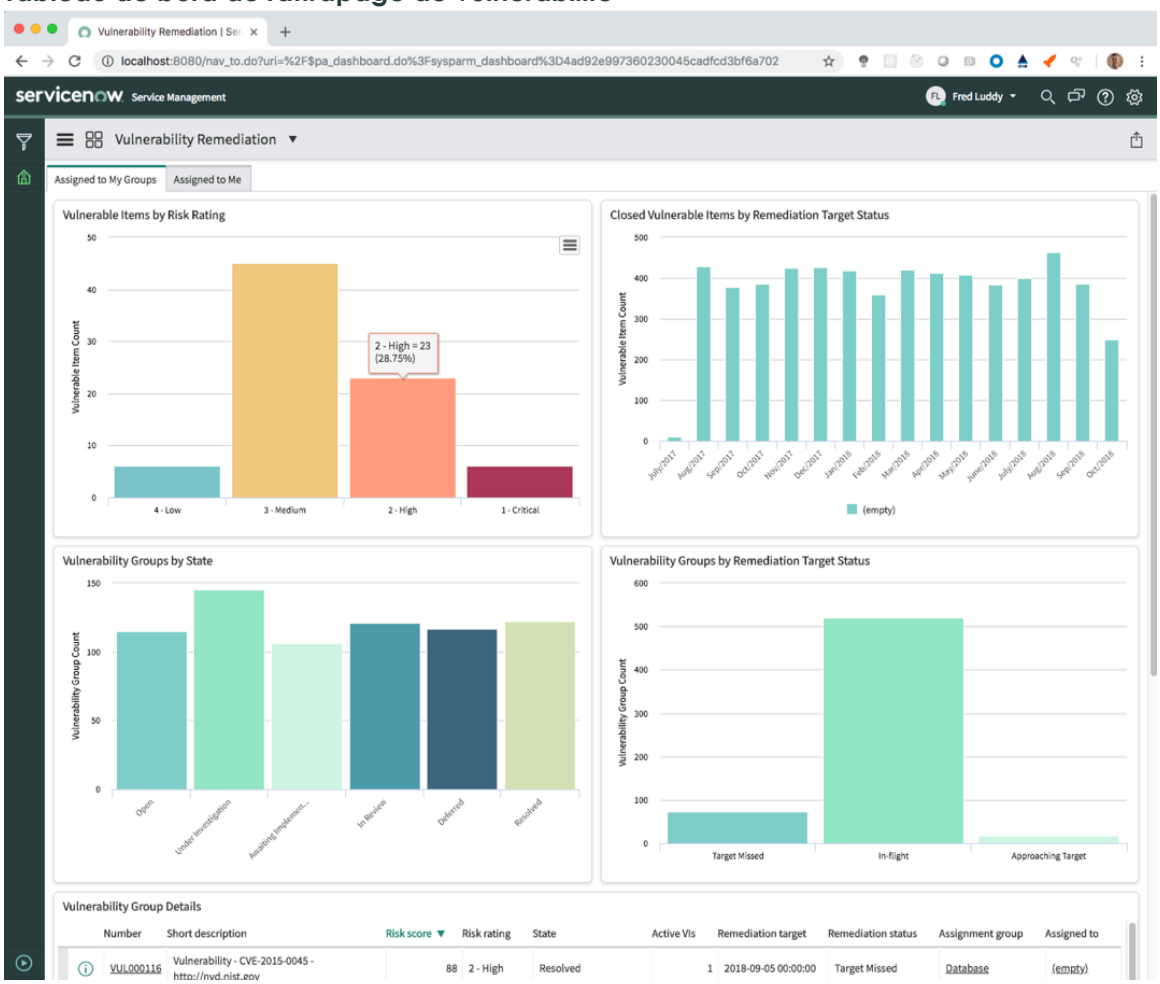


Tableau de bord de rattrapage de vulnérabilité



Rapports

Affectés à mes groupes et affectés à moi

Nom	Visuel	Description
Éléments vulnérables par cote de risque	Barre	Nombre d'éléments vulnérables actifs regroupés par cote de risque au cours de la période sélectionnée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affectés à mes groupes et affectés à moi (suite)

Nom	Visuel	Description
Éléments vulnérables fermés par état de la cible de rattrapage	Barre	Nombre d'éléments vulnérables fermés regroupés par état de la cible de rattrapage au cours de la période sélectionnée.
Tâches de remédiation par état	Barre	Nombre de tâches de rattrapage (RT) actives regroupées par état.
Tâches de remédiation par état de la cible de remédiation	Barre	Nombre de RT actifs regroupés par état de cible de rattrapage. Ce rapport exclut les éléments vulnérables différés.
Détails de la tâche de rattrapage	Liste	Tâche de rattrapage enregistre les détails dans une liste.

Demandé par moi

Nom	Visuel	Description
État des demandes d'exception et de faux positifs	Barre	Nombre de demandes actives de votre part.
Tâches de remédiation et faux positifs différés arrivant à expiration	Barre	Nombre de tâches de rattrapage (RT) reportées et faussement positives, regroupées par date de fin.

Tableau de bord des approbations de vulnérabilité

Le tableau de bord des approbations de vulnérabilité contient les rapports suivants pour les approbateurs d'exception et de faux positif.

À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Nom	Visuel	Description
Demandes d'exception et de faux positifs par âge en attente de mon approbation	Barre	Nombre d'approbations en attente pour vous, regroupées par date de création.
Mes demandes d'exception et de faux positifs rejetées	Barre	Nombre de demandes d'approbation approuvées ou rejetées, regroupées par état d'approbation.
Toutes les tâches de remédiation par cote de risque en attente d'approbation	Barre	Nombre de tâches de rattrapage en attente d'approbation, regroupées par cote de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Visuel	Description
Toutes les demandes d'approbation en attente et les faux positifs regroupées par motif	Barre 	Nombre de demandes d'approbation en attente regroupées par motif.

Solutions Analyse de la plateforme et Reporting pour la gestion des vulnérabilités

Solutions Analyse de la plateforme et Reporting comporte un contenu Analyse des performances et Reporting préparamétré pour être utilisé avec d'autres produits Now Platform. Cette solution d'analyse et de reporting vous permet de suivre le volume, les performances et la progression des vulnérabilités, depuis l'analyse et la détection initiales jusqu'au confinement ou à la correction. Vous pouvez filtrer les rapports par groupe d'affectation, exploits, cote de risque ou état.

Le Analyse des performances pour Réponse aux vulnérabilités pack de contenu n'est pas automatiquement installé avec l'application Réponse aux vulnérabilités . Il est disponible sur le sous forme d'abonnement ServiceNow Store séparé.

Analyse des performances pour Réponse aux vulnérabilités Contient deux tableaux de bord :

- Tableau de bord Gestion de la vulnérabilité (PA)
- Tableau de bord du responsable de la sécurité de l'information (CISO) de Gestion des vulnérabilités

Rôles requis, installation et affichage des tableaux de bord

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur Now Platform (admin) : installer et activer cette solution d'analyse et de génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Administrateur Analyse des performances (pa_admin) : passer en revue les indicateurs, les répartitions, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.

Pour installer cette application, consultez Installer et configurer l'application Analyse des performances pour Vulnerability Response [PA].

Remarque : Configurez et testez les solutions d'analyse et de génération de rapports sur une instance de non-production avant de les activer en production.

Les solutions d'analyse et de génération de rapports nécessitent l'analyse des applications par défaut. Personnalisez ces enregistrements pour les utiliser dans votre environnement de production. Pour plus d'informations, consultez Configurer les solutions d'analyse et de génération de rapports .

Pour afficher le tableau de bord Gestion de la vulnérabilité (PA), accédez à **Réponse aux vulnérabilités** > **Vue d'ensemble** > **.**

Pour afficher le tableau de bord CISO de Gestion des vulnérabilités, accédez à **Réponse aux vulnérabilités** > **Tableau de bord des CISO** > **.**

Termes clés

Analyse des performances (PA)

Solution qui crée des tableaux de bord de gestion, des rapports sur les indicateurs clés de performance et les mesures, et répond aux questions commerciales clés pour aider à améliorer la qualité et à réduire les coûts.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément vulnérable (VI)

Une vulnérabilité de sécurité signalée par un scanner de vulnérabilité tiers qui est présente sur un élément de configuration (CI).

Tâche de rattrapage

Les tâches de rattrapage sont créées et affectées automatiquement aux équipes informatiques en fonction du groupe associé aux éléments vulnérables dans un effort de rattrapage. Les équipes informatiques et les propriétaires de rattrapage consultent les tâches de rattrapage dans l'espace de travail de rattrapage informatique. Voir Réponse aux vulnérabilités Espaces de travail pour plus d'informations

.

Indicateur PA

Définit une mesure de performance effectuée à intervalles réguliers d'un service d'entreprise, d'une activité ou d'un comportement organisationnel, par exemple, Éléments vulnérables critiques en retard non différés.

Source de l'indicateur PA

Ensembles de données qui filtrent les enregistrements à partir d'une vue de table ou de base de données, par exemple, VI actif.

Afficher les visualisations de données en temps réel

Pour voir ce qui se passe aujourd'hui avec les éléments les plus critiques de votre Réponse aux vulnérabilités application, vous pouvez afficher certains rapports en temps réel sur le tableau de bord Gestion de la vulnérabilité (PA). L'affichage instantané de ces rapports vous aide à gérer vos éléments vulnérables (VI) les plus importants et à les corriger rapidement. Vous pouvez afficher les rapports suivants en temps réel :

- Onglet Vue d'ensemble : éléments vulnérables par groupe d'affectation
- Onglet CI vulnérables
  - Éléments de configuration (CI) vulnérables sans propriétaires
  - CI mis hors service ou volés avec des VI actifs
- Onglet Exceptions
  - Éléments vulnérables différés par motif
  - Demandes de report sur le point d'expirer
  - Éléments vulnérables différés par le gestionnaire DSI
- Onglet Rattrapage : éléments vulnérables non affectés

Pour plus d'informations, consultez Afficher les rapports d'Analyse des performances pour Vulnerability Response [PA] en temps réel.

Information associée

Solutions d'analyse et de génération de rapports

Tableau de bord Vulnerability Management des CISO

Avec le tableau de bord Vulnerability Management CISO , affichez des données telles que les mesures clés des performances (KPI) pour la correction de la vulnérabilité, affichez les risques les plus élevés, vérifiez la couverture des analyses et découvrez comment réduire les risques.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles Now Platform requis

- sn_vul.vulnerability_ciso pour afficher le tableau de bord.
- sn_vul.ciso_write pour modifier le tableau de bord.

Activer le tableau de bord CISO

Pour activer le tableau de bord CISO, vous devez installer Performance Analytics et Réponse aux vulnérabilités activer la tâche correspondante Performance Analytics. Pour plus d'informations, consultez Solutions d'analyse et de reporting pour Vulnerability Response.

Cas d'utilisation

Utilisateur	Utilisation du tableau de bord
Responsables de la sécurité de l'information (RSSI)	Les responsables de la sécurité de l'information (CISO) peuvent utiliser le tableau de bord CISO pour obtenir un aperçu du programme de gestion des vulnérabilités de leur organisation. Le tableau de bord fournit des données pour les aider à identifier en un coup d'œil les données qu'ils peuvent utiliser pour réduire les vulnérabilités de leurs environnements.

Utilisation du tableau de bord CISO

Les utilisateurs exécutifs, tels que les responsables de la sécurité de l'information (CISO) de votre organisation, peuvent consulter le tableau de bord CISO pour Vulnerability Response afin de comprendre l'efficacité de leur programme de gestion des vulnérabilités. Vous pouvez afficher le tableau de bord CISO en accédant à **Réponse aux vulnérabilités** > **Tableau de bord des CISO**. Utilisez les filtres de niveau supérieur pour filtrer les rapports par cote de risque, tranche d'âge ou accessible sur Internet. Certains rapports affichent des données de tendance sur une période donnée. Vous pouvez afficher régulièrement les tendances des mesures importantes, analyser le risque global de sécurité de l'entreprise et identifier les domaines à améliorer.

À partir de la version 19.0 de Réponse aux vulnérabilités, ce tableau de bord peut également être consulté dans l'interface utilisateur de la nouvelle expérience. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Tableaux de bord dans Vulnerability Manager Workspace et Tableaux de bord dans IT Remediation Workspace.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Exécution des travaux planifiés

Exécutez les travaux planifiés dans cet ordre pour mettre à jour les données dans les rapports :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Mettre à jour les tables du tableau de bord
2. [PA VR] Tableau de bord des CISO

Travaux planifiés pour le tableau de bord CISO

Nom de la tâche planifiée	Description
Mettre à jour les tables du tableau de bord	Tâche planifiée quotidienne que vous devez exécuter avant la tâche Tableau de bord du CISO [PA VR] afin de pouvoir collecter les données du CISO. En exécutant cette tâche planifiée, vous mettez à jour les rapports de couverture de l'analyse. Les informations mises à jour comprennent les éléments de configuration (CI) opérationnels qui ont été analysés au cours des 90 derniers jours, leurs classes et le nombre total de CI opérationnels qui correspondent à ces classes. L'exécution de cette tâche planifiée met également à jour les rapports de l'onglet **Actions recommandées** . **Remarque :** Les CI opérationnels désignent les CI dont l'état opérationnel est `Opérationnel`.
[PA VR] Tableau de bord des CISO	Une fois la tâche planifiée Mettre à jour les tables du tableau de bord terminée, exécutez cette tâche planifiée pour renseigner tous les rapports dans l'onglet **Vue d'ensemble du CISO** .

Onglets du tableau de bord du CISO

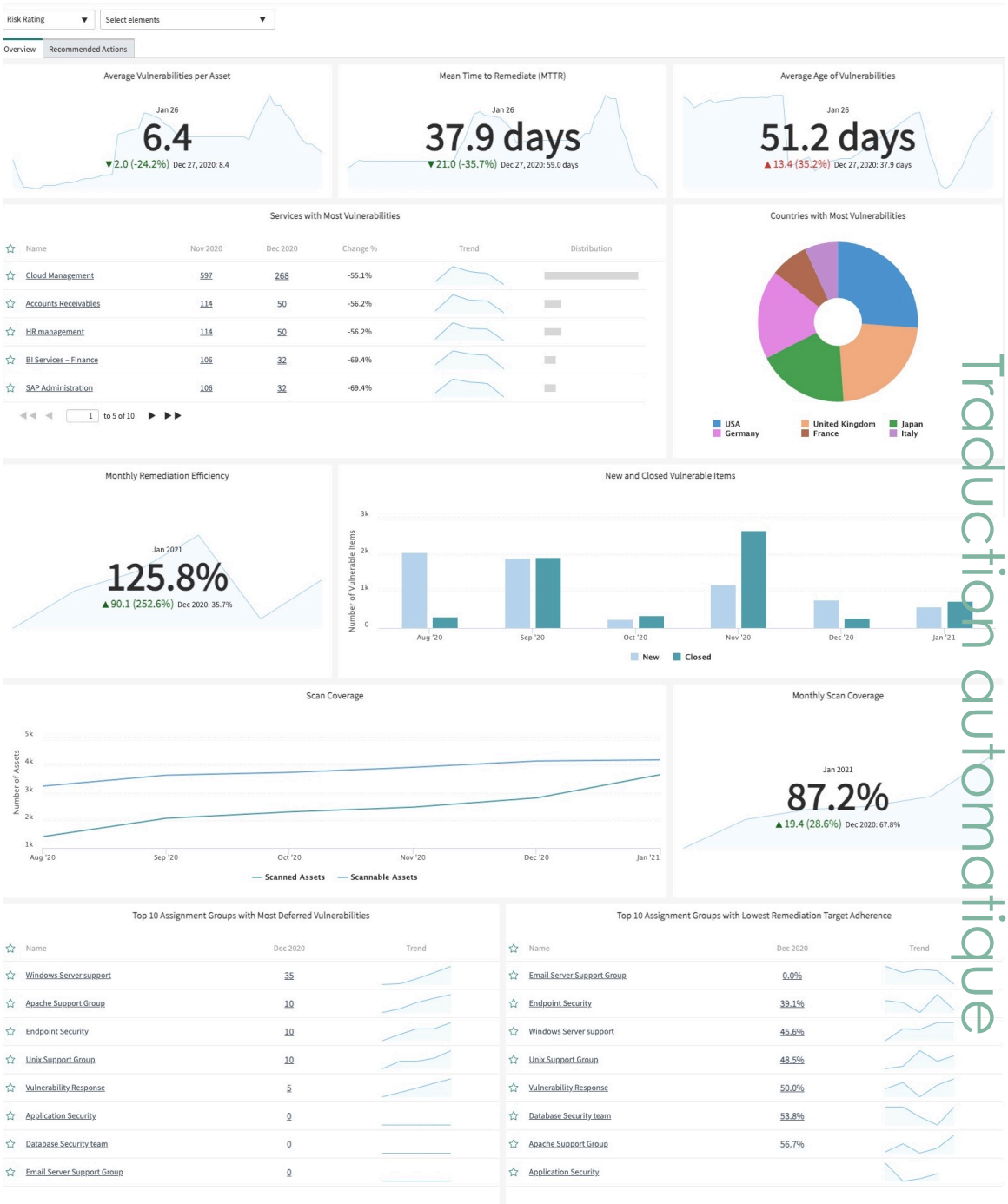
Ce tableau de bord fournit un aperçu des risques présents dans Gestion des vulnérabilités. Vous pouvez afficher les vulnérabilités et leurs données connexes par région, âge, services et autres répartitions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble

L'onglet Vue d'ensemble contient des rapports qui fournissent en un coup d'œil la posture de sécurité de votre organisation.



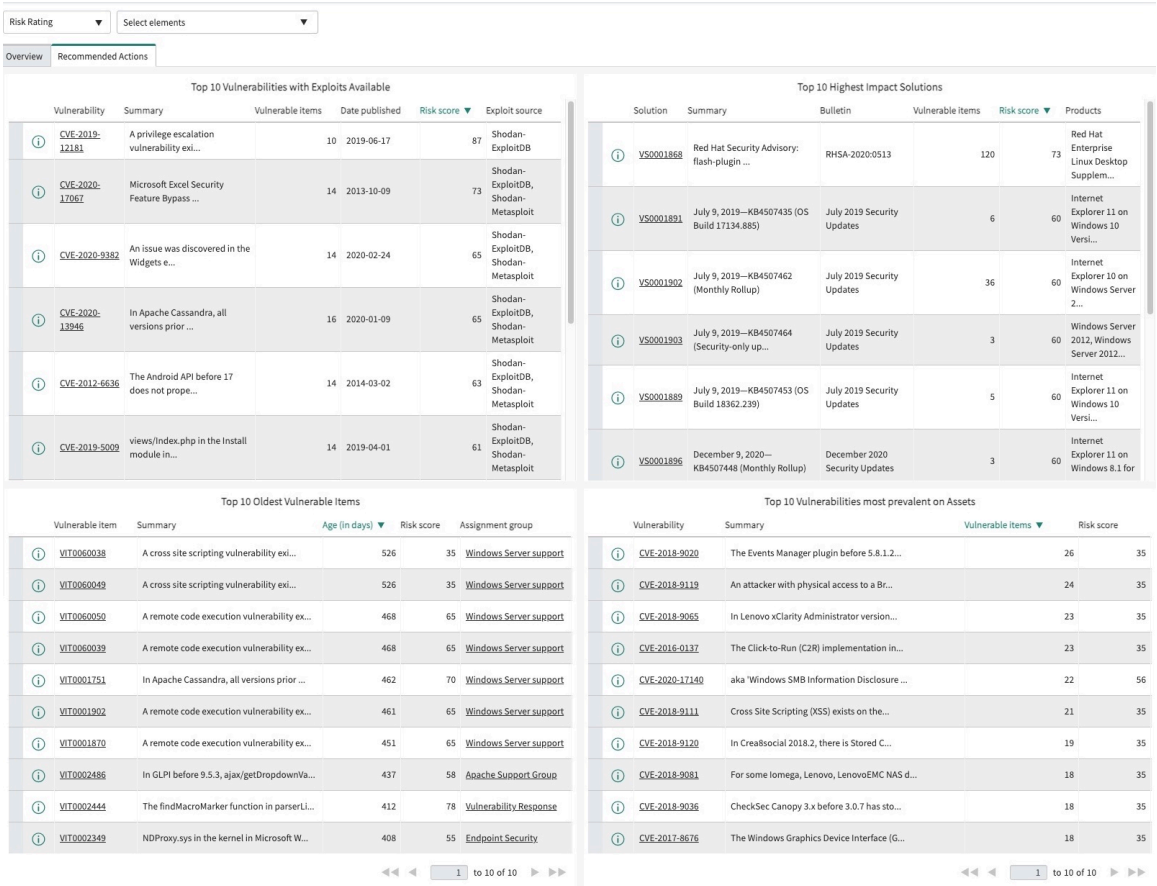
Remarque : Le filtre de niveau supérieur ne peut être utilisé que pour certains rapports.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Actions recommandées

L'onglet Actions recommandées contient des rapports qui fournissent des informations sur les vulnérabilités exploitables, vieillissantes et courantes. Il contient également des solutions qui recommandent des actions pour réduire les risques. Exécutez la tâche planifiée **Mettre à jour les tables du tableau de bord du CISO** pour mettre à jour les rapports de cet onglet.



Indicateurs

Pour afficher les indicateurs, accédez à **Analyse des performances** > **Indicateurs**.

1. Sur la page Indicateurs, recherchez le nom de l'indicateur requis dans la colonne Nom.
2. Cliquez sur le nom de l'indicateur pour ouvrir l'enregistrement et afficher ses détails.

   Par défaut, les indicateurs du tableau de bord CISO ne collectent pas d'enregistrements. Vous pouvez choisir de collecter des enregistrements en cochant la case Collecter les enregistrements.

   Durée totale des éléments vulnérables clôturés

   La durée totale des VI fermés est mesurée quotidiennement en jours. L'objectif de cet indicateur est de minimiser le score.

   Actifs analysables

   L'indicateur Actifs analysés est mesuré quotidiennement en unité #. L'objectif de cet indicateur est de maximiser le score.

   Services avec le plus de vulnérabilités

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La valeur Services avec le plus de vulnérabilités est mesurée quotidiennement en unité #. L'objectif de cet indicateur est de minimiser le score.

Nombre moyen de vulnérabilités par actif

[[Éléments vulnérables actifs]] / [[Éléments de configuration vulnérables actifs]

Éléments vulnérables clôturés

Éléments vulnérables fermés est mesuré quotidiennement en unité #. L'objectif de cet indicateur est de maximiser le score.

Délai moyen de remédiation des éléments vulnérables

[[Durée cumulée des éléments vulnérables fermés]] / [[Éléments vulnérables fermés]]

Couverture de l'analyse actuelle

Calcule la couverture de l'analyse actuelle en pourcentage.

Actifs analysés

L'indicateur Actifs analysés est mesuré quotidiennement en unité #. L'objectif de cet indicateur est de maximiser le score.

Éléments vulnérables clôturés (cible atteinte)

Éléments vulnérables fermés (cible atteinte) est mesuré quotidiennement en unité #. L'objectif de cet indicateur est de maximiser le score.

% d'éléments vulnérables clôturés ayant atteint leur cible

[[Éléments vulnérables fermés (cible atteinte) / SOMME par mois]] / [[Éléments vulnérables fermés / SOMME par mois]] *100

Éléments vulnérables actifs

Éléments vulnérables actifs est mesuré quotidiennement en unité #. L'objectif de cet indicateur est de minimiser le score.

Âge moyen des éléments vulnérables

L'indicateur Âge moyen des VI actifs est mesuré quotidiennement en unité Jours. L'objectif de cet indicateur est de minimiser le score.

Éléments de configuration des éléments vulnérables actifs

L'indicateur CI vulnérables actifs est mesuré quotidiennement en unité #. L'objectif de cet indicateur est de minimiser le score.

Efficacité de la remédiation mensuelle

[Nombre d'éléments vulnérables fermés au cours d'un mois] / [Nombre d'éléments vulnérables nouveaux ou rouverts au cours du même mois]

Nouveaux éléments vulnérables

L'indicateur Nouveaux éléments vulnérables est mesuré quotidiennement en unité #. L'objectif de cet indicateur est de minimiser le score.

Éléments vulnérables différés

Les VI différés sont mesurés quotidiennement en unité #. L'objectif de cet indicateur est de minimiser le score.

Répartitions

- Groupe d'affectation : s'applique à certains rapports de VI.
- Cote de risque : s'applique aux rapports de VI.
- Tranche d'âges : s'applique aux rapports de VI.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Âge à la fermeture : s'applique aux rapports des VI fermés.
- Accessible sur Internet : indique si le CI appartient à la classe de matériel et s'il est accessible sur Internet.
- Région : le paramètre CI CMDB utilisé est l'emplacement. Cet emplacement indique le pays d'origine de l'élément de configuration.

Visualisations des données

Nom	Type	Description
Nombre moyen de vulnérabilités par actif	Score unique	Nombre moyen d'éléments vulnérables actifs pour chaque élément de configuration
Délai moyen de rattrapage (MTTR)	Score unique	Le délai moyen de rattrapage (fermeture) d'un élément vulnérable, affiché comme moyenne d'exécution de 30 jours. **Remarque :** La valeur Âge fermé est calculée lors de la collecte des données. La valeur est la différence entre la date de la dernière ouverture et la date et l'heure de la tâche de collecte.
Âge moyen des vulnérabilités	Score unique	Âge moyen des éléments vulnérables actifs en jours.
Services avec le plus de vulnérabilités	Liste et ligne	Moyenne mensuelle des éléments vulnérables actifs pour les services de l'organisation. **Remarque :** Pour plus d'informations sur la définition des classifications de service que vous souhaitez afficher dans la génération de rapports Vulnerability Response et les listes connexes, consultez l'onglet Services dans le tableau de bord Gestion des vulnérabilités [PA].
Pays avec le plus de vulnérabilités		Top 10 des pays ayant le plus grand nombre d'éléments vulnérables.
Efficacité de la remédiation mensuelle	Score unique	Pourcentage d'éléments vulnérables fermés divisés par de nouveaux éléments vulnérables au cours du mois en cours.
Éléments vulnérables nouveaux et fermés	Barre	Nombre de nouveaux éléments vulnérables importés et nombre d'éléments vulnérables fermés en un mois.
Couverture de l'analyse	Ligne	Nombre d'actifs analysés par rapport au nombre total d'actifs analysables, affichés au fil du temps. Les classes CI incluses dans le widget sont spécifiées dans le module Configuration de la couverture d'analyse. Pour plus d'informations sur la configuration du module Couverture de numérisation, reportez-vous à la section Configurer les rapports de couverture de numérisation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Couverture de l'analyse mensuelle	Score unique	Pourcentage d'actifs analysés divisé par le nombre total d'actifs analysables pour le mois en cours. Pour plus d'informations sur la configuration du module Couverture de l'analyse, voir Configurer les rapports de couverture de l'analyse
10 premiers groupes d'affectation avec les vulnérabilités les plus différées	Liste et ligne	10 principaux groupes d'affectation ayant le nombre le plus élevé d'éléments vulnérables différés, différés en fonction de la moyenne mensuelle.
10 premiers groupes d'affectation avec l'adhésion à la cible de rattrapage la plus faible	Liste et ligne	10 principaux groupes d'affectation dont les éléments vulnérables ont le moins d'adhérence à leurs cibles de rattrapage.

Actions recommandées

Nom	Type	Table source	Description
10 principales vulnérabilités avec exploits disponibles	Liste	Élément vulnérable principal [sn_vul_analytics_top_item]	Vulnérabilités actives avec exploits disponibles pour tous les fournisseurs de renseignements sur les menaces qui utilisent le cadre de travail d'exploitation VR.
Top 10 des solutions à fort impact	Liste	Élément vulnérable principal [sn_vul_analytics_top_item]	Solutions préférées ou correctifs avec les scores de risque les plus élevés pour les éléments vulnérables actifs. Ce rapport utilise les fonctionnalités de Vulnerability Solution Management (VSM), qui met en corrélation les correctifs de Microsoft et de Red Hat avec les vulnérabilités de l'environnement. VSM permet d'identifier la solution préférée pour les vulnérabilités.
10 premiers des éléments vulnérables les plus anciens	Liste	Élément vulnérable principal [sn_vul_analytics_top_item]	Éléments vulnérables actifs avec l'âge le plus élevé. Résolvez ces éléments pour abaisser l'âge moyen de vulnérabilité dans l'onglet Vue d'ensemble.
10 principales vulnérabilités les plus répandues sur les actifs	Liste	Élément vulnérable principal [sn_vul_analytics_top_item]	Éléments vulnérables actifs disponibles pour le plus grand nombre d'actifs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les rapports de couverture de l'analyse

Permettez à vos utilisateurs d'exécuter des rapports de couverture d'analyse à partir du tableau de bord CISO. Grâce à ces rapports, vos utilisateurs peuvent voir quelle est la couverture d'analyse de l'organisation sur une période donnée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Pourquoi et quand exécuter cette tâche

La couverture de l'analyse indique le nombre d'actifs qui ont été analysés par les scanners de vulnérabilité pour les différentes classes au cours des 90 derniers jours. Ces actifs sont comparés au nombre d'actifs analysables dans le Base de données de gestion des configurations (CMDB). Par défaut, le module Configuration de la couverture d'analyse inclut CMDB des classes CI auxquelles au moins un actif analysé a été associé. Vous pouvez ajouter une classe CI à partir du rapport de couverture de l'analyse affiché sur le tableau de CMDB bord CISO. Vous pouvez inclure ou exclure les classes CI qui apparaissent dans les rapports de CMDB couverture de l'analyse.



Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Configuration de la couverture d'analyse**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Configuration de la couverture d'analyse

Champ	Description
Classe CI CMDB	Classe CI qui doit être ajoutée au rapport de couverture de l'analyse sur le tableau de bord CISO. **Remarque :** Si une classe CI existe déjà dans le module Configuration de la couverture d'analyse, elle n'est pas incluse dans cette liste.
Considérer l'élément analysable	Option permettant de définir si la classe CI doit être incluse ou non. Incluez une classe

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	CI si vous souhaitez que ses données soient ajoutées aux rapports de couverture de l'analyse. Si elles sont exclues, les données de cette classe CI ne sont pas ajoutées.

4. Cliquez sur **Envoyer**.

Configurer les indicateurs PA pour le tableau de bord CISO

Surveillez les indicateurs CISO automatisés et formulés afin de pouvoir gérer les données de vulnérabilité dans votre instance.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Réponse aux vulnérabilités comporte à la fois des indicateurs automatisés et formulés.

Termes clés

Indicateur

Définit une mesure de performance effectuée à intervalles réguliers d'un service d'entreprise, d'une activité ou d'un comportement organisationnel. Un élément vulnérable actif en est un exemple.

Source de l'indicateur

Ensembles de données constitués d'enregistrements filtrés à partir d'une vue de table ou de base de données pour une efficacité accrue. Un exemple est VI.Active (accessible sur Internet).

Répartitions

Les répartitions filtrent et regroupent les scores d'indicateur à l'aide d'attributs qualitatifs tels que la priorité, la catégorie et le groupe d'affectation.

Travaux planifiés

Des travaux planifiés sont exécutés pour renseigner les données de source d'indicateur. La tâche planifiée quotidienne du tableau de bord du CISO [PA VR] est désactivée par défaut. Vous devez l'activer pour collecter les scores d'indicateur pour le tableau de bord CISO.

Procédure

1. Accédez à la **Tout** > **Analyse des performances** > **Indicateurs** et choisissez l'une des options suivantes :
   - Indicateurs automatisés
   - Indicateurs de formule

   Pour plus d'informations sur les indicateurs, consultez Indicateurs Analyse des performances .
2. Sur la page Indicateurs, recherchez le nom de l'indicateur requis dans la colonne Nom.
3. Cliquez sur le nom de l'indicateur pour ouvrir l'enregistrement et afficher ses détails.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, les indicateurs du tableau de bord CISO ne collectent pas d'enregistrements. Vous pouvez choisir de collecter des enregistrements en cochant la case **Collecter les enregistrements** .

Remarque : L'activation de la collecte d'enregistrements dans un indicateur peut entraîner des problèmes de performances, tels que l'augmentation du temps et de la mémoire nécessaires à l'exécution de la tâche de collecte de données.

Le nombre maximal de lignes que vous pouvez extraire pour une source d'indicateur est de 1 000 000.

Tableau de bord d'intégrité de SecOps Vulnerability Response

Le tableau de bord d'intégrité de Vulnerability Response est un outil conçu pour fournir aux organisations des aperçus complets de l'implémentation et de l'utilisation de leurs applications Vulnerability Response.

L'évaluation de l'intégrité globale est déterminée en agrégeant divers facteurs critiques entre la configuration, l'implémentation, l'intégration, les performances, les données et les processus. Affichez le tableau de bord d'agrégat pour chaque catégorie pour les applications suivantes :

- Réponse aux vulnérabilités
- Application Vulnerability Response
- Conteneur Vulnerability Response
- Conformité de la configuration

Installation du tableau de bord d'intégrité de SecOps Vulnerability Response

Pour installer et configurer le tableau de bord d'intégrité SecOps Vulnerability Response pour Réponse aux vulnérabilités les applications de votre instance Now Platform, accédez au module d'extension ServiceNow® Store SecOps Health Analytics (sn_sec_analytics) et activez-le.

Rôles Now Platform requis

Rôles requis : sn_sec_analytics.admin, sn_sec_analytics.read

Tâche planifiée

Pour afficher la tâche planifiée, accédez à **Tout** > **Planificateur système** > **Travaux planifiés** > **Collecter les mesures du tableau de bord d'intégrité**. La tâche planifiée « Collecter les mesures du tableau de bord d'intégrité » est exécutée quotidiennement à 00h00. Il génère les données pour le tableau de bord d'intégrité de SecOps Vulnerability Response. Vous pouvez également choisir d'exécuter la tâche planifiée manuellement.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les membres de votre organisation utilisent ce tableau de bord, consultez les cas d'utilisation suivants.

Utilisateur	Utilisation du tableau de bord
Administrateur de vulnérabilité	Vous aide à comprendre le score d'intégrité des Réponse aux vulnérabilités applications.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur	Utilisation du tableau de bord
	Il est également utile de mettre en évidence les domaines qui doivent être améliorés. Le tableau de bord d'intégrité de Vulnerability Response traite uniquement de l'intégrité de l'implémentation et de l'utilisation. Cela n'aide pas à la gestion des vulnérabilités ou des actifs.
Administrateur de l'assistance	Permet d'identifier les problèmes de performances, de personnalisation et de configuration à l'aide des KPI. En fonction de l'intégrité de l'application, vous pouvez effectuer une analyse supplémentaire ou fournir une recommandation aux utilisateurs.
Partenaire d'implémentation	Vous aide à évaluer l'intégrité de l'implémentation Réponse aux vulnérabilités des configurations, des modules complémentaires, des personnalisations et des intégrations, et à fournir des recommandations d'amélioration pour les utilisateurs.

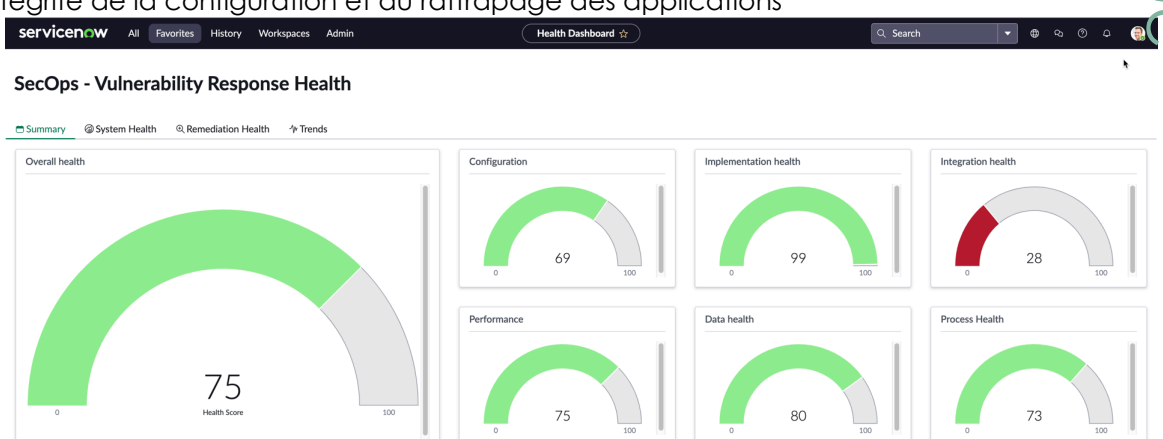
Onglets du tableau de bord d'intégrité de SecOps Vulnerability Response

Pour afficher le tableau de bord d'intégrité de SecOps Vulnerability Response, accédez à **Intégrité de Security Operations** > **Intégrité de Vulnerability Response**. Chaque couleur du tableau de bord représente les éléments suivants :

- Vert : Sûr
- Jaune : Avertissement
- Rouge : critique

Onglet Résumé

Ce tableau de bord communique le score d'intégrité global pour l'intégrité de la configuration et du rattrapage des applications VR.

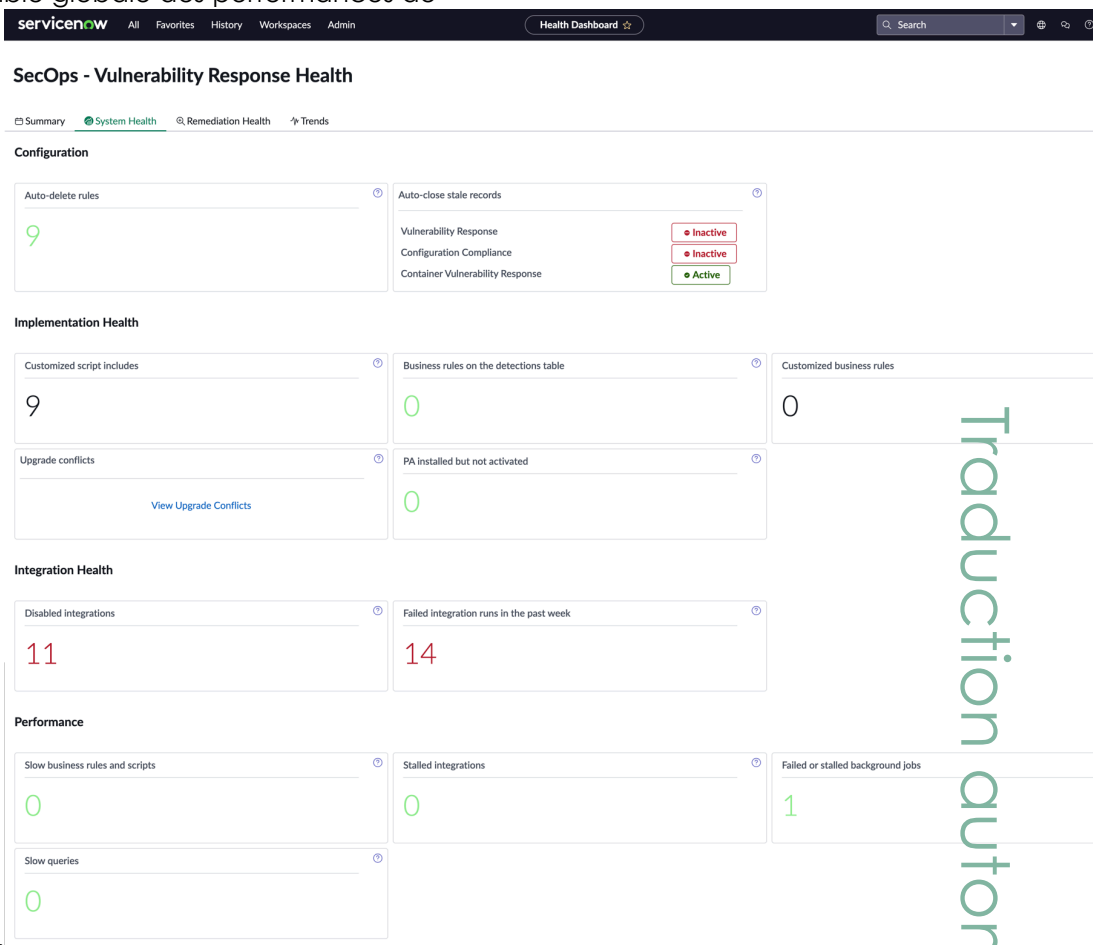


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Intégrité du système

Ce tableau de bord affiche l'intégrité de la configuration et de l'intégration de votre implémentation. Elle fournit une vue d'ensemble globale des performances de l'implémentation.

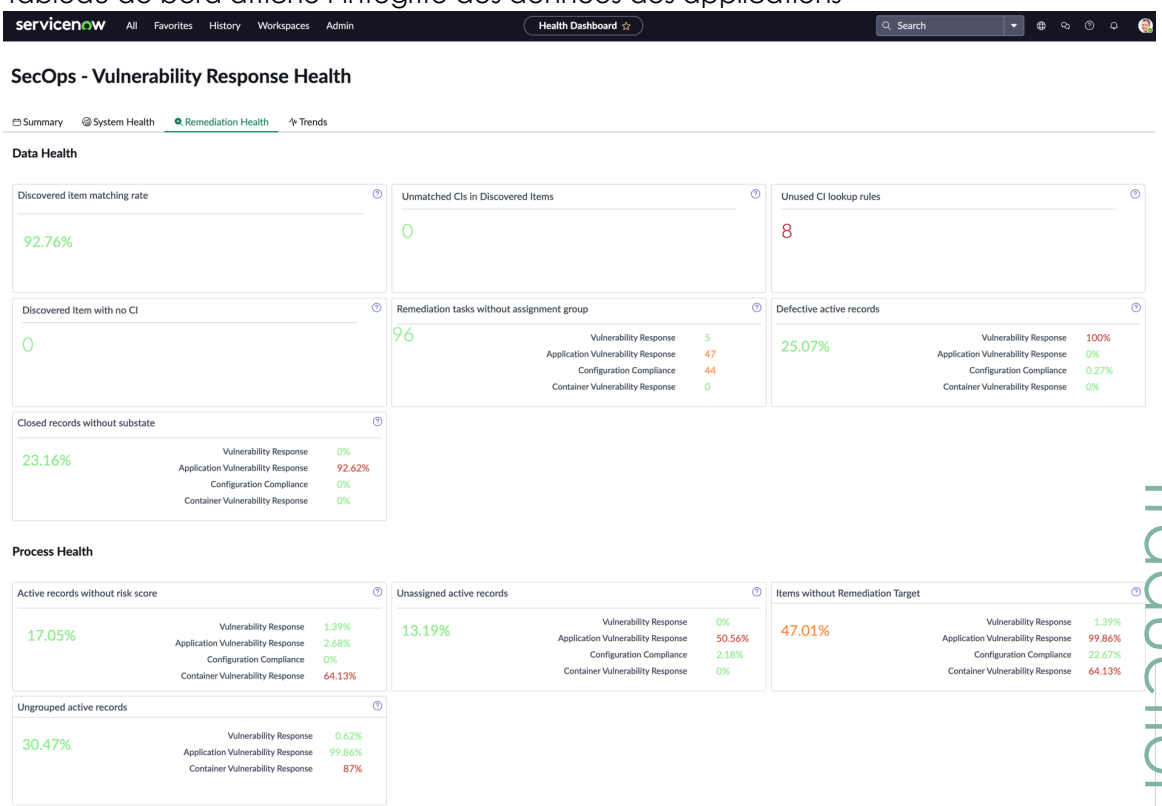


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Intégrité du rattrapage

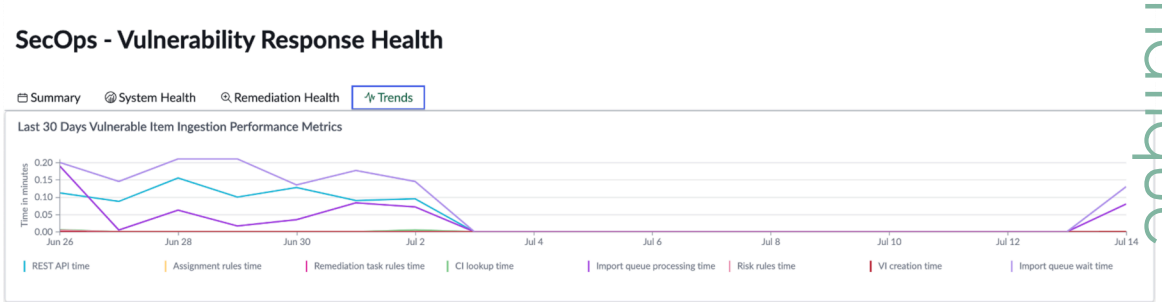
Ce tableau de bord affiche l'intégrité des données des applications



VR.

Onglet Tendances

Ce tableau de bord affiche les tendances des mesures de performances d'ingestion d'éléments vulnérables au cours des 30 derniers jours pour les applications



VR.

Rapports

Remarque : Les valeurs de seuil font partie du système de base. Vous pouvez configurer les valeurs en fonction de vos besoins.

Résumé

Titre	Description
Intégrité globale	Score d'intégrité global des applications VR. Pour plus d'informations, consultez les rapports concernant les mesures.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résumé (suite)

Titre	Description
Configuration	Intégrité de la configuration globale des applications VR.
Intégrité de l'implémentation	Intégrité globale de l'implémentation des applications VR.
Intégrité de l'intégration	Intégrité d'intégration globale des applications VR.
Performances	Score d'intégrité des performances globales des applications VR.
Intégrité des données	Intégrité globale des données des applications VR.
Intégrité des processus	Score d'intégrité global des processus des applications VR.

Intégrité du système

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
Configuration				
Règles de suppression automatique	Affiche le nombre de règles de suppression automatique activées.	Examinez et résolvez les règles de suppression automatique inactives.	3	1
Fermer automatiquement les enregistrements obsolètes	Ferme automatiquement les détections obsolètes. Pour plus d'informations, consultez la rubrique « Fermer automatiquement les détections obsolètes dans Vulnerability Response » dans docs.servicenow.com.	Réduisez le volume des détections périmées. Activez cette option pour fermer les détections obsolètes qui ne sont pas fermées par les scanners.	3	1
Intégrité de l'implémentation				
Includes de script personnalisés	Nombre d'« includes de script » personnalisés.	Réduisez les « includes de script » personnalisés	10	12

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrité du système (suite)

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
		pour faciliter les mises à niveau.		
Règles métier sur la table de détections	Nombre de règles métier personnalisées dans la table de détection.	Minimisez les règles métier pour faciliter les mises à niveau.	4	8
Règles métier personnalisées	Nombre de règles métier personnalisées avant la création d'enregistrements dans la CMDB.	Utilisez les règles métier par défaut sur les enregistrements.	5	8
Conflits de mises à niveau	Conflits tels que les règles métier et les scripts identifiés lors d'une mise à niveau.	Examinez et résolvez les conflits de mise à niveau.	10	15
PA installé mais pas activé	Indique si le tableau de bord Analyse des performances n'est pas activé.	Activez le tableau de bord PA.	10	15
Intégrité de l'intégration				
Intégrations désactivées	Nombre d'intégrations désactivées.	Examinez et activez les intégrations requises.	6	9
Exécutions d'intégration échouées au cours de la dernière semaine	Nombre d'exécutions d'intégration qui n'ont pas abouti au cours de la dernière semaine.	Examinez et résolvez la cause de l'échec des exécutions d'intégration.	9	12
Performances				
Ralentir les règles métier et les scripts	Règles métier et scripts dont le temps d'exécution moyen est supérieur à 10 ms et dont	Examinez et résolvez les règles métier à exécution lente.	10	15

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrité du système (suite)

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
	le nombre d'exécutions est supérieur à 10 000.			
Intégrations bloquées	Nombre d'intégrations qui ont expiré avant d'être terminées.	Examinez et résolvez la cause des intégrations bloquées.	10	15
Échec ou blocage des tâches en arrière-plan	Échec ou expiration des tâches en arrière-plan au cours de la dernière semaine.	Examinez et résolvez la cause des échecs des tâches.	5	10
Requêtes lentes	Requêtes dont le temps d'exécution moyen est supérieur à 10 ms et dont le nombre d'exécutions est supérieur à 10 000.	Examinez et résolvez les règles métier à exécution lente.	10	15

Intégrité du rattrapage

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
Intégrité des données				
Taux de correspondance de l'élément détecté	Nombre d'éléments détectés correspondant à des CI existants.	Vérifiez l'intégrité de votre CMDB et de la logique des règles de recherche de CI.	50	20
CI sans correspondance dans les éléments détectés	Éléments détectés dont l'état est sans correspondance.	Vérifiez l'intégrité de votre CMDB et de la logique des règles de recherche de CI.	9	12

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrité du rattrapage (suite)

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
Règles de recherche de CI non utilisées	Règles de recherche de CI qui ne sont associées à aucun élément détecté.	Changez le statut des règles de recherche de CI inutilisées en inactif.	4	6
Élément détecté sans CI	Élément détecté sans élément de configuration.	Passez en revue et réappliquez les règles de recherche de CI.	9	12
Enregistrements actifs défectueux	Enregistrements sans élément de configuration ni vulnérabilité.	Mettez les CI hors service à l'aide de l'option Gestion du cycle de vie des CI CMDB. **Remarque :** La suppression directe des CI peut entraîner des VIT orphelins.	40	60
Tâches de remédiation sans groupe d'affectation	Tâches de rattrapage actives dont le groupe d'affectation n'est pas encore affecté.	Affectez des tâches de rattrapage à un groupe d'affectation et passez en revue les règles d'affectation existantes.	40	60
Enregistrements fermés sans sous-état	Enregistrements qui sont fermés sans sous-état.	Fournissez des informations dans le champ Motif lors de la fermeture des enregistrements.	40	50
Intégrité des processus				
Enregistrements actifs sans score de risque	Enregistrements actifs avec un score de risque de 0 ou sans	Examinez et résolvez les règles de risque.	40	60

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrité du rattrapage (suite)

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
	score de risque affecté.			
Enregistrements actifs non affectés	Enregistrements sans groupe d'affectation.	Affectez un groupe aux enregistrements et passez en revue les règles d'affectation existantes.	30	50
Éléments sans cible de rattrapage	Éléments sans date cible de rattrapage.	Examinez et résolvez les règles de cibles de rattrapage. Ces règles doivent inclure tous les enregistrements.	30	50
Enregistrements actifs dégroupés	Enregistrements qui ne sont pas inclus dans une règle de tâche de rattrapage.	Passez en revue les règles de la tâche de rattrapage.	40	60

Tendances

Titre	Description
Mesures de performance d'ingestion d'élément vulnérables au cours des 30 derniers jours	Temps moyen nécessaire pour ingérer des éléments vulnérables et traiter plusieurs règles au cours des 30 derniers jours.

Modification des valeurs de seuil

Vous pouvez modifier les valeurs de seuil pour les données du tableau de bord SecOps VR Health en fonction de vos préférences.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Intégrité de Security Operations** > **Configuration** > **Mesures**.
2. Sur la page Données du tableau de bord d'intégrité, ouvrez l'enregistrement que vous souhaitez modifier.
3. Mettez à jour l'enregistrement et enregistrez.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vulnerability Management (PA) tableau de bord

Suivez le volume, les performances et la progression des vulnérabilités, de l'analyse initiale et de la détection au confinement ou à la correction. Vous pouvez filtrer les rapports par groupe d'affectation, exploits, cote de risque ou état, par exemple. Obtenez rapidement un aperçu de votre exposition aux vulnérabilités et des services d'entreprise affectés.

Rôles Now Platform requis

Rôle requis : sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst et les utilisateurs ayant sn_vul.vulnerability_read (ou qui héritent du rôle sn_vul.vulnerability_read) et pa_viewer.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Responsables informatiques, analystes informatiques, propriétaires du rattrapage des vulnérabilités	Aidez votre organisation à faire face à l'augmentation des incidents de sécurité dus à des vulnérabilités exploitées en déterminant efficacement quels éléments vulnérables présentent le plus de risques. Ces tableaux de bord fournissent une vue graphique de l'activité des éléments vulnérables et aident à concevoir des plans de rattrapage et la progression de l'état. Vous pouvez vous concentrer sur les KPI associés aux actifs affectés critiques et aux vulnérabilités à haute visibilité.

Pour afficher le tableau de bord Gestion de la vulnérabilité (PA), accédez à **Réponse aux vulnérabilités** > **Vue d'ensemble**.

Consultez les rapports qui affichent des données de tendance au fil du temps. Les rapports avec des données en temps réel sont répertoriés ci-dessous. Consultez régulièrement les tendances des mesures importantes afin d'analyser l'ensemble de vos processus business et d'identifier les domaines d'amélioration.

Pour plus d'informations sur l'affichage de vos rapports PA avec des scores en temps réel, consultez Afficher les rapports d'Analyse des performances pour Vulnerability Response [PA] en temps réel.

Traduction automatique

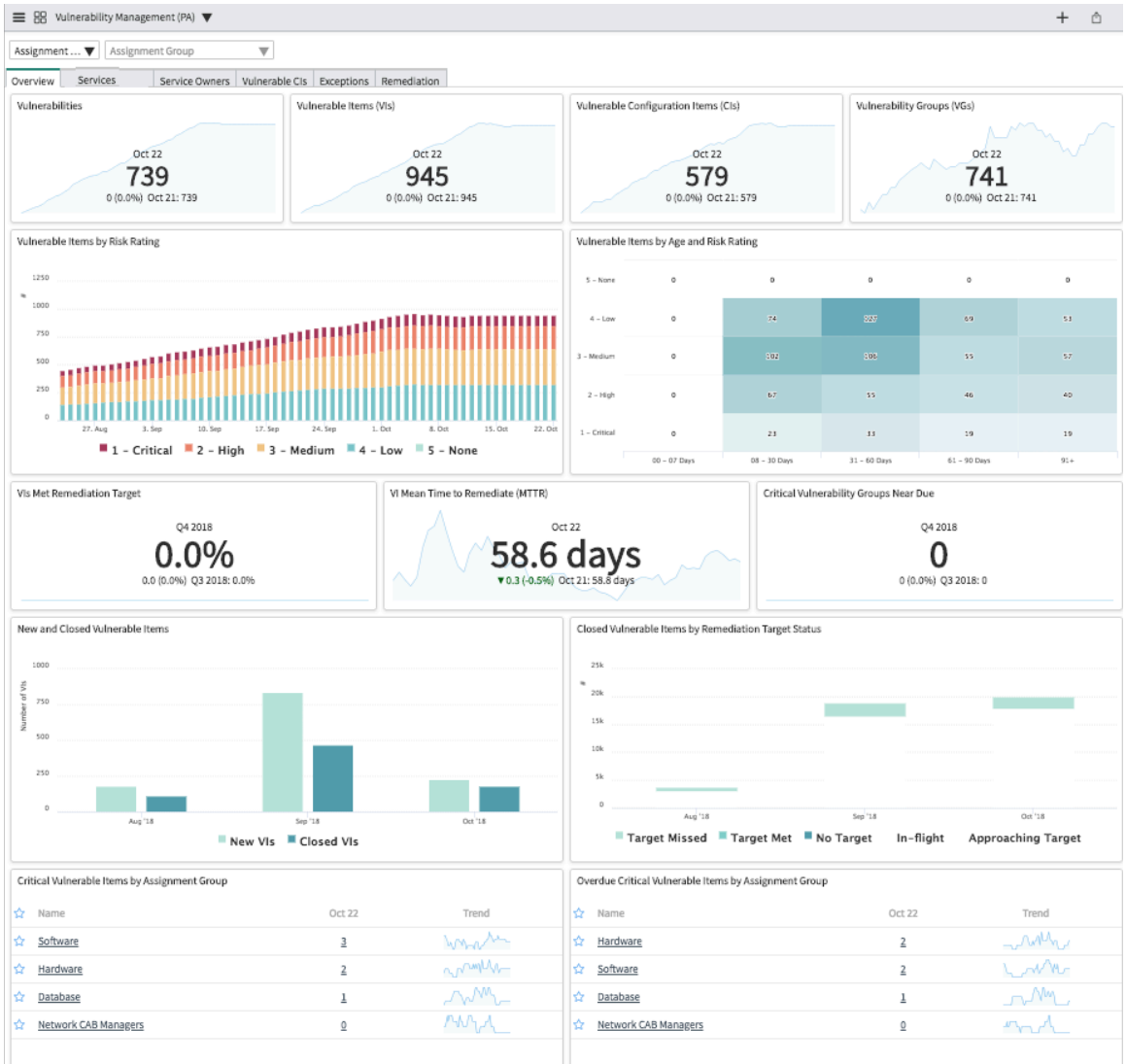
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglets du tableau de bord Gestion de la vulnérabilité [PA]

Onglet Vue d'ensemble

Ce tableau de bord communique les KPI pour le risque et la prévalence de la vulnérabilité, les actifs affectés, le respect de la cible de rattrapage et la progression du rattrapage.

Sous l'onglet Vue d'ensemble, vous pouvez afficher le rapport Éléments vulnérables critiques par groupe d'affectation exécuté en fonction de la tâche planifiée.



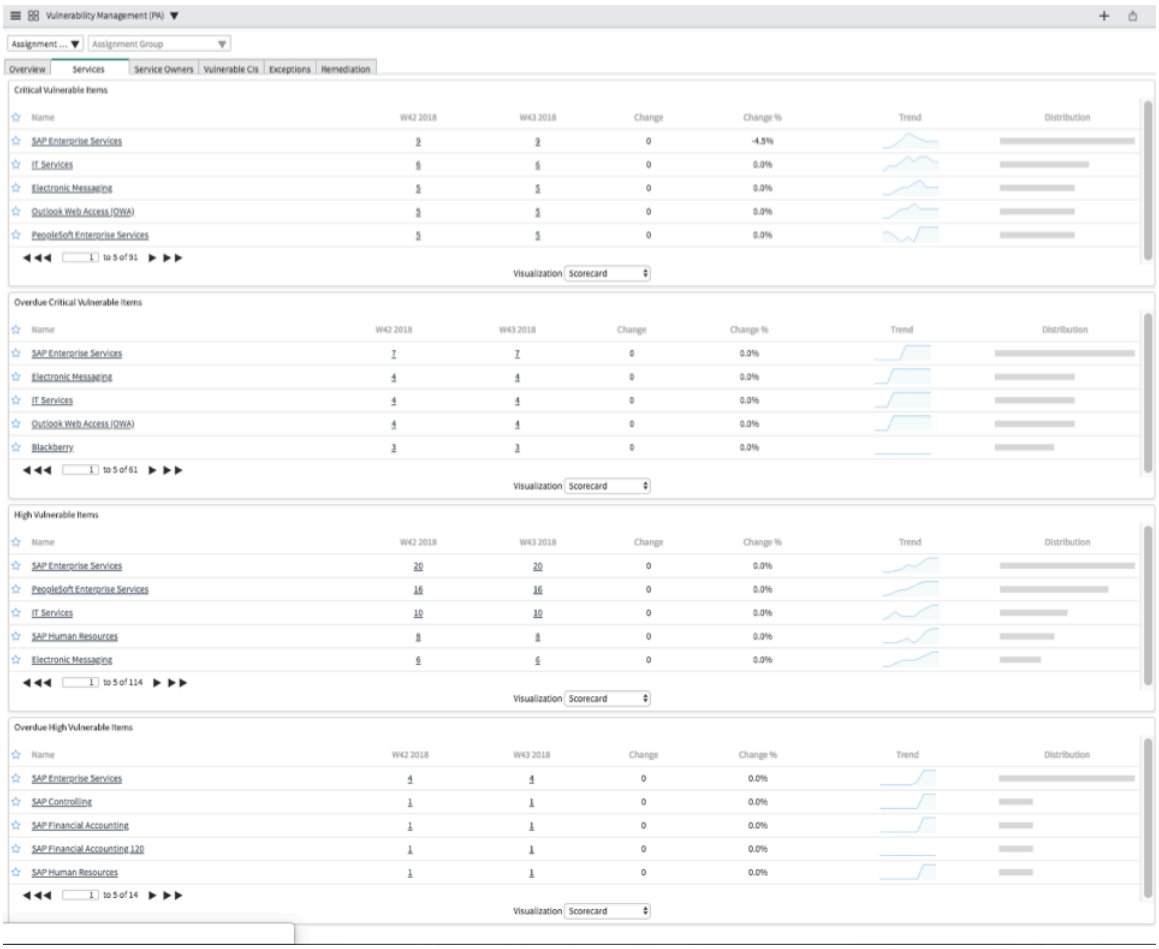
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Services d'entreprise

Ce tableau de bord expose le risque de vulnérabilité au niveau des services aux entreprises. Le partage de ces informations au sein de l'organisation peut aider les gestionnaires de services à corriger les vulnérabilités rapidement et de manière proactive, et conduire l'organisation vers un modèle de responsabilité partagée en matière de sécurité de l'information.

Vous pouvez modifier la classe de service en services techniques ou d'application à l'aide de la propriété système `sn_vul.service_classifications`.

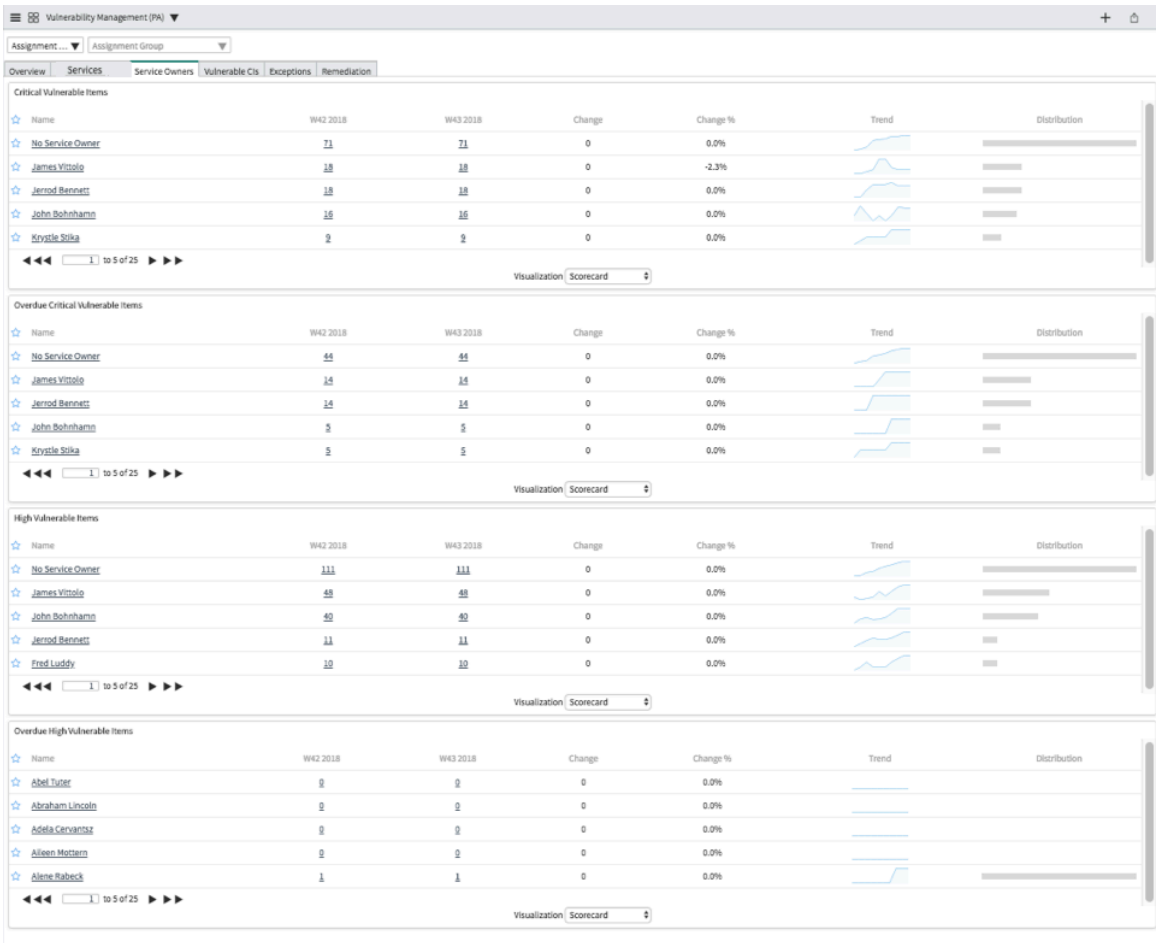


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Propriétaires de service

Ce tableau de bord agrège le risque de vulnérabilité depuis le niveau du service d'entreprise jusqu'aux propriétaires de services, c'est-à-dire aux dirigeants responsables de ces services d'entreprise. Il montre quels dirigeants assument le plus de risques de vulnérabilité et lesquels peuvent avoir le plus besoin d'aide, ce qui encourage des activités de remédiation rapides.



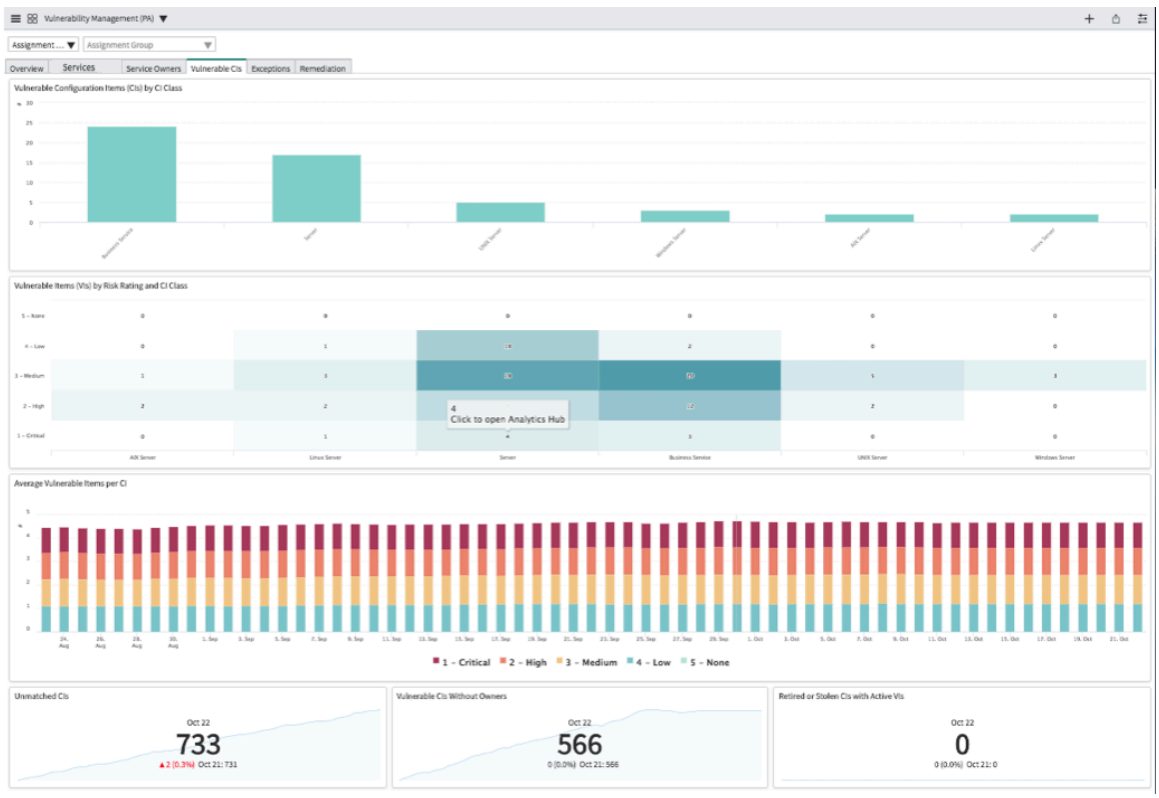
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet CI vulnérables

Ce tableau de bord présente l'étendue et la composition des CI présentant des vulnérabilités actives, ainsi que les catégories de CI qui nécessitent le plus d'attention. Identifiez les actifs déclassés avec des éléments vulnérables actifs et confirmez que les actifs ont été déclassés. Affichez le nombre de CI vulnérables pour lesquels il manque d'informations sur la propriété, afin de pouvoir identifier de manière proactive les propriétaires de ces actifs avant qu'une vulnérabilité critique n'affecte ces systèmes.

Dans l'onglet CI vulnérables, vous pouvez afficher les rapports CI vulnérables sans propriétaire et CI mis hors service ou volés avec des VI actifs en temps réel.



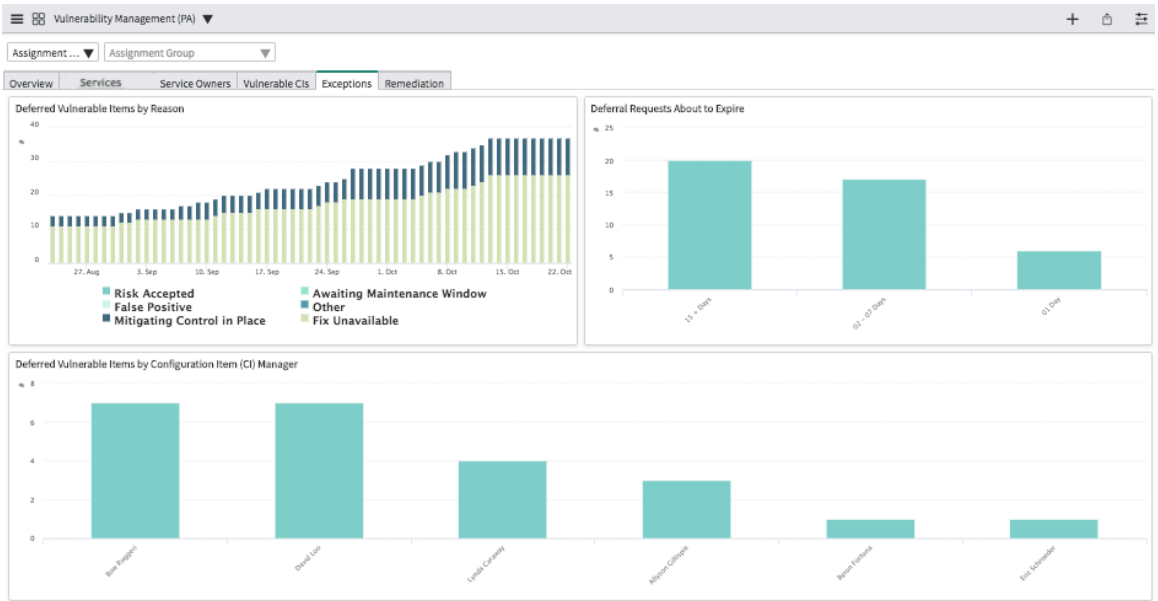
Onglet Exceptions

Ce tableau de bord vous aide à comprendre où votre organisation prend des risques en raison de reports potentiellement excessifs et à reconsidérer les options de rattrapage.

Vous pouvez afficher les éléments vulnérables différés par motif, les demandes de report arrivant à expiration, les exceptions pour les éléments vulnérables critiques par groupe d'affectation et les demandes d'exception par rapport du demandeur.

Traduction automatique

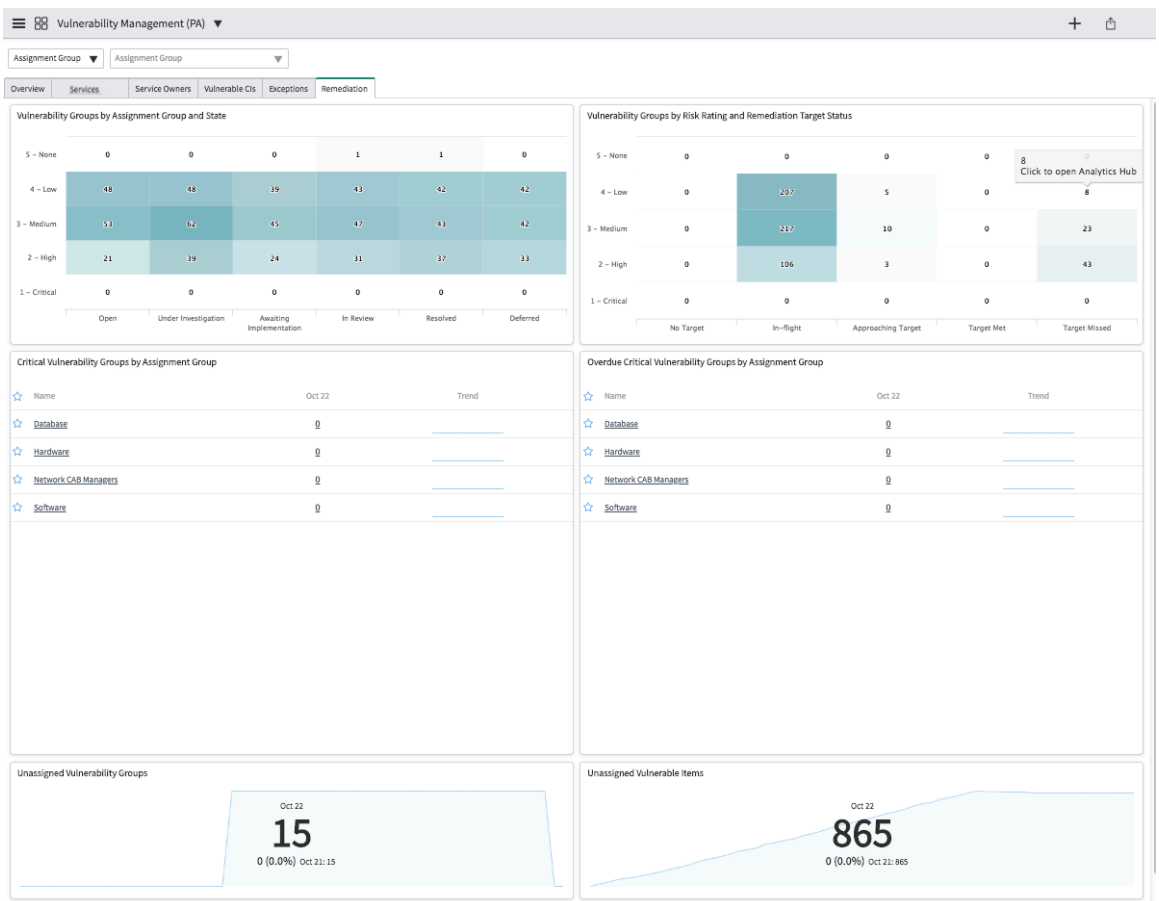
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Onglet Rattrapage

Ce tableau de bord vous aide à comprendre la progression de vos actions de rattrapage et à identifier les équipes de support qui ont le plus besoin d'aide pour les exécuter.

Dans l'onglet Rattrapage, vous pouvez afficher le rapport des éléments vulnérables non affectés en temps réel.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indicateurs

Indicateurs Vulnerability Response

Il existe un certain nombre d'indicateurs utilisés pour mesurer et suivre la progression de votre rattrapage de vulnérabilité dans l'application Réponse aux vulnérabilités .

L'option Collecter les enregistrements pour les indicateurs est désactivée par défaut pour l'application Réponse aux vulnérabilités . Cette option est désactivée afin que certains rapports puissent être consultés en temps réel. Les informations de tendance utilisées par ces indicateurs sont toujours disponibles si vous préférez activer la collecte manuelle des enregistrements et afficher les enregistrements qui composent les scores.

Vulnérabilités distinctes

Vulnérabilités distinctes avec count_active_vi > 0. L'objectif est de minimiser.

Éléments vulnérables critiques en retard non différés

Il s'agit du décompte sur la source de données VI.Active, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

% d'éléments vulnérables ayant atteint la cible de remédiation

`([[Éléments vulnérables fermés > Cible de rattrapage = Cible atteinte]] / [[Éléments vulnérables fermés]]) * 100`. L'objectif est de maximiser.

Éléments vulnérables non affectés

Tous les éléments vulnérables actifs pour lesquels le groupe d'affectation et les champs Affecté à sont vides. L'objectif est de minimiser.

Éléments vulnérables critiques (services)

Il s'agit du décompte sur la source de données VI actifs (services), qui utilise la table suivante : sn_vul_analytics_business_services_vi. L'objectif est de minimiser.

Éléments hautement vulnérables en retard (services)

Il s'agit du décompte sur la source de données VI actifs (services), qui utilise la table suivante : sn_vul_analytics_business_services_vi. L'objectif est de minimiser.

Tâches de remédiation non affectées

Toutes les tâches de rattrapage actives pour lesquelles le groupe d'affectation et les champs Affecté à sont vides. L'objectif est de minimiser.

Éléments vulnérables critiques

Il s'agit du décompte sur la source de données VI.Active, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables

Il s'agit du décompte sur la source de données VI.Active, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Nouveaux éléments vulnérables

Il s'agit du décompte sur la source de données VI.Nouveau, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Éléments de configuration vulnérables

Il s'agit du décompte distinct sur la source de données VI.Active, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Durée cumulée des éléments vulnérables fermés

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il s'agit de la somme sur la source de données VI.Fermé, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Tâches de remédiation non différées

Il s'agit du décompte sur la source de données VG. Actif, qui utilise la table suivante : sn_vul_vulnerability. L'objectif est de minimiser.

Délai moyen de remédiation de l'élément vulnérable

```
[[Durée cumulée des éléments vulnérables fermés]] / [[Éléments
vulnérables fermés]]
```

Éléments vulnérables critiques en retard (services)

Il s'agit du décompte sur la source de données VI actifs (services), qui utilise la table suivante : sn_vul_analytics_business_services_vi. L'objectif est de minimiser.

Éléments de configuration mis hors service

Il s'agit du décompte distinct sur la source de données VI.Active, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Demandes de report

Il s'agit du décompte sur la source de données Demandes de report actives, qui utilise la table : sn_vul_change_approval. L'objectif est de minimiser.

Éléments vulnérables par éléments de configuration

Il s'agit du décompte sur la source de données CI avec VI actifs, qui utilise la table : sn_vul_analytics_vi_ci_class. L'objectif est de minimiser.

Éléments vulnérables clôturés

Éléments vulnérables fermés est mesuré quotidiennement en unité #. L'objectif est de maximiser.

Éléments de configuration sans correspondance

Répertorie les hôtes découverts par les analyseurs de vulnérabilité tiers qui ne correspondent à aucun CI existant dans la CMDB.

Tâches de remédiation critiques en retard non différées

Il s'agit du décompte sur la source de données VG. Actif, qui utilise la table suivante : sn_vul_vulnerability. L'objectif est de minimiser.

Éléments de configuration vulnérables sans groupe de support

Il s'agit du décompte sur la source de données VI.Open, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Tâches de remédiation critiques non différées

Il s'agit du décompte sur la source de données VG. Actif, qui utilise la table suivante : sn_vul_vulnerability. L'objectif est de minimiser.

Éléments vulnérables différés

Il s'agit du décompte sur la source de données VI.Active, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Éléments hautement vulnérables (services)

Il s'agit du décompte sur la source de données VI actifs (services), qui utilise la table suivante : sn_vul_analytics_business_services_vi. L'objectif est de minimiser.

Éléments de configuration distincts avec des éléments vulnérables actifs

Il s'agit du décompte distinct sur la source de données CI avec VI actifs, qui utilise la table : sn_vul_analytics_vi_ci_class. L'objectif est de minimiser.

Nombre moyen d'éléments vulnérables par élément de configuration

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

`[[Éléments vulnérables actifs]] / [[CI vulnérables]]`. L'objectif est de minimiser.

Tâches de remédiation

Il s'agit du décompte sur la source de données VG. Actif, qui utilise la table suivante : sn_vul_vulnerability. L'objectif est de minimiser.

Éléments vulnérables différés critiques

Il s'agit du décompte sur la source de données VI.Active, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Demandes de report (créées)

Il s'agit du décompte sur la source de données Closed.Requests, qui utilise la table suivante : sn_vul_change_approval. L'objectif est de minimiser.

Répartitions

Les noms de répartitions suivants s'appliquent aux indicateurs sur le tableau de bord :

- Âge
- Âge clôturé
- Groupe d'affectation
- Classe CI
- Gestionnaire CI
- Âge du report
- Motif du report
- Demandeurs d'exceptions
- Vecteur d'attaque de l'exploit
- Un exploit existe
- Niveau de compétence de l'exploit
- Règle de cible de rattrapage
- État de la cible de la remédiation
- État de la cible de rattrapage (fermé)
- Cote de risque
- Service
- Criticité du service
- Propriétaire de service
- Sévérité
- État

Source de répartition

- Groupe d'affectation : s'applique aux rapports VI ou et RT
- Un exploit existe : s'applique aux rapports de VI.
- Vecteur d'attaque de l'exploit : s'applique aux rapports de VI.
- Niveau de compétence de l'exploit : S'applique aux rapports de VI.
- État de la cible de rattrapage : s'applique aux rapports VI et RT.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cote de risque : s'applique aux rapports de VI et de RT.
- État : S'applique aux rapports VI et RT.

Visualisations des données

Titre	Type	Description
Vulnérabilités	Score unique	Nombre de vulnérabilités associées à un ou plusieurs éléments vulnérables actifs.
Éléments vulnérables (VI)	Score unique	Nombre d'éléments vulnérables actifs (non fermés).
Éléments de configuration (CI) vulnérables	Score unique	Nombre d'éléments de configuration (CI) associés à un ou plusieurs éléments vulnérables actifs.
Tâches de remédiation	Score unique	Nombre de tâches de rattrapage actives (non fermées).
Éléments vulnérables par cote de risque	Barre	Nombre d'éléments vulnérables actifs regroupés par cote de risque au cours de la période sélectionnée.
Éléments vulnérables par âge et cote de risque	Carte thermique	Nombre d'éléments vulnérables actifs regroupés par cote de risque et par âge (en jours).
Cible de rattrapage de VI atteinte	Score unique	Pourcentage d'éléments vulnérables fermés qui ont atteint leur date cible de rattrapage au cours des trimestres actuels et précédents. Les cibles de rattrapage sont calculées à partir de la dernière date d'ouverture additionnée au nombre de jours (mesurés par incréments de 24 heures).
Délai moyen de rattrapage (MTTR) des VI	Score unique	Le délai moyen de rattrapage (fermeture) d'un élément vulnérable, affiché comme moyenne d'exécution de 30 jours.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre	Type	Description
		Remarque : La valeur Âge fermé est calculée lors de la collecte des données. La valeur correspond à la différence entre la date de last_opened et la date et l'heure de la tâche de collecte.
Tâches de remédiation critiques proches de l'échéance	Score unique	Nombre de tâches de rattrapage actives approchant de leur date cible de rattrapage. La date cible de rattrapage d'une tâche de rattrapage est fixée à la date d'échéance la plus proche appartenant à un élément vulnérable actif dans le groupe. Les cibles de rattrapage sont calculées à partir de la dernière date d'ouverture additionnée au nombre de jours (mesurés par incréments de 24 heures). Ce rapport exclut les tâches de rattrapage différées.
Éléments vulnérables nouveaux et fermés	Barre	Nombre d'éléments vulnérables nouveaux et fermés sur la période sélectionnée. **Remarque :** La valeur Âge fermé est calculée lors de la collecte des données. La valeur correspond à la différence entre la date de last_opened et la date et l'heure de la tâche de collecte.
Éléments vulnérables fermés par état de la cible de rattrapage	Barre	Nombre d'éléments vulnérables fermés regroupés par état de la cible de rattrapage au cours de la période sélectionnée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre	Type	Description
		Remarque : La valeur Âge fermé est calculée lors de la collecte des données. La valeur correspond à la différence entre la date de last_opened et la date et l'heure de la tâche de collecte.
Éléments vulnérables critiques par groupe d'affectation	Liste et ligne 	Nombre d'éléments vulnérables actifs avec une cote de risque critique, regroupés par groupe d'affectation.
Éléments vulnérables critiques en retard par groupe d'affectation	Liste et ligne 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par groupe d'affectation. Les cibles de rattrapage sont calculées à partir de la dernière date d'ouverture additionnée au nombre de jours (mesurés par incréments de 24 heures). Ce rapport exclut les éléments vulnérables différés.

Services d'entreprise

Nom	Type	Description
Éléments vulnérables critiques	Liste, ligne et barre de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique, regroupés par service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats.
Éléments vulnérables critiques en retard	Liste, ligne et barre de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par service d'entreprise.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Services d'entreprise (suite)

Nom	Type	Description
		Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats. Ce rapport exclut les éléments vulnérables différés.
Éléments hautement vulnérables	Liste, ligne et barre de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée, regroupés par service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats.
Éléments hautement vulnérables en retard	Liste, ligne et barre de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée et dépassant leur date cible de rattrapage, regroupés par service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats. Ce rapport exclut les éléments vulnérables différés.

Propriétaires de service

Nom	Type	Description
Éléments vulnérables critiques	Liste, ligne et barre de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique, regroupés par propriétaire de service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétaires de service (suite)

Nom	Type	Description
Éléments vulnérables critiques en retard	Liste, ligne et barre de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par propriétaire de service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats. Ce rapport exclut les éléments vulnérables différés.
Éléments hautement vulnérables	Liste, ligne et barre de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée, regroupés par propriétaire de service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats.
Éléments hautement vulnérables en retard	Liste, ligne et barre de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée et dépassant leur date cible de rattrapage, regroupés par propriétaire de service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats. Ce rapport exclut les éléments vulnérables différés.

CI vulnérables

Nom	Type	Description
Éléments de configuration (CI) vulnérables par classe CI	Barre 	Nombre d'éléments de configuration présentant des vulnérabilités actives, regroupés par classe CI dans la CMDB.
Éléments vulnérables (VI) par classe CI	Arborescence 	Nombre de VI actifs répartis par classe CI.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

CI vulnérables (suite)

Nom	Type	Description
Nombre moyen d'éléments vulnérables par CI	Barre	Nombre moyen d'éléments vulnérables appartenant à un élément de configuration, regroupés par cote de risque.
Ci sans correspondance	Score unique	Nombre d'éléments de configuration importés qui ne correspondent à aucun CI existant dans la CMDB.
CI vulnérables sans groupe de support	Score unique	Nombre d'éléments de configuration vulnérables auxquels aucun groupe de support n'a été affecté.
CI mis hors service ou volés avec des VI actifs	Score unique	Nombre d'éléments de configuration marqués comme **Mis hors service** ou **Volés** dans la CMDB qui ont des éléments vulnérables actifs.

Exception :

Nom	Type	Description
Éléments vulnérables différés par motif	Barre	Nombre d'éléments vulnérables reportés regroupés par motif de report.
Demandes de report sur le point d'expirer	Barre	Nombre de demandes de report associées à des tâches de rattrapage ou à des éléments vulnérables qui sont sur le point d'être rouverts pour examen. Ils sont regroupés par le nombre de jours restants jusqu'à leur réouverture. Si les notifications par e-mail sont définies, un e-mail est envoyé.
Éléments vulnérables différés par gestionnaire d'éléments de configuration (CI)	Barre	Nombre d'éléments vulnérables différés regroupés par le gestionnaire pour l'élément de configuration associé.

Rattrapage

Nom	Type	Description
Tâches de remédiation par cote de risque et par état	Carte thermique	Nombre de tâches de rattrapage actives regroupées par cote de risque et par état.
Tâches de remédiation par cote de risque et par état de la cible de remédiation	Carte thermique	Nombre de tâches actives regroupées par cote de risque et par état de la cible de rattrapage. Ce rapport exclut les éléments vulnérables différés.
Tâches de remédiation critiques par groupe d'affectation	Liste et ligne	Nombre de tâches de rattrapage actives avec une cote de risque critique, regroupées par groupe d'affectation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rattrapage (suite)

Nom	Type	Description
		Ce rapport exclut les tâches de rattrapage différées.
Tâches de remédiation critiques en retard par groupe d'affectation	Liste et ligne	Nombre de tâches de rattrapage actives avec une cote de risque critique et des dates cibles de rattrapage passées, regroupées par groupe d'affectation. Ce rapport exclut les tâches de rattrapage différées.
Tâches de remédiation non affectées	Score unique	Nombre de tâches de rattrapage actives sans délégataire ou groupe d'affectation.
Éléments vulnérables non affectés	Score unique	Nombre d'éléments vulnérables actifs sans délégataire ou groupe d'affectation.

Afficher les Analyse des performances pour Réponse aux vulnérabilités rapports [PA] en temps réel

Pour gérer vos éléments vulnérables (VI) les plus importants et vous aider à les corriger rapidement, affichez des rapports sur demande, en temps réel sur le tableau de bord Gestion de la vulnérabilité (PA). L'application Analyse des performances pour Réponse aux vulnérabilités est disponible avec un abonnement distinct à partir du ServiceNow Storefichier .

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pour plus d'informations sur les rapports de Analyse des performances pour Réponse aux vulnérabilités, consultez le tableau de bord Gestion de la vulnérabilité [PA].

Pour en savoir plus sur la configuration et l'installation de l'application, reportez-vous à la Analyse des performances pour Réponse aux vulnérabilités section Installer et configurer l'application Analyse des performances pour Réponse aux vulnérabilités [PA].

S'il n'est pas affiché, pour afficher le tableau de bord, accédez à **Réponse aux vulnérabilités** > **Vue d'ensemble**. Les onglets du rapport sont affichés en haut du tableau de bord.

À partir de la version 19.0 de Réponse aux vulnérabilités, ce tableau de bord peut également être consulté dans l'interface utilisateur de la nouvelle expérience. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour

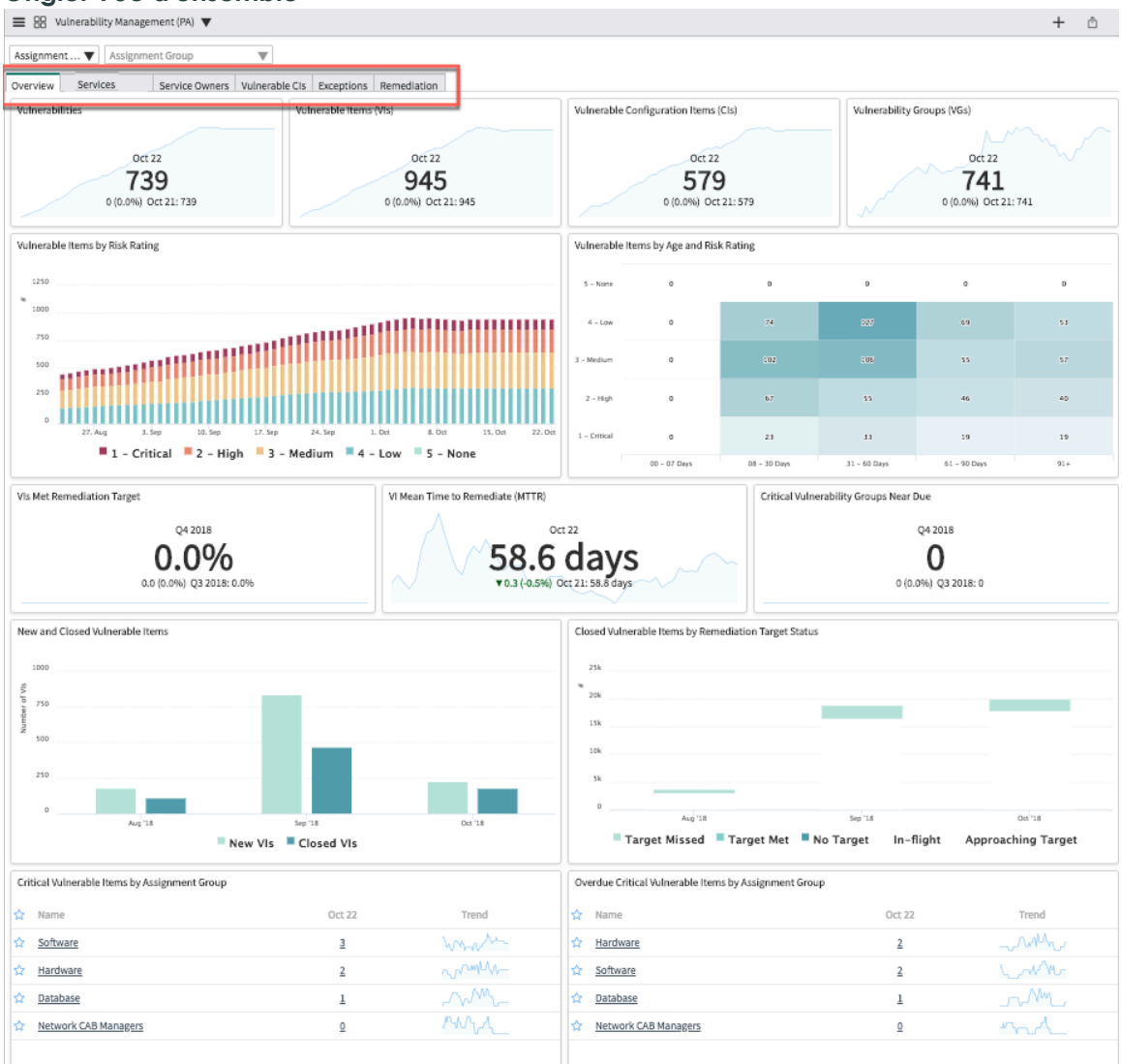
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

plus d'informations, consultez Tableaux de bord dans Vulnerability Manager Workspace et Tableaux de bord dans IT Remediation Workspace.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Onglet Vue d'ensemble



Affichez les rapports suivants en temps réel dans les onglets du tableau de bord Gestion des vulnérabilités (PA).

- Onglet Vue d'ensemble
  - Éléments vulnérables critiques par groupe d'affectation
- Onglet CI vulnérables :
  - CI vulnérables sans propriétaires
  - CI mis hors service ou volés avec des VI actifs
- Onglet Exceptions :
  - Éléments vulnérables différés par motif
  - Demandes de report sur le point d'expirer
  - Éléments vulnérables différés par le gestionnaire DSI

Traduction automatique

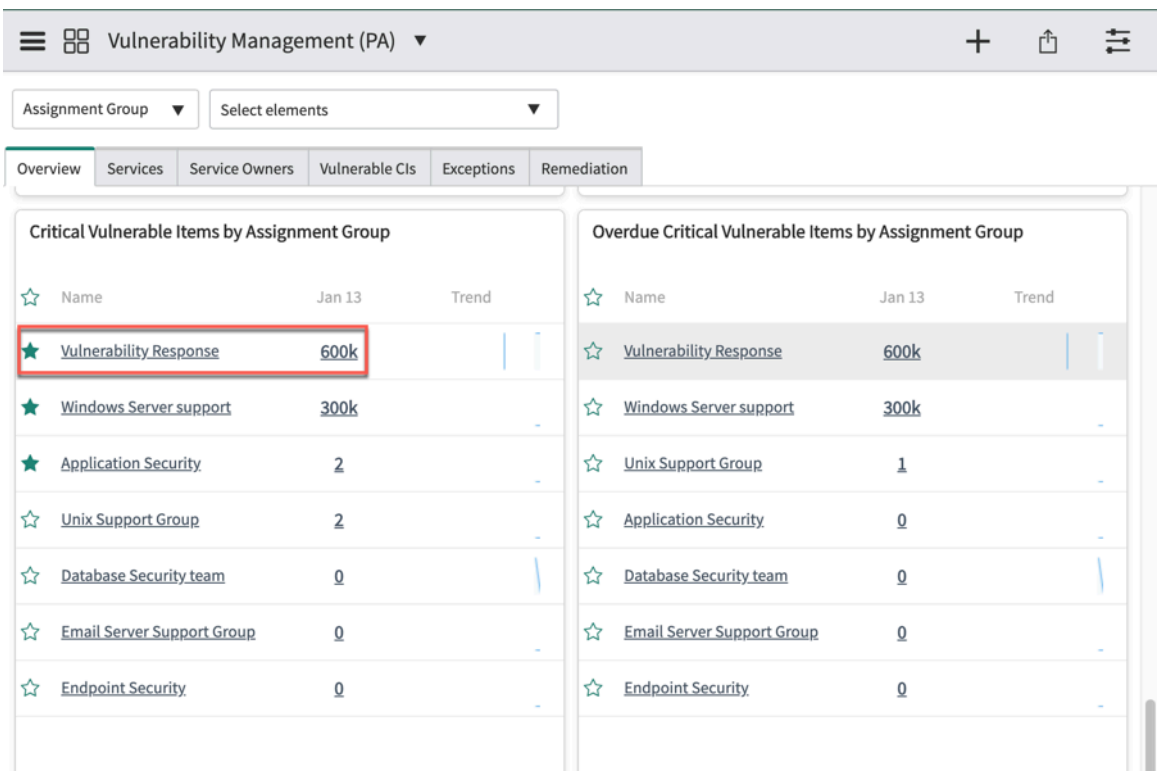
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Onglet Rattrapage :
  - Éléments vulnérables non affectés

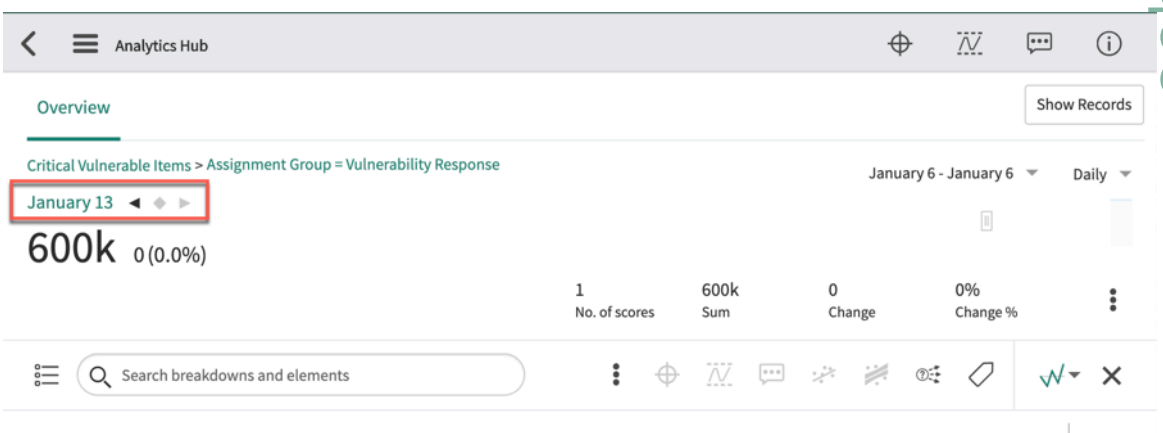
Pour afficher les scores en temps réel, avec l'un des onglets sélectionnés contenant des rapports en temps réel, procédez comme suit :

Procédure

1. Dans le rapport, par exemple, Éléments vulnérables critiques par groupe d'affectation, cliquez sur l'un des liens qui s'affichent.



2. Dans l'enregistrement qui s'affiche, cliquez sur la date.

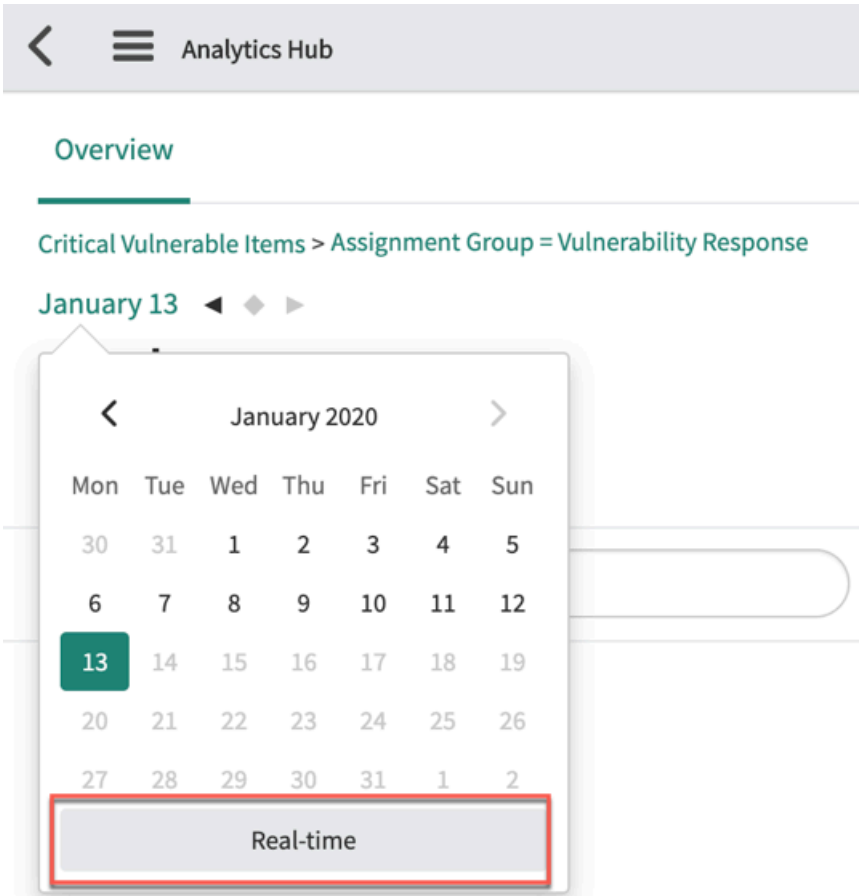


3. Dans le calendrier qui s'affiche, cliquez sur Temps réel.

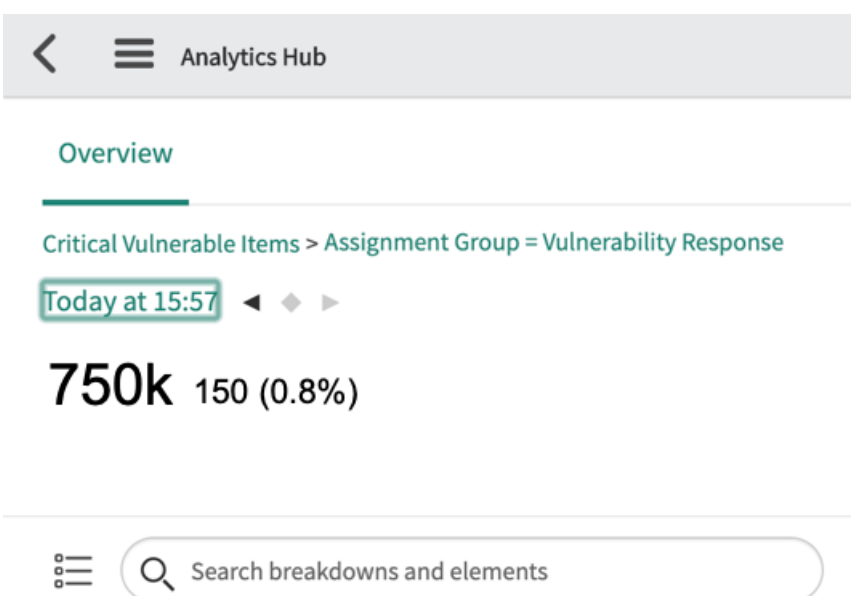
   Si un rapport ne prend pas en charge un score en temps réel, le bouton Temps réel ne s'affiche pas sur le calendrier.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La mise à jour de la valeur peut prendre quelques instants. La date actuelle, les enregistrements, le nombre de nouveaux enregistrements depuis le dernier rapport et le pourcentage de changement par rapport au dernier rapport sont également affichés.



4. Facultatif : Pour afficher les enregistrements qui composent le rapport, avec le rapport en temps réel affiché, en haut à droite, cliquez sur **Afficher les enregistrements**.
   La liste des enregistrements qui composent le score s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les Analyse des performances indicateurs pour Réponse aux vulnérabilités [PA]

Affichez les indicateurs automatisés et formulés Analyse des performances représentant les données de vulnérabilité dans votre instance.

Avant de commencer

L'option Collecter les enregistrements pour les indicateurs est désactivée par défaut pour l'application Analyse des performances - Content Pack Vulnerability Response. Cette option est désactivée afin que certains rapports puissent être consultés en temps réel. Les informations de tendance utilisées par ces indicateurs sont toujours disponibles si vous préférez activer la collecte manuelle des enregistrements et afficher les enregistrements qui composent les scores.

Remarque : L'activation de la collecte d'enregistrements dans un indicateur peut avoir un impact sur vos performances et allonger considérablement le temps et la mémoire nécessaires à l'exécution de la tâche de collecte de données.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète), ou pa.viewer

Pourquoi et quand exécuter cette tâche

Réponse aux vulnérabilités comporte à la fois des indicateurs automatisés et formulés.

Termes clés

Indicateur PA

Définit une mesure de performance effectuée à intervalles réguliers d'un service d'entreprise, d'une activité ou d'un comportement organisationnel, par exemple, Éléments vulnérables critiques en retard non différés.

Source de l'indicateur PA

Ensembles de données qui filtrent les enregistrements à partir d'une vue de table ou de base de données, par exemple, VI actif.

Collecter les enregistrements

Lorsqu'elle est activée, elle stocke les enregistrements en mémoire et fournit l'accès au centre d'analyse.

Répartitions

Les répartitions filtrent et regroupent les enregistrements collectés. Les pannes peuvent augmenter l'utilisation de la mémoire, d'autant plus que leur nombre et leur diversité augmentent.

Exclusions de répartition

Les exclusions suppriment certaines répartitions, ce qui peut réduire la consommation de mémoire.

Procédure

1. Pour les indicateurs automatisés, accédez à **Analyse des performances** > **Indicateurs** > **Indicateurs automatisés**.
2. Pour les indicateurs formulés, accédez à **Analyse des performances** > **Indicateurs de formule**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur les indicateurs, consultez Indicateurs Analyse des performances .

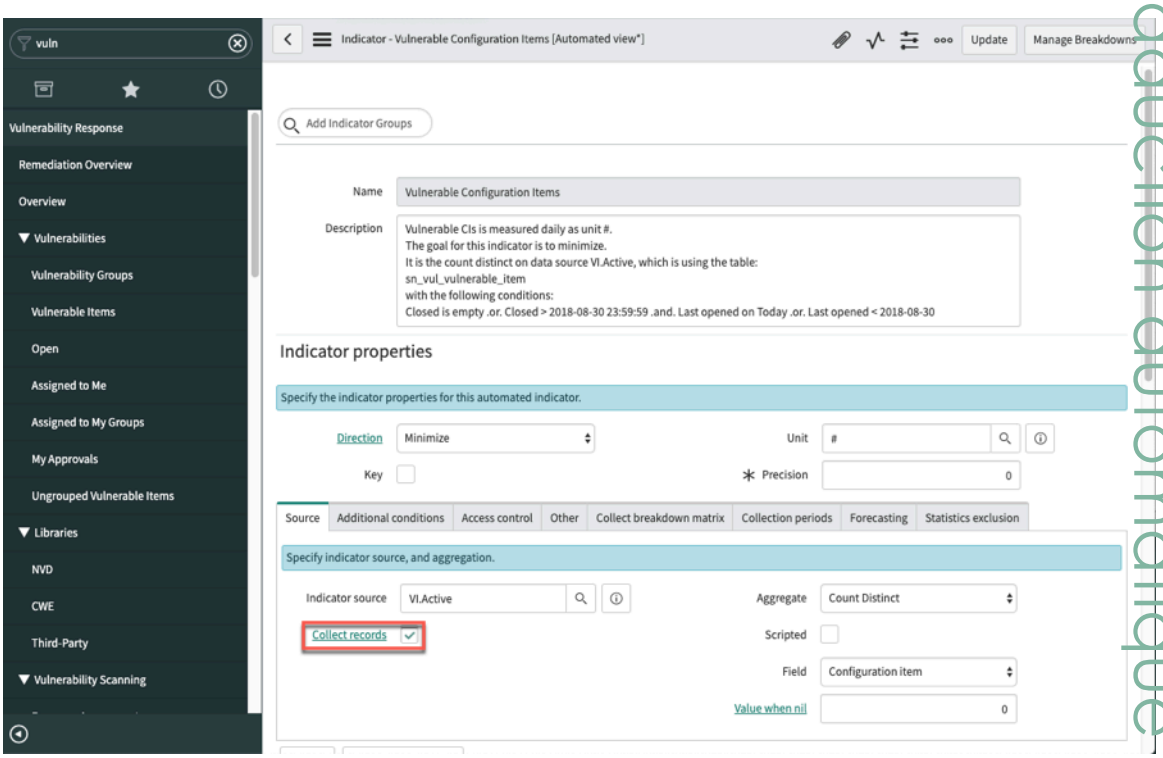
3. Dans les deux cas, effectuez une recherche sur **Application** > **Analyse des performances**.

> **Remarque :** Si ce n'est pas dans votre vue par défaut, ajoutez la colonne **Application** à l'aide de l'icône Engrenage ( ) dans le coin supérieur gauche de la page. La colonne Application s'affiche alors dans le menu déroulant Rechercher.

4. Facultatif : Pour activer Collecter les enregistrements sur une Analyse des performances pour Réponse aux vulnérabilités l'indicateur, procédez comme suit :

   a. Une fois la liste des indicateurs automatisés affichée, cliquez sur l'indicateur pour lequel vous souhaitez activer la collecte d'enregistrements.
   L'enregistrement de l'indicateur s'affiche.

   b. Dans la section Propriétés de l'indicateur avec l'onglet Source sélectionné, cochez la case Collecter les enregistrements.



   c. Choisissez-en un pour continuer.

Option	Description
Mettre à jour	Enregistrez vos mises à jour et revenez à la liste Indicateurs.
Gérer les répartitions	Réactiver les répartitions de second niveau pour les indicateurs répertoriés

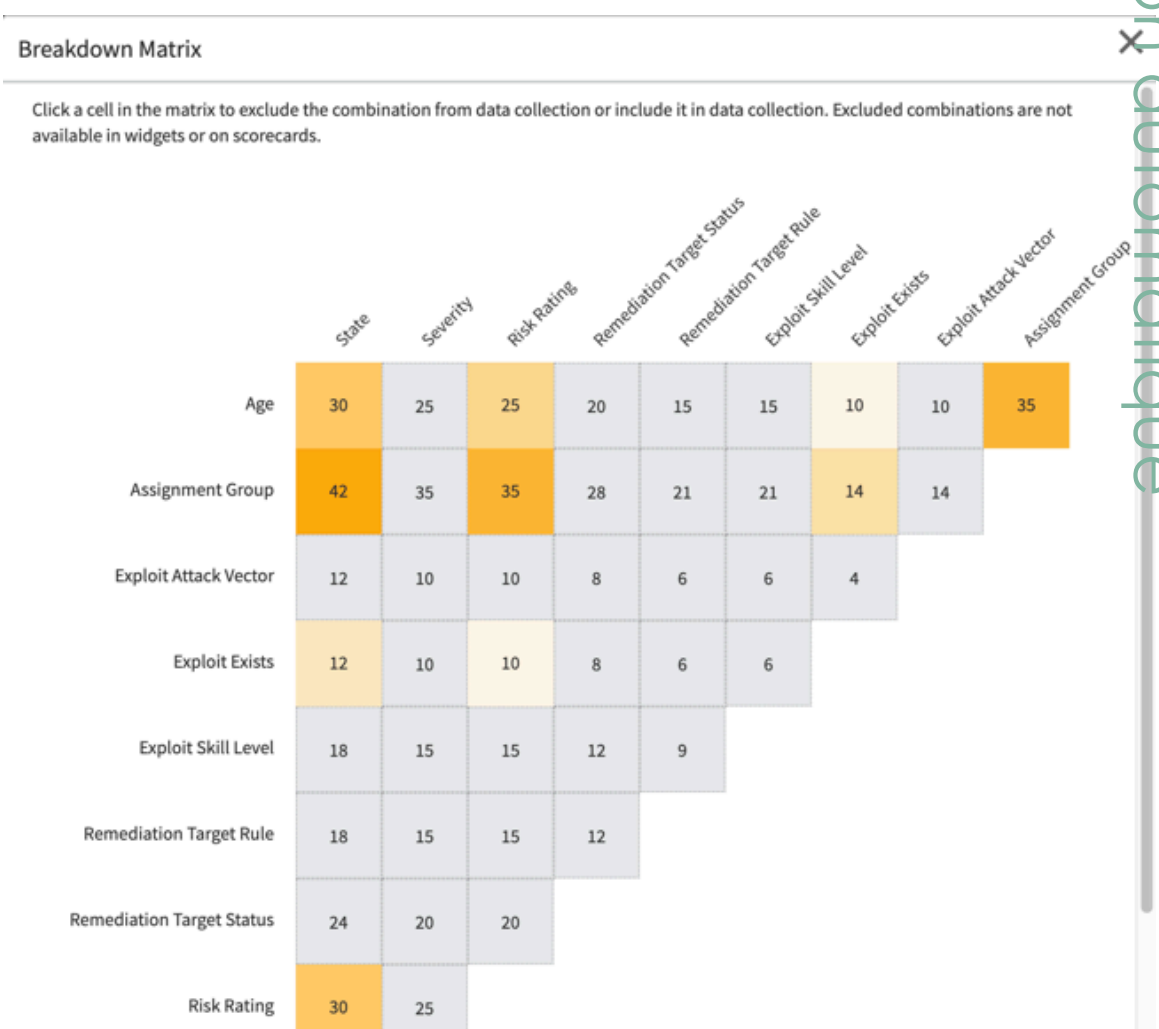
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Remarque : Si vous choisissez de réactiver les répartitions de second niveau, vous risquez d'augmenter considérablement votre consommation de mémoire et de ralentir le travail de collecte de données. Par défaut, les exclusions de répartition de second niveau ont été appliquées aux indicateurs suivants : ▪ Éléments de configuration vulnérables ▪ CI mis hors service ▪ VI différés	ou modifier les répartitions pour d'autres indicateurs. (Optional) Pour plus d'informations sur les répartitions d'Analyse des performances, consultez Répartitions d'Analyse des performances .

d. Cliquez sur **Gérer les répartitions**.

e. Dans le formulaire qui s'affiche, cliquez sur **Configurer la matrice de répartition**.
Le formulaire Breakdown Matrix (Matrice de répartition) s'affiche. Les combinaisons exclues sont sélectionnées et affichées avec des couleurs, comme illustré dans la figure suivante.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Pour supprimer l'exclusion et réactiver une combinaison exclue, cliquez sur une cellule sélectionnée.

g. En haut à droite du formulaire, cliquez sur **Fermer** pour renvoyer le formulaire Gérer la répartition.

h. Cliquez sur la flèche de retour pour revenir à l'enregistrement de l'indicateur.

i. Cliquez sur **Mettre à jour** pour enregistrer vos mises à jour et revenir à la liste Indicateurs.

Réponse aux vulnérabilités Informations de référence

Les rubriques suivantes vous fournissent des liens, des informations de référence, un dépannage et des articles de la base de connaissances, en plus des données de champ sur les formulaires et les enregistrements disponibles dans Réponse aux vulnérabilités.

Vous trouverez ci-dessous quelques liens vers d'autres ressources qui pourraient vous être utiles, en commençant par un lien vers l'article Liens vers la base de connaissances pour l'assistance et le dépannage VR/CC dans la base de connaissances HI.

- Liens vers les bases de connaissances pour l'assistance et le dépannage VR/CC
- Pour plus d'informations sur les applications et la compatibilité, consultez KB0856498 Matrice de compatibilité de Vulnerability Response et Changements de schéma de mise en production .
- Vidéos Security Operations
- Formation pour les développeurs
- Documentation pour les développeurs
- Collaborez avec un spécialiste de l'implémentation pour atteindre les résultats commerciaux souhaités avec le Customer Success Center .
- Suivez un cours Vulnerability Response pour acquérir de l'expertise et obtenir un retour sur investissement plus rapidement. Pour vous inscrire, consultez Formation et certification ServiceNow .
- Rechercher les composants installés avec une application
- Orchestration de Vulnerability Response
- Conseils pour l'écriture d'intégrations
- Poser des questions ou y répondre dans la communauté des opérations de sécurité
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Liste de vérification d'implémentation de l'application Réponse aux vulnérabilités

Cette liste de vérification répertorie les étapes requises pour une implémentation basique de l'application Réponse aux vulnérabilités sur votre Now Platform® instance. Lorsque vous avez terminé ces tâches, le système de base est prêt pour l'exploitation et la vérification.

Avant de commencer

Rôles requis : admin pour le téléchargement et l'activation d'applications et l'affectation de rôles, sn_vul.vulnerability_admin pour la configuration Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Envisagez de créer et d'imprimer un PDF de cette liste de contrôle afin de pouvoir cocher les tâches au fur et à mesure que vous les accomplissez.

2. Pour générer un PDF, cliquez sur l'icône **Enregistrer au format PDF** ( ) en haut de la rubrique, puis cliquez sur Rubrique sélectionnée.

Réponse aux vulnérabilités Tâches de liste de vérification d'implémentation de base pour l'administrateur

Élément	Description
☐	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que vous disposez des autorisations obtenues et que vous avez téléchargé (**installé**) les applications suivantes à partir de sur ServiceNow® Store votre Now Platform instance : ◦ Réponse aux vulnérabilités ◦ Réponse aux vulnérabilités Intégration dans la base de données de vulnérabilité nationale du NIST ◦ Qualys Intégration pour Security Operations **a.** Pour vérifier que les applications sont disponibles sur votre instance, naviguez vers **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout** et recherchez [sn_vul], [sn_vul_nvd] et [sn_vul_qualys]. **b.** Si vous ne parvenez pas à localiser les applications, consultez la rubrique pour plus d'informations sur l'obtention des autorisations et le téléchargement des applications.
☐	En tant qu'utilisateur disposant du rôle admin, naviguez **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation d'application d'intégration** et activez (**installez**) l'application Réponse aux vulnérabilités et ses dépendances sur votre Now Platform instance. **Remarque :** Pendant l'installation de l'application Réponse aux vulnérabilités , vous avez la possibilité d'installer des données de démonstration. Les données de démonstration sont requises si vous souhaitez exécuter des tests automatisés pour confirmer que votre instance fonctionne après l'installation. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production pour éviter les pannes et l'endommagement des données. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production. L'assistant Réponse aux vulnérabilités de configuration est installé automatiquement en même temps que l'application. L'assistant de configuration est requis pour configurer l'application Réponse aux vulnérabilités . En outre, il permet d'installer et de configurer l'intégration pour l'application Qualys Security Operations utilisée dans cet exemple, ainsi que d'autres applications qui prennent en charge et sont compatibles avec Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	Pour en savoir plus sur l'installation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités.
☐	En tant qu'utilisateur disposant du rôle administrateur, dans l'Assistant de configuration, accédez à **Tout** > **Groupes et utilisateurs de Vulnerability Response** et affectez des utilisateurs ayant les rôles de profil requis Réponse aux vulnérabilités . **a.** Dans l'Assistant de configuration, affichez les utilisateurs existants et tous les rôles déjà affectés en cliquant sur le lien du **module Administration utilisateurs** . **b.** Dans la liste, cliquez sur un nom d'utilisateur pour ouvrir l'enregistrement et cliquez sur la liste connexe **Rôles** . Tous les rôles affectés à cet utilisateur s'affichent. **c.** Revenir à **Groupes et utilisateurs de Vulnerability Response** dans l'Assistant de configuration et suivez les invites pour affecter le rôle sn_vul.vulnerability_admin. **Remarque :** Le rôle sn_vul.vulnerability_admin est requis pour poursuivre la configuration. Vous pouvez également poursuivre la configuration en tant qu'utilisateur avec le rôle administrateur. (Facultatif) Vous pouvez également affecter les rôles de gestionnaire d'éléments de configuration (CI) [sn_vul.ci_manager] et d'approbateur d'exceptions [sn_vul.exception_approver], mais ces profils ne sont pas requis pour les tâches de configuration restantes. Pour en savoir plus sur l'affectation des rôles de profil à l'aide de l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur les utilisateurs et l'affectation de rôles aux utilisateurs et aux groupes, consultez Administration utilisateurs .
☐	**a.** Accédez à la **Tout** > **Administration** > **Intégrations** vérifiez également que **l'intégration CWE Comprehensive 2000** est activée et exécutez la tâche planifiée pour importer les données. **b.** En tant qu'utilisateur disposant du rôle administrateur, accédez à **Applications système** > **Toutes les applications disponibles** et activez (**installez**) l'intégration de la réponse aux vulnérabilités avec l'application NVD. Exécutez les intégrations NVD et CWE dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit de scanner tiers. Consultez Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces et Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	plus d'informations sur l'installation, la configuration et l'affichage des bibliothèques NVD et CWE.
☐	En tant qu'utilisateur disposant du rôle admin, naviguez **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation d'application d'intégration** et activez l'application Integration pour Security Qualys Operations. Avant d'installer et d'exécuter un scanner tiers comme Qualys celui qui dispose d'une bibliothèque, vous devez d'abord installer et exécuter les intégrations NVD et CWE pour ingérer des données de vulnérabilité. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.
☐	(Facultatif) En tant qu'utilisateur disposant du rôle administrateur, si vous avez installé des données de démonstration avec l'application Réponse aux vulnérabilités , vous pouvez exécuter la Réponse aux vulnérabilités suite de tests ATF pour vérifier que les applications sont correctement installées. **Remarque :** Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production pour éviter les pannes et l'endommagement des données. Pour plus d'informations, consultez Exécuter la suite de tests Infrastructure de tests automatisés (ATF) pour Réponse aux vulnérabilités. Pour plus d'informations sur les tests automatisés, consultez Infrastructure de tests automatisés (ATF).

3. Poursuivez la configuration des applications à partir de la section Paramètres de Vulnerability Response.

   L'examen de ces paramètres vous aide à comprendre leur fonctionnement Réponse aux vulnérabilités tout au long de la configuration de votre environnement. Pour l'intégration du scanner utilisée dans cet exemple, vous devez modifier les paramètres.

   Les concepts que vous utilisez dans cet exemple de configuration pour le Qualys produit s'appliquent à d'autres applications de scanner.

   Vos Qualys informations d'identification sont requises pour configurer l'application. Vérifiez que vous disposez de tous les noms de compte, mots de passe et autres informations de service requis par Qualys les produits afin d'y avoir accès.

   Rôles requis : sn_vul.vulnerability_admin ou, alternativement, admin.

Réponse aux vulnérabilités Tâches de liste de vérification d'implémentation de base pour l'administrateur de vulnérabilité

Tâche	Description
☐	Passez en revue les règles d'affectation de vulnérabilité. Les règles d'affectation affectent automatiquement les éléments vulnérables (VI) au groupe d'affectation approprié. Pour en savoir

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	plus, consultez Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation. Pour en savoir plus sur la configuration Réponse aux vulnérabilités à l'aide de l'Assistant de configuration, reportez-vous à la section Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration.
☐	Passez en revue les règles de la tâche de rattrapage. Les règles de tâche de rattrapage regroupent automatiquement les éléments vulnérables (VI) à mesure qu'ils sont importés en fonction de certaines conditions. Pour plus d'informations, consultez Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage.
☐	Passez en revue les calculateurs de risque. Les calculateurs de risque attribuent un score aux éléments vulnérables pour définir leur ordre de priorité. Vous pouvez configurer les calculateurs de manière à incorporer les caractéristiques de l'élément de configuration (CI), de la disponibilité de l'exploitation et de la gravité de la vulnérabilité signalés par votre fournisseur d'évaluation de vulnérabilité (scanner). Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.
☐	Passez en revue les règles de cibles de rattrapage. Les règles de cibles de rattrapage définissent les chronologies de rattrapage pour les VI et les tâches de rattrapage. Pour plus d'informations, consultez Réponse aux vulnérabilités Règles de cibles de rattrapage.
☐	Dans la section Configuration de l'intégration, examinez les paramètres de l'application Qualys et définissez et planifiez vos importations de données. **a.** Cliquez sur **Intégrations de scanners**. **b.** Sur la page Applications installées, cliquez sur **Modifier**. **c.** Entrez vos informations d'identification et cliquez sur **Suivant**. **d.** Lisez les descriptions de configuration de la KnowledgeBase. **e.** Passez en revue la page de configuration de la détection d'hôte pour connaître les paramètres d'importation, les règles de recherche de CI et les calendriers d'importation. **f.** Une fois que vous êtes satisfait des paramètres sur cette page, cliquez sur **Exécuter maintenant** pour importer des données. Cliquez sur le lien **Afficher les détails** qui s'affiche pour afficher l'état d'exécution de l'intégration de vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	g. (Facultatif) Continuez à modifier les paramètres de configuration. **h.** Cliquez sur **Terminer** pour terminer l'installation et la configuration dans l'Assistant de configuration. Pour plus d'informations sur la configuration de l'application, reportez-vous à la Qualys section Configurer l'utilisation de l'assistant de Qualys Vulnerability Integration configuration.

Que faire ensuite

Félicitations ! Vous avez correctement installé l'application Réponse aux vulnérabilités et l'avez configurée, ainsi qu'une application de scanner, à l'aide de l'assistant de configuration. Le système de base est maintenant prêt à fonctionner.

Pour télécharger, installer et configurer d'autres applications pour Réponse aux vulnérabilités, suivez les mêmes étapes et concepts que ceux de la liste de vérification précédente. Consultez les rubriques spécifiques fournies pour chaque application pour plus d'informations.

Pour plus d'informations sur les applications prises en charge disponibles et mises à votre disposition à partir de pour ServiceNow StoreRéponse aux vulnérabilités, reportez-vous à la section Installation et prise en charge des Réponse aux vulnérabilités applications.

Pour plus d'informations sur l'utilisation Réponse aux vulnérabilitésde , reportez-vous à la section Exploration de l'application Réponse aux vulnérabilités.

Réponse aux vulnérabilités États des tâches de résolution

Les intégrations tierces importent des données de détection d'éléments vulnérables qui créent de nouveaux éléments de vulnérabilité (VIT) ou mettent à jour des VIT existants. Les états de détection mettent à jour les états VIT dans la mesure où ils sont Ouverts ou Fermés.

Pour plus d'informations sur la façon dont l'état d'une détection affecte l'état d'un VIT, reportez-vous à la États des détections, des tâches de rattrapage et des éléments vulnérablessection .

Avec Gestion des changements pour Réponse aux vulnérabilités, il existe une relation synchronisée entre les champs d'état des tâches de rattrapage et les champs d'état des demandes de changement (CHG) dans le produit Vulnerability Response. Au fur et à mesure qu'une demande de changement avance dans son cycle de vie, elle déplace automatiquement l'état de toutes les tâches de rattrapage connexes. Après l'implémentation d'une demande de changement, la tâche de rattrapage est automatiquement résolue. Consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage pour plus d'informations.

Remarque : À partir de la v23.0 de Réponse aux vulnérabilités:

- Le workflow **Approbation de l'état de la tâche de rattrapage** est déconseillé et remplacé par l'Approbation de l'état de la tâche de rattrapage du flux dans le Flow Designer.
- le bouton **Fermer** a été supprimé pour une tâche de rattrapage et la fermeture d'une tâche de rattrapage est pilotée par le scanner.

La table suivante répertorie les états des tâches de rattrapage et les actions que vous pouvez effectuer sur une tâche de rattrapage à l'état respectif :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des tâches de résolution

État	Description
Ouvrir	État à la création. À partir de cet état, vous pouvez : Afficher les VI en double Identifiez les VI en double signalés par plusieurs scanners du système. Vous pouvez marquer le VI en double comme Résolu ou Fermé. Les entrées en double ne sont affichées que lorsque la combinaison des vulnérabilités est créée à l'aide des vulnérabilités et expositions communes (CVE). Pour plus d'informations, consultez Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables. Démarrer l'examen Affectez cette tâche de rattrapage à une personne ou à un groupe pour commencer à enquêter. Marquer comme faux positif Marquez un élément ou un groupe comme faux positif si le scanner signale qu'une vulnérabilité existe dans le système, mais qu'en réalité il n'y a pas de vulnérabilité. Demande d'exception Demandez une exception, une date de réouverture (jusqu'à), un motif et, éventuellement, fournissez des informations supplémentaires. Reporter le rattrapage de l'élément ou du groupe jusqu'à la date à laquelle une exception est demandée. Résoudre Marquez comme Résolu pour faire passer l'élément ou le groupe à l'état Résolu. Créer un changement Créez une demande de changement ou associez une tâche de rattrapage à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. Diviser la tâche de rattrapage Pour une tâche de rattrapage comportant plusieurs éléments vulnérables, utilisez un ensemble de conditions pour filtrer un sous-ensemble d'éléments vulnérables et diviser une tâche de rattrapage. Les éléments que vous sélectionnez sont automatiquement déplacés vers une nouvelle tâche de rattrapage. Pour plus d'informations, consultez Fractionner une tâche de rattrapage dans Espace de travail de remédiation IT. Différer Sélectionnez l'état Différé, une date de réouverture, un motif et, éventuellement, fournissez des informations

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des tâches de résolution (suite)

État	Description
	supplémentaires. Reporter l'état de la tâche de rattrapage à la date de réouverture. Supprimer Confirmez la suppression. Supprime le groupe.
En cours d'examen	Déclenché par le bouton **Démarrer l'examen** . À partir de cet état, vous pouvez : Créer un incident de sécurité Pour plus d'informations, consultez Créer un incident de sécurité. Créer un changement Créez une demande de changement ou associez une tâche de rattrapage à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. Fractionner la tâche Pour une tâche de rattrapage comportant plusieurs éléments vulnérables, utilisez un ensemble de conditions pour filtrer un sous-ensemble d'éléments vulnérables et diviser une tâche de rattrapage. Les éléments que vous sélectionnez sont automatiquement déplacés vers une nouvelle tâche de rattrapage. Pour plus d'informations, consultez Diviser une tâche de rattrapage. Créer une demande de changement Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage. En attente d'implémentation Passe l'état à En attente d'implémentation. Cet état indique que les tâches de rattrapage ont été référencées en dehors d'un Réponse aux vulnérabilités. Différer Sélectionnez l'état Différé, une date de réouverture, un motif et, éventuellement, fournissez des informations supplémentaires. Reporter l'état de la tâche de rattrapage à la date de réouverture. Supprimer Confirmez la suppression. Supprime la tâche de rattrapage.
Différé	Déclenché par le bouton **Demander une exception** . Dans le cadre du workflow d'approbation, l'état Différé est En cours de révision et ne peut pas être fermé tant qu'il n'a pas été approuvé. À partir de cet état, vous pouvez : Créer un changement

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des tâches de résolution (suite)

État	Description
	Créez une demande de changement ou associez une tâche de rattrapage à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. Fractionner la tâche Pour une tâche de rattrapage comportant plusieurs éléments vulnérables, utilisez un ensemble de conditions pour filtrer un sous-ensemble d'éléments vulnérables et diviser un groupe de vulnérabilité. Les éléments que vous sélectionnez sont automatiquement déplacés vers un nouveau VG. Consultez Diviser une tâche de rattrapage. Créer un incident de sécurité Pour plus d'informations, consultez Créer un incident de sécurité. Rouvrir Revenez à un état Ouvert. Supprimer Confirmez la suppression. Supprime la tâche de rattrapage. Les informations sur le report s'affichent sous l'onglet **Fermer/Différer** . À la date de report, le groupe rouvre pour correction.
En attente d'implémentation	Déclenché par le bouton **En attente d'implémentation** . À partir de cet état, vous pouvez : Créer un incident de sécurité Pour plus d'informations, consultez Créer un incident de sécurité. Créer un changement Créez une demande de changement ou associez une tâche de rattrapage à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. Fractionner la tâche Pour une tâche de rattrapage comportant plusieurs éléments vulnérables, utilisez un ensemble de conditions pour filtrer un sous-ensemble d'éléments vulnérables et diviser un groupe de vulnérabilité. Les éléments que vous sélectionnez sont automatiquement déplacés vers une nouvelle tâche de rattrapage. Pour plus d'informations, consultez Diviser une tâche de rattrapage. Créer une demande de changement

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des tâches de résolution (suite)

État	Description
	Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage. Différer Sélectionnez l'état Différé, une date de réouverture, un motif et, éventuellement, fournissez des informations supplémentaires. Reporter l'état de la tâche de rattrapage à la date de réouverture. Résoudre Ajoutez des notes. L'état devient Résolu. Les notes s'affichent sous l'onglet **Résolution** . Supprimer Confirmez la suppression. Supprime la tâche de rattrapage.
Résolu	Déclenché à partir du bouton **Résoudre** . À partir de cet état, vous pouvez : Créer un incident de sécurité Pour plus d'informations, consultez Créer un incident de sécurité. Créer un changement Créez une demande de changement ou associez un groupe de vulnérabilité à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. Rouvrir Revenez à un état Ouvert. Supprimer Confirmez la suppression. Supprime la tâche de rattrapage. Les notes s'affichent sous l'onglet **Notes** . Les informations sur la résolution s'affichent sous l'onglet **Résolution** .
Fermé	Déclenché par le scanner. À partir de cet état, vous pouvez : Créer un incident de sécurité Pour plus d'informations, consultez Créer un incident de sécurité. Rouvrir Revenez à un état Ouvert. Supprimer Confirmez la suppression. Supprime la tâche de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des tâches de résolution (suite)

État	Description
	Les informations sur la fermeture s'affichent sous l'onglet **Fermer/ Différer** .

- Le propriétaire du rattrapage peut uniquement marquer un élément vulnérable ou une tâche de rattrapage comme étant résolu. En fonction de la confirmation de l'analyseur, cet élément résolu ou cette tâche de rattrapage peut être marqué comme fermé ou rouvert.
- Le bouton **Supprimer** est disponible pour l'administrateur lorsque plusieurs éléments vulnérables ont été créés manuellement et qu'ils doivent être fermés ou supprimés.
- Si vous déterminez que les éléments présentent un risque faible, qu'ils sont en attente d'une fenêtre de changement ou d'un correctif, vous pouvez faire passer leur tâche de rattrapage à l'état Rouge différépour une durée définie. Vous pouvez demander une exception à l'aide de l'option **Demande d'exception** .

  Remarque : Lorsque des tâches de rattrapage sont reportées ou fermées, vous pouvez spécifier des résolutions pour en préciser les motifs.

- Lorsqu'un VIT est rouvert, manuellement ou automatiquement, les événements suivants se produisent :
  - L'état VIT devient Ouvert. L'état de la tâche de rattrapage d'origine n'est pas mis à jour.
  - Le VIT est réévalué et placé dans une tâche de rattrapage nouvelle ou existante basée sur les règles de tâche de rattrapage actives.

  Cela préserve son historique tout en permettant d'autres corrections.

- Lorsqu'une tâche de rattrapage est créée (automatiquement ou manuellement) ou divisée, ses champs **État**, **Motif** et **Jusqu'à ce** sont évalués. Dans le cas de l'action de division, ces champs sont évalués à la fois pour l'ancienne et la nouvelle tâche de rattrapage. Lorsqu'un VIT est mis à jour, les champs **État**, Motif et **Jusqu'à** de toutes ses tâches de rattrapage associées sont évalués.
  - Si tous les VIT d'une tâche de rattrapage sont différés et ont le même motif, l'état de la tâche de rattrapage devient **Différé** et le motif des VIT est affecté à la tâche de rattrapage. Si le motif des VIT diffère, le motif de la tâche de rattrapage prend la valeur **Aucun**.
  - La date de **fin** la plus proche de tous les VIT est mise à jour dans le champ **Jusqu'à** de la tâche de rattrapage.
  - Si vous rouvrez un VIT, l'état de la tâche de rattrapage devient **Ouvert**.

  Cette évaluation est effectuée par la *`Rollup vulnerability item values to vulnerability and group`* tâche planifiée, qui s'exécute toutes les 15 minutes.

États des détections, des tâches de rattrapage et des éléments vulnérables

Les intégrations tierces récupèrent les données de détection des éléments vulnérables. Les détections sont des occurrences distinctes de vulnérabilités telles que signalées par les scanners.

Les données de détection sont couplées à des éléments vulnérables (VI, VIT) et l'état du VI est mis à jour en fonction de l'état des détections. Si aucun VI n'est trouvé, un nouveau VI est

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

créé. Les détections ne sont ouvertes ou fermées que par les données trouvées directement par un scanner.

Si toutes les détections sont fermées pour un élément vulnérable, cet élément vulnérable est fermé. Sur l'enregistrement VI, l'état est Fermé/Fixe. Lorsque tous les VI sont fermés pour une tâche de rattrapage, la tâche de rattrapage est fermée. Pour le reste, le flux d'état reste le même.

Les VI fermés avec un sous-état Fixe ou Périmé sont rouverts si une nouvelle détection est créée et les VI peuvent être mis en correspondance avec la nouvelle vulnérabilité.

À partir de la version 20.0 de Réponse aux vulnérabilités, si une détection est périmée et que le VI associé est à l'état Fermé, l'état du VI ne passe pas à Fermé - Périmé. Cela permet d'éviter que le VI ne se rouvre lorsqu'une nouvelle détection est identifiée, afin d'éviter de passer par l'ensemble du processus de demande et d'approbation de faux positif. Pour inverser ce comportement, décochez la case **Ignorer les détections obsolètes pour les VI fermés** sur le formulaire Configuration de fermeture automatique. Pour plus d'informations, consultez Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités.

Conformément à l'include de script, *`DetectionBase_shouldReOpenVI()`*, si le VI a été précédemment fermé avec un sous-état Fixe, Périmé ou CI désactivé, il est rouvert et la détection est mappée au VIT existant.

Par exemple, supposons que la date de fermeture d'un VI est postérieure à la dernière date trouvée d'une détection. Vous pouvez vous attendre à ce que ces enregistrements de VI restent fermés. Toutefois, si vous voyez qu'un VI précédemment fermé s'est rouvert, cela signifie que le VI a été fermé par une détection antérieure et que la vulnérabilité a été détectée à nouveau lors d'une analyse ultérieure. Lorsqu'une nouvelle détection est trouvée qui correspond au VIT fermé qui présente la même vulnérabilité sur l'élément de configuration du VI, le VI est rouvert.

Tâches de rattrapage et états des éléments vulnérables

Les états des tâches de rattrapage et des éléments vulnérables peuvent s'affecter mutuellement. La plupart du temps, l'état d'une tâche de rattrapage met à jour l'état de l'élément vulnérable, avec l'état de tâche de priorité la plus élevée utilisé pour mettre à jour les éléments vulnérables dans le groupe.

La priorité de l'État est la suivante.

Différé > **Résolu** > **En attente d'implémentation** > **En cours d'examen** > **Ouvert**

- Lorsqu'un groupe d'éléments vulnérables se trouve dans une tâche de rattrapage et n'est pas modifié au niveau individuel, ils ont le même état que leur tâche de rattrapage.
- Lorsque la tâche de rattrapage passe de l'état Ouvert à l'état En attente d'implémentation, tous les éléments vulnérables de la tâche de rattrapage passent à l'état En attente d'implémentation.
- Lorsque la tâche de rattrapage est différée, le VI l'est également. À partir de la version 16.5, vous pouvez suivre le nombre de fois où un élément vulnérable, un élément vulnérable d'application, un élément vulnérable de conteneur ou une tâche de rattrapage est différé. La tâche planifiée s'exécute *`set deferral counts`*quotidiennement pour valider les nombres des enregistrements qui sont différés plus d'une fois dans la colonne Nombre de reports dans les modules Reports multiples pour VR, AVR et CVR. Tous les décomptes des VI associés à une tâche de rattrapage sont collectés et publiés si une tâche de rattrapage est reportée plusieurs fois.

  Éléments vulnérables mis à jour uniquement par les tâches de rattrapage

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les éléments correspondent à l'état de la tâche de rattrapage, s'ils n'ont pas été mis à jour individuellement, à l'exception des éléments suivants :

- Si l'état de la tâche de rattrapage bascule sur Fermé et sa résolution sur Annulé ou Fixe avec exception, l'élément n'est pas affecté et prend l'état de toute autre tâche de rattrapage qui le contient. Si l'élément vulnérable ne se trouve dans aucune autre tâche de rattrapage, il revient à l'état Ouvert.
- Si l'état de l'élément vulnérable est Fermé/Fixe (mis à jour par une analyse ou une importation), lorsque la tâche de rattrapage change d'état, l'élément vulnérable reste à l'état Fermé/Fixe. Cette condition est vraie, quel que soit l'état de la tâche de rattrapage.

Éléments vulnérables dans des états définis individuellement

Les éléments vulnérables, dans un état mis à jour sur l'élément, tels que les éléments fermés ou différés individuellement, ne correspondent pas automatiquement à l'état de la tâche de rattrapage. Au lieu de cela, il compare son état à tous les groupes associés pour trouver l'état ayant la priorité la plus élevée à appliquer.

Remarque : L'état Fermé/Fixe est un cas particulier. Pour les éléments vulnérables définis sur l'état Fermé/Fixe, si tous les éléments vulnérables d'une tâche de rattrapage sont définis sur Fermé/Fixe, par exemple lorsqu'un analyseur détecte que toutes les vulnérabilités ont été corrigées, la tâche de rattrapage est automatiquement marquée comme étant fermée/réparée.

Les tâches de rattrapage contiennent des champs d'affectation vides

Si l'état des VI dans une tâche de rattrapage passe de Résolu à Ouvert, l'état de la tâche de rattrapage est également mis à jour de Résolu à En cours d'examen.

Toutefois, si les champs **Affecté à** et **Groupe d'affectation** de la tâche de rattrapage sont vides, la tâche de rattrapage reste à l'état Résolu et ne passe pas à l'état En cours d'examen.

Le groupe d'affectation des éléments vulnérables n'est pas toujours mis à jour lors de la mise à jour de leur tâche de rattrapage

Si le groupe d'affectation d'un VI à l'état Ouvert est mis à jour manuellement, il n'est pas mis à jour à nouveau lorsque le groupe d'affectation pour sa tâche de rattrapage est mis à jour. Ces informations ne sont pas remplacées, car le groupe d'affectation pour le VI a été mis à jour intentionnellement et peut faire partie d'une autre tâche de rattrapage.

État de la tâche de rattrapage pour les éléments vulnérables (VI) dans plusieurs groupes

Lorsqu'un VI se trouve dans plusieurs tâches de rattrapage (groupe dans les tables suivantes) et que son propre état n'a pas été défini, l'état du groupe de priorité supérieure détermine l'état de ce VI, comme indiqué dans la table suivante.

Exemples d'états d'éléments vulnérables

État de la tâche de résolution	État de l'élément vulnérable
Groupe A : **Ouvrir** > **En cours d'examen** Groupe B : **Ouvert**	**En cours d'examen** Lorsque le groupe A est En cours d'examen et que le groupe B est Ouvert, le VI passe en En

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemples d'états d'éléments vulnérables (suite)

État de la tâche de résolution	État de l'élément vulnérable
	cours d'examen. Après la recherche, entre le groupe A et le groupe B, le groupe A a l'état ayant la priorité la plus élevée.
Groupe A : **En cours d'examen** Groupe B : **Ouvrir** > **En cours d'examen**	**En cours d'examen** Lorsque le groupe B fait l'objet d'une enquête et que le groupe A fait l'objet d'une enquête, le VI reste comme faisant l'objet d'une enquête. Après la recherche, entre le groupe A et le groupe B, ils ont l'état avec la même priorité.
Groupe A : **En cours d'examen** Groupe B : **En cours d'examen** > **En attente d'implémentation**	**En attente d'implémentation** Lorsque le groupe B est en attente d'implémentation et que le groupe A est en cours d'examen, le VI passe en attente d'implémentation. Après la recherche, entre le groupe A et le groupe B, le groupe B a l'état ayant la priorité la plus élevée.
Groupe A : **En cours d'examen** > **Différé** Groupe B : **En attente d'implémentation**	**Différé** Lorsque le groupe A est Différé et que le groupe B est En attente d'implémentation, le VI passe à l'état Différé. Après la recherche, entre le groupe A et le groupe B, le groupe A a l'état ayant la priorité la plus élevée.

Élément vulnérable dans plusieurs groupes, tickets spéciaux

État de la tâche de rattrapage	État de l'élément vulnérable
Groupe A : **En cours d'examen** Groupe B : **En attente d'implémentation** > **Fermé (Fixe ou Annulé)**	**En cours d'examen** Lorsque le groupe B est Fermé/Fixe ou Fermé/Annulé et que le groupe A est En cours d'examen, le VI passe de En attente d'implémentation (auparavant la priorité la plus élevée) à En cours d'examen (actuellement la priorité la plus élevée).
Groupe A : tout état Groupe B : n'importe quel état	Si l'état de la source de l'élément vulnérable est Fixe (mis à jour par une analyse ou une importation), lorsque le groupe change d'état, l'élément vulnérable passe son état à Fermé/Fixe. Cette condition est vraie, quels que soient les états dans lesquels se trouvent les autres groupes associés. La recherche d'éléments vulnérables pour l'état du groupe n'a pas lieu.

Lorsqu'un état de VI est défini individuellement, son état est pris en compte lors de l'évaluation de la priorité, comme pour toute autre tâche de rattrapage. Lorsqu'un VI

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

appartient à plusieurs tâches de rattrapage, le tableau suivant répertorie les mises à jour effectuées.

État de l'élément vulnérable défini individuellement : cas spéciaux

État de l'élément de vulnérabilité au sein d'un groupe	État final de l'élément vulnérable
État du groupe A : **En cours d'examen** État du groupe B : **En cours d'examen** > **En attente d'implémentation** État du VI d'origine : **En cours d'examen** > **(réglé sur le VI)**	**En attente d'implémentation** Lorsque le groupe B est passé à l'état En attente d'implémentation et que le groupe A est resté en cours d'examen, le VI passe à l'état En attente d'implémentation (la priorité la plus élevée).
Groupe A : **En cours d'examen** Groupe B : **En cours d'examen** > **En attente d'implémentation** État du VI d'origine : **Différé** > **(réglé sur le VI)**	**Différé** Lorsque le groupe B est passé à l'état En attente d'implémentation et que le groupe A est resté en cours d'examen, le VI reste à l'état Différé (la priorité la plus élevée).

La table suivante montre que lorsque deux tâches de rattrapage comportant des éléments vulnérables communs sont reportées, l'état est différé jusqu'à la date la plus récente.

Cas spéciaux de l'état différé de l'élément vulnérable

État de l'élément de vulnérabilité au sein d'un groupe	État final de l'élément vulnérable
État du groupe A : **En cours d'examen (jusqu'au 10 avril)** État du groupe B : **En cours d'examen** > **En cours d'examen (jusqu'au 30 avril)** État du VI d'origine : **En cours d'examen (jusqu'au 10 avril)** > **(réglé sur le VI)**	**Reporté (jusqu'au 30 avril)** Lorsque le groupe B passe à l'état Différé (jusqu'au 30 avril) et que le groupe A reste Différé (jusqu'au 10 avril), le VI passe de l'état Différé (jusqu'au 5 avril) à l'état Différé (jusqu'au 30 avril).
Groupe A : **En cours de révision (jusqu'au 15 juillet)** Groupe B : **En cours d'examen** > **En cours d'examen (jusqu'au 10 juillet)** État du VI d'origine : **Différé** > **(jusqu'au 15 juillet)**	**Reporté (jusqu'au 15 juillet)** Lorsque le groupe B est passé en Différé (jusqu'au 10 juillet) et que le groupe A reste en Différé (jusqu'au 15 juillet), le VI reste en Différé (jusqu'au 15 juillet).

Paramètres supplémentaires pour Séparation de domaine

Pour une exécution et des résultats précis, les précautions et paramètres suivants sont requis pour la séparation de domaine dans Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration.

Pour éviter tout problème, ne modifiez pas les logiques métier et les processus dans le domaine global, de sorte que tous les derniers changements soient mis à jour à chaque mise à niveau. Dupliquez séparément l'ensemble des logiques et processus métier de chaque domaine et assurez-vous qu'ils sont inactifs dans le domaine global. Dans le cas contraire, les logiques et processus métier du domaine global prévalent sur le domaine enfant. Supposons

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que vous créiez une règle de risque dans un domaine enfant et que le domaine global dispose également d'une règle de risque similaire, alors la règle du domaine global prévaut sur la règle du domaine enfant.

Réévaluation des calculateurs et des règles

Avant la version 20.0, lorsque vous réappliquiez des calculateurs ou des règles, le marqueur de `réexécution` était défini sur vrai et une règle métier était déclenchée pour exécuter une tâche de calendrier qui réappliquait les calculateurs et les règles. À partir de la version 20.0, vous n'avez plus besoin de dépendre de l'indicateur `de réexécution` . Lorsque vous cliquez sur le bouton **Réappliquer le calculateur** , un travail en arrière-plan est déclenché qui réapplique les calculateurs et les règles. Cela vous permet de créer des calculateurs et des règles pour tous les domaines.

Paramètres pour les calculateurs de cumul

Dans un domaine, un seul calculateur de cumul doit être actif pour une table. Par exemple, considérez la table Tâche de remédiation, *sn_vul_vulnerability* avec le calculateur de déploiement, **Déploiement de la tâche de remédiation** dans le domaine global. Si vous dupliquez ce calculateur de cumul en modifiant les pondérations pour la même table dans le même domaine, il y aura des écarts dans les calculs de cumul. Par conséquent, assurez-vous d'activer un seul calculateur de déploiement s'il y a deux calculateurs de déploiement ou plus pour une table dans le même domaine.

Champs du formulaire Éléments détectés

Les actifs sont automatiquement mis en correspondance avec des éléments de configuration (CI) dans lorsqu'ils Base de données de gestion des configurations (CMDB) sont importés à l'aide des règles de recherche de CI. Les enregistrements des CI sans correspondance sont automatiquement créés lors des importations d'intégration de vulnérabilité tierce et inclus dans les éléments détectés. Toutefois, pour les actifs cloud qui ne sont pas présents dans CMDB CI, l'enregistrement est créé dans la classe de ressources cloud.

Champs des éléments détectés

Les informations contenues dans ces enregistrements sont ingérées à partir des enregistrements tiers et classées lors de l'importation.

Champ	Description
Numéro	Identificateur affecté à l'enregistrement.
ID d'élément de configuration	Élément de configuration importé à partir de l'intégration source tierce. À partir de la version 12.0, l'élément de configuration est le dernier CI de la liste des CI après filtrage des éléments désactivés.
Classe	Classe affectée au CI pendant l'importation par Réponse aux vulnérabilités.
Source	Source importée de l'intégration de la source tierce.
Règle de correspondance CI	Règle de correspondance CI utilisée pour créer l'élément.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
V18.0 : Type de correspondance pour le DI	Type de correspondance utilisé pour créer l'élément détecté. Les options sont les suivantes : • Créé par VR • Créé par IRE • Correspondant à la recherche de CI • Correspond à l'IRE Ces informations ne sont disponibles que pour les données renseignées pour Réponse aux vulnérabilités la version 18.0 et les versions ultérieures. Sur les données existantes, cette colonne ne contient aucune valeur. **Remarque :** Si vous réappliquez les règles de recherche de CI, certains CI sur les DI peuvent être mis à jour, ce qui entraîne le remplissage de cette colonne.
Autres CI appariés	Liste des autres éléments de configuration correspondant à la règle de recherche de CI.
État	État du CI déterminé lors de l'importation. Les choix possibles sont les suivants : • **En correspondance** : un élément de configuration correspondant a été trouvé dans la CMDB. • **Sans correspondance** : aucune correspondance n'a été trouvée dans la CMDB. Un enregistrement d'espace réservé est créé.
Créé	Date de création de l'enregistrement de l'élément détecté.
Mis à jour	Date à laquelle l'enregistrement de l'élément détecté a été mis à jour.
Mis à jour par	Utilisateur qui a mis à jour les données.
Balise d'hôte	Balises d'hôte affectées à cet élément détecté pendant l'importation. Vous pouvez avoir jusqu'à 31 balises d'hôte par élément détecté.
Nom de domaine complet	Données associées à ce CI trouvées dans la CMDB.
Adresse MAC	Données associées à ce CI trouvées dans la CMDB.
Système d'exploitation	Système d'exploitation associé à ce CI.
NetBIOS	NetBIOS importé à partir de l'intégration source tierce.
Adresse IP	Données associées à ce CI trouvées dans la CMDB.
Données sources	Dernières données associées à ce CI à partir de la source.
V16 : données sources initiales	Données initiales associées à ce CI à partir de la source.
V16 : réévaluer le CI	Reçoit les données du scanner. S'il y a des données mises à jour, la valeur est définie sur vrai.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Les valeurs des données sources sont recalculées en fonction des données sources les plus récentes. Lorsque des données mises à jour sont extraites du scanner, les données sources sont mises à jour. La valeur de données sources existante est déplacée vers le champ de données sources initial. Pour réévaluer les éléments détectés, activez l'option `Réappliquer les règles de recherche de CI sur la tâche planifiée Éléments détectés modifiés` .
L'agent existe	Indique `Vrai`si l'agent est installé sur l'actif. Si les valeurs `hostUID` et `UUID` de la colonne Données sources sont vides, cette valeur est renseignée comme `vrai`. **Remarque :** Ce champ apparaît à partir de la version 19.0 de Réponse aux vulnérabilités.

À partir de la version 23.0 de , la colonne % de conformité des résultats des Réponse aux vulnérabilités**tests (CI)** affiche le pourcentage de résultats des tests conformes pour le CI correspondant. Pour obtenir cette valeur, vous devez définir `calcTRComplianceForCI` sur `vrai` dans la tâche planifiée **Mettre à jour les mesures de rattrapage** .

Remarque : La valeur **% de conformité (CI) du résultat des tests** est renseignée uniquement pour les éléments détectés dont la valeur n'est pas vide dans les colonnes **Date de la dernière analyse de conformité** de la configuration ou **Date de la dernière analyse de conformité hors infrastructure** .

À partir de la version 18.0 de Réponse aux vulnérabilités, QualysTenable pour Réponse aux vulnérabilités et Rapid7 les analyseurs peuvent recevoir les métadonnées supplémentaires suivantes pour les actifs dans le cloud.

Champ	Description
Fournisseur de services dans le cloud	Nom du fournisseur de services dans le cloud qui propose des services de cloud computing. Par exemple, Amazon Web Services () Microsoft Azure et Google Cloud Platform (GCP).AWS
Région du cloud	Emplacement où la ressource a été hébergée.
Compte dans le cloud	Compte fourni par des fournisseurs de services dans le cloud tels que AWS, GCP, et ainsi de suite pour accéder aux services de cloud computing.
Type de ressource dans le cloud	Types d'actifs présents dans le cloud, tels qu'Amazon Elastic Compute Cloud (EC2), les compartiments S3, AWS etc.
ID de ressource	Identificateur unique affecté à une ressource dans un environnement de cloud computing. Cet ID est utilisé pour identifier et gérer la ressource.
Nom de la ressource	Nom défini par l'utilisateur utilisé pour identifier et gérer une ressource dans un environnement de cloud computing.
Image	Une image d'ordinateur virtuel ou image de serveur est un ordinateur virtuel préconfiguré qui contient un système d'exploitation, des

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	applications et d'autres logiciels. Par exemple, Amazon Machine Image.

Une nouvelle règle de recherche de CI, « ID de ressource dans le cloud », a été introduite pour faire correspondre les CI dans le cloud en fonction des métadonnées dans le cloud.

Réponse aux vulnérabilités Champs du formulaire de vulnérabilité

Les vulnérabilités sont créées automatiquement lorsque les enregistrements sont téléchargés à partir de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou d'intégrations tierces et stockés sous **Bibliothèques** dans Réponse aux vulnérabilités.

Champs d'entrée NVD

Les champs importés dans cette table sont en lecture seule. Les éléments vulnérables (VI), les logiciels vulnérables et les références de vulnérabilité sont automatiquement associés et des entrées peuvent être ajoutées manuellement.

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Cote de risque	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) **Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour en savoir plus sur les évaluations des risques, reportez-vous à Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité. **Remarque :** Cette **cote de risque** de base n'est pas la même que la **cote de risque** de l'enregistrement de solution.
Score du risque	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) Quantité calculée de risque que l'élément vulnérable pose à votre environnement. **Remarque :** Ce **score de risque** de base n'est pas le même que le score de risque de l'enregistrement de **solution.** Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.
Sévérité	Degré normalisé de gravité de cette vulnérabilité. Des cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations tierces. Pour plus d'informations sur la création ou l'ajustement de cartes de gravité, reportez-vous à la section Créer une carte de Réponse aux vulnérabilités gravité.
Existence de l'exploit	Oui, si au moins un exploit est associé à cette vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Niveau de compétence de l'exploit	Niveau de compétence le plus bas requis pour exploiter cette vulnérabilité.
Vecteur d'attaque de l'exploit	Vecteur d'attaque le plus vulnérable des exploits pour cette vulnérabilité. Disponible lorsque NVD SAM est activé.
VI actifs	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) Nombre d'éléments vulnérables associés à cette vulnérabilité, dont l'état n'est pas Fermé. Si aucun élément vulnérable n'est actif pour cette vulnérabilité, **la cote de risque** et le **score de risque** ne sont pas affichés.
Entrée CWE	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux.
Date de publication	Date de publication de la vulnérabilité.
Dernière modification	Date de la dernière modification de la vulnérabilité.
Résumé	Description de la vulnérabilité.
Threat Intelligence (à partir de la Réponse aux vulnérabilités version 20.0)	Renseignements sur les menaces fournis par Qualys. Grâce à ces données, vous pouvez comprendre les motivations, les cibles et les comportements d'attaque d'un acteur malveillant.
Détails des vulnérabilités	
CVSS v2	Données CVSS v2 importées
CVSS v3	Données CVSS v3 importées, non disponibles avant 2015.
Solution privilégiée	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) Solution de remplacement la plus élevée de la chaîne, dérivée des solutions référencées dans la vulnérabilité. S'il existe plus d'un remplacement le plus élevé dans la chaîne, aucune valeur n'est fixée. Toute valeur définie manuellement peut être écrasée lors des importations suivantes. La définition manuelle de cette valeur doit être effectuée sur l'élément vulnérable.
Exploitation CISA (Cet onglet n'est disponible que lorsque l'application CISA est installée.)	
Date d'échéance de CISA	Délai de résolution de la vulnérabilité.
Date d'ajout	Date à laquelle la vulnérabilité a été ajoutée au catalogue CISA.
Produit	Produit sur lequel la vulnérabilité a été identifiée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Fournisseur/Projet	Fournisseur associé à la vulnérabilité identifiée.
Rançongiciel connu À partir de la v21.0 de Réponse aux vulnérabilités.	Sélectionné lorsque le champ **Known To Be Be Used in Ransomware Campaigns (Connu pour être utilisé dans les campagnes de rançongiciels**) est ingéré à partir du catalogue des vulnérabilités exploitées connues (KEV) de CISA. Le marqueur est défini au niveau des vulnérabilités et expositions communes (CVE) et déployé jusqu'à l'entrée tierce (TPE).
État du rattrapage (Masqué lorsqu'aucun VI n'est associé à la vulnérabilité)	
Exclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
Inclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité.
Liens connexes	
Avant la version 13.0 : forcer l'importation de vulnérabilité logicielle **Remarque :** Supprimé dans la version 13.0	(Déconseillé) Recalcule le mappage des produits en Gestion des actifs logiciels pour ITSM fonction des informations provenant de NVD. Met à jour la bibliothèque de logiciels vulnérables.
Mettre à jour le statut	Affiche la date et l'heure de la dernière mise à jour. Met à jour les éléments suivants : • État de la tâche de résolution • Score et évaluation du risque • Mesures telles que VI actifs, VI totaux de la section État de rattrapage
Listes connexes	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Éléments vulnérables	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) Éléments vulnérables associés à cette vulnérabilité.
Références de vulnérabilité	Informations sur la vulnérabilité provenant de sources externes, citées par NVD.
Exploite	Exploits associés à cette vulnérabilité.
Solutions	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) Toutes les Gestion des solutions pour vulnérabilités solutions d'intégration associées à cette vulnérabilité.
Faiblesses	Données de **faiblesse** importées associées à des vulnérabilités et expositions communes (CVE).
Logiciel vulnérable	(Masqué lorsque le logiciel est associé au CVE) Données CPE (Common Platform Enumeration) importées associées à la vulnérabilité.
Kits de logiciel malveillants de vulnérabilité	Programme malveillant importé de diverses sources de scanner, pour une vulnérabilité.

Champs d'entrée de vulnérabilité CWE

Les champs importés dans cette table sont en lecture seule.

Champ	Description
ID CWE	Identificateur de cette entrée de vulnérabilité. Cet identificateur est utilisé à la fois pour les catégories et les faiblesses, et est unique entre les deux jeux de données.
Nom	Nom descriptif affecté à cet ID CWE.
Probabilité d'exploitation	Probabilité que la faiblesse soit exploitée, sur une échelle qualitative. L'un des suivants : • Faible • Moyen • Élevé
Position dans le top 10 OWASP	Position numérique de cette vulnérabilité dans la liste des 10 premiers OWASP.
SANS vers 25 positions	Position numérique de cette vulnérabilité dans la liste des 25 premiers SAN.
Classe	Type de faiblesse
Statut	L'un des suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	• Incomplet • Brouillon • Stable • Déconseillé • Obsolète • Instable
Abstraction	L'un des suivants : • Variante • Classe • Base • Composé
Mis à jour	Dernière mise à jour de l'enregistrement dans l'instance.
Domaines fonctionnels	Liste des domaines fonctionnels concernés. Par exemple, **Traitement des fichiers**. Seulement renseigné pour 24/862 faiblesses.
Ressources affectées	Liste des ressources affectées. Par exemple, **Fichier** ou **Répertoire**. Seulement renseigné pour 51/863 faiblesses.
URL	Article de la base de connaissances associé à cette vulnérabilité.
Description	Description de la vulnérabilité.
Exécution de l'intégration	L'exécution d'intégration dans laquelle cette CWE a été importée.
Sections	
Informations supplémentaires	Descriptions des concepts logiciels qui expliquent plus en détail la faiblesse. Comprend: • Description étendue • Détails en arrière-plan • Notes
Méthodes de détection	Détails sur la façon dont vous pouvez détecter cette faiblesse dans une application.
Modes d'introduction	Phases au cours desquelles la faiblesse est introduite, par exemple, **implémentation**, **architecture et conception**, etc.
Exemples démonstratifs	Codez des exemples de la faiblesse avec les descriptions qui les accompagnent.
Atténuations potentielles	Détails sur la façon d'empêcher la faiblesse, y compris la phase du cycle de vie de l'application dans laquelle elle se produit et l'efficacité de l'atténuation.
Listes connexes	
Relations	CWE associés à cette vulnérabilité. Répertorie les relations entre cette CWE et d'autres. Peut inclure parent/enfant, suit/précède,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	requiredby/requires (pour les faiblesses composites), CanAlsoBe, PeerOf, MemberOf.
Exemples observés	Quelques CVE représentatives de cette faiblesse.
Conséquences courantes	Conséquences d'un exploit réussi, en termes de portée et d'impact. Par exemple : Champ d'application : Confidentialité Impact : lire les données de l'application
Adhésions	Adhésions CWE avec cette vulnérabilité.
Plateformes applicables	Plateformes associées à cette vulnérabilité.
Entrées de vulnérabilité de l'application	Autres entrées de vulnérabilité d'application associées à une.
Références externes	Informations sur la vulnérabilité provenant de sources externes.

Champs d'entrée de vulnérabilité tierce

Les champs importés dans cette table sont en lecture seule.

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Version 16.0 : CVE	Plusieurs vulnérabilités et expositions courantes (CVE) associées à cette vulnérabilité tierce.
Source	Origine de la vulnérabilité : qu'il s'agisse d'un scanner ou d'un test physique.
Cote de risque	**Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour plus d'informations sur les cotes de risque, Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilitéreportez-vous à . **Remarque :** Cette **cote de risque** de base n'est pas la même que l'enregistrement de la solution **Cote de risque**
Score du risque	Montant de risque calculé que l'élément vulnérable pose à votre environnement, en fonction du score de risque. **Remarque :** Ce **score de risque** de base n'est pas le même que le score de risque de l'enregistrement de **solution.** Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.
Sévérité	Degré normalisé de gravité de cette vulnérabilité. Des cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	tierces. Pour plus d'informations sur la création ou l'ajustement de cartes de gravité, reportez-vous à la section Créer une carte de Réponse aux vulnérabilités gravité.
Existence de l'exploit	Oui, si au moins un exploit est associé à cette vulnérabilité.
Niveau de compétence de l'exploit	Niveau de compétence le plus bas requis pour exploiter cette vulnérabilité.
Vecteur d'attaque de l'exploit	Vecteur d'attaque le plus vulnérable des exploits pour cette vulnérabilité.
VI actifs	Nombre d'éléments vulnérables associés à cette vulnérabilité, dont l'état n'est pas Fermé.
Catégorie	Classification fournie par l'intégration tierce. Aide à l'affectation.
Type de rattrapage	Types d'actions de rattrapage. • Correctif • Changement de configuration • Correctif et changement de configuration • Contre-mesure
Entrée CWE	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux.
PCI	Lorsque la case est cochée, la vulnérabilité est marquée comme présentant un risque important d'exposition des informations de paiement.
Gravité PCI	Niveau de risque d'exposition des informations de paiement. [Qualys uniquement.]
Date de publication	Date de publication de la vulnérabilité.
Dernière modification	Date de la dernière modification de la vulnérabilité.
Résumé	Description de la vulnérabilité.
Détails des vulnérabilités	
CVSS v2	Données CVSS v2 importées
CVSS v3	Données CVSS v3 importées, non disponibles avant 2015.
Menace	Description de la menace provenant de cette vulnérabilité.
Solution privilégiée	Solution de remplacement la plus élevée de la chaîne, dérivée des solutions référencées dans la vulnérabilité. S'il existe plus d'un remplacement le plus élevé dans la chaîne, aucune valeur n'est fixée. Toute valeur définie manuellement peut être écrasée lors des importations suivantes. La définition manuelle de cette valeur doit être effectuée sur l'élément vulnérable.
Notes de rattrapage	Description de la solution de rattrapage extraite du fournisseur.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
État du rattrapage	
Exclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
Inclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité.
Liens connexes	
Mettre à jour le statut	Affiche la date et l'heure de la dernière mise à jour. Met à jour les éléments suivants : • État de la tâche de résolution • Score et évaluation du risque • Mesures telles que VI actifs, VI totaux de la section État de rattrapage
Listes connexes	
Éléments vulnérables	Éléments vulnérables associés à cette vulnérabilité.
Références de vulnérabilité	Informations sur la vulnérabilité provenant de sources externes, citées par NVD.
CVE	Enregistrement CVE (Common Vulnerability Enumeration) associé à cette vulnérabilité.
Catégories	Catégories associées à cette vulnérabilité.
Exploite	Exploits associés à cette vulnérabilité.
Kits de logiciel malveillants de vulnérabilité	Kits de programmes malveillants associés à cette vulnérabilité.
Solutions (Rapid7)	Informations sur la solution issues des intégrations de solutions Rapid7. Affiché lorsqu'il est disponible.
Cadres de travail de l'exploit	Cadres de travail d'exploitation associés à cette vulnérabilité.
Solutions	Gestion des solutions pour vulnérabilités Solutions associées à cette vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Exploitation CISA	
CISA existe	Un exploit CISA existe pour la table d'entrée des vulnérabilités tierces.
Date d'échéance de CISA	Délai de résolution de la vulnérabilité.

Champs du formulaire de tâche de rattrapage

À l'aide des tâches de rattrapage, l'analyste peut surveiller les progrès et piloter le processus de médiation plus efficacement.

Les champs importés dans cette table sont en lecture seule.

Champs de tâche de rattrapage

Champ	Description
Numéro	Numéro d'élément vulnérable (VI) généré automatiquement pour cet enregistrement.
Cote de risque	Déploiement des scores de risque des éléments vulnérables séparés en plages : Critique, Élevé, Moyen, Faible et Aucun. Pour plus d'informations sur les cotes de risque, Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilitéreportez-vous à . **Remarque :** Cette **cote de risque** de base n'est pas la même que la **cote de risque** de l'enregistrement de solution.
Score du risque	Déploiement des scores de risque de tous les éléments vulnérables associés à cette tâche de rattrapage. Quantité de risque que les éléments vulnérables, collectivement, posent à votre environnement. **Remarque :** Ce **score de risque** de base n'est pas le même que le score de risque de l'enregistrement de **solution.**
Cible de rattrapage	Date à laquelle les éléments vulnérables doivent être corrigés, dès lors qu'ils ont été identifiés pour la première fois. Pour en savoir plus sur les cibles de rattrapage, reportez-vous Réponse aux vulnérabilités Règles de cibles de rattrapageà .
État du rattrapage	État du rattrapage pour la tâche. Elle est déterminée par l'élément vulnérable dont la date d'échéance est la plus proche. Pour les groupes ouverts, les états incluent : • En cours • Cible presque atteinte • Cible manquée Pour les groupes fermés, les états incluent :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

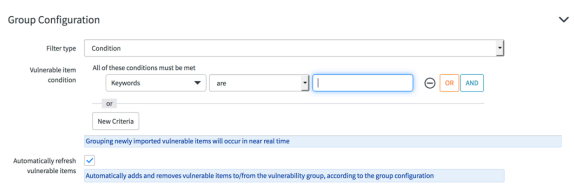
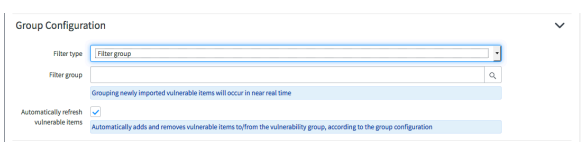
Champs de tâche de rattrapage (suite)

Champ	Description
	• Pas de cible • Cible atteinte • Cible manquée Pour les dates cibles de rattrapage calculées, si la tâche est fermée, l'état de rattrapage global de tous les éléments vulnérables fermés est affiché dans la tâche. Ceux-ci déterminent si la tâche a atteint sa date ou non. L'état de rattrapage d'une tâche fermée est **Aucun** objectif si aucun de ses éléments fermés n'a de date cible de rattrapage. Il s'agit **d'une cible manquée** si l'un de ses éléments fermés a manqué sa date cible. La **cible est atteinte** si au moins un VI fermé a atteint sa cible et qu'aucun des autres ne l'a manquée.
État	État d'avancement de la tâche. Les États sont les suivants : • Ouvrir • En cours d'examen • En attente d'implémentation • Différé • En cours de révision • Résolu • Fermé Pour en savoir plus sur les états, consultez Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables.
Date de fin pour la réduction du risque	Date d'expiration des contrôles compensatoires appliqués à la tâche de rattrapage. **Remarque :** Ce champ n'apparaît que lorsque la valeur est disponible.
Groupe d'affectation	Groupe sélectionné pour travailler sur cette tâche de rattrapage.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cette vulnérabilité.
Créé	Date de création de cette tâche de rattrapage.
Mis à jour	Date de la dernière mise à jour de cette tâche de rattrapage.
Vulnérabilité	Vulnérabilité applicable à la tâche. (Visible lorsque le groupe est formé sur la base d'une vulnérabilité unique.)
Description brève	Brève description de cette tâche de rattrapage.
En cours de révision (visible lorsque le RT est dans l'état En cours de révision)	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

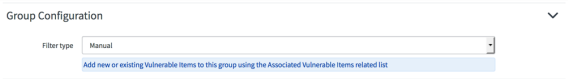
Champs de tâche de rattrapage (suite)

Champ	Description
Demandés par	Personne ayant demandé le report.
Raison souhaitée	Motif du report.
État souhaité	État demandé à l'approbateur.
Sous-état souhaité	Le motif demandé à l'approbateur.
Report (visible lorsque la tâche est dans l'état Différé)	
Différé par	Personne ayant reporté la tâche.
Différer l'expiration	Date d'expiration du report.
Raison de reporter	Motif du report.
Résolution (visible lorsque le RT est à l'état Résolu)	
Résolu par	Personne ayant résolu la tâche de rattrapage.
Date de résolution	Date à laquelle la tâche de rattrapage a été résolue.
Notes de résolution	Informations complémentaires.
Fermé (visible lorsque le RT est à l'état Fermé)	
Fermé par	Personne ayant résolu la tâche de rattrapage.
Fermé	Date à laquelle la tâche de rattrapage a été fermée.
Fermer les notes	Informations complémentaires.
Configuration du groupe (visible dans tous les états)	
Filtrer le type	Type de filtrage utilisé pour sélectionner des vulnérabilités pour le groupe : Condition  **Remarque :** Actualise une fois par heure. Groupe de filtres  **Remarque :** Actualise une fois par heure. Manuel

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de tâche de rattrapage (suite)

Champ	Description
	
État du rattrapage	
Exclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs dans cette tâche. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre total d'éléments vulnérables dans cette tâche. Ce nombre exclut les éléments vulnérables différés.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables dans cette tâche. Ce nombre exclut les éléments vulnérables différés.
Inclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs dans cette tâche.
VI totaux	Nombre total d'éléments vulnérables dans cette tâche.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables dans cette tâche.
Notes (visibles dans tous les états)	
Description	Description du groupe ou des actions de rattrapage.
Commentaires supplémentaires	Informations complémentaires.
Activités	Notes du système.
Liens connexes	
Analyser à nouveau des éléments vulnérables	Déclenche une nouvelle analyse des éléments vulnérables pour déterminer s'ils sont corrigés.
Mettre à jour l'état	Affiche la date et l'heure de la dernière mise à jour. Répète les éléments suivants à partir des VI dans la tâche : • État de la tâche de résolution • Scores des risques et évaluations des risques • Date cible et état du rattrapage (le cas échéant) • Mesures telles que VI actifs, VI totaux de la section État de rattrapage
Listes connexes	
Éléments vulnérables	Éléments vulnérables dans cette tâche.
SLA de tâche	SLA de la plateforme associés à cette tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de tâche de rattrapage (suite)

Champ	Description
Solutions privilégiées	Solutions privilégiées des éléments vulnérables dans cette tâche.
Demandes de changement	Demandes de changement associées à cette tâche.
Approbations demandées	(Visible lorsque la tâche est dans l'état En cours de révision.) Liste d'approbateurs. Une fois le report approuvé, la tâche de rattrapage passe à l'état Différé.

Champs de formulaire de configuration du questionnaire

Vous pouvez définir un questionnaire distinct pour une collection distincte de vulnérabilités ou de tâches de rattrapage en filtrant respectivement les vulnérabilités ou les tâches de rattrapage dans la section Configuration du questionnaire VR du formulaire Paramètres pour la gestion des exceptions VR.

Le formulaire Configuration du questionnaire s'affiche lorsque vous sélectionnez le bouton **Nouveau** dans la section Configuration du questionnaire VR du formulaire Paramètres pour la gestion des exceptions VR.

Champs de formulaire de configuration du questionnaire

Champ	Description
Nom	Nom du questionnaire.
Règle d'approbation	Règle d'approbation pour laquelle le questionnaire est applicable. • **Demande d'exception pour les groupes de vulnérabilités** • **Demande d'exception pour les éléments vulnérables** • **Faux positif pour les groupes de vulnérabilité** • **Faux positif pour les éléments vulnérables** • **Questionnaire pour compenser les contrôles des groupes vulnérables** pour les demandes de réduction des risques de la tâche de rattrapage. • **Questionnaire pour les contrôles de compensation des éléments vulnérables** pour les demandes de réduction des risques des éléments vulnérables.
Description	Brève description de la configuration du questionnaire.
Ordre	Le questionnaire avec l'ordre le plus bas s'affiche pendant les demandes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire de configuration du questionnaire (suite)

Champ	Description
Actif	Activé par défaut, ce qui signifie que le questionnaire est en cours d'utilisation.
Table	Table à laquelle la règle d'approbation s'applique. • Élément vulnérable [sn_vul_vulnerable_item pour les règles d'approbation relatives aux éléments vulnérables. • Tâche de rattrapage [sn_vul_vulnerability] pour les règles d'approbation liées aux tâches de rattrapage.
Condition	Condition pour les enregistrements pour lesquels le questionnaire doit apparaître. Vous pouvez appliquer une condition à tous les champs d'un élément vulnérable et d'une tâche de rattrapage, à l'exception du **motif**.
Questionnaire	Questionnaire qui s'affiche lorsqu'un propriétaire du rattrapage demande une exception, un faux positif ou une réduction du risque.

Information associée

Configurer la gestion des exceptions pour Réponse aux vulnérabilités

Configurer le questionnaire pour la réduction du risque

Réponse aux vulnérabilités Champs du formulaire d'élément vulnérable

Les éléments vulnérables sont automatiquement créés lors des importations d'intégration de vulnérabilité tierce.

Champs d'éléments vulnérables

Si vous avez activé l'analyse de vulnérabilité NVD SAM, les enregistrements sont comparés au logiciel dans le vôtre Base de données de gestion des configurations (CMDB) et des correspondances sont trouvées avec des logiciels ou des éléments de configuration (CI) vulnérables.

Champ	Description
Sélectionner une balise de sécurité	Balise de sécurité permettant d'ajouter des métadonnées à l'enregistrement ou d'identifier qui doit avoir accès à cet enregistrement d'incident de sécurité. Ce champ s'affiche uniquement une fois que l'élément vulnérable a été enregistré.
Numéro	Numéro d'élément vulnérable généré automatiquement pour cet enregistrement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Scanner qui a trouvé cet élément vulnérable.
Cote de risque	**Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour en savoir plus sur les évaluations des risques, reportez-vous à Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité. **Remarque :** Cette **cote de risque** de base n'est pas la même que la **cote de risque** de l'enregistrement de la solution.
Score du risque	Quantité calculée de risque que l'élément vulnérable pose à votre environnement. **Remarque :** Ce **score de risque** de base n'est pas le même que le score de risque de l'enregistrement de **la solution.** Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.
Vulnérabilité	ID de la vulnérabilité associée à cet élément vulnérable.
Élément de configuration	Actif affecté.
État	Ce champ est défini par défaut sur **Ouvert**, mais vous pouvez le remplacer par **En cours d'examen** si la vulnérabilité est prête pour une correction immédiate.
Date de fin pour la réduction du risque	Date d'expiration des contrôles compensatoires appliqués à l'élément vulnérable. **Remarque :** Ce champ s'affiche uniquement lorsque la valeur du score de risque d'origine est disponible.
Groupe d'affectation	Groupe sélectionné pour travailler sur cette tâche de rattrapage.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cette vulnérabilité.
Créé	Date à laquelle cet élément vulnérable a été créé dans votre instance.
Dernières ouvertures	Date à laquelle l'élément vulnérable a été ouvert pour la dernière fois dans votre instance. Initialement, il s'agit de la date de création de l'élément vulnérable. Cependant, s'il a été fermé, puis rouvert, la date Dernière ouverture contient la date et l'heure de réouverture.
Mis à jour	Date de la dernière analyse.
Vulnérabilité	
Résumé	Description de la vulnérabilité.
Sévérité	Degré normalisé de gravité de cette vulnérabilité. Des cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations tierces. Pour plus d'informations sur la création ou l'ajustement de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	cartes de gravité, reportez-vous à la section Créer une carte de Réponse aux vulnérabilités gravité.
Score de vulnérabilité (v3)	Score CVSS v3.
Score de vulnérabilité (v2)	Score CVSS v2.
Existence de l'exploit	Oui, si au moins un exploit est associé aux vulnérabilités associées à cet élément vulnérable.
Vecteur d'attaque de l'exploit	Vecteur d'attaque le plus vulnérable des exploits pour les vulnérabilités associées à cet élément vulnérable.
Niveau de compétence de l'exploit	Niveau de compétence le plus bas requis pour exploiter les vulnérabilités associées à cet élément vulnérable.
Date de publication	Date de publication de la vulnérabilité.
Dernière modification	Date de la dernière modification de la vulnérabilité.
Menace	Informations pertinentes sur la menace. Extrait de l'enregistrement d'entrée vulnérable. **Remarque :** Tous les changements apportés ici mettent à jour l'enregistrement d'entrée vulnérable.
Notes de rattrapage	Solution pertinente à la menace, extraite de l'enregistrement d'entrée vulnérable.
Étapes de rattrapage Disponible uniquement avec Gestion des solutions pour vulnérabilités.	
Solution privilégiée	Solution privilégiée importée à partir de l'enregistrement de vulnérabilité. **Remarque :** Les changements manuels effectués ici ne modifient pas l'enregistrement de vulnérabilité et restent inchangés sur le VI lors des importations suivantes.
Résumé	Résumé importé à partir de l'enregistrement de solution.
Détection initiale	
Nom DNS	Nom du nom de domaine Nom de service. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il en existe un.
Nom NetBIOS	Nom du NetBIOS. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il en existe un.
Adresse IP	Adresse IPv4 ou IPv6. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il en existe un.
Port	Adresse du port
Protocole	Nom du protocole.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
SSL	Indique si le cryptage SSL est utilisé ou non.
Détections	
Statut	État de la détection.
Première occurrence trouvée	Date à laquelle la source tierce a trouvé la détection sur cet actif pour la première fois.
Dernier trouvé	Date à laquelle la source tierce a trouvé la détection pour la dernière fois sur cet actif.
Nom DNS	Nom du nom de domaine Nom de service. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il en existe un.
Nom NetBIOS	Nom du NetBIOS. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il en existe un.
Adresse IP	Adresse IPv4 ou IPv6. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il en existe un.
Port	Adresse du port
Protocole	Nom du protocole.
SSL	Indique si le cryptage SSL est utilisé ou non.
Durées trouvées	Nombre de fois où cette vulnérabilité a été détectée sur cet actif par la source tierce.
Exécution de l'intégration	Exécution de l'intégration qui a importé la détection.
Fermer Disponible une fois que l'élément vulnérable a été corrigé et fermé. Les éléments de cette section sont en lecture seule.	
Fermé par	Qui a fermé l'élément vulnérable.
Fermé	Date à laquelle l'élément vulnérable a été fermé.
Fermer les notes	Informations incluses dans la fermeture.
Âges à la fermeture	Période après laquelle le VI a été fermé. Si le VI est rouvert, la valeur du champ Âge fermé est définie sur zéro.
Notes	
Commentaires/ notes de travail supplémentaires	Toute information pertinente. Cochez la case pour ajouter des commentaires supplémentaires. À partir de la Réponse aux vulnérabilités version 20.0, vous pouvez ajouter des notes de travail dans la section Notes pour un élément vulnérable différé.
Activité	S'affiche uniquement lorsqu'une note de travail a été créée.
Liens connexes	
Calculer le score de risque	Lorsque les calculateurs de **gravité de vulnérabilité** ou de **score de risque** sont activés, le champ **de score de risque** est mis à jour.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voici les listes connexes des éléments vulnérables.

Liste connexe	Description
Tâches de remédiation	Tâches associées à cet élément vulnérable.
Affectation des tâches	Tâches associées à cet élément vulnérable.
Adresses IP associées	Disponible si l'application Intégration des vulnérabilités Qualys Vulnerability Integration est installée. Adresses IP trouvées lors de la déduplication.
Services impactés	Services aux entreprises touchés par cet élément vulnérable. Affiché lorsque ces informations sont disponibles dans l'enregistrement `CMDB` . Ces informations peuvent être saisies manuellement ou à l'aide de l'application ServiceNow® Mappage des services . Pour plus d'informations, reportez-vous à la section Service Mapping . Si un CI affecté associé à l'élément vulnérable est ajouté ou mis à jour, les informations de cette liste connexe sont automatiquement mises à jour lorsque l'enregistrement est enregistré.
Tickets Qualys	Qualys Informations d'intégration de ticket associées à cet élément vulnérable.

Champs du formulaire Solution

Les solutions sont créées automatiquement lorsque des enregistrements sont téléchargés à partir d'intégrations de solutions tierces et stockés sous **Solutions** dans Réponse aux vulnérabilités.

Champs d'entrée d'intégration de solution

Les champs importés dans cette table sont en lecture seule.

Champ	Description
Numéro	Identificateur affecté à la solution.
Source	Origine de la solution.
ID source	Identificateur de source pour cette solution.
Cote de risque	Sépare le score de **risque** de l'enregistrement de solution en plages allant de Critique à Aucun. Pour plus d'informations sur **la cote de risque** de la solution, reportez-vous à la section Gestion des solutions pour vulnérabilités. **Remarque :** **La cote de risque** de la solution n'est pas la même que la **cote de risque** des enregistrements d'élément **vulnérable**, **d'entrée de vulnérabilité tierce** et de **tâche de rattrapage**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Score du risque	Calcul pondéré basé sur le score de **risque** et le nombre d'éléments vulnérables avec cette solution comme **solution privilégiée**. Pour en savoir plus sur le score de risque de la solution, reportez-vous à Gestion des solutions pour vulnérabilités. **Remarque :** Le **score de risque** de l'enregistrement de solution n'est pas le même que le **score de risque** de **l'enregistrement de l'élément vulnérable**, de **l'entrée de vulnérabilité tierce** et des tâches de **remédiation**. Disponible lorsque NVD SAM est activé, mais qu'aucun élément vulnérable (EV) actif n'est associé à une vulnérabilité, le **score de risque** de la solution est défini sur zéro.
Priorité la plus élevée	Indique qu'aucune solution ne la remplace.
Type de solution	Quel genre de solution c'est. Les choix possibles sont les suivants : • Solution de contournement • Atténuation • Correction du fournisseur • Correctif • Déploiement • Autorisation • Ne corrigera pas • Aucun disponible
Nécessite le redémarrage	Redémarrage nécessaire. Les choix possibles sont les suivants : • Oui • Non • Peut-être
Date de publication	Date à laquelle la vulnérabilité a été publiée par source.
Dernière modification	Date de la dernière modification de la vulnérabilité par la source.
Résumé	Résumé du rattrapage de la solution.
Bulletin	Bulletin de sécurité associé à la solution.
Catégories de produits	Catégories de produits auxquelles la solution s'applique.
Produits	Produits auxquels la solution s'applique.
Détails de la solution	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Si aucun contenu n'est disponible dans la source de la solution, vous êtes dirigé vers une autre section ou solution pertinente pour plus d'informations.
Liens	Ressources Internet importées associées à la solution.
Détails des vulnérabilités	
Notes de vulnérabilité	Résumé des vulnérabilités corrigées par la solution.
État du rattrapage	
Cibles de solutions privilégiées État du rattrapage des éléments vulnérables et de leurs éléments de configuration (CI) uniques, pour lesquels il s'agit de la solution privilégiée. **Remarque :** Un CI unique est un CI qui n'est compté qu'une seule fois, quel que soit le nombre de VI auxquels il est associé.	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre d'éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
% des VI rattrapés	Pourcentage complet pour le rattrapage d'éléments vulnérables (VI). S'applique aux éléments vulnérables pour lesquels cette solution est préférée. Ce nombre exclut les VI différés.
CI restants	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les CI des éléments vulnérables différés.
CI totaux	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les CI des éléments vulnérables différés.
% des CI rattrapés	Pourcentage de CI uniques rattrapés (ce qui signifie que tous les VI pour ce CI et cette solution sont rattrapés). Déterminé par le nombre de CI rattrapés par rapport au nombre total de CI uniques associés aux éléments vulnérables avec la solution privilégiée. Ce nombre exclut les CI des éléments vulnérables différés.
Cibles de solutions privilégiées (inclut les éléments différés) État du rattrapage pour les éléments vulnérables et leurs CI uniques, y compris différés, pour lesquels il s'agit de la solution privilégiée.	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est préférée pour le rattrapage.
VI totaux	Nombre d'éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
% des VI rattrapés	Pourcentage complet pour le rattrapage d'éléments vulnérables (VI). S'applique aux éléments vulnérables pour lesquels cette solution est préférée.
CI restants	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est préférée pour le rattrapage.
CI totaux	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage.
% des CI rattrapés	Pourcentage de CI uniques rattrapés (ce qui signifie que tous les VI pour ce CI et cette solution sont rattrapés). Déterminé par le nombre de CI rattrapés par rapport au nombre total de CI uniques associés aux éléments vulnérables avec la solution privilégiée. Ce nombre exclut les CI des éléments vulnérables différés.
Cibles potentielles de la solution État du rattrapage des éléments vulnérables et de leurs CI uniques, avec une vulnérabilité liée à cette solution.	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est une solution possible pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
CI restants	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est une solution possible pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
Cibles potentielles de la solution (y compris les éléments différés) État du rattrapage pour les éléments vulnérables et leurs CI uniques, y compris différés, avec une vulnérabilité qui peut être corrigée par cette solution, y compris les nombres de solutions préférées.	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est une solution possible pour le rattrapage.
CI restants	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est une solution possible pour le rattrapage.
Notes	
Notes internes	Champ modifiable fourni pour le spécialiste du rattrapage.
Liens connexes	
Mettre à jour le statut	Date et heure de la dernière mise à jour de l'état du rattrapage. Met à jour les éléments suivants : • État de la tâche de résolution • Score et évaluation du risque • Mesures de la section État du rattrapage
Listes connexes	

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Éléments vulnérables	Éléments vulnérables associés à cette solution comme solution privilégiée pour le rattrapage.
Vulnérabilités tierces	Vulnérabilités tierces associées à cette solution.
CVE	Vulnérabilités courantes et vulnérabilités d'exposition (CVE) associées à cette solution.
Tâches de remédiation	Les tâches de remédiation qui contiennent des éléments vulnérables connexes avec cette solution sont préférées pour le rattrapage.
Solutions précédentes	Solutions antérieures qui résolvent une ou plusieurs vulnérabilités de cette solution.
Solutions de remplacement	Solutions ultérieures qui résolvent toutes les vulnérabilités de cette solution. Cette liste est vide lorsque la case **Priorité la plus élevée** est cochée.

Configurations du workflow d'approbation pour la demande de désaffectation

Vous pouvez concevoir le workflow d'approbation pour la suppression des affectations des éléments vulnérables (VI, VIT), des tâches de rattrapage, des éléments vulnérables de l'application (AVIT) et des éléments vulnérables du conteneur (CVIT) pour vous et votre groupe.

Le VIT, la tâche de rattrapage, l'AVIT et le CVIT ont chacun une règle d'approbation par défaut. Chaque règle d'approbation dispose d'une configuration d'approbation par défaut. Chaque configuration d'approbation a un niveau d'approbateur par défaut. Les règles d'approbation pour les VIT, la tâche de rattrapage, AVIT et CVIT sont activées par défaut. En tant qu'administrateur, vous pouvez effectuer les actions suivantes en accédant à **Tout** > **Réponse aux vulnérabilités** > **Mes approbations** > **Règles d'approbation** et la sélection de la règle d'approbation appropriée.

- Activer ou désactiver une règle d'approbation.
- Créez et mettez à jour une configuration d'approbation.
- Définissez les conditions pour les éléments vulnérables et les tâches de rattrapage auxquelles les règles d'approbation s'appliquent.
- Créez et mettez à jour plusieurs niveaux d'approbateur.

La table suivante présente les règles d'approbation, les configurations d'approbation et les niveaux d'approbateur par défaut pour un VIT, une tâche de rattrapage, un AVIT et un CVIT fournis avec le système de base.

Règles d'approbation, configurations d'approbation et niveaux d'approbation par défaut

Type	Règle d'approbation	Configuration de l'approbation	Niveaux de l'approbateur
VIT ou VI	Demande de modification du champ d'élément vulnérable	Demande de modification du champ d'élément vulnérable	Demande de désaffectation de niveau 1 pour VI

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles d'approbation, configurations d'approbation et niveaux d'approbation par défaut (suite)

Type	Règle d'approbation	Configuration de l'approbation	Niveaux de l'approbateur
Tâche de rattrapage	Demande de modification du champ Groupe de vulnérabilité	Demande de modification du champ de vulnérabilité	Niveau 1 : annuler l'affectation de la demande pour VG
AVIT	Demande de modification du champ d'élément vulnérable d'application	Demande de modification du champ de vulnérabilité de l'application	Annuler l'affectation de l'élément de vulnérabilité de l'application
Le CVIT	Approbation de la gestion du conteneur	Configuration par défaut de la désaffectation du CVIT	Niveau d'approbation de désaffectation du CVIT : 1

Pour en savoir plus sur l'approbation des demandes de désaffectation, reportez-vous à la section Approuver ou rejeter une demande de désaffectation dans Réponse aux vulnérabilités.

Réponse aux vulnérabilités Exemples de règles de tâche de rattrapage

Exemples de règles de tâche de rattrapage utilisant vulnérabilité et risque, ou impact, ou élément de configuration (CI).

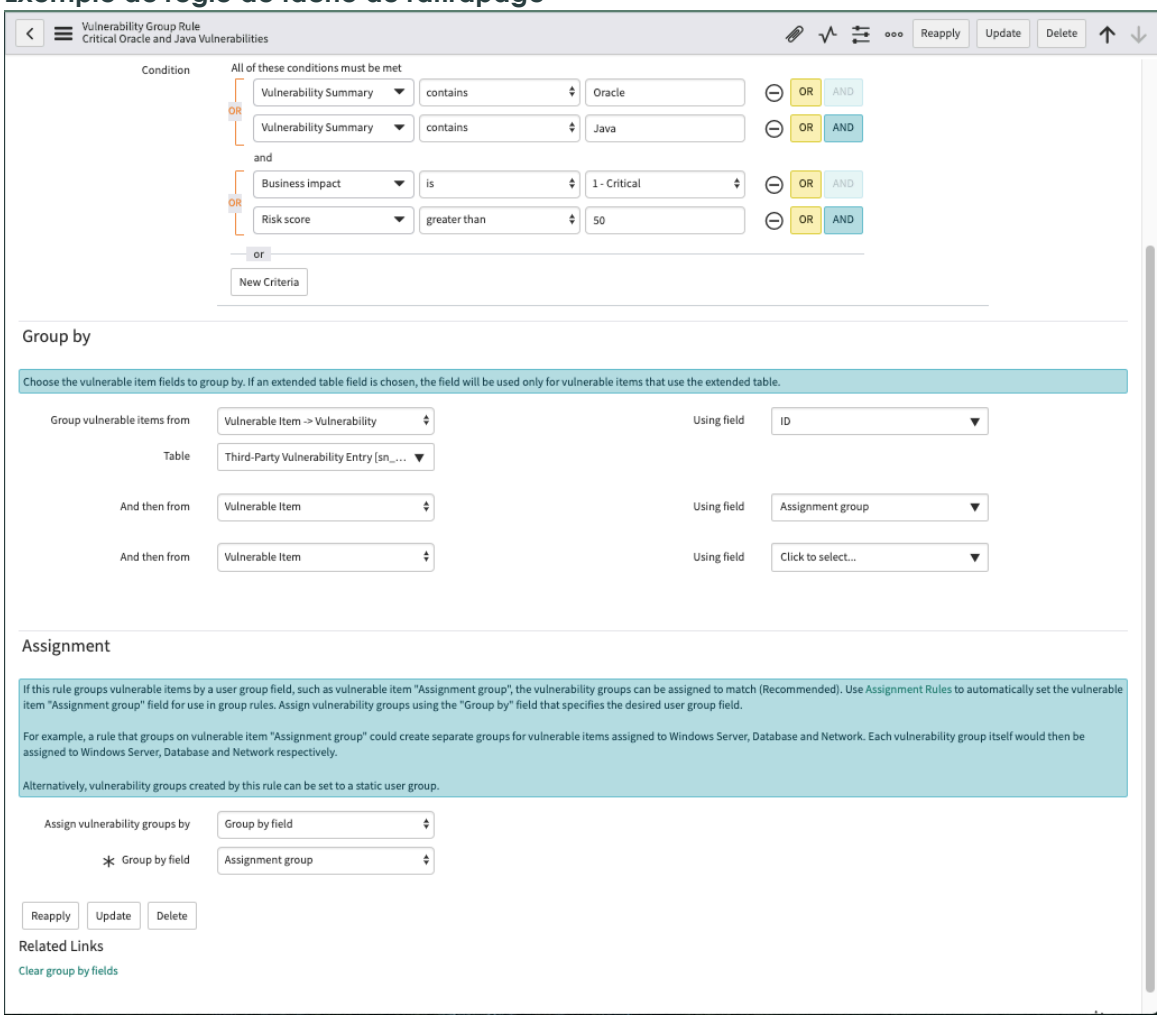
Règle de tâche de rattrapage pour regrouper les éléments vulnérables Java et Oracle à haut risque

Cet exemple montre une présentation de la règle qui regroupe les éléments vulnérables Java et Oracle par vulnérabilité et les affecte à leurs groupes de support respectifs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de règle de tâche de rattrapage



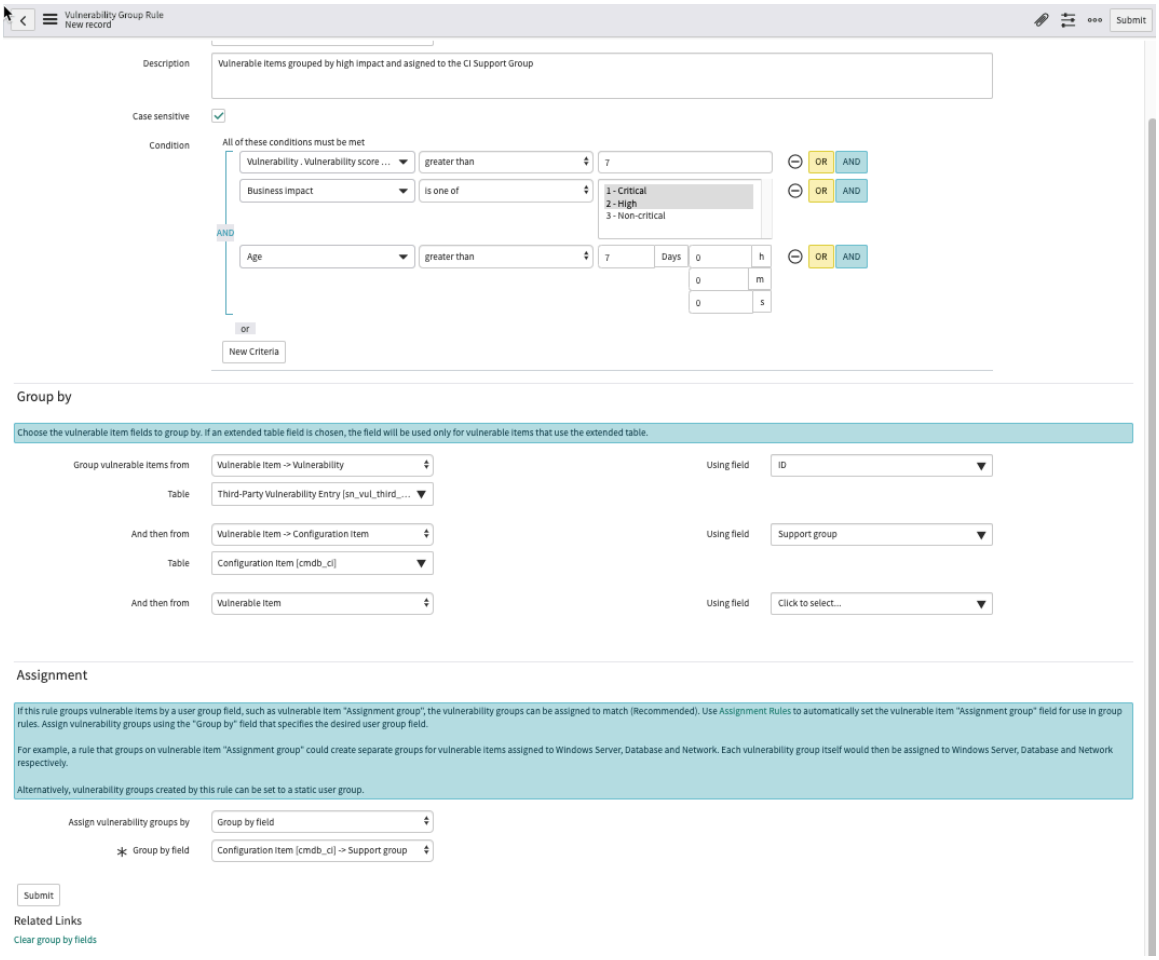
Cliquez avec le bouton droit de la souris dans l'en-tête pour **enregistrer**.

Règle de tâche de rattrapage pour regrouper tous les éléments vulnérables à impact élevé par groupe de support de vulnérabilité et de CI

Cet exemple montre les paramètres de champ de formulaire pour une règle de groupe pour les éléments vulnérables à impact élevé qui les affecte au groupe de support de CI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

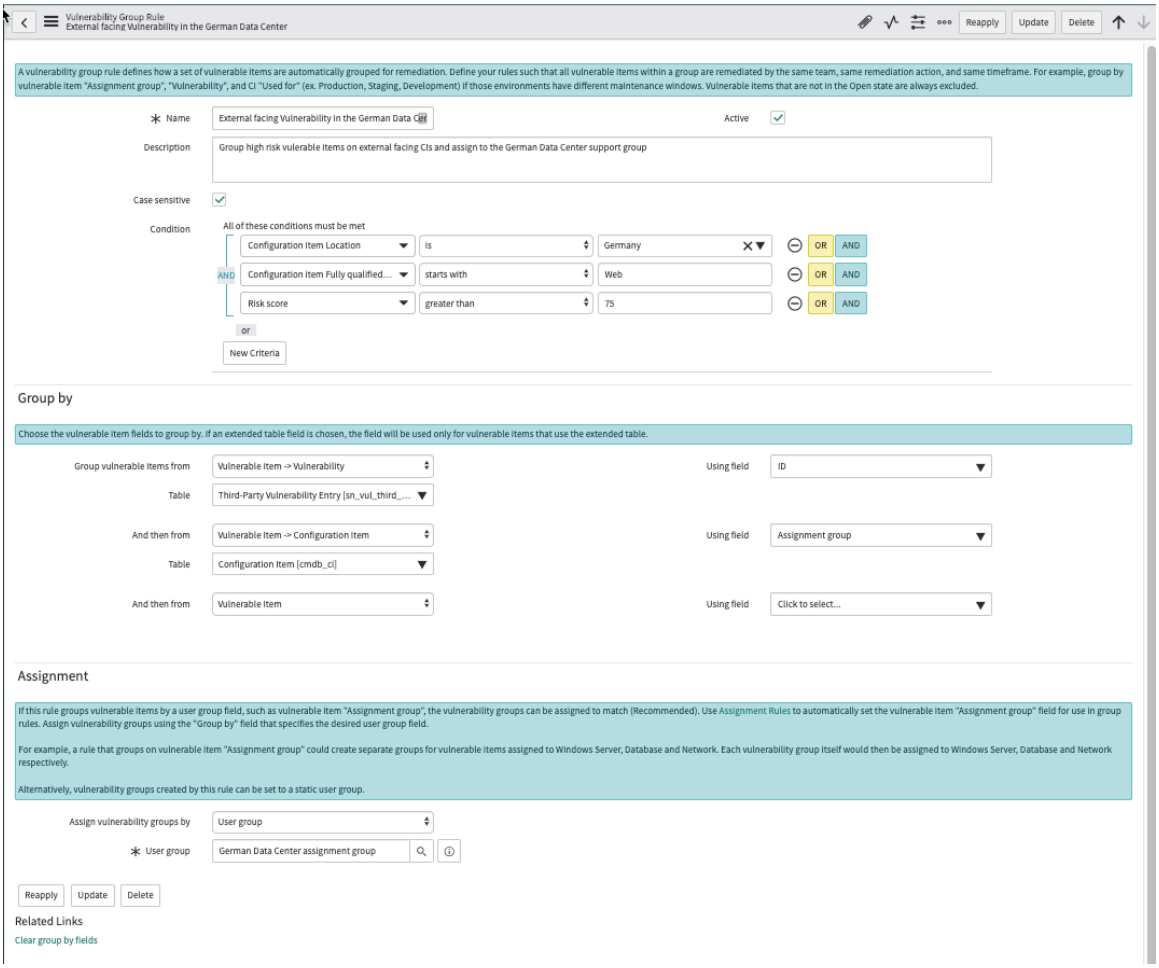


Règle de tâche de rattrapage pour regrouper toutes les vulnérabilités à haut risque sur un CI orienté vers l'extérieur dans un centre de données allemand

Cet exemple montre les paramètres de champ de formulaire d'une règle de groupe pour les vulnérabilités à risque élevé sur les CI externes dans un centre de données allemand. Ils sont affectés au groupe d'affectation du centre de données allemand.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Exemple de calcul du score de risque pour Réponse aux vulnérabilités

Vous pouvez utiliser des calculateurs de score de risque pour générer des scores de risque qui utilisent les données de vulnérabilité et d'actif propres à votre organisation.

Exemple de détermination des scores des calculateurs de règles de risque

L'exemple suivant montre comment les scores des calculateurs de règles de risque sont déterminés.

Supposons qu'un calculateur de règle de risque soit configuré avec les champs de cette table :

Champ	Pondération	Répartition du poids
Vulnérabilité.Gravité	50	Par défaut : 20 1 - Critique : 100 2 - Haute : 80 3 - Moyen : 60 4 - Faible : 40 5 - Aucun : 20

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Pondération	Répartition du poids
Vulnerability.Exploit existe	50	Par défaut : 50 Oui : 100 Non : 0

Supposons également que les éléments vulnérables affichés dans ce tableau sont présents dans le système :

ID	Gravité de la vulnérabilité	Existence d'une exploitation de la vulnérabilité
VIT00001	1 - Critique	1 - Oui
VIT00002	2 : élevé	1 - Oui
VIT00003	3 : moyen	2 – Non
VIT00004	4 : faible	2 – Non
VIT00005	5 : aucun	2 – Non

Le calcul du score de risque pour les éléments vulnérables est calculé en fonction de la formule suivante :

```
Score de risque = (W(gravité) * FV (gravité). + W(exploitexiste) *
FV(exploit existe)) / 100
```

où **W** est le poids et **FV** est le pourcentage de poids de la valeur de champ.

Le score de risque résultant pour ces éléments vulnérables est décrit dans la table suivante :

ID	Gravité de la vulnérabilité (50 %)	Existence d'une exploitation de la vulnérabilité (50 %)	Score de risque résultant
VIT00001	1 – Critique (50 % x 100)	1 – Oui (50 % x 100)	100
VIT00002	2 – Élevée (50 % x 80)	1 – Oui (50 % x 100)	90
VIT00003	3 – Moyen (50 % x 60)	2 – Non (50 % x 0)	30
VIT00004	4 – Faible (50 % x 40)	2 – Non (50 % x 0)	20
VIT00005	5 - Aucun (50 % x 20)	2 – Non (50 % x 0)	10

Remarque : Par VIT00005, car la valeur de gravité est vide, la pondération par défaut est appliquée.

Si le pourcentage de pondération est modifié pour l'une des valeurs de champ, consultez ce tableau pour les résultats :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Pondération	Répartition du poids
Vulnérabilité.Gravité	50	• Par défaut : 20 • 1 - Critique : 100 • **2 - Haute : 70** *valeur révisée • 3 - Moyen : 60 • 4 - Faible : 40
Vulnerability.Exploit existe	50	• Par défaut : 50 • Oui : 100 • Non : 0

Le score de risque pour les éléments vulnérables après réapplication du calculateur est affiché dans la table suivante :

ID	Gravité de la vulnérabilité (50 %)	Existence d'une exploitation de la vulnérabilité (50 %)	Score de risque résultant
VIT00001	1 – Critique (50 % x 100)	1 – Oui (50 % x 100)	100
VIT00002	**2 – Élevée (50 % x 70)** *valeur révisée	1 – Oui (50 % x 100)	**85** *valeur révisée
VIT00003	3 – Moyen (50 % x 60)	2 – Non (50 % x 0)	30
VIT00004	4 – Faible (50 % x 40)	2 – Non (50 % x 0)	20
VIT00005	5 - Aucun (50 % x 20)	2 – Non (50 % x 0)	10

Gestion des erreurs pour les détections

Les erreurs sont journalisées lors de la création de détections ou de la création et de la mise à jour d'éléments vulnérables lors du traitement des pièces jointes. En cas d'échec d'un processus d'intégration de vulnérabilité, les erreurs sont consignées dans l'onglet « Journal des intégrations de vulnérabilité ».

Ces erreurs sont consignées dans l'une des catégories suivantes.

Champ	Description
Création de VI	Erreur lors de la création ou de la mise à jour de la détection.
Détection	Erreur lors de la création d'une détection.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Expérience mobile pour Réponse aux vulnérabilités

En tant que propriétaire de rattrapage, vous pouvez accéder à l'application Réponse aux vulnérabilités (VR) sur votre instance Now Platform® avec votre équipement mobile Android ou iOS.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Réponse aux vulnérabilités

Pour vous familiariser avec les concepts de Vulnerability Response et la façon dont ce produit peut aider votre organisation, consultez Présentation de Vulnerability Response.

Remarque : Avant d'installer le Application Réponse aux vulnérabilités mobile mobile, familiarisez-vous avec le Agent mobile .

Vue d'ensemble

En tant qu'utilisateur disposant du rôle de propriétaire de rattrapage (sn_vul.remediation_owner), le Application Réponse aux vulnérabilités mobile vous permet d'afficher et de rechercher les vulnérabilités, les tâches de rattrapage et les affectations sur votre Now Platform instance directement à partir de votre équipement mobile ou iOS de votre Android équipement mobile.

Vous êtes notifié lorsque des tâches de rattrapage (RT) ou des VI vous ont été affectés ou ont été affectés à vous ou à votre groupe d'affectation. Cette application permet à un propriétaire de rattrapage de réaffecter à nouveau, de modifier des champs et de commencer le rattrapage sans être lié au bureau.

Vous avez accès aux vulnérabilités, aux éléments de vulnérabilité, aux modules et à toutes les solutions. Vous pouvez effectuer les tâches suivantes sur votre équipement mobile :

- Affichez et mettez à jour les tâches de rattrapage.
- Affichez les demandes de changement.
- Réaffectez une tâche de rattrapage ou un élément de vulnérabilité à un autre membre d'un groupe d'affectation.
- Affichez les notifications lorsqu'une tâche de rattrapage critique vous est affectée ou est affectée à l'un de vos groupes d'affectation.
- Modifiez un sous-ensemble de champs dans les enregistrements de tâche de rattrapage.
- Recherchez les tâches de rattrapage qui correspondent à des critères de recherche spécifiques.

La figure suivante illustre la façon dont vous vous connectez à votre Now Platform instance à partir de votre équipement mobile et l'écran d'accueil de l'instance Application Réponse aux vulnérabilités mobile qui s'affiche une fois connecté.

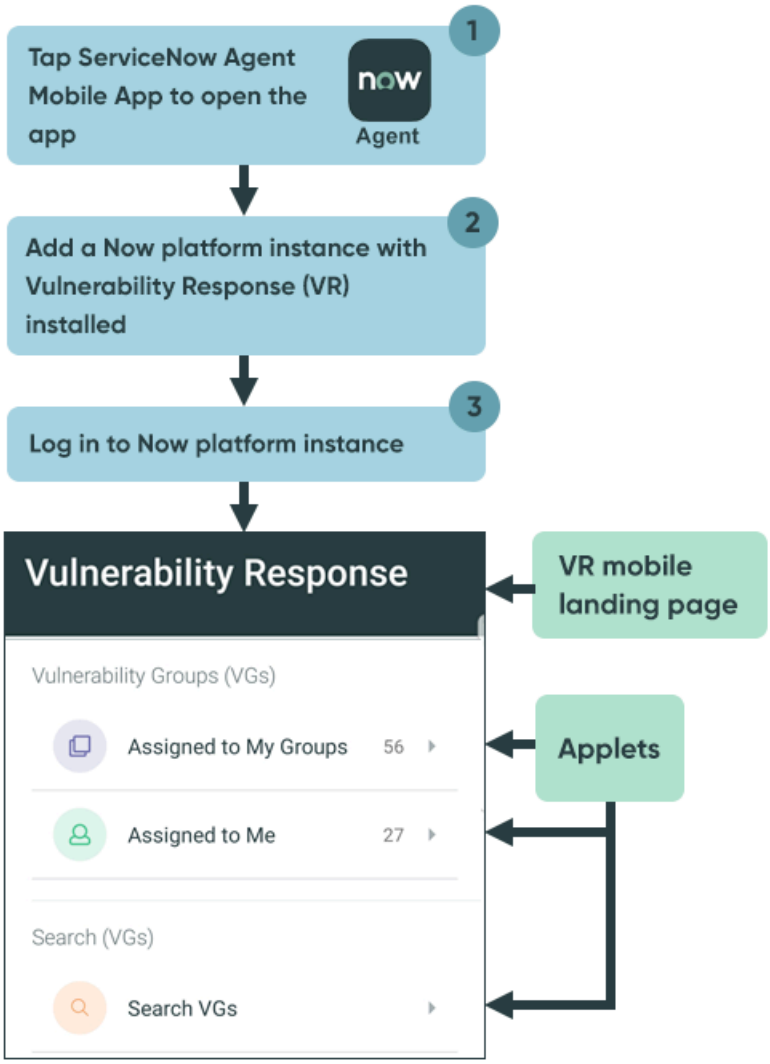
Pour obtenir des instructions détaillées sur la configuration de votre instance et l'installation de , Now PlatformApplication Réponse aux vulnérabilités mobilereportez-vous à la section Configurer une liste de vérification pour le Application Réponse aux vulnérabilités mobile.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour obtenir des instructions sur la façon de se connecter, reportez-vous à la section Connectez-vous au Application Réponse aux vulnérabilités mobile.

Application Réponse aux vulnérabilités mobile



Applications

Les applications sont les ServiceNow composants logiciels tels que Réponse aux incidents de sécurité (SIR), Réponse aux vulnérabilités (VR), Gouvernance, risque et conformité (GRC) et d'autres produits qui fournissent des fonctionnalités spécifiques au sein de ServiceNow votre Now Platform instance. Une fois que vous avez installé des applications principales qui ont des applications mobiles sur votre Now Platform instance, ces applications s'affichent sous forme d'icônes au bas de votre appareil mobile.

Icône Vulnerability Response sur l'appareil mobile

Dossiers

Chaque ServiceNow® Mobile application contient des dossiers qui séparent les applets par catégories. Dans l'image précédente, les tâches de rattrapage et la recherche (VG) sont les dossiers pour le Application Réponse aux vulnérabilités mobilefichier .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applets

Les applets sont les différentes options au sein de l'application. Dans l'image précédente, les icônes sous Tâches de rattrapage et Recherche (VG) sont les applets disponibles pour le Application Réponse aux vulnérabilités mobilefichier .

Reportez-vous aux rubriques suivantes pour plus d'informations sur les applets du Application Réponse aux vulnérabilités mobilefichier .

Configurer une liste de vérification pour le Application Réponse aux vulnérabilités mobile

La liste de vérification suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform® instance et sur votre équipement mobile avant d'utiliser le Application Réponse aux vulnérabilités mobile.

Avant de commencer

Plus d'informations suivent chaque étape dans la colonne de droite. Temps estimé pour accomplir cette tâche : 15 à 20 minutes.

Rôles requis : admin, sn_vul.remediation_owner

Vous avez correctement configuré votre équipement mobile pour le Application Réponse aux vulnérabilités mobile. L'étape suivante consiste à vous connecter et à Application Réponse aux vulnérabilités mobile ajouter une Now Platform instance à votre appareil mobile.

Procédure

1. Si vous le souhaitez, imprimez cette liste de vérification et utilisez-la pour effectuer les tâches nécessaires à l'installation du Application Réponse aux vulnérabilités mobilefichier .
2. Vérifiez que chaque élément de la liste est terminé afin de pouvoir vous connecter Application Réponse aux vulnérabilités mobile et ajouter une Now Platform instance.

Liste de vérification mobile

Élément	Description
☐	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que l'application Réponse aux vulnérabilités Core est installée sur une Now Platform instance. Il s'agit de l'instance Now Platform que vous affichez sur votre appareil mobile. **Remarque :** L'application Réponse aux vulnérabilités principale et l'instance Now Platform doivent provenir de la même version de famille. **a.** Pour vérifier que l'application principale est installée sur votre instance, accédez à **Modules d'extension** et recherchez Réponse aux vulnérabilités. **b.** Si l'application principale n'est Réponse aux vulnérabilités pas déjà installée, cliquez sur **Installer** pour l'installer. Pour en savoir plus sur l'installation de l'application principale, reportez-vous Réponse aux vulnérabilités à la section Installer Réponse aux vulnérabilités. Pour plus d'informations sur l'obtention de l'application Réponse aux vulnérabilités principale sur le , l'obtention d'autorisations, l'installation

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	ServiceNow Stored'applications principales et l'activation des dépendances, reportez-vous à la section .
☐	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que vous avez installé Now Platform l'instance Application Réponse aux vulnérabilités mobile que vous souhaitez afficher sur votre équipement mobile. **Remarque :** L'instance Application Réponse aux vulnérabilités mobile et l'instance Now Platform doivent provenir de la même version de famille. Le Application Réponse aux vulnérabilités mobile et l'application Réponse aux vulnérabilités doivent être compatibles. Pour plus d'informations sur la compatibilité des applications Vulnerability Response, consultez Vulnerability Response et Matrice de compatibilité de Configuration Compliance . Téléchargez et installez le Application Réponse aux vulnérabilités mobile à partir de sur ServiceNow Store votre Now Platform instance. Lorsque vous installez , ses Application Réponse aux vulnérabilités mobiledépendances, com.glide.sg et com.glide.sg.agent_native_client, sont également installées. Pour vérifier que ces dépendances sont installées : **a.** Accédez à la **Tout** > **Modules d'extension**. **b.** Recherchez les ID des modules d'extension (com.glide.sg et com.glide.sg.agent_native_client). **c.** S'ils ne sont pas activés, activez ces modules d'extension. Ces modules d'extension sont requis pour le Application Réponse aux vulnérabilités mobilefichier . Pour plus d'informations sur l'obtention de l'application Application Réponse aux vulnérabilités mobile sur le , l'obtention d'autorisations, l'installation ServiceNow Stored'applications et l'activation des dépendances, reportez-vous à la section .
☐	En tant qu'utilisateur disposant du rôle admin, vérifiez dans votre Now Platform instance que vous avez affecté les utilisateurs mobiles disposant des rôles requis Now Platform . **a.** Pour afficher les rôles affectés à un utilisateur, accédez à **Tout** > **Administration** > **Utilisateurs**. **b.** Sélectionnez le nom d'utilisateur suivi de la liste connexe des rôles. Tous les rôles affectés à cet utilisateur s'affichent. **c.** Vérifiez qu'un utilisateur est affecté ou affectez à un utilisateur le rôle ITIL (ITIL Bibliothèque d'infrastructures ITIL). Les utilisateurs disposant du rôle itil peuvent créer, ouvrir, mettre à jour et fermer des demandes de changement et des tâches de rattrapage. Seuls les utilisateurs disposant du rôle itil peuvent se voir affecter des tâches. **d.** Vérifiez qu'un utilisateur est affecté ou affectez un utilisateur avec le rôle de propriétaire du rattrapage (sn_vul.remediation_owner). Les utilisateurs disposant du rôle sn_vul.remediation_owner peuvent

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	lire les enregistrements de vulnérabilité et de solution. Ce rôle est automatiquement ajouté lorsque vous affectez le rôle itil. **e.** Vérifiez que vous avez créé tous les groupes d'affectation requis et affecté des utilisateurs mobiles à ces groupes. **Remarque :** Si vous disposez d'un grand nombre d'utilisateurs pour l'application mobile, vous pouvez également affecter le rôle sn_vul.remediation_owner à un groupe. Chaque utilisateur que vous ajoutez au groupe hérite de ce rôle. Pour en savoir plus sur les règles et les groupes d'affectation, reportez-vous à Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation. Pour plus d'informations sur les utilisateurs et l'affectation de rôles aux utilisateurs et aux groupes, consultez Administration utilisateurs .
☐	En tant qu'utilisateur disposant du rôle de propriétaire de rattrapage (sn_vul.remediation_owner), téléchargez l'application Agent la plus récente ServiceNow® sur votre équipement mobile.  L'application Agent la plus récente est disponible sur l'App Store d'Apple iOS et le Google Play Store.
☐	En tant qu'utilisateur disposant du rôle sn_vul.remediation_owner, vérifiez que les notifications sont activées sur votre équipement mobile et dans votre Now Platform instance. Les notifications vous informent lorsque des tâches de rattrapage critiques vous sont affectées ou sont affectées à votre groupe d'affectation. Pour vous aider à y remédier en temps opportun, après avoir activé les notifications, cliquez sur une notification dans le Application Réponse aux vulnérabilités mobile et accédez directement à l'enregistrement. Pour activer les notifications dans votre Now Platform instance afin qu'elles s'affichent sur votre équipement mobile, procédez comme suit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	a. Vérifiez que vous avez téléchargé et installé le Application Réponse aux vulnérabilités mobile sur votre Now Platform instance. **b.** Dans les paramètres système de votre Now Platform instance, sous Notifications, vérifiez que vous avez activé **l'application mobile ServiceNow**. Pour en savoir plus sur la définition des notifications, reportez-vous à la section Définition des préférences de notification dans Interface utilisateur principale . Now Platform Les notifications sont également affichées sur l'écran Messages de votre appareil mobile. Vérifiez que les notifications sont également activées dans les paramètres de votre équipement mobile.

Connectez-vous au Application Réponse aux vulnérabilités mobile

Ouvrez l'application Vulnerability Response Mobile et ajoutez une instance Now Platform avec Vulnerability Response à votre appareil mobile.

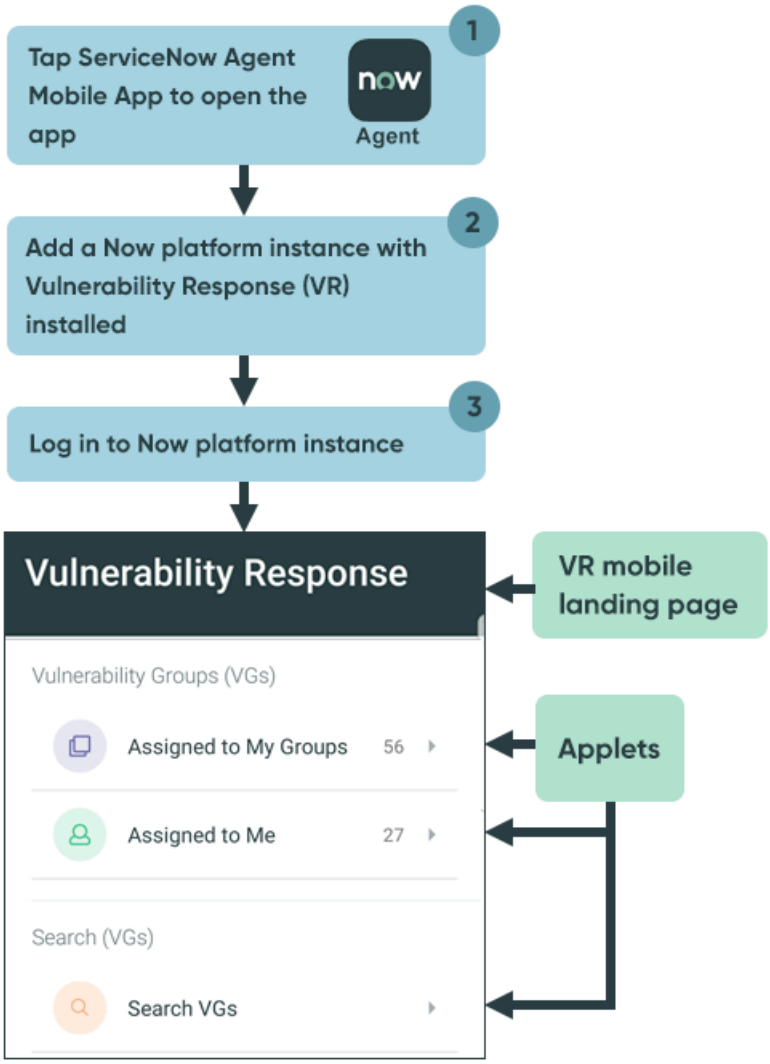
Avant de commencer

Vérifiez que vous avez terminé les étapes de configuration décrites à la section Configurer une liste de vérification pour le Application Réponse aux vulnérabilités mobile.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application Réponse aux vulnérabilités mobile

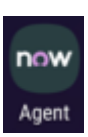


Rôle requis : propriétaire de rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche
Temps nécessaire pour accomplir cette tâche : 5 à 7 minutes.

Procédure

1. Sur votre équipement mobile, appuyez sur l'application **ServiceNow Agent** .



Si vous n'êtes pas déjà connecté à une Now Platform instance, l'écran Instances s'affiche.

2. Si l'instance Now Platform avec l'application Réponse aux vulnérabilités principale n'est pas déjà ajoutée à votre appareil mobile, procédez comme suit pour l'ajouter.

   a. Sur l'écran Instances qui s'affiche, appuyez sur l'icône plus ( )
   Un écran s'affiche et vous invite à saisir et à enregistrer l'adresse d'une Now Platform instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

b. Renseignez les champs.

Nom de champ	Description
Entrez l'adresse de l'instance ou scannez un code QR.	Choisissez-en un pour continuer : ▪ Avant le `.service-now.com`, saisissez le nom de votre Now Platform instance, par exemple, `vrmobilenewyorkagent`. ▪ Entrez une adresse. Cette adresse correspond à l'URL de l'instance Now Platform que vous souhaitez afficher sur votre équipement mobile. ▪ Scannez un code QR.
(Facultatif) Entrez le pseudonyme	entrez un surnom pour cette instance. Si plusieurs instances ont été ajoutées à l'appareil , des surnoms peuvent vous aider à localiser rapidement une Now Platform instance.

c. Appuyez sur **Enregistrer et vous connecter**

3. Sur l'écran de connexion qui s'affiche ServiceNow , saisissez le nom d'utilisateur et le mot de passe de l'instance Now Platform que vous souhaitez ajouter, puis appuyez sur **Connexion**.
L'écran d'accueil de Vulnerability Response s'affiche. Vous vous êtes connecté avec succès au Application Réponse aux vulnérabilités mobile !

4. Après vous être connecté, vérifiez que les notifications sont activées dans le Application Réponse aux vulnérabilités mobile.

a. Sur l'écran d'accueil en bas, appuyez sur **Notification**.

b. Sur l'écran Notifications, appuyez sur **Activer les notifications** si elles ne sont pas activées.
Les notifications provenant de s'affichent Now Platform sur l'écran Notifications du Application Réponse aux vulnérabilités mobile.

5. Une fois que vous êtes connecté à une instance sur votre équipement mobile, il s'agit de l'instance par défaut Now Platform sur l'appareil.
Si vous souhaitez en afficher une autre Now Platform sur l'appareil, vous devez vous déconnecter de l'instance par défaut. Pour vous déconnecter :

a. Appuyez sur l'icône **Paramètres** .

b. Appuyez sur **Déconnexion**.
L'écran Instances s'affiche avec toutes les Now Platform instances que vous avez ajoutées à l'équipement mobile.

c. Facultatif : Appuyez sur une autre instance pour vous y connecter ou, à défaut, suivez les étapes précédentes pour ajouter une autre instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Si l'écran des instances ne s'affiche Application Réponse aux vulnérabilités mobile pas après que vous avez appuyé sur l'application **ServiceNow Agent** sur votre appareil, vérifiez que **ServiceNow Agent** est autorisé en tant qu'application approuvée sur votre appareil. Pour autoriser l'accès en tant qu'application approuvée, accédez aux paramètres et à la gestion générale de l'appareil sur votre appareil et appuyez sur l'option (Application de confiance, etc.) pour autoriser l'accès.

Si un message d'erreur s'affiche une fois que vous avez saisi vos informations d'identification dans l'écran de connexion, vérifiez que votre nom d'utilisateur et votre mot de passe pour l'instance Now Platform sont corrects.

Si vous rencontrez des problèmes pour afficher l'écran d'accueil, vérifiez votre connexion réseau.

Si vous ne pouvez pas afficher l'écran des instances après avoir appuyé sur l'application **ServiceNow Agent** , essayez de la désinstaller de votre appareil. Vérifiez que vous disposez de la version la plus récente de l'application de l'App Store d'Apple iOS ou du Google Play Store et essayez de la réinstaller.

Affichez, affectez et modifiez des tâches de rattrapage avec l' Application Réponse aux vulnérabilités mobile

Affichez, affectez ou modifiez les champs des enregistrements de tâche de rattrapage (RT) affectés à votre groupe. Parcourez les vulnérabilités, les éléments de vulnérabilité, les enregistrements de solutions et les listes connexes pour afficher les solutions, les mesures de déploiement et les éléments à traiter.

Avant de commencer

Rôle requis : propriétaire de rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche

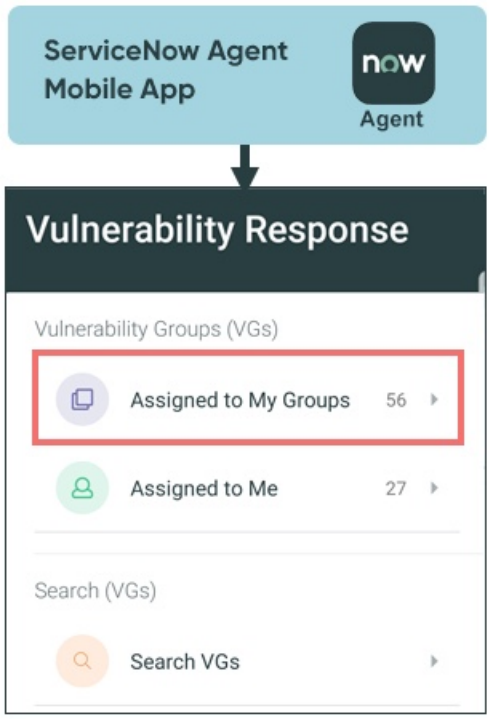
Affectez-vous des enregistrements RT (VUL) ou réaffectez-les à un autre membre de votre groupe. Vous pouvez également afficher les détails des enregistrements de tâches de rattrapage actifs, des éléments vulnérables (VI), des vulnérabilités NVD et des solutions avant de les modifier, de les affecter ou de les corriger. Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

Procédure

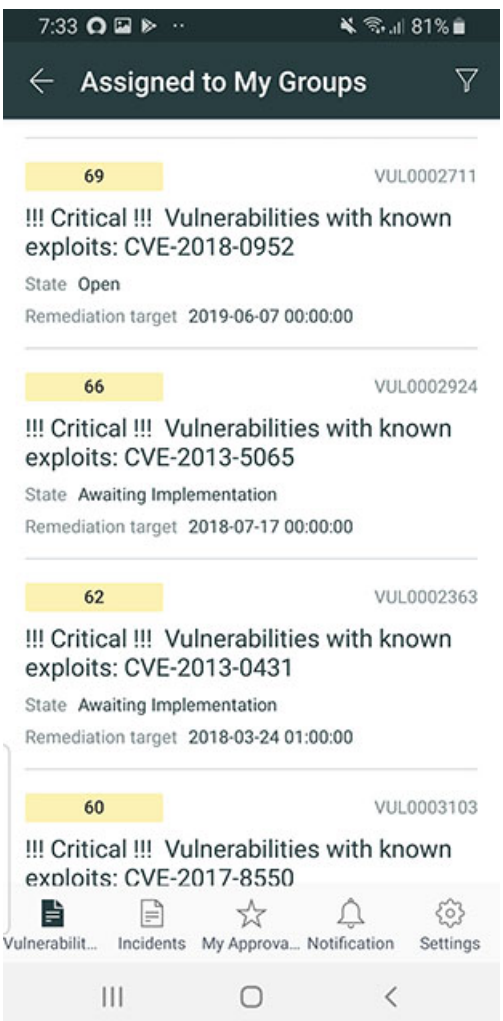
1. Si vous n'êtes pas connecté à votre Now Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Réponse aux vulnérabilités mobile.
2. Avec l'écran d'accueil de Vulnerability Response affiché, appuyez sur **Affecté à mes groupes**.
   Si vous quittez l'application Application Réponse aux vulnérabilités mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous avez affiché.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La liste des enregistrements ouverts affectés à votre groupe s'affiche.

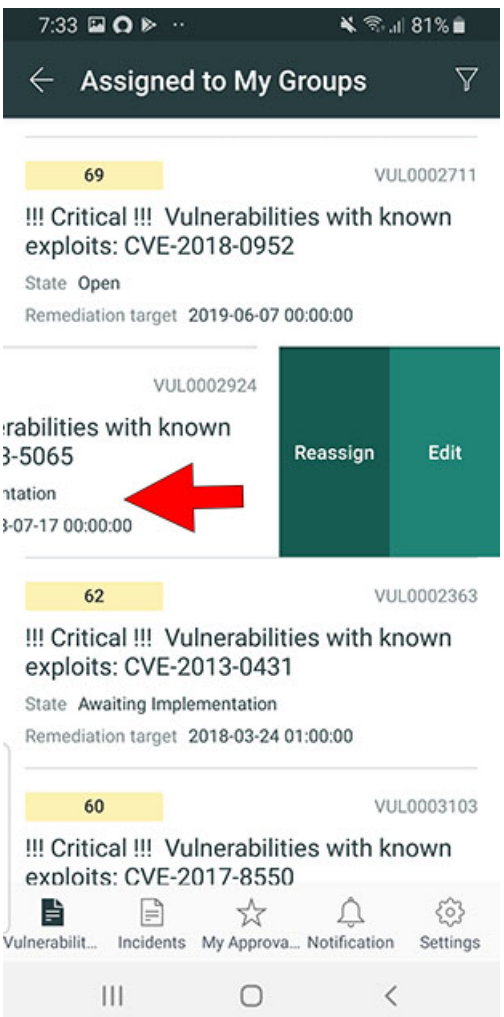


© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Facultatif : Reportez-vous à Rechercher des tâches de rattrapage avec l'attribut Application Réponse aux vulnérabilités mobile pour rechercher les enregistrements qui correspondent à des critères spécifiques.

4. Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste.
Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le Now Platform.

5. Pour réaffecter ou modifier un enregistrement directement à partir de la liste, avec la liste des enregistrements ouverts affichée, faites glisser vers la gauche sur un enregistrement pour ouvrir le menu.



6. Choisissez-en un dans le menu qui s'affiche pour continuer.

Option	Description
M'affecter	Si l'enregistrement RT vous est déjà affecté, cette option ne s'affiche pas. Appuyez sur **Me l'affecter** pour vous attribuer le RT. Votre nom s'affiche dans le champ Affecté à de l'enregistrement.

Traduction automatique

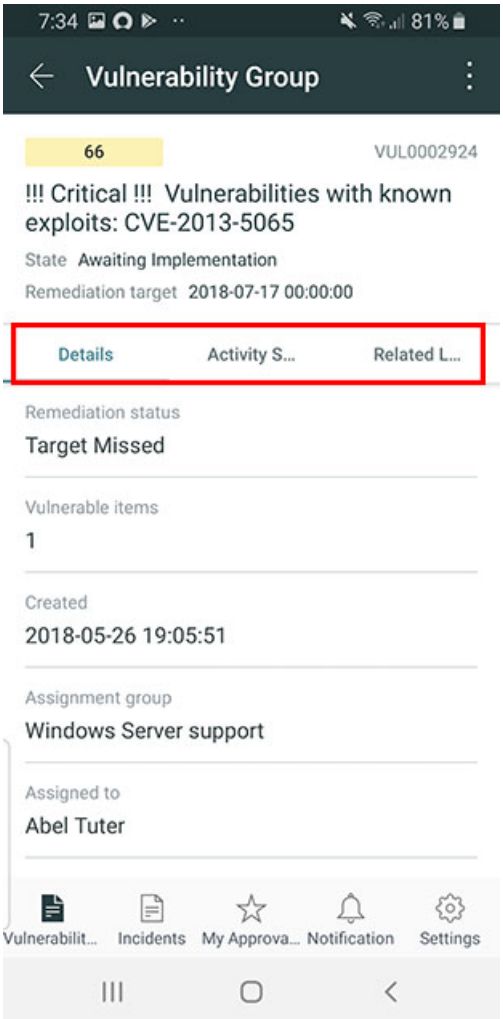
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Un message s'affiche pour confirmer l'affectation.
Réaffecter	Pour réaffecter le RT à un groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Dans la liste, appuyez sur un groupe ou saisissez du texte dans le champ de recherche. Pour affecter ou réaffecter le RT à un membre d'un groupe d'affectation : **a.** Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste affichée ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône Envoyer ( ) ou sur **Soumettre** pour enregistrer et soumettre vos modifications.
Modifier	**a.** Appuyez sur **Modifier**. **b.** Développez les champs et sélectionnez une option dans la liste affichée ou saisissez du texte dans le champ Rechercher. Appuyez sur l'icône d'envoi ( ) ou **sur Soumettre** pour enregistrer et soumettre vos modifications.

7. Pour afficher les détails d'un enregistrement de vulnérabilité ouvert et afficher plus d'enregistrements associés et de listes connexes, appuyez sur un enregistrement de la liste lorsque l'écran Affecté à mes groupes est affiché.
8. Dans l'enregistrement de tâche de rattrapage ouvert qui s'affiche, choisissez une option dans la table suivante pour afficher les notes de travail ou les listes connexes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Onglet Détails	Avec l'onglet Détails sélectionné, examinez les champs de l'enregistrement RT. Appuyez sur l'icône de menu ( ) en haut à droite de l'écran pour afficher les options disponibles. Les options affichées dans ce menu développé varient. Les actions de rattrapage que vous pouvez entreprendre sur vos éléments vulnérables varient et dépendent de la valeur affichée dans le champ État de l'enregistrement. Pour plus d'informations sur le champ État et les options de rattrapage, reportez-vous à la section Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, choisissez-en un pour continuer. ◦ Affichez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Ap-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	puyez sur l'icône plus (pour ajouter une note de travail ou joindre un fichier. ◦ Appuyez sur l'icône de menu (en haut à droite de l'écran pour afficher les options de rattrapage disponibles.
Listes connexes	Avec l'onglet Listes connexes sélectionné, affichez l'une des listes connexes de l'enregistrement RT qui sont remplies. ◦ Appuyez sur **Éléments vulnérables**. Appuyez sur un enregistrement d'élément vulnérable (VI) et accédez à l'enregistrement de solution préféré. Reportez-vous à la figure qui suit le tableau pour une carte de navigation et plus de détails. ◦ Appuyez sur **Demandes de changement**. Affichez la liste des demandes de changement associées à cet enregistrement. ◦ Lorsqu'il est affiché, appuyez sur l'icône de menu (dans le coin supérieur droit d'un écran pour afficher les options de rattrapage disponibles.

L'image suivante illustre le chemin de navigation entre l'enregistrement de la tâche de rattrapage et l'enregistrement de la solution préférée pour la vulnérabilité sélectionnée. Parcourez les enregistrements et les listes connexes pour afficher les solutions, les mesures de déploiement et les éléments à traiter.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chemin de navigation depuis la tâche de rattrapage jusqu'à un enregistrement de solution



9. Après vérification, modification ou correction, choisissez-en un pour continuer.

Option	Description
Appuyez sur une icône en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ◦ Appuyez sur l'icône Vulnerability Response pour revenir à l'écran d'accueil. ◦ Si elle est affichée, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ◦ Appuyez sur **Notification** pour afficher les notifications du et du Now PlatformApplication Réponse aux vulnérabilités mobile.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	◦ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance Now Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle Now Platform .

Affichez, réaffectez et modifiez les tâches de rattrapage qui vous sont affectées avec le Application Réponse aux vulnérabilités mobile

Affichez, affectez ou modifiez les champs des enregistrements de tâches de rattrapage qui vous sont affectés. Parcourez les enregistrements et les listes connexes pour afficher les solutions, les mesures de déploiement et les éléments à traiter.

Avant de commencer

Rôle requis : propriétaire de rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche

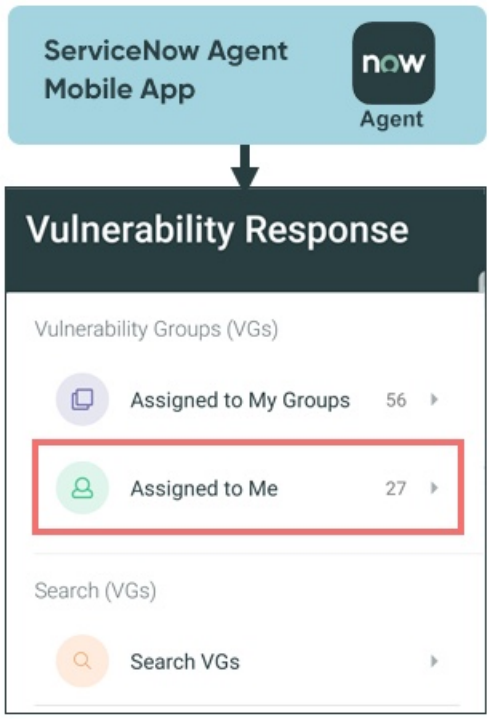
Réaffecter ou modifier les enregistrements qui vous sont affectés. Affichez les détails des enregistrements de tâches de rattrapage actifs, des enregistrements d'éléments vulnérables (VI), des vulnérabilités et des solutions avant toute modification, affectation ou correction. Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

Procédure

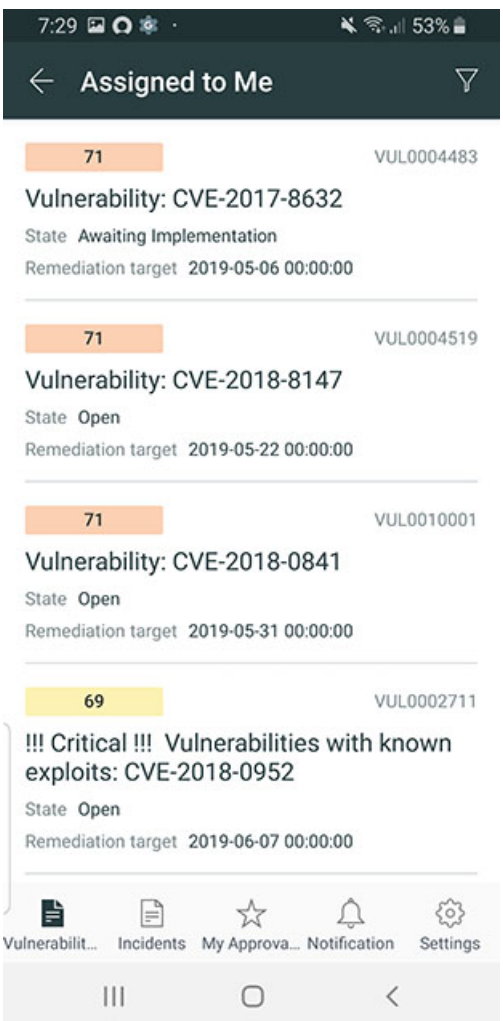
1. Si vous n'êtes pas connecté à votre Now Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Réponse aux vulnérabilités mobile.
2. Avec l'écran d'accueil de **Vulnerability Response** affiché, appuyez sur **Mes affectations**. Si vous quittez l'application Application Réponse aux vulnérabilités mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous avez affiché.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La liste des enregistrements de tâches de rattrapage qui vous sont affectés s'affiche.



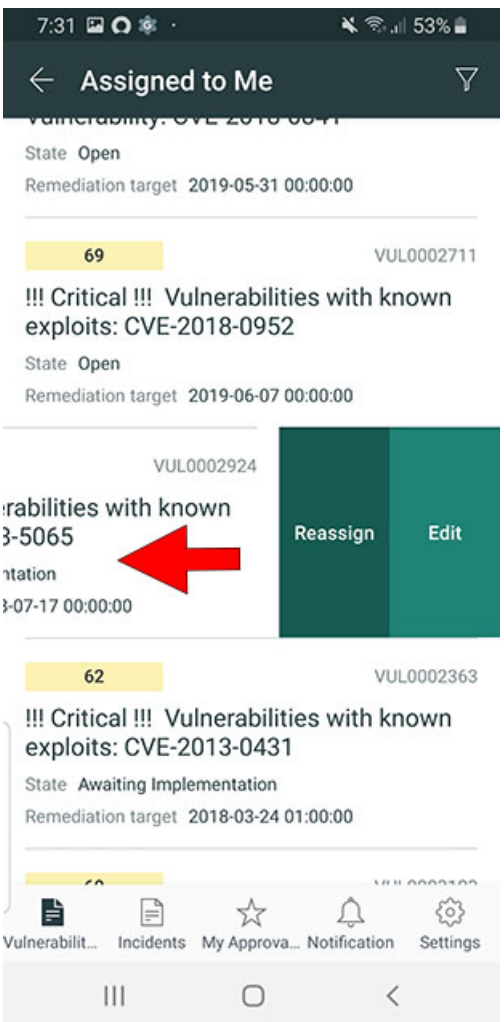
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Facultatif : Reportez-vous à Rechercher des tâches de rattrapage avec l'attribut Application Réponse aux vulnérabilités mobile pour rechercher les enregistrements qui correspondent à des critères spécifiques.

4. Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste.
   Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le Now Platform.

5. Pour réaffecter ou modifier l'enregistrement directement à partir de la liste, avec l'écran Affecté à moi affiché, balayez un enregistrement vers la gauche pour ouvrir le menu.



6. Choisissez-en un pour continuer.

Option	Description
Réaffecter	Pour réaffecter la tâche à un autre groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste affichée ou saisissez du texte dans le champ de recherche. Pour affecter ou réaffecter le RT à un membre d'un groupe d'affectation :

Traduction automatique

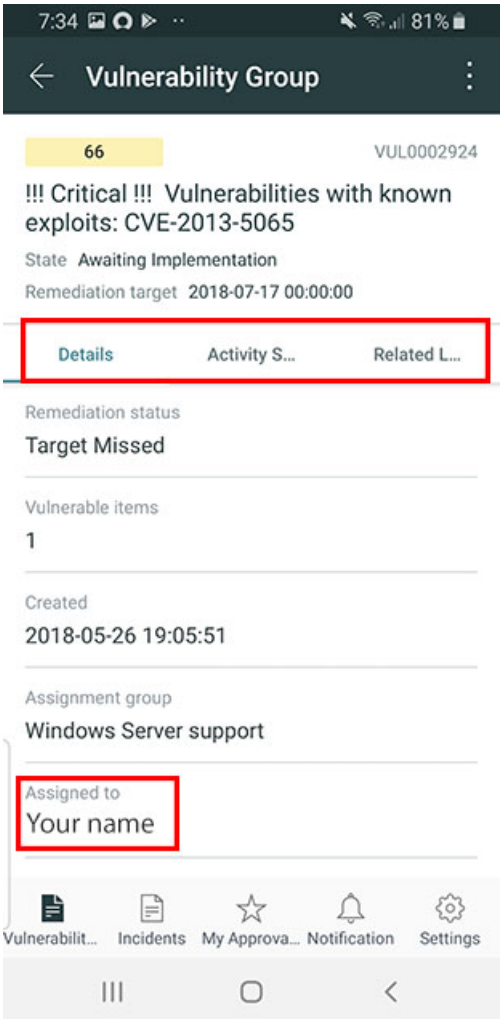
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste affichée ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône Envoyer (ou sur **Soumettre** pour enregistrer et soumettre vos modifications.
Modifier	**a.** Appuyez sur **Modifier**. **b.** Développez les champs et sélectionnez une option dans la liste qui s'affiche ou saisissez du texte. **c.** Appuyez sur l'icône d'envoi ( ) ou **sur Soumettre** pour enregistrer et soumettre vos modifications.

7. Alternativement, pour afficher les détails d'un enregistrement ouvert et pour afficher plus d'enregistrements associés et de listes connexes, avec l'écran Affecté à moi affiché, appuyez sur un enregistrement de la liste.
8. Dans l'enregistrement de tâche de rattrapage ouvert qui s'affiche, choisissez une option dans la table suivante pour afficher les notes de travail ou les listes connexes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Onglet Détails	Avec l'onglet Détails sélectionné, examinez les champs de l'enregistrement de tâche de rattrapage. Appuyez sur l'icône de menu ( ) en haut à droite de l'écran pour afficher les options disponibles. Les options affichées dans ce menu développé varient. Les actions de rattrapage que vous pouvez entreprendre sur vos éléments vulnérables varient et dépendent de la valeur affichée dans le champ État de l'enregistrement. Pour plus d'informations sur le champ État et les options de rattrapage, reportez-vous à la section Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, choisissez-en un pour continuer. ◦ Affichez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Ap-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	puyez sur l'icône plus (pour ajouter une note de travail ou joindre un fichier. ◦ Appuyez sur l'icône de menu (en haut à droite de l'écran pour afficher les options de rattrapage disponibles.
Onglet Listes connexes	Avec l'onglet Liste connexe sélectionné, affichez les listes connexes de l'enregistrement qui sont remplies. ◦ Appuyez sur **Demandes de changement**. Affichez la liste des demandes de changement associées à cet enregistrement. ◦ Appuyez sur **Éléments vulnérables**. Appuyez sur un enregistrement d'élément vulnérable (VI) et accédez à l'enregistrement de solution préféré. Reportez-vous à la figure qui suit le tableau pour une carte de navigation et plus de détails. ◦ Lorsqu'il est affiché, appuyez sur l'icône de menu (en haut à droite de l'écran pour afficher les options de rattrapage disponibles.

L'image suivante illustre le chemin de navigation entre l'enregistrement de la tâche de rattrapage et l'enregistrement de la solution préférée pour la vulnérabilité sélectionnée. Parcourez les enregistrements et les listes connexes pour afficher les solutions, les mesures de déploiement et les éléments à traiter.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chemin de navigation depuis RT jusqu'à un enregistrement de solution



9. Choisissez-en un pour continuer.

Option	Description
Appuyez sur une icône en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ◦ Appuyez sur l'icône Vulnerability Response pour revenir à l'écran d'accueil. ◦ Si elle est affichée, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ◦ Appuyez sur **Notification** pour afficher les notifications du et du Now PlatformApplication Réponse aux vulnérabilités mobile. ◦ Appuyez sur **Paramètres** et choisissez-en un pour continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	▪ Affichez des informations sur l'instance Now Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle Now Platform . Pour vous connecter, appuyez sur **Déconnexion**.

Rechercher des tâches de rattrapage avec l'attribut Application Réponse aux vulnérabilités mobile

Recherchez les tâches de rattrapage qui correspondent aux critères de recherche spécifiques que vous sélectionnez.

Avant de commencer

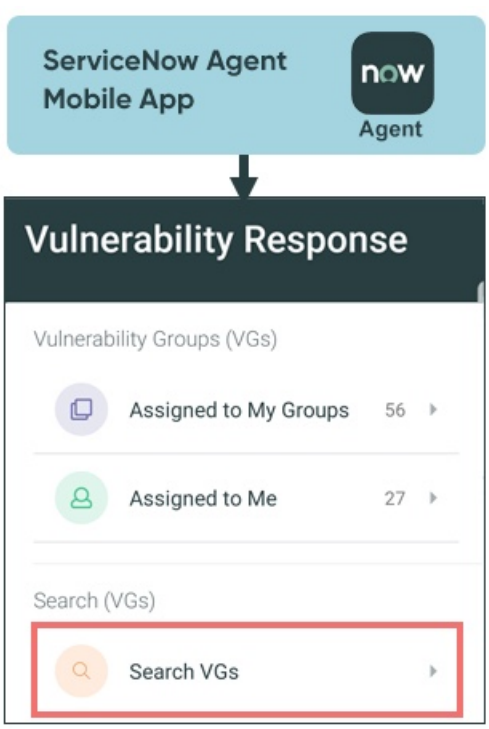
Rôle requis : propriétaire de rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche

Temps nécessaire pour accomplir cette tâche : 5 à 7 minutes.

Procédure

1. Si vous n'êtes pas connecté à votre Now Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Réponse aux vulnérabilités mobile.
2. Avec l'écran d'accueil de **Vulnerability Response** affiché, appuyez sur **Rechercher les RT.** Si vous quittez l'application Application Réponse aux vulnérabilités mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous avez affiché.



3. Sur l'écran de recherche qui s'affiche, appuyez sur les champs et remplissez le formulaire avec les critères de recherche souhaités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suivez les instructions après la table pour modifier des critères de recherche, effacer des critères de recherche ou soumettre une recherche.

Appuyer sur ce champ	**Pour ajouter une entrée sur** Android **les appareils**	**Pour ajouter une entrée sur** iOS **les appareils**
Numéro	Appuyez sur l'écran et saisissez un numéro RT, par exemple (VUL0002372) Ce numéro s'affiche en haut à droite de l'enregistrement RT. Appuyez sur l'icône en forme de coche pour ajouter votre entrée et revenir à l'écran Rechercher des RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher des RT.	Entrez un numéro RT, par exemple (VUL0002372). Ce numéro est affiché dans le coin supérieur droit de l'enregistrement RT. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
Cote de risque	Appuyez sur un ou plusieurs éléments suivis de l'icône de coche pour ajouter votre entrée et renvoyer l'écran Rechercher des RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher des RT.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments, ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
État du rattrapage	Appuyez sur un ou plusieurs éléments suivis de l'icône de coche pour ajouter votre entrée et renvoyer l'écran Rechercher des RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher des RT.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments, ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
État	Appuyez sur un ou plusieurs éléments suivis de l'icône de coche pour ajouter votre entrée et renvoyer l'écran Rechercher des RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher des RT.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments, ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appuyer sur ce champ	Pour ajouter une entrée sur Android les appareils	Pour ajouter une entrée sur iOS les appareils
		l'entrée et revenir à l'écran Rechercher des RT.
Motif	Appuyez sur un ou plusieurs éléments suivis de l'icône de coche pour ajouter votre entrée et renvoyer l'écran Rechercher des RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher des RT.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments, ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
Groupe d'affectation	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**.	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**.
Affecté à	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**.	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**.
Description brève	Appuyez sur l'écran et saisissez du texte. La fonctionnalité reconnaît les chaînes de texte et les chaînes de texte partielles dans ce champ, mais les caractères génériques (*) ne sont pas acceptés. Les majuscules ne sont pas obligatoires. Appuyez sur l'icône en forme de coche pour ajouter votre entrée et revenir à l'écran Rechercher des RT.	Saisissez du texte sur l'écran. La fonctionnalité reconnaît les chaînes de texte et les chaînes de texte partielles dans ce champ, mais les caractères génériques (*) ne sont pas acceptés. Les majuscules ne sont pas obligatoires. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
Description	Appuyez sur l'écran et saisissez du texte. La fonctionnalité reconnaît les chaînes de texte et	Saisissez du texte sur l'écran. La fonctionnalité reconnaît les chaînes de texte et les chaînes

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appuyer sur ce champ	Pour ajouter une entrée sur Android les appareils	Pour ajouter une entrée sur iOS les appareils
	les chaînes de texte partielles dans ce champ, mais les caractères génériques (*) ne sont pas acceptés. Les majuscules ne sont pas obligatoires. Appuyez sur l'icône en forme de coche pour ajouter votre entrée et revenir à l'écran Rechercher des RT.	de texte partielles dans ce champ, mais les caractères génériques (*) ne sont pas acceptés. Les majuscules ne sont pas obligatoires. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran SearchRTs.

Pour Android les appareils, une fois que l'écran Rechercher les RT s'affiche et que tous vos critères sont entrés, choisissez-en un pour continuer.

Option	Description
Effacer ou modifier les critères de recherche avant d'exécuter une recherche	Pour effacer tous les critères saisis, avec l'écran Rechercher les RT affiché, appuyez sur la flèche arrière pour effacer tous les champs et revenir à l'écran d'accueil de Vulnerability Response. La recherche n'est pas envoyée et les critères de recherche sont effacés. Alternativement, pour modifier un champ, ◦ Avec l'écran Rechercher les RT affichés, appuyez sur un champ avec des critères de recherche pour le développer. ◦ Appuyez sur un élément pour le désélectionner. Appuyez sur Tout pour sélectionner tous les éléments. Appuyez à nouveau sur **Tout** pour effacer tous les éléments. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**. ◦ Appuyez sur l'icône en forme de coche pour enregistrer les changements et revenir à l'écran Rechercher des RT.
Soumettre une recherche	Avec l'écran Rechercher des RT s'affichant avec les critères de recherche que vous avez saisis, appuyez sur l'icône d'envoi () Les enregistrements de tâche de rattrapage qui correspondent à vos critères de recherche s'affichent. Une fois la recherche terminée, les critères de recherche ne sont pas enregistrés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Pour iOS les appareils, avec l'écran Rechercher les RT affiché, choisissez-en un pour continuer.

Option	Description
Effacer ou modifier les critères de recherche avant d'exécuter une recherche	Pour effacer tous les critères et revenir à l'écran d'accueil, appuyez sur l'icône de fermeture (X). Les critères de recherche saisis ne sont pas enregistrés. Vous pouvez également modifier un champ : **a.** Avec l'écran Rechercher les RT affichés, appuyez sur un champ avec des critères de recherche pour le développer. **b.** Appuyez sur un élément de la liste pour le désélectionner ou appuyez sur **Tout effacer**. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**. **c.** Appuyez sur **Terminé** pour enregistrer les modifications et revenir à l'écran Rechercher des RT.
Soumettre une recherche	Avec l'écran Rechercher des RT s'affichant avec les critères de recherche que vous avez saisis, appuyez sur **Rechercher**. Les enregistrements RT qui correspondent à vos critères de recherche s'affichent. Une fois la recherche terminée, les critères de recherche ne sont pas enregistrés.

5. Facultatif : Si votre recherche renvoie plusieurs enregistrements, vous pouvez Filtrer les enregistrements avec l'attribut Application Réponse aux vulnérabilités mobile affiner les résultats de la recherche.

Filtrer les enregistrements avec l'attribut Application Réponse aux vulnérabilités mobile

Définissez des filtres supplémentaires pour limiter le nombre d'enregistrements qui s'affichent sur un écran. Le filtrage des enregistrements au sein de l'application mobile fonctionne comme avec un créateur de conditions sur Now Platform.

Avant de commencer
Rôle requis : propriétaire de rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche
Temps d'exécution de cette tâche : 5 minutes.

Procédure

1. Pour affiner les résultats de votre recherche ou pour entrer des critères de filtrage supplémentaires sur toute liste d'enregistrements affichée, appuyez sur l'icône de filtre (icône 
2. Une fois l'écran Filtres affiché, appuyez sur un champ pour le développer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le champ État est un champ courant pour entrer des critères de recherche pour les enregistrements de tâches de rattrapage.

3. Dans les options qui s'affichent, cochez la case ou appuyez sur un élément pour votre filtre.
   Pour de nombreux filtres, vous pouvez sélectionner plus d'une option.
4. Appuyez sur l'icône Retour (Back ou sur **TERMINÉ** pour enregistrer vos modifications dans un champ.
   Les critères que vous avez choisis s'affichent sur l'écran Filtres. Le nombre d'enregistrements qui correspondent à vos critères est également affiché en haut de l'écran. Appuyez sur **RESET** pour supprimer tous les filtres et rétablir le paramètre par défaut.
5. Facultatif : Répétez les étapes 1 à 4 avec l'écran Filtres affiché pour continuer à définir vos critères de filtrage.
6. Appuyez sur l'icône d'intersection (pour créer des conditions ET.
7. Vous pouvez également appuyer sur l'icône d'intersection ( ) pour créer des conditions OU.
8. Une fois que vous avez ajouté tous les critères que vous souhaitez, avec l'écran Filtres affiché, appuyez sur **TERMINÉ**.
   À l'écran, seuls les enregistrements qui correspondent à vos critères de filtrage s'affichent.

Information associée

Rechercher des tâches de rattrapage avec l'attribut Application Réponse aux vulnérabilités mobile

Orchestration de Vulnerability Response

Avec Orchestration de la réponse aux vulnérabilités les workflows et les activités, vous pouvez interagir et récupérer des données à partir de systèmes et d'environnements Windows ou UNIX à l'aide de l'orchestration de workflow. En enrichissant les données, vous pouvez raccourcir le cycle de vie de la correction.

Pour en savoir plus sur la modification des workflows ou la création de workflows personnalisés, reportez-vous à la section Exploration des flux .

Orchestration de la réponse aux vulnérabilités Workflows et activités

Plusieurs workflows sont inclus avec Orchestration de la réponse aux vulnérabilités. Les workflows et les activités automatisent et accélèrent vos processus. Utilisez les workflows et les activités pour créer des enregistrements d'analyse, analyser des éléments vulnérables, créer des enregistrements d'analyse, etc.

Réponse aux vulnérabilités - Workflow d'analyse de vulnérabilité

Automatisez les analyses de vulnérabilité pour un ou plusieurs éléments vulnérables à l'aide du workflow **Vulnerability Response - Analyser la vulnérabilité** inclus dans le système de base.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

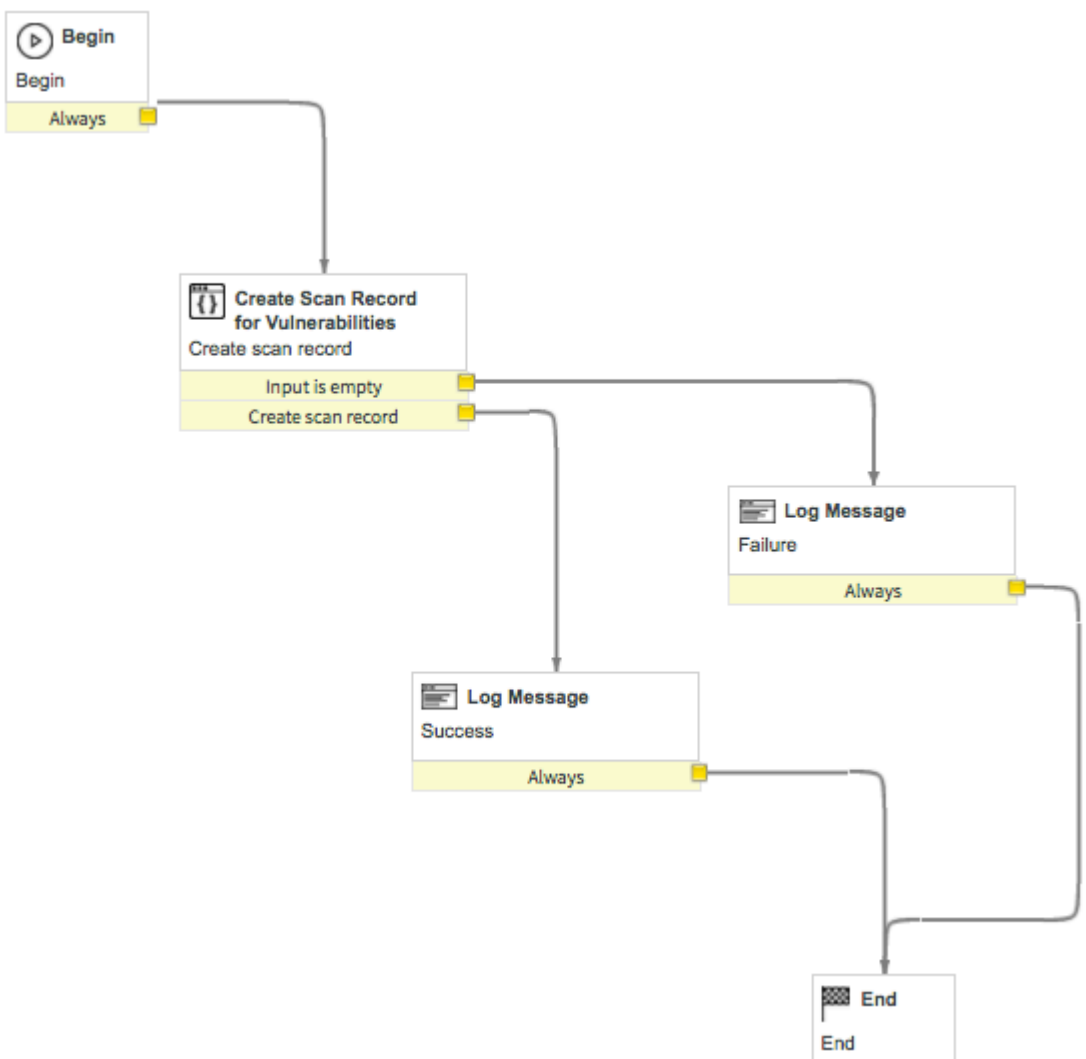
Pourquoi et quand exécuter cette tâche
Le workflow **Réponse aux vulnérabilités - Analyser la vulnérabilité** crée un enregistrement d'analyse pour la vulnérabilité ou le groupe de vulnérabilités à partir duquel il a été invoqué.

Remarque :

- Il est recommandé d'analyser à nouveau les vulnérabilités ou les éléments vulnérables après le rattrapage, lorsqu'un correctif de vulnérabilité est appliqué aux enregistrements affectés. Vous pouvez effectuer une nouvelle analyse à l'aide de la méthode décrite ou automatiser les nouvelles analyses.
- À partir de la version 23.0 de , le workflow Réponse aux Réponse aux vulnérabilités**vulnérabilités - Analyser la vulnérabilité** est déconseillé et remplacé par le flux Analyser de nouveau la vulnérabilité dans le Flow Designer.

Les activités du workflow incluent Variables pour l'activité Créer un enregistrement d'analyse pour l'activité Vulnérabilités

Vulnerability Response - Workflow Analyser la vulnérabilité



Workflow Analyser la vulnérabilité

Le champ **Réponse aux vulnérabilités** > **Analyser la vulnérabilité** Le workflow analyse à nouveau une tâche de rattrapage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : aucun

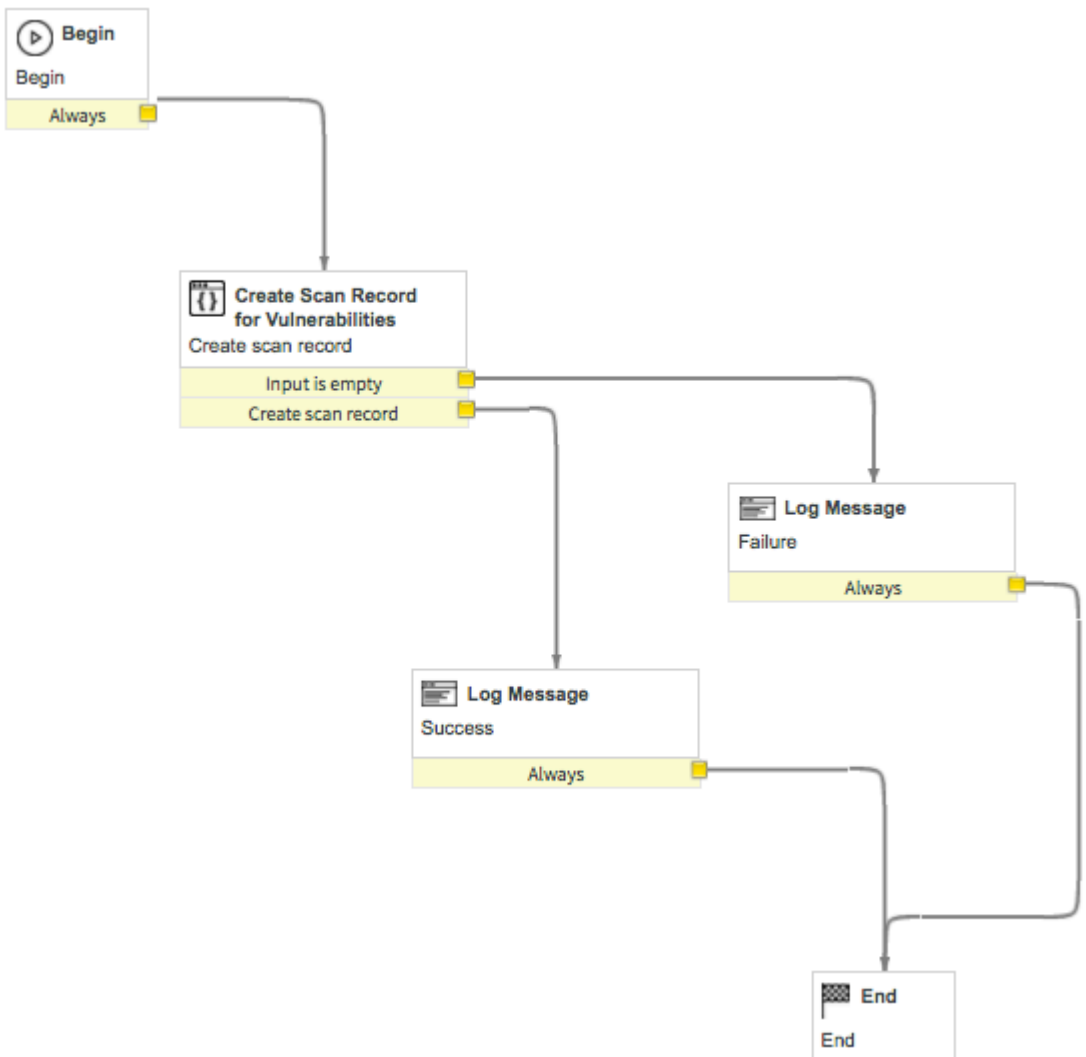
Pourquoi et quand exécuter cette tâche
Ce workflow est déclenché par **une nouvelle analyse du groupe vulnérable** lors d'une action **Fermer/Ignorer** .

Les activités de processus du workflow comprennent :

Variables pour l'activité Créer un enregistrement d'analyse pour l'activité Vulnérabilités

Journaliser le message

Workflow Analyser la vulnérabilité



Traduction automatique

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Ouvrir un enregistrement de tâche (VUL).
3. Cliquez sur **Fermer**.
4. Choisissez **Fermé** pour **l'état souhaité**.
5. Choisissez **Fixe** pour le **sous-état**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Choisissez **Attendre la confirmation de la prochaine analyse** pour **Fermer maintenant ?** Pour la tâche de rattrapage et les éléments vulnérables, **l'état** passe à **En attente de confirmation**, le **sous-état** passe à **Corrigé** et une nouvelle analyse est exécutée.

Réponse aux vulnérabilités - Workflow d'analyse des éléments vulnérables

Automatisez les analyses de vulnérabilité pour un ou plusieurs éléments vulnérables à l'aide du workflow **Réponse aux vulnérabilités - Analyser les éléments vulnérables** inclus dans le système de base.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Le workflow **Réponse aux vulnérabilités - Analyser les éléments vulnérables** crée un enregistrement d'analyse pour l'élément vulnérable ou le groupe d'éléments à partir duquel il a été invoqué.

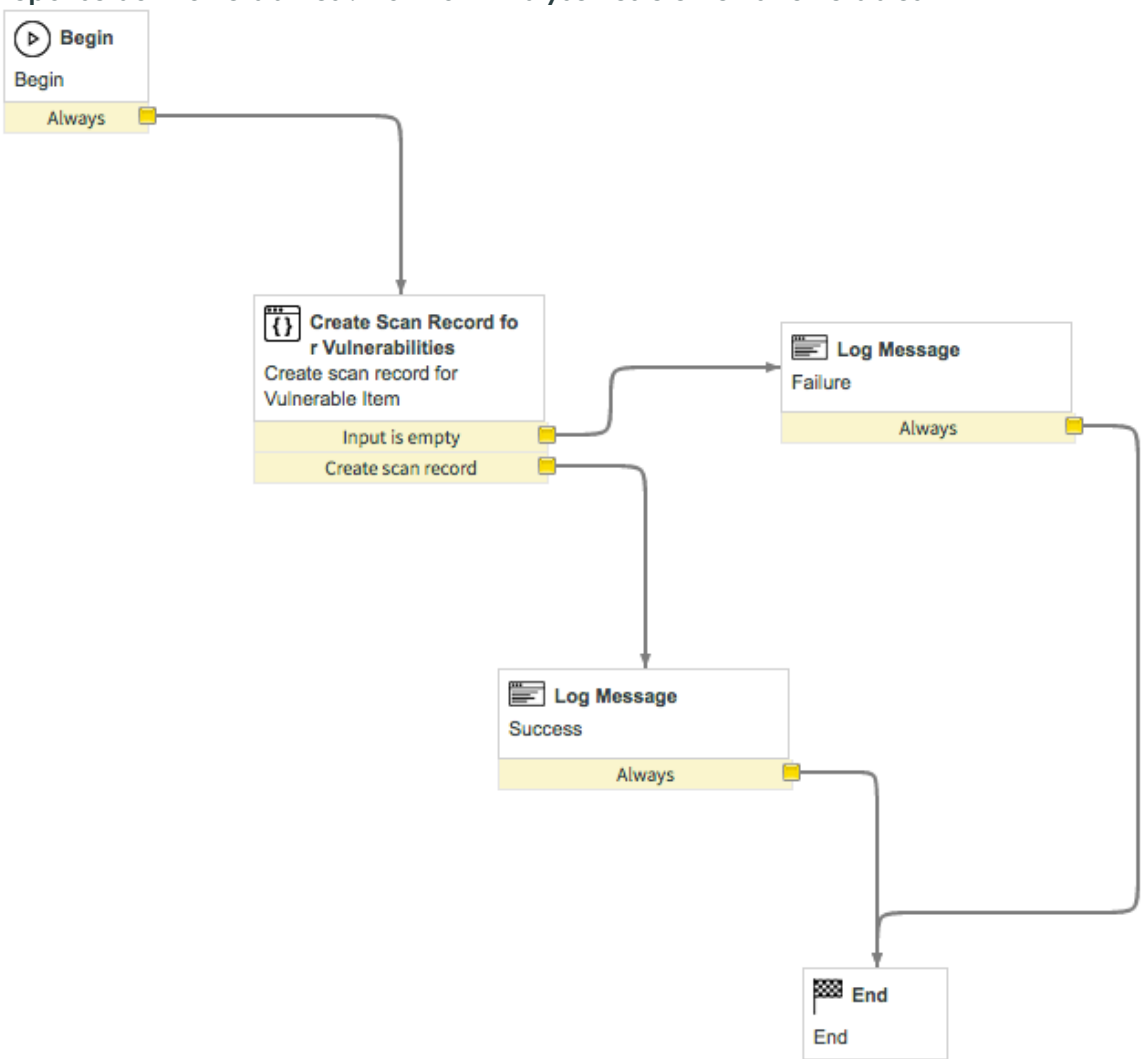
Remarque :

- Il est recommandé d'analyser à nouveau les vulnérabilités ou les éléments vulnérables après le rattrapage lorsqu'un correctif de vulnérabilité est appliqué aux enregistrements affectés. Vous pouvez effectuer une nouvelle analyse à l'aide de la méthode décrite ou automatiser les nouvelles analyses.
- À partir de la version 23.0 de Réponse aux vulnérabilités, le workflow **Réponse aux vulnérabilités - Analyser les éléments vulnérables** est déconseillé et remplacé par le flux Analyser de nouveau l'élément vulnérable dans le concepteur de flux.

Les activités de processus du workflow comprennent : Variables pour l'activité Créer un enregistrement d'analyse pour l'activité Vulnérabilités

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités : workflow Analyser les éléments vulnérables



Traduction automatique

Workflow d'élément de vulnérabilité de l'analyse

Le champ**Réponse vulnérable** > **Analyser l'élément de vulnérabilité** Le workflow analyse à nouveau un élément vulnérable.

Avant de commencer

Rôle requis : aucun

Pourquoi et quand exécuter cette tâche

Ce workflow est déclenché par **une nouvelle analyse de vulnérabilité**, lors d'une action **Fermer/Ignorer** .

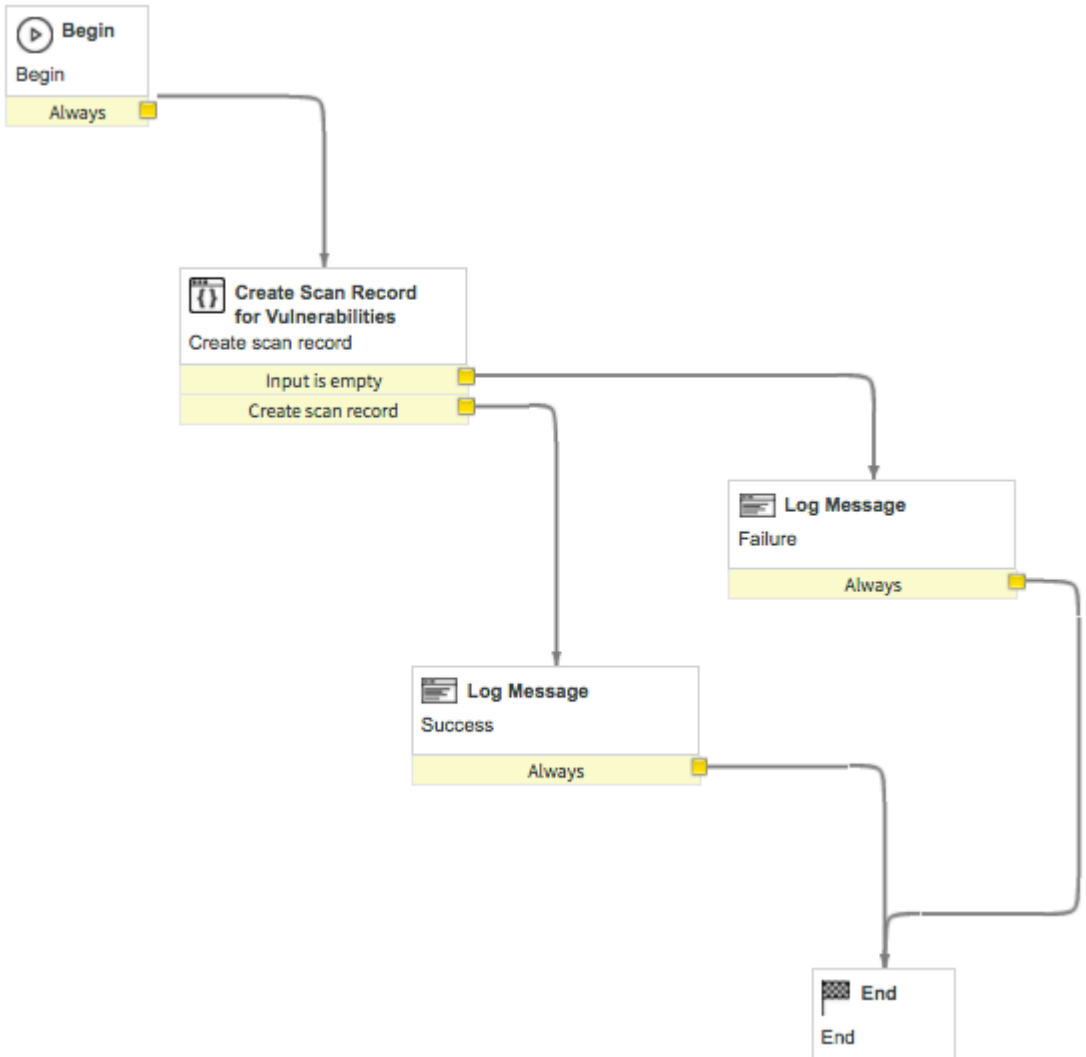
Les activités de processus du workflow comprennent :

Variables pour l'activité Créer un enregistrement d'analyse pour l'activité Vulnérabilités

Journaliser le message

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow Analyser la vulnérabilité



Traduction automatique

Procédure

1. Accédez à la **Vulnérabilité** > **Vulnérabilités** > **Éléments vulnérables**.
2. Ouvrez un élément de vulnérabilité.
3. Cliquez sur **Fermer/Ignorer**.
4. Choisissez **Fermé**pour **l'état souhaité**.
5. Choisissez **Fixe** pour le **sous-état**.
   L'état du groupe passe à **En attente de confirmation**, le **sous-état** passe à **Corrigé** et une nouvelle analyse est exécutée.

Orchestration de la réponse aux vulnérabilités Activités du workflow

Orchestration de la réponse aux vulnérabilités Les activités permettent aux utilisateurs de déterminer si une vulnérabilité a déjà été vue dans d'autres incidents de sécurité ou sur d'autres systèmes à l'aide d'Orchestration de workflow.

Variables pour l'activité Créer un enregistrement d'analyse pour l'activité Vulnérabilités

Les analyses de vulnérabilité pour un ou plusieurs éléments vulnérables peuvent être exécutées à l'aide de l'activité **de workflow Créer un enregistrement d'analyse pour les vulnérabilités** incluse dans le système de base. Lorsque l'entrée est transmise à l'activité, un enregistrement d'analyse est créé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
taskids [chaîne]	Une chaîne de sysId séparés par des virgules qui définissent les entrées attendues. Ce champ est obligatoire.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
scanResult [booléen]	Renvoie la valeur true si l'entrée n'est pas vide. Un enregistrement d'analyse est créé pour les taskIds.

Application Vulnerability Response

La Réponse aux vulnérabilités des applications fonctionnalité (AVR) de l'application importe les éléments vulnérables de l'application ServiceNow® Réponse aux vulnérabilités (AVIT) et, selon les règles, vous permet de corriger les vulnérabilités des applications. Réponse aux vulnérabilités est disponible par abonnement distinct.

À partir de la version 19.0 d'AVR, certains noms de tables et de colonnes clés ont été mis à jour. Par conséquent, vous verrez des références aux noms plus anciens et plus récents dans la documentation. Pour obtenir la liste complète des termes mis à jour, reportez-vous à la section Vue du produit Réponse aux vulnérabilités des applications.

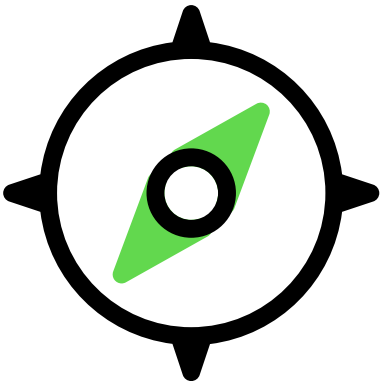
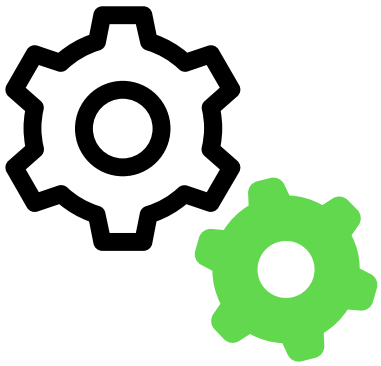
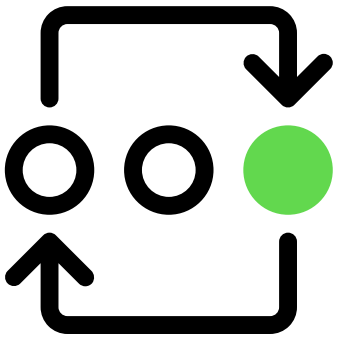
À partir de la version 19.0 de , vous pouvez ingérer des données d'analyse de composition logicielle Réponse aux vulnérabilités(SCA) et de nomenclature logicielle (SBOM) pour vous aider à identifier les faiblesses de vos applications logicielles. Pour plus d'informations, consultez Explorer Nomenclature logicielle et Veracode Vulnerability Integration.

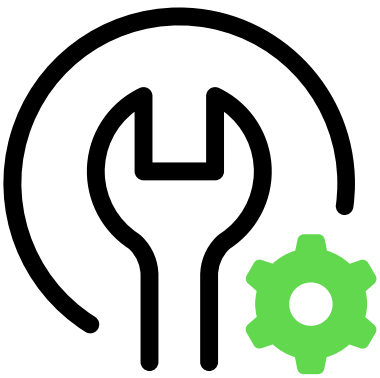
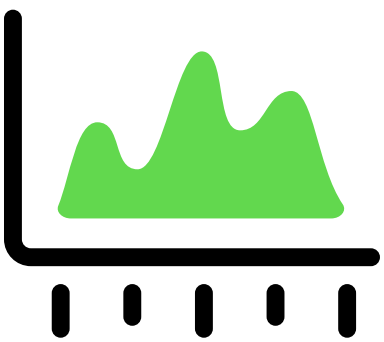
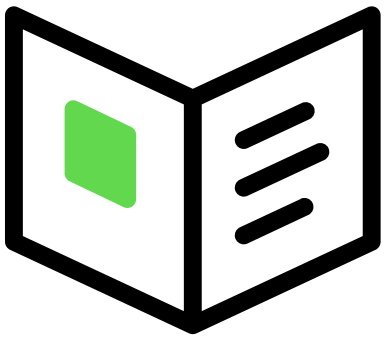
À partir de la version 18.0 de Réponse aux vulnérabilités, vous pouvez surveiller et corriger les AVIT dans Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT respectivement. Pour plus d'informations, consultez Espace de travail du gestionnaire de vulnérabilités et Exploration de l'Espace de travail de remédiation ITEspace de travail de remédiation IT.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications

Explorer	Configurer	Intégrer
		
Découvrez les concepts et les fonctionnalités d'Application Vulnerability Response.	Configurez Application Vulnerability Response.	Étendre Application Vulnerability Response en l'intégrant à d'autres applications.

Corriger	Analyse et génération de rapports	Référence
		
Découvrez comment corriger des vulnérabilités d'applications.	Afficher l'analyse Application Vulnerability Response	Obtenir des détails sur les composants d'Application Vulnerability Response tels que les champs, les tables et les propriétés.

Traduction automatique

Explorer Réponse aux vulnérabilités des applications

Les vulnérabilités d'application sont des vulnérabilités sur vos applications logicielles personnalisées qui sont analysées tout au long du cycle de vie de développement de l'application.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble Réponse aux vulnérabilités des applications et versions disponibles

Réponse aux vulnérabilités des applications (AVR) est la partie de l'application qui traite les vulnérabilités de l'application Réponse aux vulnérabilités .

Versions disponibles

Version	Notes de publication
Réponse aux vulnérabilités v23.0 Réponse aux vulnérabilités v22.0 Réponse aux vulnérabilités v21.0 Réponse aux vulnérabilités v20.0 Réponse aux vulnérabilités v19.0 Réponse aux vulnérabilités v18.2	Notes de publication Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Fonctionnement

Les données de vulnérabilité sont importées de sources internes et externes, telles que Common Weakness Enumeration (CWE) ou d'intégrations tierces. Une fois les données importées, elles sont comparées aux données d'application dans votre Base de données de gestion des configurations (CMDB) application et traitées dans l'application Réponse aux vulnérabilités des applications . S'il existe une correspondance entre les données de vulnérabilité de l'application importées et les données de votre CMDB, un élément vulnérable de l'application (AVIT) est créé.

Il Réponse aux vulnérabilités des applications comprend les fonctionnalités clés suivantes :

- Intégrez des scanners tiers pris en charge pour importer des données de vulnérabilité.
- Comparez les données liées à la vulnérabilité de l'application et déterminez si des vulnérabilités de l'application sont détectées dans une application.
- Prioriser, corriger et gérer les éléments vulnérables de l'application (AVIT). Chaque vulnérabilité d'application représente une entrée de vulnérabilité dans la CWE ou dans les bibliothèques tierces.
- À partir de la version 18.0 de Réponse aux vulnérabilités, vous pouvez surveiller et corriger les AVIT dans et respectivement Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT . Pour plus d'informations, consultez Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT.
- Corrélez Réponse aux vulnérabilités des applications les données à l'aide de calculatrices et de bibliothèques pour vous aider à effectuer les tâches suivantes.
  - Créez automatiquement des éléments vulnérables d'application à l'aide des **règles de recherche de CI**. Pendant l'importation, des vulnérabilités tierces sont associées à une CWE pour créer un AVIT.
  - Créez des règles d'affectation pour automatiser les affectations d'éléments vulnérables d'application.

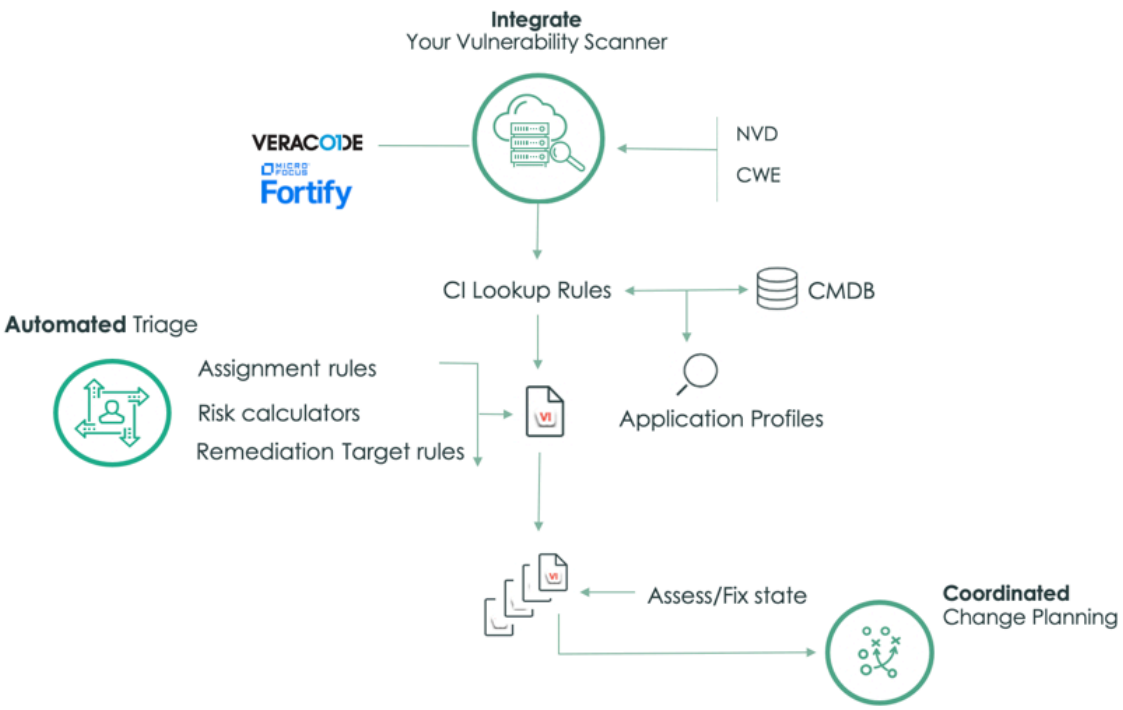
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Utilisez des groupes de calculateurs pour déterminer l'impact sur l'entreprise, spécifier différentes conditions à l'aide de filtres, appliquer des calculs simples ou utiliser un script.
- Créez des règles de cibles de rattrapage qui définissent le délai prévu pour le rattrapage des éléments vulnérables de l'application afin de surveiller les activités de rattrapage à venir.

- Associez une seule vulnérabilité tierce à plusieurs entrées CWE et trouvez la CWE primaire pour une vulnérabilité afin de vous aider à déterminer le risque. Pour plus d'informations sur **CWE primaire**, reportez-vous à la section Champs de vulnérabilité de l'application.
- Utilisez les enregistrements CWE qui sont téléchargés à partir de la base de données CWE ou importés à partir d'intégrations tierces pour référence afin de vous aider à décider si vous devez remonter une vulnérabilité. Chaque enregistrement CWE inclut également un article de la base de connaissances associé qui décrit la faiblesse.

Permet Réponse aux vulnérabilités des applications de suivre le flux d'informations, de l'intégration à la résolution, en passant par l'enquête.



Types de données de vulnérabilité importées

Réponse aux vulnérabilités des applications prend en charge les types suivants de données de vulnérabilité des applications importées.

Remarque : Avant la version 19.0, les données SAST, SCA, IAST et les tests d'intrusion n'étaient pas ingérées et pouvaient expliquer les différences entre ce qui est affiché dans Veracode, Fortifyet Invicti et ce qui apparaît dans Réponse aux vulnérabilités des applications.

Test dynamique de sécurité des applications (DAST)

Les analyses DAST détectent les vulnérabilités des applications en envoyant des entrées à vos applications et en surveillant leurs réponses pendant qu'elles sont en cours d'exécution. Cette approche pourrait imiter une attaque extérieure. Au cours de l'analyse dynamique, une URL de service en cours d'exécution est

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

analysée pour détecter les vulnérabilités. Les résultats de vulnérabilité incluent l'emplacement URL d'une vulnérabilité détectée.

Test statique de sécurité des applications (SAST)

Les analyses SAST examinent le code source des applications au repos et vous aident à trouver des vulnérabilités dans la façon dont vous avez écrit votre code. L'analyse SAST a lieu sur du code source non compilé et existe donc indépendamment de tout service d'application. Les résultats renvoyés incluent l'emplacement d'un fichier et d'un numéro de ligne d'une vulnérabilité détectée.

Test interactif de sécurité des applications (IAST)

Les analyses IAST détectent les vulnérabilités logicielles en interagissant avec le programme pendant qu'il est en cours d'exécution. L'observation humaine, les tests automatisés et les capteurs sont utilisés en combinaison pour interagir avec l'application afin de localiser les vulnérabilités.

Analyse de la composition logicielle (SCA)

À partir de la version 19.0 de , vous pouvez ingérer des vulnérabilités telles Réponse aux vulnérabilitésque Software Composition Analysis (SCA). Données de vulnérabilité SCA pour vous aider à identifier les faiblesses des logiciels open source utilisés dans vos applications logicielles.

Test de pénétration

Vous configurez des demandes d'évaluation de test de pénétration pour Réponse aux vulnérabilités des applications vous aider à comprendre où se trouvent les faiblesses de votre application et ce que vous pouvez faire pour les corriger.

Nomenclature logicielle

Chargez Nomenclature logicielle (SBOM) des données pour identifier les vulnérabilités dans vos composants open source. Consultez Explorer Nomenclature logicielle pour plus d'informations.

Cas d'utilisation

Certains des cas d'utilisation DAST suivants sont pris en charge :

- Reliez chaque vulnérabilité des résultats de l'analyse à une sorte de cmdb_ci (classe enfant).
- Associez les résultats de l'analyse DAST à une application existante lorsqu'il existe un enregistrement dans l'DE Découverte ou une intégration tierceCMDB.
- Associez le résultat de l'analyse DAST à une application numérisée nouvellement insérée lorsqu'une nouvelle application n'a pas été préalablement identifiée et/ou stockée dans la CMDB.
- Stockez les résultats de l'analyse DAST pour une CMDB lorsque vous gérez vos applications dans un produit autre que ServiceNow®.
- Stockez les résultats d'analyse DAST pour une CMDB si vous les avez préalablement personnalisés à d'autres fins.
- Créez manuellement une application pour le référentiel de code source.

Certains des cas d'utilisation SAST pris en charge sont pris en charge :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Reliez chaque vulnérabilité des résultats de l'analyse à une sorte de cmdb_ci (classe enfant).
- Créez manuellement un CI pour le référentiel de code source.
- Stockez les résultats de l'analyse SAST qui n'ont pas de service d'application associé.

Intégrations tierces

Les intégrations tierces prises en charge par Réponse aux vulnérabilités des applications sont disponibles en tant qu'applications distinctes dans le ServiceNow Store. Consultez Intégrer Réponse aux vulnérabilités des applications avec d'autres applications pour plus d'informations.

Fonctionnalités principales

- Une API partagée importe les données DAST, SAST, IAST et SCA ainsi que les résultats des tests manuels au stylet. Consultez Test de pénétration.
- Une API distincte est utilisée pour importer les données SBOM. Pour plus d'informations, consultez Explorer Nomenclature logicielle et Veracode Vulnerability Integration.

Règles de recherche de CI

: Rechercher automatiquement les correspondances dans les données de l'application Base de données de gestion des configurations (CMDB).

Règles d'affectation

: Affectez automatiquement des vulnérabilités d'applications en fonction des groupes d'utilisateurs, des champs de groupe d'utilisateurs et des scripts.

Calculateurs de risque

: Hiérarchisez et évaluez automatiquement l'impact des AVIT à l'aide de calculateurs, en fonction de n'importe quel critère, à l'aide de filtres de condition.

Mappage de sévérité

: Calculez automatiquement les valeurs initiales des champs sur les éléments vulnérables de l'application. Les entrées de vulnérabilité ont à la fois une gravité de source et une gravité normalisée (en fonction du mappage de gravité). La gravité est liée à l'énumération des faiblesses courantes (CWE).

Règles de cibles de rattrapage

: Définissez le délai prévu pour le rattrapage d'un élément vulnérable de l'application.

Reporting

: Obtenez rapidement un aperçu de votre posture de sécurité, des tendances de rattrapage et des 10 principales applications ou unités business avec les AVIT les plus critiques.

Le point commun aux deux types d'analyses est la version de l'application. Une version de l'application, qui définit une chaîne **de nom** , est le point de liaison pour regrouper les résultats de vulnérabilité analysés côté scanner. De cette façon, AVR sait à quelle version de l'application les résultats appartiennent lors de l'importation des résultats d'analyse via l'intégration.

Une table enfant d'élément de configuration [cmdb_ci], Applications numérisées [sn_vul_app_scanned_application], a été créée dans l'application et le Réponse aux

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérabilités périmètre. Cette table stocke l'abstraction de la version de l'application et fournit un mappage des services par le biais de ses relations CMDB. Ils peuvent être consultés à partir du **Tout** > **Application Vulnerability Response** > **Administration** > **Applications** module. La vue de liste des applications numérisées contient le **département** et le **groupe de support** ajoutés lors de la configuration.

Éléments vulnérables de l'application (AVIT)

Pour les vulnérabilités d'application, AVR associe une vulnérabilité à une application pour créer l'enregistrement d'élément vulnérable de l'application (AVIT). En raison des multiples définitions de ce qui constitue une application dans la CMDB, Réponse aux vulnérabilités des applications limite les applications aux applications numérisées. Les applications analysées sont les applications analysées dans votre environnement identifiées par AVR **sous les** noms et **ID.** Les AVIT sont basés sur le dernier résumé de l'analyse jusqu'à ce qu'ils soient **confirmés** par le scanner. Si un AVIT n'est plus trouvé, il reste lié au résumé de l'analyse où il a été vu pour la dernière fois.

Les éléments vulnérables de l'application peuvent être affichés à partir de **Tout** > **Application Vulnerability Response** > **Vulnérabilités** > **Éléments vulnérables** module.

Si une application est supprimée de la CMDB, tous les AVIT associés sont fermés.

Pour plus d'informations sur les champs de formulaire AVIT, reportez-vous à la section Champs d'éléments vulnérables d'applications.

Groupes d'utilisateurs et rôles dans Réponse aux vulnérabilités des applications

Souvent, une équipe travaille ensemble pour créer, gérer et superviser la gestion des vulnérabilités des applications. Des rôles stratégiques, ainsi que des rôles opérationnels, sont attribués aux membres de l'équipe. Dans la plupart des organisations, vous pouvez endosser plusieurs rôles et souvent partager des rôles avec d'autres. Réponse aux vulnérabilités des applications utilise trois groupes d'utilisateurs contenant des rôles granulaires : Gestionnaire de sécurité des applications, Champion de sécurité des applications et Développeur. Consultez la rubrique Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs pour en savoir plus sur ces groupes et rôles.

Réponse aux vulnérabilités des applications États

Réponse aux vulnérabilités des applications propose un modèle d'état pour l'état des éléments vulnérables de votre application (AVIT) et vous aide à déterminer quand et comment corriger vos AVIT.

Un élément vulnérable d'application a plusieurs états possibles, consultez États des éléments vulnérables de l'application (AVI) pour plus d'informations.

Configurer Réponse aux vulnérabilités des applications

Avant de l'exécuter Réponse aux vulnérabilités des applications dans votre Now Platform instance, vous devez la configurer.

Configurer Réponse aux vulnérabilités des applications

Effectuez les étapes de configuration suivantes avant de procéder à la configuration, afin de vous assurer que votre configuration est terminée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, reportez-vous à la section Installer Réponse aux vulnérabilités.
Vérifiez que la Analyse des performances pour Réponse aux vulnérabilités est installé et activé pour afficher les Réponse aux vulnérabilités des applications rapports.	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, reportez-vous à la section Installer et configurer l'application Analyse des performances pour Réponse aux vulnérabilités [PA].
Vérifiez que le Veracode Vulnerability Integration est installé, activé et configuré. (N'exécutez pas les intégrations à ce stade.)	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, reportez-vous à la section Installer l'intégration de ServiceNow Vulnerability Response avec Veracode.
Vérifiez que l'intégration CWE 2000 s'exécute dans Réponse aux vulnérabilités.	Pour vérifier l'intégration, reportez-vous à la section Vérifiez que la tâche planifiée de mise à jour des enregistrements NVD est en cours d'exécution.
[Facultatif] Vérifiez que NVD Integration est en cours d'exécution dans Réponse aux vulnérabilités.	Pour vérifier, reportez-vous à la section Vérifiez que la tâche planifiée de mise à jour des enregistrements CWE est en cours d'exécution.
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • S'il n'est pas déjà affecté, l'utilisateur disposant du rôle administrateur installe l'application et affecte les utilisateurs aux groupes d'utilisateurs suivants : Gestionnaire App-Sec, Champion de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	sécurité et Développeur. Pour en savoir plus sur les rôles de groupe, reportez-vous à la section Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs. • Le groupe Gestionnaire de sécurité des applications supervise la configuration et vérifie les résultats attendus. **Remarque :** Réponse aux vulnérabilités des applicationsn'est pas disponible à partir de la fonctionnalité Assistant de configuration de .Réponse aux vulnérabilités

Rôle requis : groupe d'utilisateurs du gestionnaire App-Sec

Procédure

1. Accédez à la **Security Operations** > **CMDB** > **Règles de recherche**.
   Reportez-vous à la rubrique Créer une règle de recherche de CI pour créer ou modifier des règles de recherche de CI pour votre environnement.
2. Accédez à la **Application Vulnerability Response** > **Administration**.
3. Sélectionnez **Règles d'affectation**.
   Consultez Créer ou modifier des Réponse aux vulnérabilités des applications règles d'affectation pour créer ou modifier des règles d'affectation d'application pour votre environnement.
4. Sélectionnez **Calculateurs de vulnérabilité**.
   Reportez-vous à la rubrique Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications pour créer ou modifier des calculateurs de vulnérabilité d'application pour votre environnement.
5. Sélectionnez **Règles de cibles de rattrapage**.
   Reportez-vous à la rubrique Créer ou modifier des règles de cibles de rattrapage d'application pour créer ou modifier des cibles de rattrapage d'application pour votre environnement.
6. Sélectionnez des **cartes de gravité normalisées**.
   Consultez Mapper automatiquement la gravité d'un élément vulnérable de l'application pour créer ou modifier des cartes de gravité pour votre environnement.
7. Accédez à l'un ou l'autre des modèles suivants : **Intégration de vulnérabilité Veracode** > **Intégrations** ou **Fortify Vulnerability Integration** > **Intégrations**.
8. Ouvrez l'intégration de liste d'applications Veracode ou l'intégration de liste d'applications Fortify à la demande.
9. Si ce n'est pas déjà fait, sélectionnez **Exécuter maintenant**.

   Remarque : L'autre Veracode ou Fortify les intégrations sont inactives par défaut.

   Pour connaître les états d'exécution de l'intégration, consultez Afficher l'état de l'exécution de l'importation de l'intégration de vulnérabilité de l'application Veracode ou Afficher l'état de l'exécution de l'importation Fortify Vulnerability Integration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Une fois que l'intégration de la liste d'applications Veracode ou Fortify à la demande a terminé son exécution, accédez à **Application Vulnerability Response** > **Administration** > **Applications**.
11. Pour chaque application, entrez une valeur pour Groupe de **support** (utilisé par les règles d'affectation) et Département (utilisé dans **la** génération de rapports).
    Pour mettre à jour plusieurs entrées, consultez Modifier plusieurs enregistrements dans une liste à l'aide de l'éditeur de liste pour terminer la tâche en bloc.

    Remarque : Pour afficher **l'unité business** mise à jour automatiquement, actualisez la page. Pour plus d'informations sur les champs du formulaire Application numérisée, reportez-vous à la section Champs d'application analysés.

12. Revenez à la liste Intégrations et activez l'autre Veracode ou Fortify les intégrations. Consultez la rubrique Activer Réponse aux vulnérabilités des applications les intégrations pour définir vos importations d'intégration de données delta.

    Les Veracode intégrations et Fortify sont liées et s'exécutent consécutivement lorsqu'elles sont activées.

13. Facultatif : Accédez à la **Application Vulnerability Response** > **Administration** > **Règles d'affectation**.

    a. Facultatif : Si vous avez choisi **Élément de configuration : groupe de support** pour le **champ Groupe d'utilisateurs** lors de la création ou de la modification de vos règles d'affectation précédemment, les valeurs que vous avez ajoutées à la vue de liste Applications numérisées peuvent désormais être utilisées.
    Vos règles d'affectation sont modifiées.

    b. Sélectionnez **Mettre à jour**.

    c. Dans la vue de liste Règles d'affectation de vulnérabilité, sélectionnez **Appliquer les modifications** pour réappliquer les règles d'affectation à vos AVI.

Résultats
Votre Réponse aux vulnérabilités des applications configuration est maintenant terminée.

Que faire ensuite
Accédez à la **Application Vulnerability Response** > **Vue d'ensemble** et consultez le tableau de bord Gestion de la vulnérabilité des applications [PA] pour plus d'informations sur votre posture de sécurité globale.

Vérifiez que la tâche planifiée de mise à jour des enregistrements CWE est en cours d'exécution

Utilisez les enregistrements CWE (Common Weakness Enumeration) téléchargés à partir de la base de données CWE pour référence lorsque vous décidez si une vulnérabilité doit être remontée. Mettez à jour régulièrement les enregistrements de faiblesses courantes à partir de la base de données Common Weakness Enumeration. Vous pouvez également mettre à jour le script par défaut ou écrire vos propres scripts, selon vos besoins.

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec
Chaque enregistrement CWE inclut également un article de la base de connaissances associé qui décrit la faiblesse.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Intégrations**.
2. Sélectionnez la tâche planifiée **CWE Comprehensive 2000 Integration** .
3. Vérifiez que la case **Actif** est cochée.

   Remarque : Les paramètres de ce formulaire sont partagés par Réponse aux vulnérabilités et Réponse aux vulnérabilités des applications. La modification des paramètres d'intégration nécessite une coordination et une expertise dans Réponse aux vulnérabilités et ServiceNow.

4. Si la case est cochée, vous avez terminé.

   Remarque : Si la case n'est pas cochée, il peut être nécessaire de configurer cette intégration dans Réponse aux vulnérabilités. Consultez Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces pour plus d'informations avant de le sélectionner.

   Au besoin, consultez Afficher les bibliothèques de vulnérabilité pour afficher les entrées importées.

   Le champ **CWE primaire** contient l'entrée CWE. Si plusieurs CWE sont associés à une vulnérabilité, consultez Champs de vulnérabilité de l'application pour en savoir plus sur la façon dont le CWE primaire est déterminé.

Vérifiez que la tâche planifiée de mise à jour des enregistrements NVD est en cours d'exécution

Identifiez les référentiels que vous souhaitez mettre à jour régulièrement. Vous pouvez exécuter une tâche planifiée pour mettre à jour les enregistrements de la base de données de vulnérabilité nationale (NVD) tous les soirs ou toutes les semaines. Si elle n'est pas déjà en cours d'exécution, vous pouvez activer la tâche

Avant de commencer

Rôles requis : groupe de gestionnaires App-Sec

L'intégration NVD s'exécute par défaut en tant que tâche planifiée tous les lundis à 00:00:00.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Intégrations**.
2. Sélectionnez la tâche planifiée **NIST National Vulnerability Database** .
3. Vérifiez que la case **Actif** est cochée.

   Remarque : Les paramètres de ce formulaire sont partagés par Réponse aux vulnérabilités et Réponse aux vulnérabilités des applications. La modification des paramètres d'intégration nécessite une coordination et une expertise dans Réponse aux vulnérabilités et ServiceNow.

4. Si la case est cochée, vous avez terminé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si la case n'est pas cochée, il peut être nécessaire de configurer cette intégration dans Réponse aux vulnérabilités. Consultez Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces pour plus d'informations avant de le sélectionner.

Au besoin, consultez Afficher les bibliothèques de vulnérabilité pour afficher les entrées importées.

Activer Réponse aux vulnérabilités des applications les intégrations

Activer Réponse aux vulnérabilités des applications les intégrations pour effectuer des mises à jour régulières.

Avant de commencer

Rôle requis : App-Sec Manager

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Intégrations**.
2. Sélectionnez une intégration.
3. Sélectionnez la case à cocher **Activé**.
4. Sélectionnez **Mettre à jour**.
5. Répétez l'opération au besoin pour chaque intégration.
   Après l'exécution initiale, les intégrations sont chaînées pour effectuer des importations delta pour les exécutions suivantes.

Définir les Réponse aux vulnérabilités des applications notifications par e-mail

Configurez des notifications par e-mail pour partager des informations utiles sur les mises à jour et les activités importantes, telles que l'approbation et le rejet des demandes de faux positifs. La création d'une notification par e-mail implique de spécifier quand l'envoyer, qui la reçoit et ce qu'elle contient.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Modèles d'e-mail**.
2. Sélectionnez **Nouveau**.

Pour obtenir des instructions détaillées sur la création de notifications par e-mail, reportez-vous à la section Créer une notification par e-mail .

Résultats

À partir de la version 21.0 de , lorsqu'un destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans ou Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT en fonction de Réponse aux vulnérabilitésson rôle.

- Les liens s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs disposant du rôle sn_vul.app_sec_manager.
- Les liens s'ouvrent dans le Espace de travail de remédiation IT pour les utilisateurs disposant du rôle sn_vul.app_security_champion ou sn_vul.app_developer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si le destinataire n'a aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Créer ou modifier des notifications de cibles de rattrapage dans Réponse aux vulnérabilités des applications

Les administrateurs de vulnérabilité peuvent modifier les notifications de cible de rattrapage ou en ajouter de nouvelles, en spécifiant le moment d'envoi de la notification, qui reçoit la notification et quel contenu contient la notification.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Notifications**.
2. Sélectionnez l'enregistrement de notification de cible de rattrapage ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Pour plus d'informations sur les champs de formulaire, consultez Créer une notification par e-mail .
4. Sélectionnez **Prévisualiser la notification** pour afficher le message.

Résultats

À partir de la version 21.0 de , lorsqu'un destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans ou Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT en fonction de Réponse aux vulnérabilitésson rôle.

- Les liens s'ouvrent dans la section pour les Espace de travail du gestionnaire de vulnérabilités utilisateurs ayant le rôle sn_vul.app_sec_manager.
- Les liens s'ouvrent dans le Espace de travail de remédiation IT pour les utilisateurs disposant du rôle sn_vul.app_security_champion ou sn_vul.app_developer.

Si le destinataire n'a aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Gestion des exceptions dans Réponse aux vulnérabilités des applications

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive de sécurité ou de gestion des vulnérabilités publiée, vous pouvez demander une exception. La gestion des exceptions implique de demander, examiner, approuver ou rejeter des exceptions à un élément vulnérable de l'application (AVI) qui ne peuvent pas être corrigés conformément à la politique.

Certaines vulnérabilités peuvent ne pas disposer d'un correctif, d'un correctif ou d'une solution existante. Lorsqu'une exception est approuvée, cela signifie également que vous acceptez un risque, car vous reconnaissez et acceptez les conséquences de ne pas corriger la vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

À partir de la version 21.0 de Réponse aux vulnérabilités des applications, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable de l'application passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable de l'application ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Cycle de vie d'une exception

Définition d'une exception

Une exception est une demande de différer le rattrapage d'un AVI pour une période spécifiée. Par exemple, en tant que développeur, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine.

Demande d'une exception

En tant que développeur, vous pouvez demander une exemption pour un AVI à l'aide du processus de gestion des exceptions. Une fois que l'analyste de sécurité des applications a approuvé cette demande, l'AVI passe à l'état **Différé** .

Règles d'exception

À partir de la version 20, vous pouvez créer des règles d'exception pour différer automatiquement les éléments vulnérables de l'application (AVI) existants et nouveaux pendant une période spécifique s'ils correspondent aux conditions de la règle. L'utilisation de règles d'exception pour différer automatiquement les AVI minimise le risque de manquer des accords de niveau de service. Les règles peuvent vous aider à gérer plusieurs éléments, car vous éliminez une intervention manuelle. Reportez-vous à la section Créer une règle d'exception.

Demande d'extension pour une règle d'exception

À partir de la version v20, vous pouvez soumettre une demande d'extension de la date de **fin différée** d'une règle d'exception. Vous pouvez demander une extension d'une règle si vous constatez qu'un grand nombre d'enregistrements créés par la règle ne sont pas résolus par sa Date de **fin de report,** date à laquelle la tâche de rattrapage cesse d'accepter de nouveaux AVI. L'extension met à jour la règle d'exception de sorte qu'elle prolonge automatiquement la date de report de votre règle existante. Vous pouvez saisir des dates jusqu'à un an à partir de la date actuelle, et vous devez inclure un motif pour la prolongation. Une demande d'extension nécessite l'approbation à deux niveaux de groupes d'approbation distincts.

Approuver une demande d'exception

Les AVI qui ne peuvent pas être corrigés immédiatement sont examinés par des analystes de sécurité des applications, évalués pour le risque et approuvés pour le report jusqu'à ce qu'ils puissent être corrigés. L'approbation d'une demande d'exception peut être un flux à deux niveaux. Si seul l'approbateur de premier niveau est présent, l'exception peut être demandée et approuvée. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Consultez Ajouter un approbateur d'exception pour Réponse aux vulnérabilités des applications pour plus d'informations.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Une fois qu'une demande d'exception pour un AVI est approuvée, vous pouvez effectuer les actions suivantes :

- Rouvrir
- Obtenir plus de détails

Suivi d'une demande d'exception

Après avoir émis l'exception, vous pouvez suivre son état à l'aide de l'onglet **Approbations de changement d'état** de l'AVI.

Expiration d'une demande d'exception et demande d'extension d'une règle d'exception

Lorsqu'une demande d'exception pour un AVI particulier expire, l'AVI impacté revient à son état **Ouvert** .

Toutefois, à partir de la version 20, vous pouvez soumettre une demande d'extension de la date **de fin de** report sur la règle d'exception.

Configurer la gestion des exceptions pour Réponse aux vulnérabilités des applications

Limitez la durée d'une demande d'exception et ajoutez un questionnaire à la demande d'exception ou de faux positif à l'aide du module. Par défaut, une exception est demandée à l'aide du ServiceNow® Réponse aux vulnérabilités des applications module. Vous pouvez également demander une exception à l'aide de l'intégration GRC : gestion de la politique et de la conformité .

Avant de commencer

Rôle requis : sn_vul.app_manage_exception_configuration

Pourquoi et quand exécuter cette tâche

Si Réponse aux vulnérabilités cette option est activée, vous pouvez limiter la durée pendant laquelle une exception peut être demandée. De même, si le GRC : gestion de la politique et de la conformité module est installé, vous pouvez le sélectionner GRC : gestion de la politique et de la conformité sur l'écran de configuration. L'activation de cette option vous permet de demander une exception qui spécifie l'objectif de politique et de contrôle à partir de GRC.

Si vous ajoutez un questionnaire, il est envoyé à la personne qui émet l'exception ou la demande de faux positif. Vous pouvez utiliser le questionnaire par défaut ou en créer un en fonction de vos besoins.

Il est utile que l'approbateur de l'exception comprenne le motif de la demande d'exception.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire Configuration de la gestion des exceptions, sélectionnez la façon dont vous souhaitez gérer une exception en sélectionnant une option dans la liste Gérer les exceptions à l'aide de.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la Réponse aux vulnérabilités version 17.1, vous pouvez sélectionner ou GRC : gestion de la politique et de la conformitéRéponse aux vulnérabilités . Vous devez activer le GRC module d'extension à utiliser GRC : gestion de la politique et de la conformité pour demander une exception. La modification de la configuration n'a pas d'impact sur les données existantes.

3. Renseignez les champs du formulaire en fonction de l'option que vous avez sélectionnée.
   - Si vous avez sélectionné l'option Réponse aux vulnérabilités , renseignez les champs du formulaire.

Formulaire Paramètres pour VR Exception Management

Champ	Description
Durée	Période pour laquelle une exception peut être demandée.
Unité	Unité de temps pour la période spécifiée.
Activer le questionnaire pour demander une exception	Option permettant d'ajouter un questionnaire à la demande d'exception émise.
Questionnaire pour demander une exception	Option permettant d'afficher le questionnaire que vous avez sélectionné pour demander une exception. Le questionnaire d'exceptions est affiché par défaut.
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Questionnaire pour marquer comme faux positif	Option permettant d'afficher le questionnaire que vous avez sélectionné pour le marquer comme faux positif. Le questionnaire des demandes de faux positif est affiché par défaut.

   - Si vous avez sélectionné l'option GRC : gestion de la politique et de la conformité , renseignez les champs du formulaire.

Formulaire Paramètres pour VR Exception Management

Champ	Description
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Questionnaire pour marquer comme faux positif	Option permettant d'afficher le questionnaire que vous avez sélectionné pour le marquer comme faux positif. Le questionnaire des demandes de faux positif est affiché par défaut.

4. Sélectionnez **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les règles d'approbation pour la gestion des exceptions

À partir de la Réponse aux vulnérabilités des applications version 15.0, utilisez le concepteur de flux pour approuver les demandes d'exception pour la gestion des exceptions, les règles d'exception et la gestion des faux positifs. Si vous déployez Réponse aux vulnérabilités des applications (AVR) pour la première fois, Flow Designer est activé par défaut.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Si vous êtes un utilisateur VR existant, l'option par défaut est workflow.
Si vous avez déployé Réponse aux vulnérabilités des applications la version 15.0 ou ultérieure, la valeur de la propriété *sn_vul.flow_designer_activation* système est définie sur true. Cela signifie que Flow Designer est activé par défaut.

Si vous utilisez Réponse aux vulnérabilités des applications déjà une version antérieure à la version 15.0, la valeur de cette propriété système est définie sur false. Vous pouvez activer le concepteur de flux en changeant la valeur sur vrai.

Remarque : Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer. Pour une comparaison détaillée entre le workflow et Flow Designer, reportez-vous à la section Comparaison du workflow de gestion des exceptions et de Flow Designer.

Pour utiliser le concepteur de flux, créez des règles à l'aide du module Règles d'approbation. À l'aide de ce module, vous pouvez configurer des règles d'approbation pour chacun des workflows de gestion des exceptions suivants.

- Demande d'exception pour les tâches de rattrapage
- Demande d'exception pour les éléments vulnérables de l'application
- Règle d'exception
- Faux positif pour les tâches de remédiation
- Faux positif pour les éléments vulnérables de l'application

Remarque : Vous pouvez également définir des conditions contenant plusieurs niveaux d'approbation au sein d'une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant.

Procédure
1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Règles d'approbation**.
2. Sur la page Règles d'approbation, sélectionnez le groupe pour lequel vous souhaitez définir la règle d'approbation.
3. Renseignez les champs du formulaire.

Formulaire Règle d'approbation

Champ	Description
Nom	Nom de configuration de l'approbation.
Table	Table sur laquelle la règle est appliquée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	La valeur par défaut est Vulnerability Response.
Type de règle	Spécifie le type de règle. Par exemple, gestion des exceptions, faux positif ou règle d'exception.
Actif	Activé par défaut, ce qui signifie que la règle d'approbation est utilisée.
Description	Brève description des règles d'approbation.
Expiration de l'approbation (jours) À partir de la v21.0 de Réponse aux vulnérabilités des applications	Date jusqu'à laquelle l'approbateur peut approuver la demande.
Notification de l'approbateur (jours) À partir de la v21.0 de Réponse aux vulnérabilités des applications	Date après laquelle l'approbateur est invité à prendre des mesures.

4. Sélectionnez **Mettre à jour**.
   Dans l'onglet Configurations d'approbation, deux niveaux d'approbateurs sont configurés par défaut. Vous pouvez sélectionner une règle pour définir les conditions en fonction de différents cas d'utilisation au sein d'une règle.

   Remarque : Dans chaque page de configuration, vous pouvez créer plusieurs niveaux d'approbation.

Example:
En fonction des différents cas d'utilisation, vous pouvez définir différents processus d'approbation pour les mêmes vulnérabilités trouvées sur différents éléments de configuration.

Différer le rattrapage dans Réponse aux vulnérabilités des applications

À partir de la version 20.0, vous pouvez différer le rattrapage avec l'état **En attente d'implémentation** disponible pour les éléments vulnérables d'application (AVI) et les tâches de rattrapage à mesure qu'ils avancent dans leur cycle de vie. Vous pouvez uniquement faire passer manuellement les enregistrements à cet état en sélectionnant **En attente d'implémentation** à partir d'AVI et les enregistrements de tâche de rattrapage à l'état **En cours d'examen** .

Cas d'utilisation

En tant que spécialiste du rattrapage, vous pouvez déplacer un enregistrement vers **En attente d'implémentation** pour faire savoir à votre équipe que vos recherches et votre travail sur une tâche sont terminés. Vous pouvez choisir cette mise à jour si vous constatez qu'un correctif est prêt à être implémenté, mais qu'il n'est pas disponible. Un correctif logiciel est un exemple de correctif non disponible. Si la fenêtre de maintenance d'un correctif n'est pas disponible lorsque vous avez terminé votre recherche, vous pouvez déplacer la tâche vers **En attente d'implémentation** jusqu'à ce que le correctif puisse être déployé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs obligatoires

Deux champs obligatoires et modifiables sur les enregistrements AVI et de tâche de rattrapage sont à l'état En attente d'implémentation :

Date de l'engagement de rattrapage

Date de rattrapage planifiée.

Plan de rattrapage

Description du plan de rattrapage pour le rattrapage. Ce texte s'affiche dans les notes de l'enregistrement.

Champs et propriétés système

Deux propriétés système sont définies par défaut sur `vrai` pour le modal qui s'affiche lorsque vous passez un enregistrement à l'état **En attente d'implémentation**. S'ils sont conservés dans leurs paramètres par défaut :

sn_vul.remediation_fields

Définit la **date d'engagement de rattrapage** et le **plan de rattrapage** comme champs obligatoires. Si la valeur est définie sur `faux`, ces champs sont facultatifs.

sn_vul.awaiting_implementation

Affiche le modal avec la **date d'engagement** de rattrapage et les champs **Plan de rattrapage** après avoir sélectionné En **attente d'implémentation** sur un enregistrement. Si elle est définie sur `faux`, vous pouvez changer l'état d'un AVI en En attente d'implémentation sans être invité à saisir une date d'engagement ou un plan.

Module de date de l'engagement de rattrapage non respecté

Affichez tous les AVI qui ont manqué leur date d'engagement de rattrapage dans le module **Date d'engagement de rattrapage manquée** . Naviguer **Application Vulnerability Response** > **Éléments vulnérables** > **Date de l'engagement de rattrapage non respectée** pour afficher la liste.

Restauration de l'état des tâches de rattrapage vers les AVI

Le bouton d'action d'interface utilisateur pour faire passer un enregistrement en **attente d'implémentation** n'est visible que sur les enregistrements d'éléments vulnérables et de tâches de rattrapage de l'application dont l'état est **En cours d'examen** . Pour la restauration de l'état, sur le modal qui s'affiche lorsque vous sélectionnez **En attente d'implémentation** sur une tâche de rattrapage, il existe une option permettant de **remplacer les AVI existants**.

Option	Description
Sélectionnez **Remplacer les AVI existants**.	Sélectionnez cette option pour remplacer les dates d'engagement de rattrapage et les plans de rattrapage de tous les AVI existants dans la tâche déjà dans l'état **En attente d'implémentation** . Si elle est sélectionnée, cette fonctionnalité affiche la date et les données du plan sur la tâche de rattrapage vers les AVI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Laissez **le remplacement des AVI existants** désactivé.	Laissez l'option désactivée pour conserver intactes la date et les valeurs de plan de tous les AVI existants sur la tâche déjà à l'état **En attente d'implémentation** . Si cette option est désactivée, les AVI déjà en **attente d'implémentation** conservent leur date et leurs données de plan existantes et ne sont pas impactés par la restauration de l'état.

Exemples de rolldowns

Supposons que vous souhaitiez faire passer une tâche de rattrapage de **Ouverte** à En **attente d'implémentation** afin de pouvoir mettre à jour la date d'engagement de la tâche et les informations de plan pour une fenêtre de maintenance des correctifs logiciels. Supposons qu'un AVI dans cette tâche est à l'état **En attente d'implémentation** et que vous souhaitez mettre à jour sa date d'engagement et ses informations de plan pour qu'elles correspondent à la tâche de rattrapage.

Pour remplacer la date de l'AVI et les données du plan afin qu'elles correspondent à la tâche de rattrapage, cochez la case pour **remplacer les AVI existants** lorsque vous y êtes invité. Les valeurs de date et de plan de l'AVI deviennent les valeurs de plan et de date que vous saisissez pour la tâche dans l'invite lorsque vous sélectionnez **En attente d'implémentation**.

Si vous ne sélectionnez pas l'option de remplacement dans ce cas et qu'un AVI est en **attente d'implémentation**, la date d'origine et les données de plan sur l'AVI restent intactes. Les valeurs de plan et de date que vous saisissez pour la tâche dans l'invite lorsque vous sélectionnez **En attente d'implémentation** ne sont pas utilisées sur les AVI déjà à l'état **En attente d'implémentation** dans la tâche.

Si un AVI sur une tâche est **en état Résolu** ou **Fermé-résolu** et que vous faites passer la tâche en **En attente d'implémentation**, le fait de sélectionner **Remplacer les AVI existants** ne modifie pas les AVI de **Fermé-Fixe** et **Résolu** à **En attente d'implémentation en raison** d'une priorité d'état supérieure.

Si le remplacement n'est pas sélectionné lors du déplacement de la tâche vers En **attente d'implémentation** et qu'un AVI est déjà en **attente d'implémentation** et que vous replacez la tâche vers **Ouvert** ou **En cours d'examen**, l'AVI reste en **attente d'implémentation**.

Ajouter un approbateur d'exception pour Réponse aux vulnérabilités des applications

Ajoutez des utilisateurs aux groupes d'approbation afin de pouvoir demander une exception.

Avant de commencer

Rôle requis : sn_vul.app_exception_approver

Pourquoi et quand exécuter cette tâche

Une demande d'exception pour un élément vulnérable de l'application est approuvée à l'aide du flux d'approbation à deux niveaux par défaut. La demande peut être approuvée par deux niveaux d'approbateurs. L'ajout d'utilisateurs au groupe de premier niveau est obligatoire. S'il n'y a pas d'utilisateurs au deuxième niveau, la demande est approuvée après l'approbation de premier niveau.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Groupes**.
2. Dans la colonne Nom, recherchez **Exception**, puis cliquez sur **Approbateur d'exception d'application : niveau 1**.

> **Remarque :** À partir de la Réponse aux vulnérabilités des applications version 12.8.1, vous pouvez utiliser les propriétés système fournies dans le système de base pour les approbations d'exceptions via le workflow de la table Propriétés système [sys_properties]. Ainsi, lorsqu'une demande d'exception ou de faux positif est émise via le workflow, elle est envoyée pour approbation aux ID de groupe définis dans la propriété système. Accédez à la **Tout** > **Propriétés système** et sélectionnez *sn_vul.app_exception_approver_L1*, *sn_vul.app_exception_approver_L2* ou *sn_vul.app_false_positive_approver_group* pour modifier la valeur de la propriété.

3. Dans le formulaire Approbateur d'exception d'application de groupe - Niveau 1, cliquez sur la liste connexe Membres du groupe.
4. Cliquez sur **Nouveau** pour créer une liste.
5. Renseignez les champs du formulaire.

Formulaire d'utilisateur

Champ	Description
ID d'utilisateur	Identificateur unique pour l'utilisateur.
Prénom	Prénom de l'utilisateur.
Nom de famille	Nom de famille de l'utilisateur.
Titre	Fonction de l'utilisateur. Saisissez un titre ou une description de poste, ou sélectionnez-en un dans la liste.
Département	Département de l'utilisateur.
Mot de passe	Mot de passe affecté à l'utilisateur. Ce mot de passe peut être permanent ou temporaire.
Mot de passe à réinitialiser	Option permettant à l'utilisateur de réinitialiser le mot de passe pour garantir la sécurité.
Verrouillé	Option permettant de verrouiller l'utilisateur hors de l'instance et de mettre fin à toutes les sessions actives de l'utilisateur. Le système empêche les utilisateurs disposant du rôle administrateur de se verrouiller eux-mêmes.
Actif	Option pour rendre cet utilisateur actif. Vous seul pouvez voir un utilisateur inactif dans ces zones :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Listes d'utilisateurs ◦ Liste de sélection sur les champs de référence (icône de loupe) ◦ Liste de saisie semi-automatique qui s'affiche lorsque vous entrez du texte dans un champ de référence
Accès au service Web uniquement	Option permettant de désigner cet utilisateur comme utilisateur non interactif.
Utilisateur d'intégration interne	Option permettant de désigner cet utilisateur en tant qu'utilisateur d'intégration interne.
E-mail	Adresse e-mail de l'utilisateur.
Langue	Langue préférée de l'utilisateur.
Intégration du calendrier	Calendrier utilisé pour gérer le calendrier de travail. Par exemple, Outlook.
Fuseau horaire	Fuseau horaire de l'emplacement de cet utilisateur.
Format de date	Format préféré de l'utilisateur pour les dates.
Tél. professionnel	Téléphone professionnel de l'utilisateur.
Tél. mobile	Téléphone portable de l'utilisateur.
Photo	Photo que vous pouvez télécharger en cliquant sur **Cliquer pour ajouter...**.

6. Cliquez sur **Envoyer**.
7. Facultatif : Répétez les étapes 1 à 5 pour créer un approbateur d'exceptions d'application de niveau 2.
   L'approbateur doit accéder à **Application Vulnerability Response** > **Mes approbations** et approuver les demandes.

La demande et l'approbation d'une exception dans Réponse aux vulnérabilités des applications

Vous pouvez demander à différer le rattrapage d'un élément vulnérable de l'application et une tâche de rattrapage pendant une période spécifiée.

Par exemple, en tant que développeur, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine. Les approbateurs qui y ont accès peuvent approuver les demandes d'autres utilisateurs.

Vous pouvez également créer des règles d'exception et demander une extension d'exception pour une règle d'exception. Par défaut, deux niveaux d'approbation sont requis pour les reports, les règles d'exception et les demandes d'extension d'exception.

Pour demander ou approuver une exception, consultez :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Demander une exception pour un élément vulnérable de l'application
- Demander une exception pour les vulnérabilités d'applications à l'aide de GRC : gestion de la politique et de la conformité
- Approuver les règles d'exception et les demandes d'extension des règles d'exception dans Réponse aux vulnérabilités des applications
- Demander une extension pour une règle d'exception dans Réponse aux vulnérabilités des applications

Remarque :

Des notifications par e-mail sont envoyées à chaque étape de la gestion des exceptions, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'une exception est demandée, le demandeur reçoit un e-mail confirmant que la demande est émise. L'approbateur reçoit également un e-mail l'informant qu'une exception a été demandée.

À partir de la version 21.0 de Réponse aux vulnérabilités des applications, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable de l'application passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable de l'application ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Demander une exception pour un élément vulnérable de l'application

Demandez une exception pour un élément vulnérable de l'application qui ne peut pas être corrigé immédiatement. Par exemple, en tant que développeur, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine.

Avant de commencer

Rôle requis : groupe de développeurs

Procédure

1. Accédez à la **Application Vulnerability Response** > **Éléments vulnérables de l'application** > **Tout** et sélectionnez l'élément pour lequel vous souhaitez demander une exception. L'élément sélectionné doit être à l'état Ouvert ou En cours d'examen.

   Remarque :

   À partir de la version 21.0 de , l'état précédent d'un élément vulnérable de Réponse aux vulnérabilités des applicationsl'application est stocké dans le champ **backup_state** .

2. Sur le formulaire Élément vulnérable de l'application, cliquez sur **Demande d'exception**.

   Remarque : Selon que est Réponse aux vulnérabilités sélectionné ou GRC : gestion de la politique et de la conformité dans le **Application Vulnerability Response** > **Gestion des exceptions** , le formulaire Demande d'exception change. Si GRC : gestion de la politique et de la conformité, consultez Demander une exception pour les vulnérabilités d'applications à l'aide de GRC : gestion de la politique et de la conformité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Si Réponse aux vulnérabilités cette option est sélectionnée dans l'écran Gestion des exceptions, renseignez les champs du formulaire Demande d'exception.

Formulaire Demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée sélectionnée dans le **Tout** > **Application Vulnerability Response** > **Administration** > **Gestion des exceptions** écran. Lorsque la demande d'exception expire, le groupe revient à son état **Ouvert** . **Remarque :** À partir de la version 18.0 de (AVR), un élément vulnérable d'application Réponse aux vulnérabilités des applications différé peut être fermé et rouvert par un scanner. Si l'élément rouvre avant l'expiration de la fenêtre d'exception, l'état de l'AVIT revient à l'état Différé, conformément à la fenêtre d'exception active. Pour activer cette fonctionnalité, définissez la valeur de la propriété système sn_vul.auto_defer_avit_in_active_exception_window sur vrai. De plus, la date de fin de report persiste même après la fermeture de l'AVIT ou l'expiration de l'exception. Le rôle requis est sn_vul.app_manage_exception_configuration pour la lecture et l'écriture.
Motif	Sélectionnez le **motif**. Les choix possibles sont les suivants : ◦ Risque accepté ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Contrôle d'atténuation en place ◦ Autre Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous Définir le mappage de motif de politiqueà .
Information supplémentaire	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ obligatoire doit être mis à jour par le propriétaire du rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Demander l'approbation** pour soumettre la demande d'exception.
   L'état de l'élément de vulnérabilité de l'application devient En cours de révision. Utilisez l'onglet **Approbation de changement d'état** pour suivre l'état de la demande d'exception.

Demander une exception pour les vulnérabilités d'applications à l'aide de GRC : gestion de la politique et de la conformité

Demandez des exceptions de politique à l'aide de l'option GRC de gestion des exceptions de politique de l'application à partir de .Gestion de la politique et de la conformitéRéponse aux vulnérabilités des applications

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions de politique, vous devez télécharger l'application GRC : gestion de la politique et de la conformité à partir du ServiceNow Store.

Rôle requis : sn_vul.remediation_owner

Vous pouvez également demander des exceptions dans l'interface utilisateur classique :

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Éléments vulnérables de l'application** (ou **Tâches de rattrapage**)>**Tous**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.
   L'élément ou le groupe sélectionné doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Sur le formulaire sélectionné, cliquez sur **Demande d'exception**.
3. Si GRC : gestion de la politique et de la conformité cette option est sélectionnée dans l'écran Gestion des exceptions, renseignez les champs du formulaire Demande d'exception.

Formulaire Demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas sélectionnée, tous les objectifs de contrôle sont listés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date du jour. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale (jours) de l'exception** que vous avez définie pour la politique dans Policy and Compliance. Pour plus d'informations, reportez-vous à la section Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ obligatoire doit être renseigné par le propriétaire du rattrapage.

a. Cliquez sur **Demander l'approbation** pour soumettre la demande d'exception. L'état des éléments vulnérables passe à En cours de révision et une exception de politique est créée. Utilisez l'onglet **Approbation de changement d'état** pour suivre l'état de la demande d'exception.

b. Cliquez sur la liste connexe Exceptions de politique pour afficher l'exception de politique.

c. Cliquez sur le numéro d'exception de politique.

d. Dans le champ **Approbateur** , sélectionnez le nom de l'approbateur.

e. Cliquez sur l'onglet Source et sélectionnez un objectif de contrôle dans le champ **Objectif de contrôle** .

f. Cliquez sur l'onglet Évaluation des risques et sélectionnez l'évaluation des risques dans le champ **Évaluation des risques** .

g. Enregistrez le formulaire.

h. Cliquez sur l'onglet Contrôles impactés, puis sur Ajouter pour ajouter les contrôles.

i. Enregistrez le formulaire.

Remarque : Vous pouvez soumettre un examen de conformité en cliquant sur **Demander un examen de conformité**.

j. Le formulaire d'approbation est envoyé à l'approbateur.

k. En tant qu'approbateur, vous pouvez approuver la demande en cliquant sur **Approuver** ou demander une approbation supplémentaire en cliquant sur **Demander une approbation supplémentaire**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'état de l'enregistrement devient Différé. Le motif indiqué est celui que vous avez sélectionné lors de l'émission de la demande d'exception. L'onglet Report fournit des notes supplémentaires sur l'enregistrement.

Remarque : Si la demande est rejetée, l'enregistrement passe à son état précédent.

4. Cliquez sur **Envoyer**.
   Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez la configuration facultative de Gestion de la politique et de la conformité .

Demander une exception pour une tâche de rattrapage d'une application

Demandez une exception pour différer une tâche de rattrapage d'application pendant une période spécifiée si elle ne peut pas être résolue immédiatement.

Avant de commencer

Vous pouvez demander des exceptions à partir Réponse aux vulnérabilités des espaces de travail. Consultez Demander une exception dans le Espace de travail de remédiation IT.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Rôles requis : sn_vul.remediation_owner, sn_vul.app_security_champion ou sn_vul_container.remediation_owner.

Vous pouvez également demander des exceptions pour les tâches de rattrapage d'applications dans l'environnement classique.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Tâches de rattrapage** > **Tout**.
2. Sélectionnez le groupe pour lequel vous souhaitez demander une exception.
   La tâche sélectionnée doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Dans l'enregistrement de tâche de rattrapage de l'application, sélectionnez **Demande d'exception**.
4. Renseignez les champs du formulaire.

Formulaire Demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée d'exception définie dans la configuration.
Motif	Justification de la demande d'exception.
Information supplémentaire	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	doit être mis à jour par le propriétaire du rattrapage.

5. Cliquez sur **Demander l'approbation**.

Approuver les règles d'exception et les demandes d'extension des règles d'exception dans Réponse aux vulnérabilités des applications

Approuvez les demandes d'exception pour les éléments vulnérables de l'application qui ne peuvent pas être corrigés immédiatement. Vous devez évaluer les risques de ces demandes, puis approuver leur report jusqu'à ce qu'elles puissent être corrigées.

Avant de commencer

Rôle requis : sn_vul.app_exception_approver

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Définir le mappage de motif de politique

Vous pouvez définir les choix de motifs afin qu'ils soient disponibles pour n'importe quel utilisateur qui demande une exception.

Avant de commencer

L'application GRC : Policy and Compliance Management doit être installée. Cette application est disponible à partir ServiceNow® Store du avec un abonnement distinct.

Pour plus d'informations sur la configuration système requise et la compatibilité des familles, consultez la liste des applications sur le site Web ServiceNow Store .

Rôle requis : sn_vul.compliance.manager et sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tout** > **Politique et Conformité** > **Exceptions de politique** > **Registre d'intégration**.

   Remarque : Vous pouvez sélectionner un motif parmi les choix de motifs disponibles dans la table Choix du motif ou ajouter un nouveau motif.

2. Cliquez sur le registre d'intégration de votre application, par exemple, **Application Vulnerability Response**, **Vulnerability Response**, etc.
3. Pour ajouter un choix de motif existant, procédez comme suit :
   a. Dans la liste Choix du motif, cliquez sur **Nouveau**.
   b. Cliquez sur l'icône en forme de loupe pour sélectionner un motif.
4. Pour ajouter de nouveaux choix de motifs à la table Choix du motif, procédez comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans la liste Choix du motif, cliquez sur **Nouveau**.

b. Cliquez sur l'icône de la loupe.

c. Cliquez sur **Nouveau**.

d. Renseignez les champs du formulaire.

Formulaire de liste de choix de motifs

Champ	Description
Étiquette	Étiquette unique pour ce choix.
Valeur	Valeur unique pour ce choix. Cette valeur est mappée dans la table Mappages de motifs d'exception de politique pour les applications respectives. Pour accéder à cette table, saisissez sn_vul_policy_reason_mapping. LIST dans le navigateur de filtre.
Ordre	Ordre pour ce choix. Les motifs sont classés en fonction de ce nombre.
Par défaut	Option pour indiquer que ce choix de motif sera disponible chaque fois qu'une exception de politique sur demande est demandée. Si le registre d'intégration ne contient pas de choix spécifiques à l'application, tous les choix de motif pour lesquels le champ **Par défaut** est sélectionné sont disponibles.
Actif	Option permettant d'afficher le choix dans la liste des choix de motifs.

5. Cliquez sur **Envoyer**.

Demander une extension pour une règle d'exception dans Réponse aux vulnérabilités des applications

Demandez une prolongation pour une règle d'exception différée avant qu'elle n'atteigne sa date de report jusqu'à échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôles requis : Gestionnaire App-Sec sn_vul.app_sec_manager, Champion de sécurité sn_vul.app_security_champion.

Pourquoi et quand exécuter cette tâche

Sur un enregistrement de règle d'extension, vous pouvez demander une prolongation pour la date **de fin de report** uniquement si la règle est dans l'état **Approuvé** . Vous pouvez demander cette extension à une règle si vous constatez qu'un grand nombre d'enregistrements créés par la règle ne sont pas résolus par sa Date de **fin de report,** date à laquelle la tâche de rattrapage cesse d'accepter de nouveaux AVI. L'extension met à jour la règle d'exception de sorte qu'elle prolonge automatiquement la date de report de votre règle existante.

Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Règles d'exception**.
2. Sélectionnez une règle d'exception approuvée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle la règle d'exception doit être prolongée.
Motif	Entrez le motif du report de la règle d'exception. Les choix sont les suivants : ◦ Risque accepté ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les champs Différé jusqu'à, Motif et Informations supplémentaires sont mis à jour sur la règle d'exception et les tâches de rattrapage et les éléments vulnérables de l'application associés. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure de l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une règle d'exception différée est à nouveau étendue, le nombre de reports prolongés augmente dans le back-end.

Demander une prolongation pour une tâche de rattrapage différée dans Réponse aux vulnérabilités des applications

Demandez une prolongation pour une tâche de rattrapage différée (VUL) avant qu'elle n'atteigne sa date de report jusqu'à l'échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Tâches de remédiation**.
2. Ouvrez une tâche de rattrapage différée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date à laquelle l'état Différer expire et à laquelle la tâche de rattrapage est réactivée.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les modifications apportées à la tâche de rattrapage sont également étendues aux éléments vulnérables de l'application, qui font partie de la tâche de rattrapage. Toutefois, les éléments vulnérables de l'application doivent être à l'état Différé et leur date actuelle jusqu'à ce que les données précèdent la date de fin de mise à jour. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure de l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une tâche de rattrapage différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

Demander une extension pour un élément vulnérable différé de l'application dans Réponse aux vulnérabilités des applications

Demandez une extension pour un élément vulnérable d'application différé avant qu'il n'atteigne sa date de report jusqu'à échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche
Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités.

Procédure
1. Accédez à la **Tout** > **Application Vulnerability Response** > **Éléments vulnérables**.
2. Ouvrez un élément vulnérable différé de l'application.
3. Sélectionnez **Demande d'extension**.

> **Remarque :** Le bouton Demande d'extension n'est visible que lorsque l'état de l'élément vulnérable de l'application est Différé.

4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle l'élément vulnérable d'application différé doit être prolongé pour le rattrapage.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Un e-mail est déclenché lors de l'envoi de la demande et de l'action ultérieure de l'approbateur.

> **Remarque :**
> ◦ La demande passe par deux niveaux d'approbation.
> ◦ Si une règle d'exception différée est à nouveau étendue, le nombre de reports prolongés augmente dans le back-end.

6. Une fois la demande approuvée, les notes Jusqu'à, Motif et Report sont mises à jour.

Créer, supprimer et annuler une règle d'exception pour Réponse aux vulnérabilités des applications

Créez une règle pour demander automatiquement une exception pour les éléments vulnérables de l'application (AVI) qui répondent à des conditions spécifiques.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Par exemple, vous pouvez créer une règle avec une condition basée sur une vulnérabilité spécifique connue ou critique que vous savez que vous ne pouvez pas corriger immédiatement. Avec cette règle, vous pouvez différer automatiquement les AVI nouveaux et existants s'ils correspondent à la condition de règle approuvée.

- La règle d'exception s'applique à partir de la **date de début de validité** jusqu'à la date **de fin de validité** que vous saisissez dans l'enregistrement de règle.
- La tâche de rattrapage (AVUL) est créée après l'approbation de la règle pour établir une correspondance avec les AVI à l'état **Différé** .
- La méthode de regroupement de cet AVUL est connue sous le nom de règles d'exception.
- Vous ne pouvez pas fermer, rouvrir ou supprimer cet AVUL. Les AVI nouveaux et rouverts sont différés et ajoutés à cet AVUL à partir de la date **de début de validité** jusqu'à l'expiration du groupe à la date **de fin de validité** .

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de la règle d'exception. Ces e-mails fournissent l'état et d'autres détails d'une demande. Par exemple, lorsqu'une règle d'exception est demandée, le demandeur reçoit un e-mail qui confirme que la demande est envoyée.

Si la règle est rejetée, vous pouvez la rouvrir à l'état Brouillon, la mettre à jour, puis la soumettre à nouveau pour approbation.

Rôles requis : gestionnaire SEC d'application sn_vul.app_sec_manager et champion de sécurité sn_vul.app_security_champion.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Règles d'exception**.
2. Sur la page Règle d'exception nouvel enregistrement, sélectionnez **Nouveau**.
3. Renseignez les champs.

Champ	Description
Nom	Nom de la règle d'exception.
État	Lecture seule : brouillon
Début de validité	Date à partir de laquelle cette règle est active pour différer les AVI.
Ordre d'exécution	Ordre unique pour chaque règle d'exception. Une valeur inférieure précède une valeur supérieure.
Date de fin de validité	Date à laquelle la tâche de rattrapage cesse d'accepter de nouveaux AVI.
Reporté jusqu'à	Date avant le report des tâches de rattrapage et des AVI. À cette date, les AVUL sont fermés et tous les AVI sortent des tâches et sont rouverts. Les règles de groupe sont réappliquées à ces AVI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Motif	Raison pour laquelle cette règle d'exception a été créée.
Groupe d'affectation	Groupe auquel la tâche de rattrapage est affectée pour le suivi des AVI différés.
Information supplémentaire	Informations supplémentaires que le demandeur souhaite fournir à l'approbateur. Ces informations sont renseignées dans le champ de description de la tâche de rattrapage.
Condition	Conditions de filtre pour spécifier quels AVI correspondent à cette règle.
Exécuter sur les données existantes	Option qui vous permet d'exécuter cette règle sur des données existantes la première fois que cette règle est exécutée. Si vous laissez cette option désactivée, votre règle s'exécute quotidiennement par la tâche *Associate existing AVIs with Auto Exception Rule* planifiée en commençant par de nouvelles données. Si vous activez l'option Exécuter sur les données existantes, une tâche planifiée s'exécute une seule fois sur les données existantes à la date **de début de validité** .

4. Ajoutez le groupe d'affectation lors de la création de la règle.
5. Choisissez-en un.

Option	Description
Enregistrer la règle	Enregistrez vos changements et la règle s'affiche dans la liste Règles d'exception [sn_vul_auto_exception_rule]. Tant que vous n'avez pas soumis la règle d'exception pour approbation, elle reste à l'état **Brouillon** .
Soumettre la règle	Si vous soumettez la règle, l'état de la demande devient **En cours de révision**. Une approbation de règle d'exception nécessite deux niveaux d'approbation, l'un de l'approbateur d'exception d'application de niveau 1 et l'autre de l'approbateur d'exception d'application de niveau 2.

Une fois la règle approuvée, elle passe à l'état **Approuvé** . Votre règle évalue les AVI avec la *Associate existing AVIs with Auto Exception Rule scheduled*tâche. Si vous avez sélectionné **Exécuter sur les données existantes**, cela évalue les AVI existants. Une tâche de rattrapage est automatiquement créée pour la règle, et tous les AVI correspondants qui remplissent ses conditions sont associés à la tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La tâche planifiée exécute la règle d'exception une seule fois sur les données existantes. La règle ne s'exécute pas à nouveau sur les données existantes, même si aucun AVI n'est trouvé. Il évalue uniquement les nouvelles données, car les AVI existants qui correspondaient à la règle ont déjà été différés.

6. Pour supprimer une règle, sélectionnez **Supprimer** dans l'enregistrement de règle d'exception.
   Le message suivant s'affiche : `Si vous supprimez la règle, la tâche de rattrapage associée sera supprimée et les éléments vulnérables associés seront rouverts. Les règles de tâche de rattrapage sont ensuite appliquées aux AVI individuels et la règle d'exception est supprimée.`
7. Sélectionnez**Conserver la règle** pour arrêter ou **Supprimer la règle** pour continuer.
8. Pour désactiver une règle tout en la conservant dans la liste Règles d'exception, sélectionnez **Annuler**.
   Le message suivant s'affiche : `Si vous annulez cette règle, la tâche de rattrapage associée sera supprimée et les éléments vulnérables associés seront rouverts. Les règles de tâche de rattrapage sont ensuite appliquées aux éléments vulnérables individuels et la règle d'exception passe à l'état Brouillon.`
9. Sélectionnez**Conserver la règle** pour arrêter ou **Annuler** pour déplacer la règle vers les **brouillons** et la désactiver.

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

Configurez les tâches de rattrapage (AVUL) pour aider les analystes et les spécialistes du rattrapage à organiser les éléments vulnérables de l'application (AVI) et à les analyser en bloc. Les critères utilisés pour la formation des tâches de rattrapage sont configurés de façon à ce que les AVI soient automatiquement affectés à des tâches de rattrapage. Les tâches de rattrapage vous permettent de surveiller la progression et de piloter le processus de rattrapage plus efficacement.

Suivi des nombres de reports pour les éléments vulnérables de l'application et les tâches de rattrapage

Suivez le nombre de fois où un élément vulnérable, un élément vulnérable d'application, un élément vulnérable de conteneur ou une tâche de rattrapage est différé. La *`set deferral counts`* tâche planifiée s'exécute quotidiennement pour publier les nombres des enregistrements qui sont différés plus d'une fois dans la colonne Nombre de reports. Les enregistrements s'affichent dans les modules Reports multiples pour VR, AVR et CVR.

Présentation des règles de tâche de rattrapage

Les règles de tâche de rattrapage vous permettent de définir la manière dont les éléments vulnérables de l'application sont automatiquement regroupés et affectés. Une règle par défaut **La vulnérabilité** est incluse dans le système de base qui rassemble les AVI en fonction de leurs vulnérabilités. Toutefois, vous pouvez effectuer un regroupement par n'importe quel autre ensemble de valeurs dans des colonnes accessibles à partir de l'AVI. Ces valeurs peuvent inclure l'élément de configuration (CI), l'entrée de vulnérabilité, etc.

Des règles de tâche pour Application Vulnerability Response sont incluses dans l'application Réponse aux vulnérabilités disponible lorsque vous l'activez.

Vous pouvez créer plusieurs conditions à l'aide du Créateur de conditions. Dans la section Grouper par, une fois que vous avez défini une paire de champs, une autre ligne apparaît.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez avoir jusqu'à six **sélections Grouper par** . Vous pouvez également automatiser l'affectation de groupe. Voir Affecter automatiquement les éléments vulnérables de Réponse aux vulnérabilités des applications l'application et Filtrage au sein de Réponse aux vulnérabilités pour plus d'informations.

Par exemple, vous pouvez regrouper les éléments vulnérables de votre application par élément de configuration ou par modèle de produit. Vous pouvez avoir une règle de tâche pour les vulnérabilités de faible gravité ou les CI à faible risque. Vous pouvez avoir une autre règle de tâche pour les serveurs critiques et les vulnérabilités qui exposent l'entreprise à plus de risques. Consultez Créer, modifier et supprimer Réponse aux vulnérabilités des applications des règles de tâche de rattrapage pour plus d'informations sur les options qui s'offrent à vous.

Un autre ensemble de règles peut être utilisé pour les éléments vulnérables de l'application qui exposent la société à davantage de risques. Le nom de la tâche de rattrapage est ajouté à la règle de la tâche de rattrapage **Grouper par** valeurs pour créer la description brève du nouvel enregistrement.

Lorsqu'un nouvel élément vulnérable de l'application est créé, importé ou rouvert après avoir été fermé, les règles sont évaluées par rapport à celui-ci. Un AVI n'est évalué qu'une seule fois, automatiquement, sauf s'il est rouvert après avoir été fermé ou si les règles sont réappliquées manuellement.

Le processus suivant est utilisé pour chaque nouvel AVI ou réouverture :

- Pour chaque règle de tâche de rattrapage, l'AVI est comparé au filtre de règle de tâche de rattrapage.

- Pour chaque règle dans laquelle la condition de la règle de tâche de rattrapage correspond, la règle extrait les données des sélections **Grouper par** sur l'AVI. Il crée un nom de groupe et un champ. Dans ce cas, **Risque élevé : QID-32342 :** *résumé de QID-3242* (Nom : ID de vulnérabilité : résumé de la vulnérabilité).

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

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

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

Plusieurs règles de tâche de rattrapage peuvent être définies pour regrouper différents types de vulnérabilités. Étant donné que chaque vulnérabilité est comparée aux conditions de règles de tâche de rattrapage avant de la placer dans une tâche de rattrapage, un trop grand nombre de règles peut avoir un impact sur les performances. Configurez vos règles de tâche afin que les conditions vous aident à éviter de créer des tâches de rattrapage en double.

Par défaut, les règles de tâche de rattrapage utilisent le groupe d'affectation défini par les **règles d'affectation** sur l'AVI lors du regroupement des éléments et affectent la tâche de rattrapage pour qu'elle corresponde aux AVI.

Dans le cadre de la règle de tâche par défaut, l'affectation de ces tâches de rattrapage est contrôlée par les règles du module **Règles d'affectation** . Pour en savoir plus sur les

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

règles d'affectation, reportez-vous à Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Lorsqu'une règle de tâche est supprimée du formulaire ou de la vue de liste, vous avez la possibilité de supprimer toutes les tâches **ouvertes** créées par cette règle. Les tâches qui ne sont pas dans l'état **ouvert** sont exclues.

Réapplication des règles de tâche de rattrapage

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

Réappliquer vérifie uniquement les tâches de rattrapage existantes.

Une fois que vous avez sélectionné **Réappliquer**, le message suivant s'affiche : `La réapplication de cette règle de tâche de rattrapage supprimera et recréera les tâches de rattrapage pour cette règle. Les tâches de` rattrapage qui ne sont pas à l'état ouvert ne sont pas supprimées.

Création de tâches de rattrapage et ajout manuel d'AVI

Vous créez une tâche de rattrapage de l'application (AVUL) à partir d'un autre enregistrement de tâche de rattrapage de l'application et ajoutez manuellement des éléments vulnérables de l'application (AVIT). Consultez Créer manuellement une tâche de rattrapage d'application dans Réponse aux vulnérabilités des applications pour plus d'informations.

Règles de tâche de rattrapage et création et mise à jour AVI

Si un CI ou un modèle de produit issu d'une analyse est associé à une vulnérabilité connue, un AVI est créé. Une fois créé, l'AVI est évalué par rapport aux conditions des règles de tâche de rattrapage d'une correspondance. S'il existe une correspondance avec une tâche de rattrapage existante, l'AVI est ajouté. Si aucune tâche de rattrapage correspondante n'est trouvée, une tâche est créée pour l'AVI.

Si une propriété capturée dans les conditions de filtrage de la tâche de rattrapage est mise à jour ou modifiée sur un AVI, l'AVI mis à jour est également évalué par rapport aux règles de tâche de rattrapage d'une correspondance. S'il existe une correspondance avec une tâche de rattrapage existante, l'AVI est ajouté. Si aucune tâche de rattrapage correspondante n'est trouvée, une tâche est créée pour l'AVI.

Déploiement d'état et déploiement

Si vous mettez à jour une tâche de rattrapage sur Ouvert, ou d'Ouvert à En cours d'examen, le nouvel état s'étend à tous les AVI associés. La restauration de l'état se produit immédiatement après la modification de l'état.

Le déploiement de l'état des AVI vers la tâche de rattrapage ne se produit que si tous les AVI de la tâche sont à l'état **Différé** ou **Fermé (fixe**). Le déploiement est effectué avec la *`Rollup application vulnerable item values to vulnerability and group`* tâche planifiée, qui s'exécute toutes les 15 minutes. L'état n'est pas déployé tant que la tâche n'est pas exécutée. Pour qu'un état soit déployé entre AVI et la tâche de rattrapage, tous les AVI doivent être dans le même état.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer, modifier et supprimer Réponse aux vulnérabilités des applications des règles de tâche de rattrapage

Vous pouvez créer des règles pour regrouper automatiquement les éléments vulnérables de l'application (AVI) dans les tâches de remédiation (AVUL) en fonction des conditions de filtre. Ces règles regroupent automatiquement les AVI au fur et à mesure qu'ils sont importés ou créés manuellement.

Avant de commencer

Si vous créez une nouvelle règle, elle ne s'applique pas aux données existantes. Une fois que vous l'avez soumis, il est exécuté par rapport aux nouvelles importations.

Rôle requis : App-Sec Manager

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Règles de la tâche de rattrapage**.
2. Ouvrez la règle ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire ou modifiez-les.

Règle de la tâche de rattrapage

Champ	Description
Nom	Nom de la règle de tâche.
Actif	Indique si la tâche est active.
Description	Description de la règle.
Sensible à la casse	Détermine si une condition est sensible à la casse ou non. **Remarque :** La valeur par défaut n'est pas sensible à la casse.
Condition	Conditions de filtre facultatives pour la règle. Par défaut (case **sensible à la casse** non cochée), le texte de recherche que vous saisissez dans le générateur de conditions sur les enregistrements et formulaires de règles de tâche n'est pas sensible à la casse. Vous pouvez activer les recherches sensibles à la casse sur les enregistrements de tâches et les formulaires. Voici un exemple de condition **Vulnérabilité** > **est** > **VULNENT123451** (une vulnérabilité importée connue). Tous les AVI présentant cette vulnérabilité correspondent à cette condition.
Grouper par (jusqu'à six ensembles de conditions sont disponibles)	
Regrouper les éléments vulnérables de l'application à partir de	Table que la règle utilise pour regrouper les AVI. Sélectionner les éléments de l'arborescence : ◦ Élément vulnérable de l'application [sn_vuln_vulnerable_item] ◦ Élément vulnérable de l'application Élément de configuration [cmdb_ci] ◦ Élément vulnérable de l'application Vulnérabilité de l'application [sn_vul_third_party_entry] ◦ Modèle de produit d'élément vulnérable d'application

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si vous choisissez une table étendue, le **champ Utilisation** n'est appliqué qu'aux éléments vulnérables de l'application qui utilisent cette table étendue.
Utilisation du champ	Champ de la table que la règle utilise pour regrouper les AVI. Sélectionnez des conditions dans l'arborescence. **Remarque :** Vous pouvez créer un groupe par conditions afin que tous les AVI qui partagent des données ne soient pas affectés à la même tâche de rattrapage. Par exemple, si vous sélectionnez Groupe d'affectation et Adresse IP comme champs Utilisation et que plusieurs AVI correspondent à la condition de filtrage initiale **Vulnérabilité**, ces AVI peuvent être affectés à des groupes d'affectation distincts pour le rattrapage à l'aide des nombreuses options disponibles dans la section Grouper par. Les conditions Grouper par vous donnent la possibilité de créer des tâches de rattrapage distinctes qui peuvent être affectées à différents groupes, même s'ils partagent certaines données.
Affectation	
Affecter la tâche de rattrapage par	Lors de l'affectation automatique des tâches de rattrapage, le choix Affectation est utilisé en plus des choix **Grouper par** pour regrouper les éléments vulnérables. De nouvelles tâches sont créées, selon les besoins, de sorte que chaque AVI est placé dans une tâche avec un ensemble de groupes d'affectation correspondant. Pour automatiser l'affectation des tâches créées en fonction de cette règle, choisissez l'une des options disponibles. ◦ Regrouper par champ : si vous avez sélectionné un champ de groupe d'utilisateurs à partir des valeurs du **champ Utilisation** dans la section **Grouper par**, il apparaît dans le menu déroulant. ◦ Groupe d'utilisateurs : utilisez la liste de recherche pour sélectionner un groupe d'utilisateurs statique.

Si vous supprimez une règle de la vue de formulaire ou de la vue de liste, vous avez la possibilité de supprimer toutes les tâches de rattrapage **ouvertes** créées par cette règle. Les groupes qui ne sont pas dans l'état **Ouvert** sont exclus.

4. Sélectionnez **Soumettre** pour de nouvelles règles.
   Une fois que vous avez sélectionné **Soumettre**, votre règle s'affiche dans la liste Règles de tâche de rattrapage [sn_vul_grouping_rule]. Les situations suivantes initient votre règle.
   - Lorsque de nouveaux AVI sont créés.
   - Lorsque vous sélectionnez **Réappliquer**. Vous sélectionnez **Réappliquer** pour évaluer les règles de tâche sur les tâches de rattrapage existantes uniquement.
   - Lorsque les AVI sont mis à jour, soit par vous, soit par le système.

     Si un AVI est mis à jour, les règles de tâche sont évaluées pour vérifier leur correspondance avec les tâches de rattrapage existantes. Voici quelques mises à jour courantes qui déclenchent une vérification des règles :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lorsque l'état passe de Fermé à Ouvert, ou de Fermé à En cours d'examen.
- L'élément de configuration (CI) est modifié.
- La vulnérabilité est modifiée.

Le système vérifie toutes les règles de tâche pour voir s'il y a des correspondances avec l'AVI mis à jour. Si les conditions d'une règle correspondent aux conditions d'une tâche de rattrapage, les AVI correspondants lui sont affectés.

Si aucune correspondance n'est trouvée, une nouvelle tâche de rattrapage est créée.

Pour plus d'informations sur le déploiement de l'état des AVI vers les tâches de rattrapage et sur le déploiement de l'état des tâches de rattrapage vers les AVI, reportez-vous à la section Réponse aux vulnérabilités des applications Vue d'ensemble des tâches de rattrapage et des règles de tâche.

Pour obtenir un exemple de règle de tâche de rattrapage, reportez-vous à Réponse aux vulnérabilités des applications Exemples de règles de tâche de rattrapage.

5. Pour supprimer une règle de tâche, sélectionnez-la dans la liste Règles de tâche de rattrapage, puis sélectionnez **Supprimer**.
Le message suivant s'affiche : `La règle de tâche de rattrapage sélectionnée a créé n tâches de rattrapage. Parmi les tâches de rattrapage, n sont à l'état` Ouvert.

Option	Description
Case à cocher désactivée (par défaut).	Supprimez uniquement la règle. Les tâches qui ne sont pas dans l'état **ouvert** sont exclues.
Case à cocher.	Inclure les tâches de rattrapage dans l'état **Ouvert** lorsque vous supprimez la règle de tâche de rattrapage. Supprimez la règle et toutes les tâches de rattrapage à l'état **Ouvert** .

6. Choisissez une option et sélectionnez **Supprimer**.

Créer manuellement une tâche de rattrapage d'application dans Réponse aux vulnérabilités des applications

Créez une tâche de rattrapage de l'application (AVUL) à partir d'un autre enregistrement de tâche de rattrapage de l'application et ajoutez manuellement des éléments vulnérables de l'application (AVIT).

Avant de commencer
Rôle requis : sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Tâches de remédiation** > **Tout**.
2. En haut à droite de la page, sélectionnez **Nouveau**.
3. Dans l'onglet Configuration du groupe, pour Méthode de regroupement, sélectionnez **Manuel**.
4. Sélectionnez **Soumettre**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Localisez votre nouvel enregistrement de tâche (AVUL) sur la table Tâches de rattrapage de l'application [sn_vul_app_vulnerability].
   L'enregistrement est créé à l'état **Ouvert** .
6. Ouvrez l'enregistrement et ajoutez des éléments vulnérables d'application nouveaux ou existants à ce groupe à l'aide de la liste connexe des éléments vulnérables d'application (**modifier** ou **ajouter**).
7. Sélectionnez **Mettre à jour** pour sauvegarder l'enregistrement ou d'autres actions d'interface utilisateur pour faire passer l'enregistrement à un autre état.

Créer des règles de fermeture automatique

Utilisez les règles de fermeture automatique pour fermer automatiquement les AVIT plus anciens en fonction des conditions de filtre que vous définissez.

Avant de commencer

Rôle requis : sn_vul.app_manage_auto_close_rules

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Règles de fermeture automatique**.
   Le système de base fournit les règles de fermeture automatique suivantes :

   Dernière analyse des vulnérabilités de l'application Les vulnérabilités non signalées au cours des 90 derniers jours passent à **l'état Périmé** .
2. Sélectionnez **Nouveau** pour créer une règle de fermeture automatique.
3. Renseignez les champs du formulaire.

Champ	Valeur
Nom	Nom de la règle de fermeture automatique.
Actif	Option permettant d'activer la règle. Si elle est activée, elle ferme automatiquement toutes les détections qui correspondent à ses critères de filtrage.
Ordre d'exécution	Valeur unique pour l'exécution de la règle de fermeture automatique. Cette valeur détermine l'ordre d'exécution. La valeur par défaut est 100.
Type d'intégration	Intégration de vulnérabilité de l'application
Description	Description de la règle de fermeture automatique.
Condition	Conditions de filtre utilisées pour identifier les détections qui doivent être fermées.

4. Sélectionnez **Soumettre**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les travaux **planifiés des règles de fermeture automatique** s'exécutent tous les soirs. Il identifie les AVIT en fonction des conditions spécifiées et fait passer celles qui correspondent à l'état **Périmé** . Dans les cas où des AVIT ont à la fois l'état « Fermé » et l'état « Périmé », l'AVIT est fermé avec le sous-état défini sur **Fixe**.

Configurer les tests de pénétration

Vous pouvez configurer la durée du sprint et l'effort estimé pour les types d'évaluations de tests de pénétration. Cela fournit la fonctionnalité de planification pour les propriétaires d'applications, les aidant à déterminer un délai provisoire pour leurs demandes d'évaluation de test de pénétration.

Avant de commencer
Rôle requis : Hacker éthique

Pourquoi et quand exécuter cette tâche
La configuration des paramètres d'évaluation du test d'intrusion pour l'équipe de piratage éthique permet également de déterminer le groupe et le point de contact qui reçoivent la demande d'évaluation du test d'intrusion.

À partir de la version 19.0 de , si vous utilisez , Veracode Vulnerability Integrationles tests d'évaluation Réponse aux vulnérabilitésde pénétration dans le Veracode Vulnerability Integration sont des résultats manuels de Veracode. Elles ne sont pas liées aux demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour plus d'informations sur les évaluations des tests d'intrusion de Veracode, reportez-vous à la Veracode Vulnerability Integrationsection .

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Configuration du test de pénétration**.
2. Utilisez la première section pour configurer le groupe d'affectation.
3. Renseignez les champs du formulaire.

Formulaire de configuration du test de pénétration

Champ	Description
Groupe d'utilisateurs de l'équipe de test de pénétration	Groupe auquel la demande d'évaluation de test de pénétration est affectée.
Délégataire par défaut des demandes d'évaluation de test de pénétration	Point de contact pour la demande d'évaluation de test de pénétration.

4. Sélectionnez **Mettre à jour**.
5. Utilisez la deuxième section pour configurer les sprints.
   Pour plus de détails, voir Configurer les sprints pour les tests de pénétration.
6. Utilisez la troisième section pour configurer les types d'évaluation.
   Pour plus de détails, voir Configurer les types d'évaluation pour les tests de pénétration.

Configurer les sprints pour les tests de pénétration

Configurez la durée et la capacité du sprint pour l'équipe de piratage éthique afin qu'elle puisse gérer la capacité du sprint pour les évaluations des tests de pénétration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : Ethical Hacking

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Configuration du test de pénétration**.
2. Sélectionnez l'option **Configurer** pour Configurer les sprints.
3. Renseignez les champs du formulaire.

Formulaire de configuration du sprint

Champ	Description
Durée du sprint (jours)	Nombre de jours dans un sprint.
Date de début	Date de début de la durée du sprint.
Nombre de sprints	Nombre de sprints pouvant être générés, en fonction des dates de début et de fin de la plage de sprints.
Date de fin	Date de fin de la durée du sprint.
Capacité de sprint	
Capacité de sprint (h)	Capacité d'un sprint en heures.

4. Sélectionnez **Générer des sprints**.
   Pour afficher les sprints **créés, sélectionnez Afficher les sprints**.

> **Remarque :** Une fois les sprints générés et en cours, si vous sélectionnez **Générer des sprints** pour la même durée, le sprint actuel est terminé comme d'habitude. Les sprints restants sont recalculés en fonction de la configuration de sprint mise à jour.

Configurer les types d'évaluation pour les tests de pénétration

Configurez l'effort estimé pour chaque type d'évaluation de test de pénétration. Cela vous permet de gérer la capacité de chaque sprint, en estimant l'effort requis pour chaque type d'évaluation.

Avant de commencer
Rôle requis : Ethical Hacking

Pourquoi et quand exécuter cette tâche
Chaque sprint est affecté à une demande de test d'intrusion. En fonction de l'effort estimé pour le type d'évaluation, les heures sont ajustées pour refléter le solde d'heures pour le sprint.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Configuration du test de pénétration**.
2. À partir de la version 19.0 de , sélectionnez **Configurer** pour afficher les types d'évaluation, la taille de Réponse aux vulnérabilitésl'application et l'effort estimé.
3. Facultatif : Sélectionnez un enregistrement de type d'évaluation pour mettre à jour les champs selon vos besoins ou créer de nouveaux enregistrements.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(Optional) Les valeurs de taille de l'application vous offrent plus d'options pour vous aider à estimer plus précisément le temps et l'effort de test. Vous pouvez modifier les heures de ces enregistrements ou sélectionner **Nouveau** pour créer vos propres combinaisons.

Vous pouvez modifier le type d'évaluation et la taille de l'application sur les valeurs des enregistrements de demande de test de pénétration existants afin de pouvoir planifier les tests pour qu'ils correspondent à la capacité de sprint. Par exemple, si vous remplissez une demande de test, il est possible que vous ne voyiez pas le nombre de sprints que vous avez configurés, car certains sprints sont déjà pris pour être testés. Si les heures d'effort estimées d'un sprint correspondent à la combinaison requise pour le type et la taille d'un test, elles ne sont pas disponibles pour les nouvelles demandes.

Vous pouvez voir les sprints affectés aux demandes de test dans les enregistrements de la liste Sprints de tests de pénétration à l'adresse suivante : **Tout** > **Application Vulnerability Response** > **Administration** > **Configuration du test de pénétration** > **Configurer les sprints**. Consultez Configurer les sprints pour les tests de pénétration pour plus d'informations sur la configuration des sprints.

Les valeurs de base pour le type d'évaluation, la taille de l'application et l'effort estimé sont les suivantes :

Formulaire de configuration du type d'évaluation de test de pénétration

Type d'évaluation	Taille de l'application	Efforts estimés (h)
Test ciblé	Petit	20
Test ciblé	Moyen	30
Test ciblé	Grand	40
Test ciblé	Standard	40
Tester à nouveau	Petit	10
Tester à nouveau	Moyen	15
Tester à nouveau	Grand	20
Tester à nouveau	Standard	20
Test de pénétration complet	Petit	60
Test de pénétration complet	Moyen	70
Test de pénétration complet	Grand	80
Test de pénétration complet	Standard	80

4. Sélectionnez Mettre à jour pour enregistrer vos changements ou Soumettre pour un nouvel enregistrement.
5. Avant la version 19.0, sélectionnez l'option **Configurer** pour Configurer les types d'évaluation.
6. Mettez à jour les valeurs des types d'évaluation selon les besoins.
   Les valeurs de base sont les suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de configuration du type d'évaluation de test de pénétration

Type d'évaluation	Efforts estimés (h)
Test ciblé	40
Tester à nouveau	20
Test de pénétration complet	80

7. Enregistrez les changements.

Intégrer Réponse aux vulnérabilités des applications avec d'autres applications

Réponse aux vulnérabilités inclut la prise en charge des intégrations tierces.

Intégrations tierces

Les intégrations de vulnérabilité de l'application permettent d'enrichir les données de vulnérabilité de l'application sur votre instance en récupérant des données provenant de systèmes externes et de fournisseurs. Consultez les rubriques de vue d'ensemble suivantes pour en savoir plus sur les intégrations prises en charge :

- Fortify Vulnerability Integration
- GitHub Application Vulnerability Integration
- Invicti Vulnerability integration
- Veracode Vulnerability Integration
- Intégration Atlassian Jira

Important : Dans Vulnerability Manager Workspace, vous pouvez créer manuellement un problème Agile à l'aide de l'action de liste et de l'action de formulaire pour suivre le rattrapage des AVIT et des RT.

Remarque :

Les intégrations multisources ne sont pas prises en charge dans Réponse aux vulnérabilités des applications. Les intégrations tierces sont traitées séparément. Si plusieurs applications d'intégration tierces sont utilisées dans votre environnement, il n'y a pas de déduplication des éléments vulnérables d'application (AVI) entre les intégrations.

Notes supplémentaires pour les intégrations

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités des applications, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Intégration de Réponse aux vulnérabilités avec Black Duck

L'intégration Réponse aux vulnérabilités utilise Intégration de Réponse aux vulnérabilités avec Black Duck les données importées de l'outil d'analyse de la composition logicielle (SCA) Black Duck pour vous aider à déterminer l'impact et la priorité des failles dans votre code.

Vue d'ensemble de l'intégration

Avec la commande , vous pouvez collecter des Intégration de Réponse aux vulnérabilités avec Black Duckdonnées SCA et les mettre à la disposition du Now Platform. À partir de la version 22.0.5 de Réponse aux vulnérabilités, vous pouvez importer des données de vulnérabilités SCA dans votre instance afin de pouvoir identifier les vulnérabilités dans vos applications logicielles. Pour plus d'informations, consultez Explorer Nomenclature logicielle.

Une API partagée ingère les données SCA.

Remarque : Chaque enregistrement d'intégration a un utilisateur d'exécution en tant que configuré. La valeur par défaut pour cet utilisateur est Système VR. Ne changez pas cette valeur.

Chaque jour, les travaux planifiés invoquent automatiquement les intégrations dans l'ordre dans lequel elles sont répertoriées. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Versions disponibles

Versions disponibles pour l'intégration de Black Duck

Version	Notes de publication
Intégration de Réponse aux vulnérabilités avec Black Duck 1.0.5	Notes de publication Réponse aux vulnérabilités des applications

Groupe d'utilisateurs et rôles

Il Intégration de Réponse aux vulnérabilités avec Black Duck est installé par un utilisateur ayant le rôle administrateur et configuré par un membre du groupe App-Sec Manager. Pour en savoir plus, voir Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour connaître les états d'exécution de l'intégration, consultez Afficher l'état de l'exécution de l'importation Intégration de Réponse aux vulnérabilités avec Black Duck

Pour afficher les données dans les vulnérabilités tierces, reportez-vous à la section Afficher les bibliothèques de vulnérabilité.

Préparer les tâches préalables à l'intégration pour Intégration de Réponse aux vulnérabilités avec Black Duck

Planifiez et exécutez les tâches préalables à l'intégration pour que Intégration de Réponse aux vulnérabilités avec Black Duck votre intégration soit réussie. Cela Intégration de Réponse aux vulnérabilités avec Black Duck suppose que vous connaissez l'application et les API de Black Duck Software Composition Analysis (SCA).

Avant de commencer

Avant d'installer et de configurer , Intégration de Réponse aux vulnérabilités avec Black Duckvous devez exécuter et installer l'intégration Common Weakness Enumeration (CWE), qui est également utilisée par Réponse aux vulnérabilités des applications. L'intégration CWE est installée par Réponse aux vulnérabilités défaut.

Remarque : Bien que les données de la base de données de vulnérabilité NIST (NVD) ne soient pas nécessaires pour installer l'intégration de vulnérabilité de l'application Black Duck, il serait utile de les avoir. Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces.

Chaque enregistrement d'intégration a un utilisateur d'exécution en tant que configuré. La valeur par défaut pour cet utilisateur est VR. Système. Ne changez pas cette valeur.

Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter l'intégration, apportez les changements de configuration nécessaires en fonction de vos besoins.

Validez le dimensionnement de votre instance par le nombre d'éléments vulnérables de l'application que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service et assistance client.

Ils nécessitent une URL et un jeton d'API Intégration de Réponse aux vulnérabilités avec Black Duck .

Procédure

Créez le jeton d'API et les informations d'identification de clé.

a. Connectez-vous à la plateforme Black Duck.

b. Accédez au menu Compte d'utilisateur et sélectionnez **Informations d'identification de l'API**.

c. Sélectionnez **Générer des informations d'identification d'API**.

d. Enregistrez vos informations d'identification pour une utilisation ultérieure.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installez le ServiceNow Intégration de Réponse aux vulnérabilités avec Black Duck

Avant d'exécuter l'intégration sur votre instance, vous devez effectuer les étapes d'installation et de configuration afin que l'outil Analyse de la composition logicielle (SCA) de Black Duck s'intègre correctement à Réponse aux vulnérabilités des applications.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Vous devez effectuer ces tâches de configuration afin que l'outil Analyse de la composition logicielle (SCA) Black Duck s'intègre correctement à Réponse aux vulnérabilités des applications.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, reportez-vous à la section Installer Réponse aux vulnérabilités.
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si elle n'est pas déjà affectée, l'utilisateur disposant du rôle administrateur installe l'application et affecte les utilisateurs au groupe App-Sec Manager. Pour en savoir plus sur les rôles de groupe, reportez-vous à Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs. • Le groupe Gestionnaire de sécurité des applications supervise la configuration et vérifie les résultats attendus.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Cet outil SCA est disponible sous forme d'abonnement distinct.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez l'installer Intégration de Réponse aux vulnérabilités avec Black Duck .
2. Accédez au ServiceNow Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans le ServiceNow Store, recherchez Vulnerability Response Integration avec l'application Black Duck.
4. Sélectionnez la vignette de l'application.
   Les détails de l'application que vous installez s'affichent.

   Remarque : pensez à lire les sections Autres exigences et Dépendances, le cas échéant.

5. Sélectionnez **Demande d'application** et entrez vos Now Support informations d'identification de connexion.
6. Sélectionnez **Obtenir**.
7. Entrez le nom de l'instance et le motif de l'instance, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demander**.
   Vous recevrez un e-mail avec les instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Configurez le Intégration de Réponse aux vulnérabilités avec Black Duck pour votre environnement. Reportez-vous à la rubrique Configurez la Intégration de Réponse aux vulnérabilités avec Black Duck..

Configurez la Intégration de Réponse aux vulnérabilités avec Black Duck.

Avant d'exécuter la Intégration de Réponse aux vulnérabilités avec Black Duck sur votre instance, vous devez effectuer les étapes d'installation et de configuration afin que l'outil Analyse de la composition logicielle (SCA) Black Duck s'intègre correctement à l'application Réponse aux vulnérabilités des applications .

Avant de commencer

Rôle requis : groupe d'utilisateurs du gestionnaire App-Sec

Pourquoi et quand exécuter cette tâche

Le Intégration de Réponse aux vulnérabilités avec Black Duck est disponible sous forme d'abonnement distinct.

Procédure

1. Accédez à la **Tout** > **Intégration de Vulnérabilité Blackduck** > **Configuration**.
2. Sélectionnez le type d'authentification de base.
   L'authentification de base nécessite un Pour Serveur MID les instances locales. Vous pouvez générer le jeton d'API requis pour l'authentification de base à partir de votre compte Black Duck.
3. Renseignez les champs du formulaire.
   Authentification de base

Champ	Description
URL D'API	URL de l'API Black Duck pour les instances d'entreprise ou locales. L'instance locale est l'URL de votre point de terminaison Black Duck.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Jeton d'API	Jeton que vous avez généré à partir de votre console Black Duck.
Serveur MID	Serveur MID requis pour les instances locales pour l'authentification de base.
Inclure SCA	Vulnérabilités des analyses de composition logicielle (SCA) incluses par défaut. Les analyses SCA identifient les vulnérabilités dans les composants open source.
Sélectionner l'option pour gérer les faux positifs dans ServiceNow	ServiceNow Option de gestion des faux positifs. Laissez cette option activée si vous souhaitez trier les éléments vulnérables de l'application (AVI) importés avec les états **de source** qui sont marqués comme **faux positif** ou **faux positif potentiel**. Les AVI avec ces états **source** , qui sont normalement mappés à un état **Fermé** dans votre instance, sont mappés à **Ouvert**. Vous pouvez demander un **faux positif** à partir de l'enregistrement AVI. ◦ Désactivez l'une ou les deux options si vous souhaitez conserver les états **source** qui ont été importés à partir de votre scanner. ◦ Si cette option est désactivée, les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVI.
Instance d'intégration	Instance que vous utilisez pour importer les données.

4. Sélectionnez **Enregistrer et tester les informations d'identification**.
5. Exécutez l'intégration de la **liste des projets Black Duck** avant d'exécuter d'autres intégrations.
   Les autres intégrations de Black Duck, telles que l'intégration de la liste des applications Black Duck et l'intégration des éléments vulnérables des applications Black Duck, dépendent des données du projet et de l'application actuelles que vous avez importées à partir de l'intégration de la liste des projets.

Afficher l'état de l'exécution de l'importation Intégration de Réponse aux vulnérabilités avec Black Duck

Vérifiez la réussite de vos exécutions d'intégration, localisez les problèmes et confirmez vos décisions de rattrapage en consultant la liste connexe Exécutions de l'intégration de vulnérabilité.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Intégration de Vulnérabilité Blackduck** > **Intégrations**.
2. Sélectionnez une intégration.
3. Sélectionnez la liste connexe Exécutions de l'intégration de vulnérabilité.
4. Vérifiez que toutes les importations ont réussi.
   Dépannage:

   Les causes les plus courantes d'un échec d'exécution sont les suivantes :

   - Interruption du réseau.
   - Un problème dans le transfert de données qui entraîne la corruption des données lors d'une transformation.

   Si vous rencontrez l'une de ces conditions, sélectionnez **Exécuter maintenant**, puis réexécutez l'intégration.
5. Pour afficher les référentiels importés, accédez à la liste des intégrations et sélectionnez l'enregistrement Black Duck Integration.
6. Sélectionnez la liste connexe Exécutions de l'intégration de vulnérabilité et ouvrez un enregistrement.

Transformation des données pour le Intégration de Réponse aux vulnérabilités avec Black Duck

Une fois que vous avez identifié les données que vous souhaitez importer, elles sont récupérées à partir du Intégration de Réponse aux vulnérabilités avec Black Duck, traitées via un ensemble de sources de données et transformées dans votre instance.

Intégration de Réponse aux vulnérabilités avec Black Duck

Les données de l'API sont d'abord chargées dans la table Importation d'élément [sn_vul_blackduck_appvul_item_import] Black Duck et la transformation d'élément AppVul Black Duck est utilisée pour transformer les informations importées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez **Black Duck AppVul Item Transform**. La table suivante répertorie les champs de carte de transformation par intégration.

Canard noir Champs de carte de transformation d'élément AppVul

Champ source	Champ cible	Description
app_id	source_app_id	ID d'application.
ID du problème	source_avit_id	ID AVIT.
app_name	app_name	Nom de l'application.
version	app_version	Version d'application.
build_id	source_scan_id	ID de build de l'application.
account_id	account_id	ID de compte.
sandbox_id	sandbox_id	ID de bac à sable.
last_update_time	last_scan_date	Heure de la dernière mise à jour.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Canard noir Champs de carte de transformation d'élément AppVul (suite)

Champ source	Champ cible	Description
app_name + last_scan_date	scan_summary_name	Synthèse de l'analyse.
life_cycle_stage	source_sdlc_status	État SDLC de la source.
niveau	source_severity	Gravité de la source.
category_name	catégorie	Catégorie.
source_severity	source_severity	Gravité de la source.
category_id + " CWE- » + cweld	source_entry_id	ID de l'entrée source.
source_vulnerability_summary	source_vulnerability_summary	Résumé de vulnérabilité source.
source_recommendation	source_recommendation	Recommandation de source.
description	description	Description tirée de la source.
description	source_vulnerability_explanation	Explication de vulnérabilité source.
mitigation_status_desc	source_mitigation_status	État de l'atténuation de la source.
remediation_status	source_remediation_status	État du rattrapage de la source.
ligne	line_number	Ligne sur laquelle se trouve la faille.
module	application_module	Module d'application.
Fichier source	source_notes	Notes de la source.
affects_policy_compliance	complies_with_policy	Les valeurs peuvent être Oui ou Non selon que les informations sur la source sont vrai ou faux.
Chemin d'accès du fichier source + fichier source	emplacement	Le mappage d'emplacement est une faille statique.
URL	emplacement	Mappage d'emplacement pour une faille dynamique.
périmètre, type, niveau d'exploitation	source_additional_info	Champ de valeur de nom renseigné avec les valeurs de la source pour les défauts statiques.

La table suivante répertorie les scripts de transformation exécutés au cours du processus de transformation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calendrier et objectif du script de carte de transformation de Black Duck

Canard noir Script de carte de transformation

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour traiter l'enregistrement et mettre à jour le nombre d'entités créées, mises à jour ou inchangées et celles importées dans le cadre de cette intégration. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation)	Script utilisé pour définir le comportement des enregistrements qui ne sont pas valides et doivent être ignorés. Également utilisé pour définir l'objet global pour le traitement des enregistrements. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Canard noir Mappage de l'état d'intégration

Le tableau suivant présente les états sources de l'intégration de vulnérabilité Black Duck et leurs états cibles dans votre instance.

États sources du Canard noir et leurs états correspondants Now Platform

États sources de Canard noir	Description des états de la source	État cible dans Now Platform
Nouveau	La vulnérabilité affecte cette version de composant.	Ouvrir
Requiert une revue	Impossible de déterminer si une vulnérabilité affecte cette version de composant.	Ouvrir
Rattrapage requis	Une correction est requise pour cette version.	Ouvrir
Remédiation terminée	Le rattrapage de cette vulnérabilité est terminé.	Fermé
Atténué	La vulnérabilité a été atténuée.	Fermé
Patché	Une vulnérabilité a été corrigée.	Fermé
Ignoré	La vulnérabilité a été ignorée.	Fermé

Importer les informations du projet à partir de l'instance d'intégration Black Duck

Importez les informations du projet à partir de l'instance d'intégration Black Duck pour vous assurer que les intégrations de vulnérabilité s'exécutent de manière séquentielle. Une intégration réussie vous aide à identifier et à ingérer les éléments vulnérables de l'application (AVI).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche
Vous pouvez importer toutes les informations sur le projet à partir de Intégration de Réponse aux vulnérabilités avec Black Duck la table des projets [sn_vul_blackduck_project] Black Duck. Tous les attributs requis, par exemple, le GUID du projet, qui sont requis pour interroger différentes versions du projet, sont capturés dans la table des projets [sn_vul_blackduck_project] Black Duck.

Procédure
1. Accédez à la **Tout** > **Intégration de Vulnérabilité Blackduck** > **Intégrations**.
2. Sélectionnez une intégration.
   Par exemple, vous pouvez sélectionner **l'intégration de liste de projets Black Duck.**
3. Sélectionnez **Exécuter maintenant**.

   Remarque : Chacun d'entre eux Intégration de Réponse aux vulnérabilités avec Black Duck est destiné à fournir la récupération de données la plus complète possible. L'exécution de ces intégrations dans le désordre peut entraîner des données incomplètes et nécessite ServiceNow une expertise d'Application Vulnerability Response.

   Une fois l'importation terminée, vous pouvez voir les détails du projet dans la table des projets Canard noir [sn_vul_blackduck_project].
4. Pour connaître les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation Intégration de Réponse aux vulnérabilités avec Black Duck.
5. Facultatif : Si vous souhaitez modifier d'autres paramètres d'intégration, vous devez accéder à l'instance d'intégration.

Importer Intégration de Réponse aux vulnérabilités avec Black Duck les versions du projet dans la table Applications détectées

Importez l'intégration de Vulnerability Response avec les versions de projet Black Duck dans la table Applications détectées [sn_vul_release] afin que les intégrations de Black Duck Vulnerability s'exécutent séquentiellement. Une intégration réussie vous aide à identifier et à ingérer les éléments vulnérables de l'application (AVI).

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche
Vous pouvez ajouter et afficher toutes les différentes versions des projets (voir les détails dans le tableau des projets Black Duck) qui ont été importées à partir du Intégration de Réponse aux vulnérabilités avec Black Duck tableau Applications détectées [sn_vul_release].

Procédure
1. Accédez à la **Tout** > **Intégration de Vulnérabilité Blackduck** > **Intégrations** .
2. Sélectionnez une intégration.
   Par exemple, vous pouvez sélectionner **l'intégration de la liste des applications Black Duck**.
3. Sélectionnez **Exécuter maintenant**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Chaque version de projet des intégrations est destinée à fournir la récupération de données la plus complète. L'exécution de ces intégrations dans le désordre peut entraîner des données incomplètes et nécessite une expertise de ServiceNow et d'Application Vulnerability Response.

Une fois l'importation terminée, vous pouvez voir les différentes versions d'un projet dans la table Applications détectées [sn_vul_release]. Si vous utilisez des règles de recherche de CI, ces applications détectées sont liées à la table d'éléments de configuration [cmdb_ci].

4. Affichez l'état des exécutions de votre intégration.
   Pour plus d'informations, consultez Afficher l'état de l'exécution de l'importation Intégration de Réponse aux vulnérabilités avec Black Duck.

Importer les éléments vulnérables de l'application à partir de Intégration de Réponse aux vulnérabilités avec Black Duck

Importez les éléments vulnérables de l'application (AVI) à partir de l'intégration de Vulnerability Response avec Black Duck afin que l'intégration s'exécute de manière séquentielle. Une intégration réussie vous aide à identifier et à ingérer les AVI.

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche
Vous pouvez afficher les résultats de l'analyse à partir du Intégration de Réponse aux vulnérabilités avec Black Duck, insérer des AVI dans votre instance et enrichir vos données de vulnérabilité tierces. Par défaut, si l'enregistrement du scanner est à l'état Fermé, les AVI ne sont pas créés. Vous pouvez contrôler les AVI existants à l'aide de la propriété sn_vul_create_closed.

Procédure

1. Accédez à la **Tout** > **Intégration de la vulnérabilité Black Duck** > **Intégrations**.
2. Sélectionnez une intégration.
   Par exemple, vous pouvez sélectionner **l'intégration des éléments vulnérables de l'application Black Duck**.
3. Sélectionnez **Exécuter maintenant**.

Remarque : L'objectif Intégration de Réponse aux vulnérabilités avec Black Duck est de vous fournir la récupération de données la plus complète possible. L'exécution de ces intégrations dans le désordre pourrait entraîner des données et des besoins ServiceNow et Réponse aux vulnérabilités des applications une expertise incomplets.

Une fois que vous avez importé toutes les vulnérabilités SCA à partir du Intégration de Réponse aux vulnérabilités avec Black Duck, vous pouvez afficher les AVI et les données de vulnérabilité tierces.

Définir les heures d'importation pour le Intégration de Réponse aux vulnérabilités avec Black Duck

Définissez l'heure de début des Intégration de Réponse aux vulnérabilités avec Black Duck importations. Vous pouvez définir les intégrations à l'avance afin d'obtenir de meilleures performances et d'accélérer les exécutions d'importation.

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche
Après l'importation initiale, les intégrations de vulnérabilité Black Duck procèdent à une importation complète à chaque exécution.

Procédure
1. Accédez à la **Tout** > **Intégration de la vulnérabilité Black Duck** > **Intégrations**.
2. Sélectionnez une intégration.
3. Définissez la nouvelle **heure de début**.
   L'heure est calculée en heures en heure locale. L'heure par défaut pour les importations de l'intégration de la liste d'applications Black Duck est 00:00:00. Les autres intégrations sont **à la demande** et sont chaînées, ce qui signifie qu'elles suivent une séquence à exécuter après l'intégration de la liste des applications Black Duck. La modification de **l'heure de début** nécessite un niveau avancé ServiceNow et Gestion de la vulnérabilité des applications une expertise.
4. Sélectionnez **Mettre à jour**.
   La nouvelle heure est utilisée pour la prochaine importation planifiée.

Inclure les éléments vulnérables de l'application Canard noir fermés

Incluez les éléments vulnérables de l'application (AVI) fermés lors des importations d'intégration des éléments vulnérables Black Duck, car par défaut, ils ne sont pas créés lors des importations d'intégration. Si vous souhaitez les créer, vous devez modifier la propriété système.

Avant de commencer
Assurez-vous que le est installé et en cours d'exécution Intégration de Réponse aux vulnérabilités avec Black Duck .

Rôle requis : administrateur

Procédure
1. Dans le filtre de navigation, saisissez `sys_properties.list`.
2. Dans le champ **Nom** de la liste, saisissez `sn_vul.create_closed`.
3. Double-cliquez sur le champ **Valeur** et définissez-le sur **Vrai**
4. Enregistrez en sélectionnant l'icône de coche verte .
   Les enregistrements à l'état Fermé lors de la prochaine importation de Black Duck sont créés en tant qu'AVI dans Réponse aux vulnérabilités des applications.

Fortify Vulnerability Integration

Le Fortify Vulnerability Integration utilise des Fortify données importées du produit pour vous aider à déterminer l'impact et la priorité des failles dans votre code.

Fortify Vulnerability Integration

Le Fortify produit collecte les données du scanner et met ces données à la disposition du Now Platform®. Il s'intègre facilement à la ServiceNow® Réponse aux vulnérabilités des applications fonctionnalité de mappage des Réponse aux vulnérabilités vulnérabilités tierces, enrichissant ainsi les données de votre instance.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chaque jour, les travaux planifiés invoquent automatiquement les intégrations. Une fois que toutes les intégrations sont activées, elles sont enchaînées pour s'exécuter en séquence. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Versions disponibles

Version	Notes de publication
Intégration de Vulnerability Response avec Fortify v2.4 Fortify v2.3 Fortify v2.2 Fortify v2.1	Notes de publication Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Fortify Vulnerability Integration

Pour afficher le Fortify Vulnerability Integration, accédez à **Intégration de vulnérabilité Fortify** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base. Ces intégrations ne sont pas toutes actives par défaut.

Après l'exécution initiale, chaque jour, des travaux planifiés sont enchaînés pour exécuter automatiquement les intégrations dans l'ordre. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Fortify Intégrations de vulnérabilité

Intégration	Description
Fortify Intégration de la liste des applications sur demande	Récupère les données du scanner d'applications Fortify (vulnérabilités, métadonnées) et enrichit vos données d'applications tierces. Cette intégration est définie pour s'exécuter quotidiennement à 00:00:00. Il est actif par défaut.
Fortify Intégration de synthèse de l'analyse sur demande	Récupère les enregistrements d'analyse à partir de Fortify. Cette intégration est chaînée pour s'exécuter après l'intégration de la liste d'applications Fortify sur demande lorsqu'elle est activée. Il est inactif, par défaut.
Fortify Intégration d'éléments	Récupère les résultats d'analyse de Fortify, insère les AVIT et enrichit vos données de vulnérabilité tierces. Si l'enregistrement du scanner est **à**

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fortify Intégrations de vulnérabilité (suite)

Intégration	Description
vulnérables d'applications sur demande	l'état Fermé, les AVIT ne sont pas créés. Les AVIT existants sont toujours mis à jour. À partir de la version 2.3, affichez les détails tels que les délais de traitement totaux, les temps moyens des processus d'exécution avant et après l'intégration, et les rapports sur les enregistrements d'exécution de l'intégration pour l'intégration des éléments vulnérables de l'application. Cette intégration est chaînée pour s'exécuter après l'intégration de synthèse de l'analyse Fortify sur demande lorsqu'elle est activée. Il est inactif, par défaut.

Pour les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation Fortify Vulnerability Integration.

Pour afficher les données dans les vulnérabilités tierces, reportez-vous à la section Afficher les bibliothèques de vulnérabilité.

Se préparer à la Fortify Vulnerability Integration

Une réussite Fortify Vulnerability Integration nécessite la planification et l'exécution de tâches préalables à l'intégration. Préparez l'intégration en effectuant ces tâches. suppose Fortify Vulnerability Integration que vous connaissez le produit et l'API Fortify .

Avant de commencer

L'intégration CWE (Common Weakness Enumeration) est également utilisée par Réponse aux vulnérabilités des applications et doit être exécutée avant l'installation et la configuration de .Fortify Vulnerability Integration

Remarque : Il n'est pas nécessaire d'installer les données de la Fortify Vulnerability Integrationbase de données de vulnérabilité NIST (NVD), mais elles fournissent un enrichissement et seraient utiles d'avoir.

Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Rôle requis : App-Sec Manager

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter l'intégration, apportez tout changement de configuration nécessaire en fonction de vos besoins.

Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables de l'application que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service et assistance client.

Le nécessite une clé API, un secret API et une URL racine d'API Fortify Vulnerability Integration , disponibles à partir de votre Fortify compte à la demande.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Pour créer une clé secrète d'API :

a. Connectez-vous à votre Fortify portail à la demande.

b. Accédez à la **Tout** > **Administration** > **Paramètre** > **API**.

c. Ajoutez ServiceNow en tant qu'application.

d. Cliquez sur **Nouveau secret** pour générer un secret API.

e. Enregistrez votre secret API pour une utilisation ultérieure.

Installer l'intégration de ServiceNow® Vulnerability Response avec Fortify

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit s'intègre Fortify correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe App-Sec Manager. Pour plus d'informations sur les rôles de groupe, Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateursreportez-vous à la section . • Le groupe Gestionnaire de sécurité des applications supervise la configuration et vérifie les résultats attendus.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : App-Sec Manager

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez l'installer Fortify Vulnerability Integration .
2. Accédez au ServiceNow Store.
3. Dans le ServiceNow Store, recherchez l'intégration de Vulnerability Response à Fortify l'application.
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **Dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Configurez le Fortify Vulnerability Integration pour votre environnement. Consultez Configurez la Fortify Vulnerability Integration..

Configurez la Fortify Vulnerability Integration.

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le Fortify produit s'intègre correctement à la Réponse aux vulnérabilités des applications fonctionnalité .Réponse aux vulnérabilités Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Rôles requis : Gestionnaire App-Sec

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que l'intégration à Fortify l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer l'intégration de ServiceNow Vulnerability Response avec Fortifyreportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe App-Sec Manager. • Le gestionnaire App-Sec supervise la configuration et vérifie les résultats attendus.
Pour le Fortify Vulnerability Integration, préparez votre **ID API** et votre **clé API** .	Contact Fortify permettant d'obtenir **l'ID API** et la **clé API**.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer les intégrations de vulnérabilité de l'application Fortify .
2. Accédez au ServiceNow Store.
3. Dans le ServiceNow Store, recherchez l'intégration à Fortify l'applicationRéponse aux vulnérabilités.
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **Dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Votre application est automatiquement installée sur votre instance.
11. Une fois l'installation terminée, accédez à **Intégration de vulnérabilité Fortify** > **Configuration de FoD**.
12. Renseignez les champs du formulaire.

Formulaire de configuration de Fortify sur demande

Champ	Description
URL racine de l'API	URL de l'instance Fortify de l'utilisateur.
Clé API	Identificateur unique envoyé à l'API Fortify .
Secret API	Secret client fourni par Fortify.
Inclure DAST	Option permettant d'inclure les vulnérabilités des analyses DAST. Les analyses DAST identifient les vulnérabilités dans le comportement de l'ensemble de votre application.
Inclure SAST	Option permettant d'inclure les vulnérabilités des analyses SAST. Les analyses SAST identifient des vulnérabilités dans le code.
Triage des exceptions et des faux positifs dans ServiceNow (à partir de la version 20.0 de Vulnerability Response)	Sélectionnez des options pour gérer la gestion des exceptions et les faux positifs pour AVI avec ServiceNow des workflows automatiquement lors de l'importation. Ces options sont activées par défaut. Pour consulter un exemple de cas d'utilisation, reportez-vous à la section Gestion du mappage d'état pour les reports et les faux positifs dans Réponse aux vulnérabilités des applications. Gérer les exceptions dans ServiceNow Laissez cette option activée si vous souhaitez trier les AVI importés marqués pour l'état **Différé** . Les AVI dont les états **sources** sont normalement mappés à un état **Différé** dans votre instance sont à la place mappés à **Ouvert**. Vous **demandez une exception** à partir de l'enregistrement AVI. Gérer les faux positifs dans ServiceNow Laissez cette option activée si vous souhaitez trier les AVI importés avec des états **source**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	marqués comme **Faux positif** ou **Faux positif potentiel**. Les AVI avec ces états **source** , qui sont normalement mappés à un état **Fermé** dans votre instance, sont mappés à **Ouvert**. Vous demandez un **faux positif** à partir de l'enregistrement AVI. ◦ Décochez l'une des cases ou les deux si vous souhaitez conserver les états **source** importés à partir de votre scanner. ◦ Ces AVI sont mappés aux états cibles et aux états de motif cible au fur et à mesure qu'ils sont importés, mais ne sont pas triés par les workflows d'exception et de faux positif. Les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVI.
Triage dans ServiceNow (avant la version 20.0 de Vulnerability Response)	Gérez le triage de vulnérabilité de votre application dans l'instance ServiceNow : ◦ Cochez la case pour trier les AVI dans ServiceNow. Si cette option est sélectionnée, les AVI sont importés à l'état Ouvert. Vous pouvez ensuite demander une exception ou marquer l'AVI comme faux positif. ◦ Pour conserver l'état source, c'est-à-dire l'état importé du scanner, assurez-vous que la case n'est pas cochée. **Remarque :** Les options **Marquer comme faux positif** et **Demander une exception** ne sont disponibles que pour les AVI triés dans .ServiceNow

13. Sélectionnez **Enregistrer et tester les informations d'identification**.

Que faire ensuite

Si votre environnement nécessite des importations séparées par domaine, reportez-vous à la section Créer des importations séparées par domaine pour une intégration.

Lors de l'installation initiale, reportez-vous à la section Configurer Réponse aux vulnérabilités des applications pour plus d'instructions.

Après l'installation initiale, pour les modifications, reportez-vous à la section Fortify Vulnerability Integration Modification et activités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher l'état de l'exécution de l'importation Fortify Vulnerability Integration

Utilisez la liste connexe **Exécutions de l'intégration de vulnérabilité** pour vérifier la réussite de vos exécutions d'intégration, localiser les problèmes et prendre des décisions de rattrapage.

Avant de commencer

Pour afficher l'état de l'exécution de l'importation Fortify :

- Les Réponse aux vulnérabilités applications and Fortify Vulnerability Integration doivent être installées et configurées.
- Les Fortify Vulnerability Integration importations doivent être planifiées et en cours d'exécution.

Rôle requis : App-Sec Manager

Pourquoi et quand exécuter cette tâche

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités des applications, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Fortify** > **Intégrations**.
2. Sélectionnez une intégration.
3. Cliquez sur la liste connexe **Exécutions de l'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.
5. À partir de la version 2.3, affichez des détails tels que les durées totales de traitement, les durées moyennes des processus d'exécution avant et après l'intégration, ainsi que des rapports sur les enregistrements d'exécution de l'intégration pour les intégrations d'éléments vulnérables d'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fortify Vulnerability Integration Modification et activités

Configurez des modifications facultatives spécifiquement pour le Fortify Vulnerability Integration.

Remarque : La modification d'autres Fortify Vulnerability Integration paramètres, autres que ceux répertoriés ici, nécessite une expertise avancée ServiceNowRéponse aux vulnérabilités des applications et dépasse le cadre de la documentation du produit.

Importer manuellement Fortify la vulnérabilité de l'application

Si votre importation initiale a échoué, ou si vous ne souhaitez pas attendre l'importation initiale planifiée, vous pouvez effectuer une importation de données complète indépendamment de la tâche planifiée quotidienne.

Avant de commencer

Rôle requis : App-Sec Manager

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Fortify** > **Intégrations**.
2. Choisissez une intégration, par exemple, l'intégration de liste d'applications Fortify .
3. Sélectionnez **Exécuter maintenant**.

Remarque : Pour une récupération complète des données, exécutez les intégrations de vulnérabilité de l'application Fortify dans l'ordre.

Importer des données à l'aide de Fortify Vulnerability Integration

Importez des données à partir du scanner Fortify pour mapper les éléments vulnérables de l'application (AVI), enrichissant ainsi les données dans votre instance.

Avant de commencer

Rôle requis : App-Sec Manager

Pourquoi et quand exécuter cette tâche

Après l'importation initiale, Fortify les intégrations de vulnérabilité procèdent à une importation delta à chaque fois qu'elles s'exécutent, récupérant ainsi les données les plus récentes. Voir Importer manuellement Fortify la vulnérabilité de l'application pour plus d'informations sur les importations complètes.

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Fortify** > **Intégrations**.
2. Choisissez une intégration.
3. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom de l'exécution de l'intégration.
Actif	Option permettant d'activer une intégration.
Exécuter	Fréquence d'exécution de l'intégration.
Heure	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Application contenant cet enregistrement.
Intégration source	Intégration source pour cette intégration.
Instance source	Instance source pour cette intégration.
Intégration suivante	Intégration suivante dans la séquence, à exécuter après l'exécution de l'intégration actuelle.
Heure de début	Date et heure de début de la dernière exécution réussie de l'intégration. L'heure est calculée en heures en heure locale. L'heure par défaut pour l'exécution initiale est 00:00:00.
Détails de l'intégration	
Script d'intégration	Include de script qui étend le *VulnerabilityIntegrationBase* à exécuter lorsque l'intégration s'exécute. Ce script définit comment récupérer des données à partir d'un système tiers.
Script de l'instanciateur d'intégration	Script qui définit la façon de construire l'include de script sélectionné pour le script d'intégration.
Stratégie de processeur de rapport	Stratégie que vous souhaitez utiliser pour gérer les données retournées par le script d'intégration lors de l'exécution de l'intégration.

4. Sélectionnez **Exécuter maintenant** pour exécuter l'intégration.

Inclure les éléments vulnérables de l'application Fortify sur demande fermés

Par défaut, les éléments vulnérables de l'application (AVIT) **fermés** ne sont pas créés lors des importations d'intégration Fortify d'éléments vulnérables. Si vous souhaitez les créer, vous devez modifier une propriété système.

Avant de commencer

Ils Fortify Vulnerability Integration doivent être installés et en cours d'exécution.

Rôle requis : App-Sec Manager

Procédure

1. Dans la zone de texte **Navigateur de filtre** de navigation de gauche, saisissez `sys_properties.list`.
2. Dans la zone de recherche **Nom** de la liste, saisissez `sn_vul.create_closed`.
3. Double-cliquez sur le champ **Valeur** et définissez sur **Vrai**
4. Cliquez sur l'icône en forme de coche pour enregistrer.
   Les enregistrements à l'état **Fermé** lors de l'importation suivante Fortify sont créés en tant qu'AVIT dans Réponse aux vulnérabilités des applications.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

GitHub Application Vulnerability Integration

Il GitHub Application Vulnerability Integration importe des données de test statique de sécurité des applications (SAST) et d'analyse de la composition logicielle (SCA) pour vous aider à afficher les alertes de vulnérabilité dans les référentiels de votre GitHub environnement.

GitHub Application Vulnerability Integration

Le GitHub Application Vulnerability Integration collecte les données du scanner et les met à la disposition du Now Platform®. Il s'intègre facilement à la ServiceNow® Réponse aux vulnérabilités des applications fonctionnalité de Réponse aux vulnérabilités mapper les vulnérabilités et GitHub les alertes tierces dans votre instance.

L'environnement GitHub prend en charge plusieurs organisations. Ces organisations, à la fois sur site et d'entreprise, peuvent contenir différents départements, tels que l'ingénierie, la qualité, la documentation, etc. Chaque organisation, à son tour, peut prendre en charge plusieurs référentiels. Après avoir importé vos données d'application avec l'intégration GitHub du référentiel, vous pouvez importer les données de vulnérabilité et d'alerte à partir de ces référentiels. Les données importées sont traitées comme une application dans l'application Réponse aux vulnérabilités des applications . Lorsque les analyseurs détectent des vulnérabilités et génèrent des alertes pour les référentiels, les vulnérabilités sont créées dans Réponse aux vulnérabilités des applications.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Versions disponibles

Version	Notes de publication
GitHub Application Vulnerability Integration v1.2, v1.1, 1.0	Notes de publication Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Intégrations de GitHub

Intégration	Description
GitHub Intégration de référentiel	À partir de la version 1.1, importez toutes les données d'application pour vos GitHub comptes sur site et Cloud (Enterprise). L'intégration importe les applications à partir des référentiels que vous avez configurés pour une organisation (sur site) ou de votre environnement d'entreprise (cloud). Exécutez cette intégration avant d'exécuter les autres GitHub intégrations, car elles dépendent des données d'application actuelles importées à partir de l'intégration de référentiel.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
GitHub Intégration CodeScan	Récupère les alertes de vulnérabilité de l'analyse de code à partir des référentiels pour détecter les vulnérabilités de sécurité et les erreurs de GitHub codage. Les données importées sont mappées aux résultats SAST dans votre instance.
GitHub Intégration Dependabot	Récupère les alertes Dependabot pour les dépendances avec des vulnérabilités connues à partir des référentiels. Les données importées sont mappées aux résultats SCA dans votre instance.
GitHub Analyse secrète	Récupère les secrets du code de votre organisation ainsi que les résultats des tests de sécurité des applications. Les données sont mappées aux résultats SCA de votre instance.
GitHub Emplacement d'analyse secrète	Récupère l'emplacement et les numéros de ligne des secrets analysés dans le code de votre organisation pour aider vos développeurs à y remédier.

Chargement SBOM de fichiers vers le Now Platform® à partir de vos GitHub référentiels

Déterminez si SBOM les fichiers générés dans vos pipelines CI/CD (intégration continue et livraison/déploiement continus) ont été correctement mis en file d'attente dans votre Now Platform® instance.

- Protégez vos environnements contre les composants potentiellement dangereux pendant les cycles de développement logiciel avec GitHub les actions que vous lancez à partir de votre GitHub environnement.
- Obtenez toutes les actions requises GitHub pour SBOM le chargement dans GitHub Marketplace.

Les SBOM applications sont nécessaires pour télécharger SBOM des fichiers. Consultez Explorer Nomenclature logicielle pour plus d'informations.

Affichage des données importées

Les données d'application importées à partir de l'intégration de référentiel GitHub sont affichées dans la table Applications détectées [sn_vul_app_release]. Exécutez d'abord cette intégration.

L'intégration du référentiel importe les balises et les rubriques que vous avez configurées pour un référentiel de votre GitHub compte à partir du menu Paramètres. Toutes les propriétés personnalisées se trouvent dans le menu sous votre référentiel. Les valeurs que vous définissez pour les propriétés sont importées sous forme de paires clé-valeur. Pour savoir où afficher ces informations dans votre instance, reportez-vous à la section Afficher l'état de l'exécution de l'importation et les GitHub Application Vulnerability Integration données du référentiel importées.

Les données importées (résultats) de l'intégration GitHub Dependabot sont affichées dans les tables suivantes.

- Applications détectées [sn_vul_app_release].
- Synthèses de numérisation de vulnérabilité de l'application [sn_vul_app_vul_scan_summary].

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Éléments vulnérables de l'application [sn_vul_app_vulnerable_item].
- Paquets [sn_vul_app_package].

Les données importées à partir de l'intégration GitHub CodeScan sont affichées dans les tables suivantes.

- Applications détectées [sn_vul_app_release].
- Synthèses de numérisation de vulnérabilité de l'application [sn_vul_app_vul_scan_summary].
- Entrées de vulnérabilité de l'application [sn_vul_app_vul_entry].
- Éléments vulnérables de l'application [sn_vul_app_vulnerable_item].

Se préparer à la GitHub Application Vulnerability Integration

Préparez l'intégration en effectuant ces tâches. suppose GitHub Application Vulnerability Integration que vous connaissez le produit et l'API GitHub.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Rôles requis :

- Administrateur pour télécharger, installer et activer des applications et affecter des rôles.
- Administrateur GitHub pour obtenir des informations d'identification et générer des jetons dans la console GitHub.
- administrateur pour configurer les connexions et les enregistrements d'alias dans votre instance.

Tâches de configuration

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que le est GitHub Application Vulnerability Integration installé et activé.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installez le ServiceNow GitHub Application Vulnerability Integrationreportez-vous à la section .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration (suite)

Tâches de configuration	Description
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe d'utilisateurs App-Sec Manager. • Le gestionnaire App-Sec supervise la configuration et vérifie les résultats attendus. • sn_vul_github_config_integration est héritée par le groupe d'utilisateurs App-Sec Manager. Ce rôle contient les rôles connection_admin et oauth_admin.
Obtenez vos informations d'identification et de compte GitHub.	Les informations de compte sont requises sur les enregistrements que vous créez pour l'authentification. Pour Création d'informations d'identification OAuth 2.0 pour GitHub les applications : JWT pour le GitHub Application Vulnerability Integration plus d'informations sur les détails, consultez votre besoin et la configuration des enregistrements requis pour l'authentification OAuth.
Vérifiez que vous importez des données Common Weakness Enumeration (CWE).	L'intégration CWE (Common Weakness Enumeration) est également utilisée par Réponse aux vulnérabilités des applications l'intégration GitHub Vulnerability Integration et doit être en cours d'exécution avant celle-ci. Il est installé avec Réponse aux vulnérabilités, par défaut. **Remarque :** Les données de la base de données de vulnérabilité NIST (NVD) ne sont pas nécessaires pour installer l'intégration de vulnérabilité GitHub, cependant, elles fournissent un enrichissement et seraient utiles d'avoir. Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces.

Création d'informations d'identification OAuth 2.0 pour GitHub les applications : JWT pour le GitHub Application Vulnerability Integration

Procédez comme suit pour intégrer vos GitHub applications à l'aide du jeton JWT Bearer pour le GitHub Application Vulnerability Integration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles requis :

- sn_vul.app_sec_manager et admin pour les enregistrements de votre Now Platformfichier .
- Aucun rôle d'instance requis pour les tâches de votre GitHub compte.

.

Créez et configurez l'application GitHub pour le GitHub Application Vulnerability Integration

Créez une application personnalisée GitHub à partir de votre GitHub compte pour activer l'authentification OAuth 2.0 avec vous GitHub Application Vulnerability Integration dans votre instance.

Avant de commencer
Rôle requis : aucun rôle d'instance requis

Pourquoi et quand exécuter cette tâche
Suivez ces étapes à partir de votre GitHub compte. Reportez-vous à Bâtiment GitHub Applications sur le site Developer pour obtenir des instructions sur la création et la GitHub configuration d'applications personnalisées.

Procédure
1. À partir de votre GitHub compte, créez votre GitHub application en accédant à **Paramètres de développeur** > **Applications GitHub**.
2. Dans le champ URL de la **page d'accueil** , saisissez `https://<nom-instance>.service-now.com`.
3. Dans le champ **URL de rappel d'autorisation de l'utilisateur** , saisissez `https://<nom-instance>.service-now.com/oauth_redirect.do`.
4. Dans la section **Identification et autorisation des utilisateurs** , désélectionnez le champ **Faire expirer les jetons d'autorisation de l'utilisateur** .
5. Dans la section **Webhook** , sélectionnez le champ **Actif** .
6. Dans le champ **URL Webhook** , saisissez `https://instance-name>.service-now.com/`.
7. Laissez les champs restants vides (par défaut).
8. Dans la section **Autorisations du référentiel** , configurez les paramètres suivants.

Analyse de code	Lecture seule
Contenus	Lecture seule
Propriétés personnalisées	Lecture seule
Alertes Dependabot	Lecture seule
Métadonnées	Lecture seule

Remarque : Si vous utilisez déjà une application GitHub et que vous mettez à jour l'une des autorisations, vous devez vérifier et accepter ces autorisations pour votre application GitHub. Vous pouvez accéder à votre application, puis sélectionner **Configurer > demande d'examen > Accepter de nouvelles autorisations**.

9. Laissez les autorisations restantes sur `Aucun accès` (par défaut).
10. Dans la section **S'abonner aux événements** , sélectionnez l'option **Règle de protection du déploiement** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. Cliquez avec le bouton droit de la souris dans l'en-tête pour enregistrer les modifications.
12. Installez l'application nouvellement créée GitHub sur les comptes de votre choix.

    a. Sur la page des paramètres des applications GitHub, sélectionnez votre application.

    b. Dans la barre latérale gauche, sélectionnez **Installer l'application**.

    c. Sélectionnez **Installer** à côté du compte d'organisation ou personnel contenant le référentiel approprié.

    d. Installez l'application sur tous les référentiels ou sélectionnez des référentiels. Pour plus d'informations, consultez Installation d'applications GitHub .

13. Après l'installation, sélectionnez les paramètres (icône d'engrenage) de votre application et notez ou notez les informations suivantes.

    Ces détails sont requis lorsque vous créez le registre d'application dans votre Now Platform instance.

    - ID d'application
    - ID client
    - Secret client.
    - Notez le jeton dans l'URL. Il s'agit de l'ID de jeton que vous saisissez dans l'URL du jeton de votre instance.

14. Faites défiler la page vers le bas et générez une nouvelle clé privée et enregistrez-la sur votre ordinateur.

Générer le certificat JKS pour le GitHub Application Vulnerability Integration

Générez un certificat JKS pour l'authentification JWT pour le GitHub Application Vulnerability Integration.

Avant de commencer

Vous devez noter le mot de passe que vous utilisez pour générer le fichier .jks (mot de passe KeyStore).

Rôle requis : sn_vul.app_sec_manager

Procédure

1. Créez un certificat signé par une autorité de certification à l'aide de la clé privée de l'application GitHub :

```
openssl req -new -x509 -key <file-name>.pem -out <certificate-name>.pem
 -days 1095
```

2. Saisissez les informations requises.
3. Créez le fichier PKCS 12 à l'aide de la clé privée de l'application et du certificat signé par l'autorité de GitHub certification :

```
openssl pkcs12 -export -in <certificate-name>.pem -inkey
 <file-name>.pem -certfile <certificate-name>.pem -out
 <PKCS-12-file-name>.p12
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Fournissez le mot de passe d'exportation.
5. Créez le fichier JKS :

```
keytool -importkeystore -srckeystore <PKCS-12-file-name>.p12
 -srcstoretype pkcs12 -destkeystore <JKS-certificate-filename>.jks
 -deststoretype JKS
```

6. Fournissez les mots de passe de magasin de clés de destination et source.

Joindre le GitHub certificat Java Key Store à votre instance pour le GitHub Application Vulnerability Integration

Activez l'authentification du jeton JWT Bearer Grant en joignant le certificat GitHub Java KeyStore (JKS) valide à votre instance.

Avant de commencer

Un certificat Java KeyStore valide.

Rôle requis : sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Certificats**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire.

Champs du formulaire Certificat X.509

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement de façon unique. Par exemple, `Certificat de mon application GitHub pour AVR`.
Notification à l'expiration	Option permettant de spécifier les utilisateurs à notifier lorsque le certificat expire.
Avertissement avant l'expiration (en jours)	Nombre de jours avant l'expiration du certificat.
Actif	Option permettant d'activer le certificat.
Type	Option permettant de sélectionner le type de certificat. Sélectionnez **le magasin de clés Java**.
Échéance en jours	Nombre de jours avant l'expiration du certificat.
Mot de passe de magasin de clés	Mot de passe associé au certificat (indice : le mot de passe KeyStore de destination précédemment créé).
Description brève	Résumé du certificat.

4. Sélectionnez l'icône de pièces jointes et joignez un certificat JKS.
5. Sélectionnez **Valider les stocks/certificats**.
   Un message key_store valide s'affiche pour les fichiers de certificat valides.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une clé de signature JWT pour le GitHub certificat JKS pour le GitHub Application Vulnerability Integration

Créez une clé de signature JSON Web Token (JWT) à affecter à votre GitHub certificat Java KeyStore.

Avant de commencer

Rôles requis :

- administrateur
- sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Clés JWT**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire.

Champs du formulaire Clés JWT

Champ	Description
Nom	Nom permettant d'identifier de façon unique la clé de signature JWT. Par exemple, `Clé JWT de mon application GitHub pour AVR`.
Magasin de clés de signature	Sélectionnez le certificat JKS valide que vous avez joint lors de la tâche précédente.
ID de clé	Laissez ce champ vide.
Algorithme de signature	Laissez cette valeur sur RSA 256.
Signature avec le mot de passe de clé	Mot de passe associé à la clé de signature. Il s'agit du mot de passe que vous avez utilisé pour générer le fichier JKS.
Actif	Option permettant d'activer la clé.

4. Cliquez avec le bouton droit de la souris n'importe où dans l'en-tête gris de la page et sélectionnez **Enregistrer**.

Créer un fournisseur JWT pour votre GitHub clé de signature pour le GitHub Application Vulnerability Integration

Ajoutez un fournisseur JSON Web Token (JWT) à votre ServiceNow instance pour GitHub.

Avant de commencer

Rôles requis :

- administrateur
- sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Fournisseurs JWT**.
2. Sélectionnez **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Renseignez les champs du formulaire.

Champs du formulaire Fournisseur JWT

Champ	Description
Nom	Nom permettant d'identifier de façon unique le fournisseur JWT. Par exemple, `Mon application GitHub Fournisseur JWT pour AVR`.
Intervalle d'expiration (s)	Nombre de secondes pour définir la durée de vie des jetons de fournisseur JWT. Vous pouvez conserver ce paramètre par défaut.
Configuration de la signature	Sélectionnez la clé JWT que vous avez créée lors des étapes précédentes.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
5. Entrez votre GitHub**ID d'application** d'application pour la valeur **de la** réclamation iss, dans la liste connexe des réclamations standard.
   Il s'agit de l'ID de l'application dans votre GitHubGitHub console que vous avez créé lors des étapes précédentes.
6. Laissez **les valeurs aud** et **sub** vides (par défaut).
7. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.

Enregistrer GitHub en tant que fournisseur OAuth (JWT) pour GitHub Application Vulnerability Integration

Utilisez les informations générées pendant GitHub la configuration du compte d'application pour vous inscrire GitHub en tant que fournisseur OAuth et permettre à l'instance de demander des jetons OAuth 2.0.

Avant de commencer

Rôles requis :

- administrateur
- sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Registre d'application**.
2. Sélectionnez **Nouveau**.
   Le message Quel type d'application OAuth ? s'affiche.
3. Sélectionnez **Se connecter à un fournisseur OAuth tiers**.
4. Renseignez les champs du formulaire.

Champs du formulaire Registre d'application

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement de façon unique. Par exemple, saisissez `Fournisseur de mon application GitHub pour AVR`.
ID client	ID client de votre GitHub application. L'ID client provient de l'application dans votre GitHubGitHub console que vous avez créée lors des étapes précédentes. Cet ID est disponible dans la section **À propos** de votre GitHub configuration d'application dans GitHub.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

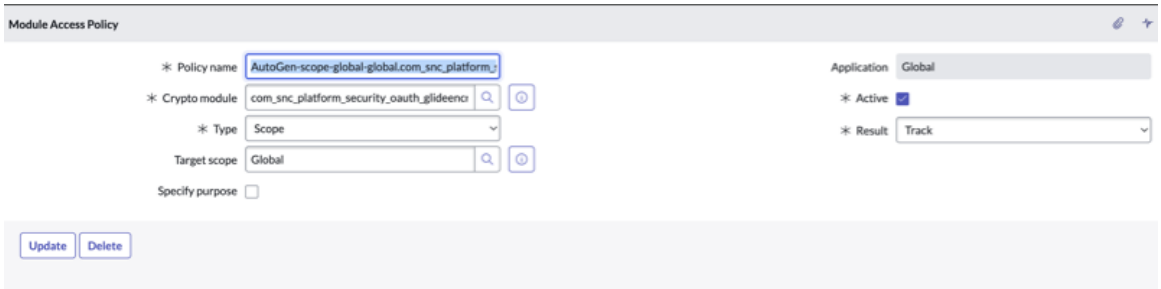
Champ	Description
Accessible	Conservez la valeur actuelle de ce paramètre.
Secret client	Secret client de votre GitHub application. Le secret client provient de l'application dans votre GitHubGitHub console que vous avez créée lors des étapes précédentes. Cet ID est disponible dans la section **À propos** de votre GitHub configuration d'application dans GitHub.
Actif	Option permettant d'activer la clé. Laissez cette option sélectionnée.
URL d'autorisation	Cette URL est générée automatiquement.
URL de jeton	Emplacement du point de terminaison de jeton que l'instance utilise pour récupérer et actualiser les jetons. Saisissez le jeton à partir de l'URL dans votre GitHub application. Il s'agit du jeton affiché dans l'URL une fois votre application installée dans GitHub. Dans la section Installer l'application de votre configuration d'application GitHub dans GitHub, sélectionnez l'engrenage. Le jeton est affiché dans l'URL de la page Web. ◦ Pour le cloud : https://api.github.com/app/installations/49374672/access_tokens . ID d'installation : 9374672. ◦ Pour les services sur site : https://github-372.secops-eng.com/api/v3/app/installations/7/access_tokens/api/v3 .
Script de l'API OAuth	Option qui vous permet de référencer un include de script OAuthUtil modifié. Sélectionnez **OAuthGitHubJWTHandler**.
Type d'accord par défaut	Type de subvention associé au registre d'application. Sélectionnez **Support JWT**.

5. Laissez les autres champs de formulaire par défaut.
6. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
7. Faites défiler l'écran jusqu'à la liste connexe **Profils des entités OAuth** , sélectionnez-la et ouvrez le profil par défaut qui a été créé dans la liste.
8. Renseignez le champ **Fournisseur JWT** avec le fournisseur JWT précédemment créé et enregistrez le formulaire.
9. Revenez au fichier de registre de l'application et enregistrez-le.
10. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > **Tout**.
11. Sélectionnez la politique qui a `com_snc_platform_security_oauth_glideencrypter` comme valeur de champ du **module Chiffrement** et l'include de script : `OAuthGitHubJWTHandler`.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



12. Vérifiez que le champ **Résultat** est défini sur `Suivre` et enregistrez vos changements.

Créez des informations d'identification et des connexions pour le GitHub Application Vulnerability Integration

Créez un enregistrement d'informations d'identification auprès du fournisseur d'application GitHub précédemment créé pour autoriser les actions.

Avant de commencer

Rôles requis :

- administrateur
- sn_vul.app_sec_manager

Procédure

1. Accédez à la **Informations d'identification et connexions** > **Informations d'identification**.
2. Sélectionnez **Nouveau**.
3. Sélectionnez **Informations d'identification OAuth 2.0**.
4. Sélectionnez **Nouveau** et renseignez les champs.

Champ	Description
Nom	Nom unique de l'enregistrement.
Concerne	Sélectionnez les informations d'identification OAuth 2.0 dans la liste.
Profil de l'entité OAuth	Sélectionnez l'icône de recherche et localisez le profil d'entité que vous avez créé lors des étapes précédentes.
Autres champs	Laissez ces champs dans leurs valeurs par défaut.

5. Cliquez avec le bouton droit de la souris n'importe où dans l'en-tête de la page et sélectionnez **Enregistrer**.
   La liste des informations d'identification s'affiche.
6. Ouvrez l'enregistrement que vous venez de créer et sélectionnez le lien connexe **Obtenir un jeton OAuth** .
   Un message s'affiche indiquant que le jeton OAuth a été importé avec succès.
7. Accédez à la **Informations d'identification et connexions** > **Connexions**.
8. Sélectionnez **Nouveau**.
9. Sélectionnez **Connexion HTTP(s).**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Sélectionnez **Nouveau** et renseignez les champs.

Champ	Description
Nom	Nom de l'enregistrement.
Application	Lecture seule.
Alias parent (facultatif)	Sélectionnez l'icône de recherche et choisissez-en une dans la liste.
Type	Connexion et informations d'identification.
Type de connexion	HTTP.
Prise en charge de plusieurs connexions actives (facultatif)	Désactivé.
Politique des nouveaux essais par défaut	Politique des nouveaux essais HTTP par défaut
Modèle de configuration	À laisser vide.

11. Sélectionnez **Soumettre**.
La liste des alias de connexion et d'informations d'identification s'affiche.

12. Ouvrez votre enregistrement et, dans l'onglet de la liste connexe Connexions, sélectionnez **Nouveau** et remplissez les champs de l'enregistrement de connexion HTTP.

Champ	Description
Nom	Nom de l'enregistrement.
Actif	Activé.
Informations d'identification	Sélectionnez l'enregistrement Informations d'identification que vous avez créé lors des étapes précédentes.
Alias de connexion	Votre enregistrement s'affiche.
Générateur d'URL	Désactivé.
URL de connexion	Il s'agit de l'URL de base : https://api.github.com pour Enterprise. L'élément sur site correspond à l'URL de votre point de terminaison GitHub.
Utiliser un serveur MID (facultatif)	Serveur MID est requis sur site. C'est facultatif pour les entreprises.
Délai de connexion	Saisissez une valeur.

13. Sélectionnez **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La liste des alias de connexion et d'informations d'identification s'affiche. Vous êtes maintenant prêt à effectuer les étapes pour Configurez la GitHub Application Vulnerability Integration.. Dans le champ Connexion, saisissez les informations d'identification que vous avez créées lors des étapes précédentes.

Installez le ServiceNow® GitHub Application Vulnerability Integration

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le s'intègre GitHub Application Vulnerability Integration correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez l'installer GitHub Application Vulnerability Integration .
2. Accédez au ServiceNow Store.
3. Dans le , recherchez GitHub Application Vulnerability Integration l'applicationServiceNow Store.
4. Sélectionnez la vignette de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **Dépendances** , le cas échéant.

5. Sélectionnez **Demande d'application** et entrez vos Now Support informations d'identification de connexion.
6. Sélectionnez **Obtenir**.
7. Entrez le **nom** et le **motif de l'instance**, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demander**.
   Vous recevez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer**.
    Votre application est automatiquement installée sur votre instance.

Configurez la GitHub Application Vulnerability Integration.

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit GitHub s'intègre correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Rôles requis :

- Groupe d'utilisateurs du gestionnaire App-Sec
- sn_vul.app_sec_manager requis pour la configuration OAuth

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité de GitHub** > **Configuration**.
2. Choisissez **Authentification de base** ou **OAuth** pour Type d'authentification.
   - L'authentification de base nécessite un serveur MID pour les instances sur site. Générez le jeton d'API requis pour l'authentification de base à partir de votre GitHub compte.
   - OAuth nécessite l'application OAuth, les informations d'identification et la configuration de la connexion décrites à la section Création d'informations d'identification OAuth 2.0 pour GitHub les applications : JWT pour le GitHub Application Vulnerability Integration.
3. Renseignez les champs en fonction du type que vous choisissez.
   Authentification de base

Champ	Description
URL D'API	L'URL d'API appropriée GitHub pour entreprise ou sur site. L'URL par défaut est https://api.github.com . Sur site est votre GitHub URL de point de terminaison.
Jeton d'API	Jeton que vous avez généré à partir de votre GitHub console.
Type d'API	Sélectionner un élément : Organisation Choisissez cette option si vous souhaitez importer des données pour une organisation spécifique par nom. L'environnement GitHub prend en charge plusieurs organisations. Chaque organisation peut prendre en charge plusieurs référentiels. Si vous saisissez une organisation, seules les données de cette organisation sont importées. Entreprise L'environnement d'entreprise prend en charge plusieurs organisations. Choisissez cette option si vous souhaitez importer des données de vulnérabilité depuis toutes les organisations de votre environnement d'entreprise (Cloud).
Nom de l'organisation	Nom de votre GitHub référentiel. Seules les données de l'organisation que vous saisissez sont importées.
Serveur MID	Pour les instances sur site pour l'authentification de base, un serveur MID est requis.
Sélectionnez des options pour gérer la gestion des exceptions et les faux positifs.	Sélectionnez les options pour gérer automatiquement la gestion des exceptions et

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	des faux positifs pour les éléments vulnérables d'applications (AVI) avec ServiceNow des workflows lors de l'importation. Gérer les exceptions dans ServiceNow Laissez cette option activée si vous souhaitez trier les AVI importés marqués pour l'état **Différé** . Les AVI dont les états **sources** sont normalement mappés à un état **Différé** dans votre instance sont à la place mappés à **Ouvert**. Vous **demandez une exception** à partir de l'enregistrement AVI. Gérer les faux positifs dans ServiceNow Laissez cette option activée si vous souhaitez trier les AVI importés avec des états **source** marqués comme **Faux positif** ou **Faux positif potentiel**. Les AVI avec ces états **source** , qui sont normalement mappés à un état **Fermé** dans votre instance, sont mappés à **Ouvert**. Vous demandez un **faux positif** à partir de l'enregistrement AVI. ◦ Décochez l'une des cases ou les deux si vous souhaitez conserver les états **source** importés à partir de votre scanner. ◦ Si cette option est désactivée, les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVI.
Instance d'intégration	Instance dans laquelle vous importez des données.

OAuth

Champ	Description
URL D'API	L'URL d'API appropriée GitHub pour entreprise ou sur site. L'URL par défaut est https://api.github.com . Sur site est votre GitHub URL de point de terminaison.
Connexion	La connexion que vous avez créée, décrite à la section Création d'informations d'identification OAuth 2.0 pour GitHub les appli-

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	cations : JWT pour le GitHub Application Vulnerability Integration.
Type d'API	Sélectionner un élément : Organisation Choisissez cette option si vous souhaitez importer des données pour une organisation spécifique par nom. L'environnement GitHub prend en charge plusieurs organisations. Chaque organisation peut prendre en charge plusieurs référentiels. Si vous saisissez une organisation, seules les données de cette organisation sont importées. Entreprise L'environnement d'entreprise prend en charge plusieurs organisations. Choisissez cette option si vous souhaitez importer des données de vulnérabilité depuis toutes les organisations de votre environnement d'entreprise (Cloud). **Remarque :** GitHub Les applications ne prennent pas en charge les API au niveau de l'entreprise.
Nom de l'organisation	Nom de l'organisation de vos GitHub référentiels. Seules les données des référentiels de l'organisation que vous saisissez sont importées.
Sélectionnez des options pour gérer la gestion des exceptions et les faux positifs.	Sélectionnez les options pour gérer automatiquement la gestion des exceptions et des faux positifs pour les éléments vulnérables d'applications (AVI) avec ServiceNow des workflows lors de l'importation. Gérer les exceptions dans ServiceNow Laissez cette option activée si vous souhaitez trier les AVI importés marqués pour l'état **Différé** . Les AVI dont les états **sources** sont normalement mappés à un état **Différé** dans votre ins-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	tance sont à la place mappés à **Ouvert**. Vous **demandez une exception** à partir de l'enregistrement AVI. Gérer les faux positifs dans ServiceNow Laissez cette option activée si vous souhaitez trier les AVI importés avec des états **source** marqués comme **Faux positif** ou **Faux positif potentiel**. Les AVI avec ces états **source** , qui sont normalement mappés à un état **Fermé** dans votre instance, sont mappés à **Ouvert**. Vous demandez un **faux positif** à partir de l'enregistrement AVI. ◦ Décochez l'une des cases ou les deux si vous souhaitez conserver les états **source** importés à partir de votre scanner. ◦ Si cette option est désactivée, les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVI.

4. Sélectionnez **Enregistrer et tester les informations d'identification**.
5. Exécutez l'intégration du GitHub référentiel avant d'exécuter les autres intégrations. Les autres GitHub intégrations dépendent des données d'application actuelles importées à partir de l'intégration de référentiel. Les données issues de l'intégration du référentiel sont stockées dans la table Applications détectées [sn_vul_app_release]. Consultez Afficher l'état de l'exécution de l'importation et les GitHub Application Vulnerability Integration données du référentiel importées pour plus d'informations.

Afficher l'état de l'exécution de l'importation et les GitHub Application Vulnerability Integration données du référentiel importées

Utilisez la liste connexe **Exécutions de l'intégration de vulnérabilité** pour vérifier la réussite de vos exécutions d'intégration, localiser les problèmes et prendre des décisions de rattrapage.

Avant de commencer

Rôle requis : sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité GitHub** > **Intégrations**.
2. Sélectionnez une intégration.
3. Sélectionnez la liste connexe **Exécutions de l'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Trouble?

Les causes les plus courantes d'un échec d'exécution sont les suivantes :

- Interruption du réseau.
- Un problème dans le transfert de données entraînant la corruption des données pendant la transformation.

Si vous rencontrez l'une de ces conditions, sélectionnez **Exécuter maintenant**, puis réexécutez l'intégration.

5. Pour afficher les référentiels importés, revenez à la liste des intégrations et sélectionnez l'enregistrement de l'intégration du GitHub référentiel.
6. Sélectionnez la liste connexe **Exécutions de l'intégration de vulnérabilité** et ouvrez un enregistrement.
   Le nombre de référentiels que vous avez importés avec une exécution d'intégration est affiché dans la colonne Éléments importés.

   Toutes les balises et rubriques que vous avez configurées pour un référentiel dans votre GitHub compte à partir du menu Paramètres sont importées. Toutes les propriétés personnalisées importées se trouvent dans le menu sous votre référentiel.

   Les balises, les rubriques et les propriétés personnalisées ne sont importées dans votre instance que si elles sont configurées dans votre GitHub compte.

   Si elles sont importées, ces GitHub informations s'affichent dans votre instance dans la colonne Informations supplémentaires de la table Applications détectées [sn_vul_app_release] et dans la section Informations supplémentaires de la source sur un enregistrement d'application détectée. Les propriétés personnalisées sont affichées sous forme de paires clé-valeur, et les balises et les rubriques sont affichées dans des tableaux.

Afficher GitHub Application Vulnerability Integration les jeux d'importation

Afficher les détails des informations d'importation pour le GitHub Application Vulnerability Integration.

Avant de commencer

Rôle requis : sn_vul.app_sec_manager

Procédure

1. Accédez au **Intégration de vulnérabilité GitHub** > **Tables des jeux d'importation**.
2. Sélectionnez un enregistrement pour une intégration.
3. Sélectionnez un lien connexe pour afficher les informations suivantes :
   - Numéros des jeux d'importation
   - Cartes de transformation
   - Historique de transformation

Invicti Vulnerability integration

Le Invicti Vulnerability integration utilise des données d'application importées à partir du produit Invicti pour vous aider à déterminer l'impact et la priorité des failles dans votre code.

Invicti Vulnerability integration

Le Invicti Vulnerability integration collecte les données du scanner et les met à la disposition du Now Platform®. Il s'intègre facilement à la ServiceNow® Réponse aux vulnérabilités

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

des applications fonctionnalité permettant de mapper les informations de Réponse aux vulnérabilités vulnérabilité des applications tierces importées dans votre instance.

L'intégration importe les types de données analysées suivants.

- Test dynamique de sécurité des applications (DAST)
- Test interactif de sécurité des applications (IAST)

Pour plus d'informations sur DAST et IAST, reportez-vous à la section Explorer Réponse aux vulnérabilités des applications.

Versions disponibles

Version	Notes de publication
Invicti Vulnerability integration v1.1 Invicti Vulnerability integration 1.0	Notes de publication Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Intégrations

Les intégrations suivantes sont incluses dans le système de base. Les intégrations sont enchaînées de sorte qu'après l'achèvement réussi d'une intégration, l'intégration suivante est lancée. Les intégrations s'exécutent dans l'ordre indiqué dans la table suivante.

Après l'exécution initiale, chaque jour, des travaux planifiés sont enchaînés pour exécuter ces intégrations automatiquement dans l'ordre. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Intégrations de vulnérabilité des applications Invicti

Intégration	Description
Application de liste des applications Invicti	Importe les applications analysées par Invicti dans la table Applications détectées [sn_vul_app_release] ou la table Application numérisée [sn_vul_app_scanned_application] en fonction de la façon dont la *sn_vul.use_product_model* propriété système est définie pour les enregistrements de règle de recherche de CI. • Si la propriété de modèle de produit est définie sur true, une application est insérée dans la table de mise en production Application détectée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de vulnérabilité des applications Invicti (suite)

Intégration	Description
	• Si la propriété de modèle de produit est définie sur false, une application est insérée dans la table Application analysée. Vous pouvez choisir d'activer des règles de recherche avec des éléments de configuration (CI) comme cibles de recherche en modifiant la propriété système. Si vous le modifiez, vous devez également activer les règles de recherche de CI pour qu'elles correspondent à la cible de recherche. Pour en savoir plus, consultez : • Configurez la Invicti Vulnerability integration. • Créer une règle de recherche de CI • Réapplication des règles de recherche de CI dans Réponse aux vulnérabilités des applications
Intégration de la liste des analyses Invicti	Cette intégration est lancée une fois l'intégration de la liste d'applications terminée avec succès. Cette intégration importe des données sur la date et l'heure d'exécution d'une analyse.
Intégration d'éléments vulnérables de l'application Invicti	Cette intégration est lancée une fois l'intégration de la liste d'analyses terminée avec succès. À partir de la version 1.1, affichez des détails tels que les durées de traitement totales, les durées moyennes des processus d'exécution avant et après l'intégration, et des rapports sur les enregistrements d'exécution de l'intégration pour l'intégration des éléments vulnérables de l'application. Chaque vulnérabilité dans Invicti a un type, par exemple, **DirectoryListing**. Ce type est mappé en tant qu'ID unique dans votre instance et affiché dans le cadre de la valeur du champ Vulnérabilité de l'enregistrement d'élément vulnérable de l'application (AVI) : **Invicti-DirectoryListing**. Pour plus d'informations sur le mappage, reportez-vous à la section Invicti Vulnerability integration Mappage de l'état.

La limite supérieure d'éléments par page pour les trois intégrations est de 200.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préparez-vous pour le Invicti Vulnerability integration

Une intégration réussie nécessite la planification et l'exécution de tâches préalables à l'intégration. Préparez l'intégration en effectuant ces tâches. Le Invicti Vulnerability integration suppose que vous connaissez le produit et l'API Invicti.

L'intégration Common Weakness Enumeration (CWE) est également utilisée par Réponse aux vulnérabilités des applications Invicti Vulnerability Integration et doit être en cours d'exécution avant l'installation et la configuration de l'intégration des vulnérabilités.

Remarque : Les données de la base de données de vulnérabilité NIST (NVD) ne sont pas nécessaires pour installer l'intégration, mais elles fournissent un enrichissement de vulnérabilité et sont utiles.

Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Remarque : Avant d'exécuter l'intégration, apportez tout changement de configuration nécessaire en fonction de vos besoins.

Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables de l'application que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service et assistance client. Le rôle administrateur est nécessaire pour installer et configurer des applications sur votre instance Now Platform.

Obtenez vos informations d'identification API et votre jeton d'API sur votre console Invicti. Consultez les informations disponibles sur le site Web du produit Invicti à l'adresse Vue d'ensemble de l'API .

Installer l'intégration de ServiceNow® Vulnerability Response avec Invicti

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que l'application s'intègre Invicti Vulnerability integration correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez l'installer Invicti Vulnerability integration .
2. Accédez au ServiceNow Store.
3. Dans le ServiceNow Store, recherchez l'application Invicti Vulnerability integration .
4. Sélectionnez la vignette de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **Dépendances** , le cas échéant.

5. Sélectionnez **Demande d'application** et entrez vos Now Support informations d'identification de connexion.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sélectionnez **Obtenir**.
7. Entrez le **nom** et le **motif de l'instance**, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demander**.
   Vous recevez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer** pour l'activer.
    Votre application est automatiquement installée sur votre instance.

Configurez la Invicti Vulnerability integration.

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées pour que le Invicti Vulnerability integration fonctionne correctement avec la Réponse aux vulnérabilités des applications fonctionnalité .Réponse aux vulnérabilités

Avant de commencer

Rôles requis :

- Administrateur pour installer et activer des applications
- Groupe d'utilisateurs App-Sec Manager pour configurer l'intégration

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que le est Invicti Vulnerability integration installé et activé.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer l'intégration de ServiceNow Vulnerability Response avec Invictireportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	• Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe App-Sec Manager. • Le gestionnaire App-Sec supervise la configuration et vérifie les résultats attendus.
Pour l'intégration de vulnérabilité Inviciti, préparez votre **ID utilisateur** et votre **jeton d'API** .	Contactez votre administrateur Invicti pour obtenir **l'ID d'utilisateur** et le **jeton d'API** si vous ne les connaissez pas. Pour plus d'informations, consultez le site Web du produit Invicti à l'adresse Vue d'ensemble de l'API .

Procédure

1. Accédez à la **Tout** > **Invicti** > **Configuration Invicti**.
2. Renseignez les champs.

Champ	Description
URL D'API	URL d'instance Invicti de l'utilisateur. Il s'agit des informations que vous avez obtenues à partir de Préparez-vous pour le Invicti Vulnerability integration.
ID d'utilisateur	ID d'utilisateur unique.
Jeton d'API	Jeton d'API que vous avez généré à partir de votre console Invicti. Il s'agit des informations que vous avez obtenues à partir de Préparez-vous pour le Invicti Vulnerability integration.
Choisissez le type d'analyse. Vous devez en sélectionner au moins un.	
Importer DAST	Option permettant d'inclure les vulnérabilités des analyses DAST. Les analyses DAST détectent dynamiquement les vulnérabilités d'une application pendant qu'elle est en cours d'exécution. Cette approche pourrait imiter une attaque extérieure.
Importer IAST	Option permettant d'inclure les vulnérabilités des analyses IAST. Les analyses IAST détectent les vulnérabilités logicielles en interagissant avec le programme pendant qu'il est en cours d'exécution. L'observation humaine, les tests automatisés et les capteurs sont utilisés en combinaison pour interagir

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	avec l'application afin de localiser les vulnérabilités.
Format de date	Paramètre qui convertit l'heure de début au format pris en charge par l'API Invicti utilisé par l'intégration d'éléments vulnérables de l'application Invicti. Ce paramètre doit correspondre au format que vous avez défini ou sélectionné dans votre compte Invicti, par exemple, **jj/MM/aaaa.** Vérifiez que les formats de date et d'heure de votre console Invicti correspondent à ceux que vous entrez pour le format de date de votre Now Platform instance. Pour modifier ce format dans votre console Invicti : **a.** Connectez-vous à Invicti Sign In . **b.** Sélectionnez **Nom d'utilisateur** en haut à droite. **c.** Accédez à la **Paramètres utilisateur** > **Format de date et d'heure**. **Remarque :** Des échecs d'importation peuvent se produire si vous entrez un format de date non valide dans votre Now Platform instance. Si vous entrez un format valide dans votre instance qui diffère du format de date de votre console Invicti, Invicti renverra une charge utile vide.
Gérer les exceptions dans ServiceNow	Sélectionner un élément : Activé (sélectionné) Les éléments vulnérables de l'application (AVIT) d'Invicti avec des états tels que **Présent** et **RisqueAccepté** qui peuvent être différés dans votre instance sont plutôt mappés pour **Ouvrir** automatiquement. Désactivé (non sélectionné) Les états sources des éléments vulnérables de l'application (AVIT) importés depuis Invicti sont conservés. Vous devez gérer les exceptions pour ces

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	AVIT (les différer) à partir des enregistrements AVIT. Pour plus d'informations sur les états sources et les champs cibles Invicti, consultez Invicti Vulnerability integration Mappage de l'état.
Gérer les faux positifs dans ServiceNow	Sélectionner un élément : Activé (sélectionné) Les AVIT avec des états d'Invicti tels que **Présent** et **Faux positif** qui peuvent passer à **l'état Fermé** dans votre instance sont à la place mappés pour **Ouvert** automatiquement. Désactivé (non sélectionné) Les états AVIT importés d'Invicti sont conservés. Vous devez gérer les faux positifs ou les faux positifs potentiels pour ces AVIT à partir des enregistrements AVIT.

3. Sélectionnez **Enregistrer et tester les informations d'identification**.
4. Facultatif : Modifiez vos règles de recherche afin qu'elles soient basées sur des éléments de configuration.

   (Optional) Par défaut, la propriété système **sn_vul.use_product_model** est activée (définie sur `vrai`) pour vos règles de recherche répertoriées dans la table [sn_sec_cmn_ci_lookup_rule] en fonction du modèle de produit. Lorsque cette règle est activée :

   - Cette règle identifie les correspondances entre les données importées et les données de votre Base de données de gestion des configurations (CMDB) en fonction du modèle de produit.
   - Les enregistrements sont créés ou mis à jour dans la table Applications détectées [sn_vul_app_release].
   - Lorsque vous créez ou modifiez vos règles de recherche pour Invicti, le **modèle de produit** s'affiche dans le champ **Cible de recherche** du formulaire de règle.

   Pour modifier vos règles de sorte qu'elles soient basées sur des éléments de configuration, vous devez désactiver manuellement (définir sur `faux`) la propriété système **sn_vul.use_product_model** .

   a. Accédez à la **Tout** > **Propriétés système** et localiser l'enregistrement **sn_vul.use_product_model** et définir la valeur sur `faux`.

   b. Sélectionnez **Mettre à jour**.

   c. Accédez à la **Tout** > **Security Operations** > **CMDB** > **Règles de recherche**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Localisez les règles Nom d'application et ID d'application source qui ont la cible Rechercher comme **élément de configuration**.

e. Cochez la case Actif pour ces règles.

f. Sélectionnez **Mettre à jour**.
Lorsque vous créez ou modifiez vos règles de recherche pour Invicti, notez que **l'élément de configuration** est affiché dans le champ **Cible de recherche** du formulaire de règle.
Les enregistrements sont créés ou mis à jour dans la table Applications numérisées [sn_vul_app_scanned_application].

Affichage de l'état et des enregistrements de l'exécution de l'importation Invicti Vulnerability integration

Utilisez la liste connexe **Exécutions de l'intégration de vulnérabilité** pour vérifier la réussite de vos exécutions d'intégration, localiser les problèmes et prendre des décisions de rattrapage.

Affichage de l'état de l'importation, des jeux d'importation et des enregistrements

Pour afficher l'état de vos importations, en tant qu'utilisateur dans le groupe d'utilisateurs App-Sec Manager, accédez à **Tout** > **Intégration de vulnérabilité Invicti** > **Intégrations** et sélectionnez un enregistrement d'intégration. Sélectionnez la liste connexe **Exécutions de l'intégration de vulnérabilité** .

À partir de la version 1.1, affichez des détails tels que les durées de traitement totales, les durées moyennes des processus d'exécution avant et après l'intégration, et des rapports sur les enregistrements d'exécution de l'intégration pour l'intégration des éléments vulnérables de l'application.

Pour afficher les ensembles d'importation, accédez à **Tout** > **Intégration de vulnérabilité Invicti** > **Intégrations** > **Tables des jeux d'importation** et sélectionnez une intégration.

L'intégration de la liste des applications crée ou met à jour des enregistrements en fonction de la cible de recherche :

- Modèle de produit : table Applications détectées [sn_vul_app_release]
- Élément de configuration : table Applications numérisées [sn_vul_app_scanned_application]

L'intégration de la liste des analyses crée ou met à jour des enregistrements dans la table Applications numérisées [sn_vul_app_scan_summary].

L'intégration des éléments vulnérables de l'application crée ou met à jour des enregistrements dans la table des éléments vulnérables de l'application [sn_vul_app_vulnerable_item] et des CWE [sn_vul_cwe].

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Chaque vulnérabilité dans Invicti a un « type », par exemple, ProductDirectoryListing. Ce type est importé, mappé en tant qu'ID unique dans votre instance et affiché dans le cadre de la valeur du champ Vulnérabilité de l'enregistrement d'élément vulnérable de l'application (AVIT). Dans cet exemple, la valeur est `Invicti-ProductDirectoryListing`, et cette valeur est également affichée en tant qu'ID unique sur l'enregistrement Entrée de vulnérabilité de l'application. Les AVIT Invicti prennent en charge plusieurs entrées Common Weakness Enumeration (CWE), de sorte que les CWE ne sont pas utilisés comme ID uniques. Les CWE sont également affichés sur l'enregistrement AVIT.

Pour les AVIT Invicti, s'il existe des types de doublons dans Invicti pour une vulnérabilité, le mot « personnalisé » est inséré dans la valeur, par exemple, `Invicti-custom-ProductDirectoryListing`. Si vous créez un type personnalisé pour les vulnérabilités, l'ID de vulnérabilité peut être `Invicti-Custom-<title of vulnerability>`.

Nouveaux champs : pour le `type d'analyse = Invicti`, les paramètres affectés et les champs personnalisés peuvent inclure des données qui peuvent vous aider à comprendre la vulnérabilité et à la corriger. S'il n'y a pas de données, ces champs ne sont pas affichés sur l'AVIT.

Invicti Vulnerability integration Mappage de l'état

Les états sources suivants à partir de et Invicti Vulnerability integration leurs états cibles dans votre instance sont répertoriés dans la table suivante.

États sources Invicti et leurs états Now Platform correspondants

États des sources Invicti	Description des états de la source	État cible dans Now Platform
Présent	Le problème est identifié.	Ouvrir
Présent, RisqueAccepté, Ressuscité	Le problème a été pris en compte et est marqué comme une vulnérabilité à faible risque.	Différé
Présent, faux positif	Le problème a été pris en compte et est marqué comme n'étant pas une véritable vulnérabilité.	Fermé
CorrigéNon confirmé, Corrigé Non confirmé	Le problème a été corrigé mais n'a pas été confirmé par Invicti Enterprise.	Résolu
Fixed (Confirmed), FixedConfirmed, FixedConfirmed, AcceptedRisk, FixedConfirmed, False Positive	Le problème a été corrigé et confirmé par Invicti Enterprise et aucune autre action n'est requise.	Fermé
Corrigé (impossible de retester)	Le problème a été identifié, mais Invicti ne peut pas effectuer de nouveau test pour confirmer si le problème a été résolu ou non.	Résolu

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États sources Invicti et leurs états Now Platform correspondants (suite)

États des sources Invicti	Description des états de la source	État cible dans Now Platform
Ranimé	Le problème a été résolu dans les analyses précédentes, mais a été trouvé à nouveau.	Ouvrir
Différé, ignoré	Le problème a été ignoré par l'utilisateur. Dans Invicti Enterprise, pour ignorer un problème, un utilisateur met à jour son état sur « risque accepté ».	Risque accepté

Mappage de version de l'application

Champ source	Champ cible sur Now Platform
ID	source_app_id
Heure de création	app_creation_date
Heure de mise à jour	app_updation_date
Nom	app_name
URL de racine	Source_additional_info
Description	description
Balises	Balises

Mappage de vulnérabilité

Champ source	Champ cible sur Now Platform
Type	Nom de catégorie
Détail de la vulnérabilité	Résumé
Impact	Menace
Références des sources	Références Web
Recommandation de source	Solution
Type	source_entry_id/ID
Gravité	source_severity
Classification["CWE"]	Liste CWE
CvssVectorString (en anglais seulement)	Champs CVVS v3

Mappage de la synthèse de l'analyse

Champ source	Champ cible

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Source	Source
Nombre total de vulnérabilités	Detected_flaw_count
Date de déclenchement	Date de l'analyse dynamique
id	source_scan_id

Mappage des éléments vulnérables de l'application (AVIT)

Champ source	Champ cible sur Now Platform
Type	Type d'analyse
ID du site web	ID d'application source
ID	ID AVIT source
Date de la dernière consultation	Dernier trouvé
Date de la première consultation	Première occurrence trouvée
Date de la dernière mise à jour	Date de la dernière analyse
paramètres	Paramètre affecté
URL	URL affectée
Gravité	Gravité de la source
URL	Lien source
Détail de la vulnérabilité	Résumé de vulnérabilité source
Références externes	Références des sources
Références Remedy + Remedy	Recommandation de source
État	État du rattrapage de la source
Impact	Explication de vulnérabilité source

Veracode Vulnerability Integration

L'intégration Réponse aux vulnérabilités avec Veracode l'application utilise des Veracode données importées du produit pour vous aider à déterminer l'impact et la priorité des failles dans votre code.

Veracode Vulnerability Integration

Le Veracode produit collecte des données DAST (Dynamic Application Security Testing), SAST (Static Application Security Testing) et des scanners manuels, et les met à la disposition du Now Platform®. Il s'intègre facilement à la Réponse aux vulnérabilités des applications fonctionnalité de mappage des Réponse aux vulnérabilités vulnérabilités tierces, enrichissant ainsi les données de votre instance.

À partir de la version 19.0 de , vous pouvez importer des données de vulnérabilité de l'analyse de Réponse aux vulnérabilitéscomposition logicielle (SCA) et Nomenclature logicielleSBOM() pour vous aider à identifier les faiblesses de vos applications logicielles. Pour plus d'informations, consultez Explorer Nomenclature logicielle.

Une API partagée ingère les données DAST, SAST, SCA et les résultats des tests d'intrusion manuels.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Chaque jour, les travaux planifiés invoquent automatiquement les intégrations dans l'ordre où elles sont répertoriées. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en gardant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Obtenir plus de détails à partir de Veracode

À partir de la version 4.2, sélectionnez **Obtenir plus de détails** sur les éléments vulnérables de l'application (AVIT) qui ont Veracode comme source dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item] ou à partir des vues de listes dans les espaces de travail Vulnerability Response pour afficher les données suivantes Veracode .

- Les détails de la demande source HTTP et de la réponse source pour les analyses de Test dynamique de sécurité des applications (DAST) sont affichés dans la liste connexe Demande/réponse HTTP.
- Les recommandations de solutions de Veracode sont affichées dans la liste connexe Résultats.
- La demande source HTTP, la réponse source et les recommandations sont affichées dans l'onglet Détails dans les espaces de travail Vulnerability Response Réponse aux vulnérabilités .
- La colonne Description est prise en charge dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item].

Versions disponibles

Version	Notes de publication
Veracode v4.3 Veracode v4.2 Veracode v4.1	Notes de publication Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Groupe d'utilisateurs et rôles

Il Veracode Vulnerability Integration est installé par un administrateur système [admin] et configuré par un membre du groupe App-Sec Manager. Consultez Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs pour plus d'informations.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Veracode Vulnerability Integration

Pour afficher les intégrations de Veracode vulnérabilité, accédez à **Tout** > **Intégration de vulnérabilité Veracode** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base.

Veracode Vulnerability Integration

Intégration	Description
À partir de la version 4.1 : Veracode Intégration des projets Link	Cette intégration est activée par défaut. Récupère tous les projets associés pour chaque application à partir de Veracode. Les applications peuvent avoir plusieurs projets dans l'application Veracode . Les données importées de cette intégration sont affichées sur les enregistrements suivants : • **La date de la dernière analyse SCA**, la **date de création de l'application** et la **date de mise à jour de l'application** sont répertoriées dans les enregistrements dans **les applications détectées**. • Sur les enregistrements de synthèse de l'analyse de vulnérabilité de l'application et les éléments vulnérables de l'application (AVIT), **l'état SDLC (** cycle de vie du développement logiciel) de la source s'affiche. • **L'exploitabilité de la source** s'affiche dans les enregistrements d'éléments vulnérables de l'application (AVI).
Veracode Intégration de liste d'applications (JSON)	Cette intégration est désactivée par défaut. Récupère les données du scanner d'application (vulnérabilités Veracode , métadonnées) et enrichit vos données d'application. Récupère les enregistrements d'analyse Veracode via une API basée sur JSON.
Veracode Intégration de liste d'applications (XML)	Cette intégration est désactivée par défaut. La version XML de cette intégration a été désactivée (déconseillée). Récupère les données du scanner d'application (vulnérabilités Veracode , métadonnées) et enrichit vos données d'application. Cette intégration est définie pour s'exécuter quotidiennement à 00:00:00. **Remarque :** Une API basée sur JSON est Veracode utilisée pour récupérer la liste des applications. Cette API importe la « date de la dernière vérification de conformité de la politique » pour ces applications, indiquant quand ces applications ont été analysées pour la dernière fois par Veracode.
Veracode Nomenclature logicielle (SBOM) Intégration	La version 4.3 de la Veracode Vulnerability Integration inclut les améliorations suivantes avec Veracode SBOM les fichiers : • Si vous avez installé SBOM Response, vous avez la possibilité d'inclure les vulnérabilités trouvées par Veracode pour les fichiers SBOM que vous téléchargez. • Veracode est mappé au champ **Source** pour les enregistrements de la table Nomenclature [sn_sbom_doc] pour les Veracode fichiers SBOM.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Veracode Vulnerability Integration (suite)

Intégration	Description
	Cette intégration est activée par défaut. À partir de la version 4.2, importe les Nomenclature logicielle fichiers aux formats CycloneDX et SPDX générés par Veracode et les mettent en file d'attente pour analyse dans votre instance. Vous devez avoir installé les Nomenclature logicielle applications pour importer ces données et les visualiser.
Veracode Intégration de synthèse de l'analyse (JSON)	Cette intégration est désactivée par défaut. Récupère les enregistrements d'analyse Veracode via une API basée sur JSON. Cette intégration remplace l'intégration de l'API basée sur XML. Il est chaîné et suit l'intégration de la liste des applications lorsqu'il Veracode est activé.
Veracode Synthèse de l'analyse (XML)	Cette intégration est désactivée par défaut. La version XML de cette intégration a été désactivée (déconseillée). Récupère les enregistrements d'analyse à partir de Veracode. Cette intégration est chaînée et suit l'intégration de liste d'applications lorsqu'elle Veracode est activée. **Remarque :** Suit automatiquement l'intégration de la liste d'applications Veracode lorsqu'elle est activée. Avec la « Dernière date de vérification de conformité de politique » pour les applications de Veracode, cette intégration récupère uniquement les données des applications qui ont été analysées après la « delta_start_time » de cette intégration.
Veracode Intégration JSON d'élément vulnérable de l'application	À partir de la version 4.2, affichez des détails tels que les durées totales de traitement, les durées moyennes des processus d'exécution avant et après l'intégration, et des rapports sur les enregistrements d'exécution de l'intégration pour les intégrations d'éléments vulnérables d'application. Cette intégration est désactivée par défaut. Récupère les résultats de l'analyse avec plus de données de vulnérabilité que l'intégration basée sur XML à partir de Veracode. Il insère les AVI et enrichit vos données de vulnérabilité tierces.
Veracode Intégration d'éléments vulnérables d'applications (XML)	À partir de la version 4.2, affichez des détails tels que les durées totales de traitement, les durées moyennes des processus d'exécution avant et après l'intégration, et des rapports sur les enregistrements d'exécution de l'intégration pour les intégrations d'éléments vulnérables d'application. Cette intégration est désactivée par défaut. Récupère les résultats d'analyse de Veracode, insère les éléments vulnérables de l'application (AVIT) et enrichit vos données de vulnérabilité tierces. Par défaut, si l'enregistrement du scanner est **à** l'état Fermé, les AVIT ne sont pas créés. Les AVIT existants sont toujours mis à jour. Cette intégration est chaînée et suit l'intégration Synthèse de l'analyse lorsqu'elle Veracode est activée. L'API basée sur XML est déconseillée pour l'intégration JSON du résumé de l'analyse Veracode .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Veracode Vulnerability Integration (suite)

Intégration	Description
	Remarque : Suit automatiquement l'intégration de la synthèse de l'analyse Veracode . Avec la « Dernière date de vérification de conformité de politique » pour les applications de Veracode, cette intégration récupère uniquement les données des applications qui ont été analysées après la « delta_start_time » de cette intégration.
Veracode Intégration des catégories	Cette intégration est désactivée par défaut. Récupère les données de catégories améliorées à partir de Veracode.
Veracode Intégration CWE	Cette intégration est activée par défaut. Récupère les données CWE (Common Weakness Enumeration) spécifiques pour obtenir des informations sur les menaces et formuler des Veracode recommandations de rattrapage. Ces données sont renseignées et mises à jour dans les enregistrements d'entrée de vulnérabilité de l'application. Cette intégration CWE fonctionne indépendamment de la tâche planifiée pour l'intégration CWE Comprehensive 2000 que vous activez pour l'application Réponse aux vulnérabilités . Vos données ne sont pas dupliquées si vous avez activé l'intégration Veracode CWE et l'intégration CWE Comprehensive 2000.
Veracode Intégration DevOps	Cette intégration est désactivée par défaut. L'intégration est visible dans la liste Intégrations de vulnérabilité d'application dans Réponse aux vulnérabilités des applications. Si vous disposez d'une licence DevOps Change Velocity, cette fonctionnalité est structurée de sorte que les utilisateurs DevOps n'ont pas besoin d'une licence SecOps pour afficher les détails du résumé des analyses de vulnérabilité tierces. Il n'y a aucun impact ni changement sur Réponse aux vulnérabilités des applications.

Pour les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation de l'intégration de vulnérabilité de l'application Veracode.

Pour afficher les données dans les vulnérabilités tierces, reportez-vous à la section Afficher les bibliothèques de vulnérabilité.

Se préparer à la Veracode Vulnerability Integration

Une réussite Veracode Vulnerability Integration nécessite la planification et l'exécution de tâches préalables à l'intégration. Préparez l'intégration en effectuant ces tâches. suppose Veracode Vulnerability Integration que vous connaissez le produit et l'API Veracode .

Avant de commencer

L'intégration CWE (Common Weakness Enumeration) est également utilisée par Réponse aux vulnérabilités des applications et doit être exécutée avant l'installation et la configuration de .Veracode Vulnerability Integration Il est installé avec Réponse aux vulnérabilités, par défaut.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les données de la base de données de vulnérabilité NIST (NVD) ne sont pas nécessaires pour installer Application Veracode Vulnerability Integration, cependant, elles fournissent un enrichissement et seraient utiles d'avoir. Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. Système**. Ne modifiez en aucun cas cette valeur.

Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter l'intégration, apportez les changements de configuration nécessaires en fonction de vos besoins.

Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables de l'application que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service et assistance client.

Ils Veracode Vulnerability Integration nécessitent un ID et une clé API.

Procédure

Pour créer l'ID d'API et les informations d'identification clés :

a. Connectez-vous à la Veracode plateforme.

b. Accédez au menu Compte d'utilisateur et sélectionnez **Informations d'identification de l'API**.

c. Cliquez sur **Générer les informations d'identification de l'API**.

d. Enregistrez vos informations d'identification pour une utilisation ultérieure.

Installer l'intégration de ServiceNow® Vulnerability Response avec Veracode

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit s'intègre Veracode correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe App-Sec Manager. Pour plus d'informations sur les rôles de groupe, Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateursreportez-vous à la section . • Le groupe Gestionnaire de sécurité des applications supervise la configuration et vérifie les résultats attendus.

Rôle requis : administrateur

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez l'installer Veracode Vulnerability Integration .
2. Accédez au ServiceNow Store.
3. Dans le ServiceNow Store, recherchez l'intégration de Vulnerability Response à Veracode l'application.
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **Dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Configurez le Veracode Vulnerability Integration pour votre environnement. Consultez Configurez la Veracode Vulnerability Integration..

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurez la Veracode Vulnerability Integration.

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit s'intègre Veracode correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que l'intégration à Veracode l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer l'intégration de ServiceNow Vulnerability Response avec Veracodereportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe d'utilisateurs App-Sec Manager. • Le gestionnaire App-Sec supervise la configuration et vérifie les résultats attendus.
Pour l'intégration de la vulnérabilité de l'application Veracode , préparez votre **ID API** et votre **clé API** .	Contact Veracode permettant d'obtenir**l'ID API** et la **clé API**. Consultez Se préparer à la Veracode Vulnerability Integration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	À partir de la version 4.0, si vous utilisez le Veracode Vulnerability Integration, les tests d'évaluation de pénétration dans le Veracode Vulnerability Integration sont des résultats manuels à partir de Veracode. Ces résultats ne sont pas liés aux demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour en savoir plus sur les demandes de tests de pénétration dans , reportez-vous Configurer les tests de pénétrationà Réponse aux vulnérabilités des applications.

Rôle requis : groupe d'utilisateurs du gestionnaire App-Sec

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Veracode** > **Configuration**.
2. Renseignez les champs **ID API** et **Clé API** .
3. Choisissez les résultats de vos tests.

Option	Description
Variante 4.0 :	**a.** Sélectionnez les types **de données DAST** ou **SAST** à inclure dans l'importation. **Remarque :** Vous pouvez choisir l'un ou l'autre, ou les deux, mais vous devez en sélectionner au moins un. **b.** Sélectionnez **SCA** pour importer les vulnérabilités de l'analyse de la composition logicielle (SCA). **c.** Sélectionnez **Inclure manuel** pour importer les résultats des tests d'intrusion manuels à partir de Veracode. Les AVIT sont créés pour ces résultats.
Version 3.0	Sélectionnez les types **de données DAST** ou **SAST** à inclure dans l'importation. **Remarque :** Vous pouvez choisir l'un ou l'autre, ou les deux, mais vous devez en sélectionner au moins un.
Variante 1.0 :	Les résultats des tests de sécurité des applications dynamiques sont sélectionnés par défaut.

4. Ajoutez le niveau Veracode **de gravité** pour filtrer vos données importées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette valeur est importée à partir de Veracode. Vous pouvez ajouter plusieurs valeurs au champ. Si elle est renseignée, l'importation collecte uniquement les données qui correspondent aux niveaux de gravité que vous avez ajoutés.

5. Enregistrez et validez vos choix.

Option	Description
Variante 3.0 :	Cliquez sur **Enregistrer et tester les informations d'identification**. **Remarque :** La configuration est terminée avec succès, sauf si un message d'erreur s'affiche. Si un message d'erreur s'affiche pendant la configuration, saisissez à nouveau vos données.
Variante 1.0 :	Cliquez sur **Enregistrer**. Vérifiez la configuration correcte en cliquant sur **Informations d'identification de test**. **Remarque :** La configuration est terminée avec succès, sauf si un message d'erreur s'affiche. Si un message d'erreur s'affiche pendant la configuration, saisissez à nouveau vos données.

6. Sélectionnez la façon dont vous souhaitez gérer les exceptions et les faux positifs pour les AVIT lors de l'importation.
Les options permettant de gérer les AVIT lors de l'importation avec les ServiceNow workflows Gestion des exceptions et Faux positif sont activées par défaut. Les workflows sont déclenchés en fonction de la façon dont les états **source** des AVIT sont mappés dans votre instance. Pour consulter un exemple de cas d'utilisation, reportez-vous à la section Gestion du mappage d'état pour les reports et les faux positifs dans Réponse aux vulnérabilités des applications.

Activé	Gérer les exceptions dans ServiceNow Laissez cette option activée si vous souhaitez trier les AVIT importés marqués pour l'état **Différé** . Les AVIT dont les états **sources** sont normalement mappés à un état **Différé** dans votre instance sont plutôt mappés sur **Ouvert**. Vous **demandez une exception** à partir de l'enregistrement AVI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	Gérer les faux positifs dans ServiceNow Laissez cette option activée si vous souhaitez trier les AVIT importés avec des états **Source** marqués comme **Faux positif** ou **Faux positif potentiel**. Les AVIT avec ces états **source** , qui sont normalement mappés à un état **Fermé** dans votre instance, sont mappés à **Ouvert**. Vous demandez un **faux positif** à partir de l'enregistrement AVIT.
Désactivé	Décochez l'une des cases ou les deux si vous souhaitez conserver les états **source** importés à partir de votre scanner. Ces AVIT sont mappés aux états **Cible** et **Motif cible** au fur et à mesure de leur importation, mais ne sont pas triés par les workflows d'exception et de faux positif. Les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVIT.

7. À partir de la version 4.3, choisissez ou vérifiez les paramètres des paramètres suivants.

Paramètre	Description
Région de l'API	Sélectionnez une région dans la liste.
Délai d'expiration de l'API	La valeur par défaut est 30K. Vous préférerez peut-être laisser ce champ dans ses paramètres par défaut.
Inclure les vulnérabilités SBOM	Sélectionnez cette option pour inclure toutes les vulnérabilités ingérées par les Veracode intégrations dans les Veracode SBOM fichiers que vous chargez. Laissez le champ vide afin que Veracode les vulnérabilités ne soient pas analysées sur Veracode SBOM les fichiers.

8. Sélectionnez **Enregistrer et tester les informations d'identification**.

Que faire ensuite

Si votre environnement nécessite des importations séparées par domaine, reportez-vous à la section Créer des importations séparées par domaine pour une intégration.

Lors de l'installation initiale, reportez-vous à pour plus d'instructions Configurer Réponse aux vulnérabilités des applications .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après l'installation initiale, pour les modifications, reportez-vous à la section Veracode Vulnerability Integration Modifications et activités.

Afficher l'état de l'exécution de l'importation de l'intégration de vulnérabilité de l'application Veracode

Utilisez la liste connexe **Exécutions de l'intégration de vulnérabilité** pour vérifier la réussite de vos exécutions d'intégration, localiser les problèmes et prendre des décisions de rattrapage.

Avant de commencer

Pour afficher l'état de l'exécution de l'importation Veracode Vulnerability Integration :

- Réponse aux vulnérabilités des applications et le Veracode Vulnerability Integration doit être installé et configuré.
- Les Veracode Vulnerability Integration importations doivent être planifiées et en cours d'exécution.

Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités des applications, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à **Tout** > **Intégration de vulnérabilité Veracode** > **Intégrations**.
2. Sélectionnez une intégration.
3. Cliquez sur la liste connexe **Exécutions de l'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.

Trouble?

Les causes les plus courantes d'un échec d'exécution sont les suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Interruption du réseau.
- Un problème dans le transfert de données entraînant la corruption des données pendant la transformation.

Si vous rencontrez l'une de ces conditions, cliquez sur **Exécuter maintenant**, puis réexécutez l'intégration.

5. À partir de la version 4.2, affichez des détails tels que les durées de traitement totales, les durées moyennes des processus d'exécution avant et après l'intégration, et des rapports sur les enregistrements d'exécution de l'intégration pour les intégrations d'éléments vulnérables d'application.
   Pour plus d'informations sur l'affichage des détails supplémentaires importés par Veracode, reportez-vous à la rubrique Pour en savoir plus dans Veracode Vulnerability Integration.

Afficher Veracode les résumés de l'analyse

Affichez les détails des informations de synthèse de l'analyse pour l'intégration Veracode des vulnérabilités.

Avant de commencer

Rôle requis : groupe de gestionnaires App-Sec

Procédure

1. Accédez à la table Résumés de numérisation de vulnérabilité de l'application [sn_vul_app_vul_scan_summary_list].
2. Sélectionner un enregistrement pour une Veracode analyse.
3. À partir des versions 19.0 et Réponse aux vulnérabilités 4.0 de Veracode Vulnerability Integration, utilisez l'icône Personnaliser la liste (icône Engrenage) pour afficher les colonnes suivantes.
   - Taille de l'analyse statique
   - Nombre de bibliothèques tierces
   - Nombre de bibliothèques tierces vulnérables
   - Nombre de failles tierce par gravité
   - Nombre de problèmes de bibliothèques tierces
   - Nombre de problèmes de licences tierces
   - Nombre de failles mixtes
   - Nombre de failles atténuées
   - Nombre de failles non atténuées
   - Nombre de failles statiques par gravité
   - Nombre de nouvelles failles par gravité
   - Nombre de failles non atténuées par gravité
   - Nombre total de failles par gravité
   - Dernière évaluation de l'analyse SCA
   - Date de la dernière analyse SCA
   - Date de publication de l'analyse
   - Balises

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Transformation des données pour l'intégration de Veracode vulnérabilité

Une fois que vous avez identifié les données que vous souhaitez importer, celles-ci sont récupérées à partir de l'application Veracode , traitées via un ensemble de sources de données et transformées dans votre instance.

Veracode Intégration d'éléments vulnérables d'applications

Les données de l'API sont d'abord chargées dans la table Importation d'élément Veracode AppVul [sn_vul_veracode_appvul_item_import] et la transformation d'élément Veracode AppVul est utilisée pour transformer les informations importées.

Pour accéder à cette carte de transformation, naviguez et *System Import Sets > Transform Maps* recherchez Veracode la transformation d'élément AppVul. La table suivante répertorie les champs de carte de transformation par intégration.

Veracode Champs de carte de transformation d'élément AppVul

Champ source	Champ cible	Description
app_id	source_app_id	ID d'application.
ID du problème	source_avit_id	ID AVIT.
app_name	app_name	Nom de l'application.
version	app_version	Version d'application.
build_id	source_scan_id	ID de build de l'application.
account_id	account_id	ID de compte.
sandbox_id	sandbox_id	ID de bac à sable.
last_update_time	last_scan_date	Heure de la dernière mise à jour.
app_name + last_scan_date	scan_summary_name	Synthèse de l'analyse.
life_cycle_stage	source_sdlc_status	État SDLC de la source.
niveau	source_severity	Gravité de la source.
category_name	catégorie	Catégorie.
source_severity	source_severity	Gravité de la source.
category_id + " CWE- » + cweId	source_entry_id	ID de l'entrée source.
source_vulnerability_summary	source_vulnerability_summary	Résumé de vulnérabilité source.
source_recommendation	source_recommendation	Recommandation de source.
description	description	Description tirée de la source.
description	source_vulnerability_explanation	Explication de vulnérabilité source.
mitigation_status_desc	source_mitigation_status	État de l'atténuation de la source.
remediation_status	source_remediation_status	État du rattrapage de la source.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Veracode Champs de carte de transformation d'élément AppVul (suite)

Champ source	Champ cible	Description
ligne	line_number	Ligne sur laquelle se trouve la faille.
module	application_module	Module d'application.
Fichier source	source_notes	Notes de la source.
affects_policy_compliance	complies_with_policy	Les valeurs peuvent être Oui ou Non selon que les informations sur la source sont vrai ou faux.
Chemin d'accès du fichier source + fichier source	emplacement	Mappage de localisation en cas de *static* défaut.
URL	emplacement	Mappage de localisation en cas de *dynamic* défaut.
périmètre, type, niveau d'exploitation	source_additional_info	Champ de valeur de nom renseigné avec les valeurs de la source en cas de défauts statiques.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Veracode Minutage et objectif du script de carte de transformation

Lorsque le script est exécuté	Objectif
onComplete (lorsqu'un jeu d'importation a terminé la transformation)	Script utilisé pour traiter la source de données et mettre à jour le nombre d'AVIT créés, mis à jour ou non modifiés, ainsi que ceux importés dans le cadre de cette intégration à partir de Veracode. Ce script est destiné à une utilisation interne et ne doit pas être modifié ou supprimé.

Veracode Vulnerability Integration Modifications et activités

Configurez des modifications facultatives spécifiquement pour le Veracode Vulnerability Integration.

Affichage des données supplémentaires importées par le Veracode Vulnerability Integration

Remarque : La modification d'autres Veracode Vulnerability Integration paramètres, autres que ceux répertoriés ici, nécessite une expertise avancée ServiceNowRéponse aux vulnérabilités des applications et dépasse le cadre de la documentation du produit.

Obtenir plus de détails à partir de Veracode

À partir de la version 4.2, sélectionnez **Obtenir plus de détails** sur les éléments vulnérables de l'application (AVIT) qui ont Veracode comme source dans la table Élément vulnérable de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'application [sn_vul_app_vulnerable_item] ou à partir des vues de listes dans les espaces de travail Vulnerability Response pour afficher les données suivantes Veracode .

- Les détails de la demande source HTTP et de la réponse source pour les analyses de Test dynamique de sécurité des applications (DAST) sont affichés dans la liste connexe Demande/réponse HTTP.
- Les recommandations de solutions de Veracode sont affichées dans la liste connexe Résultats.
- La demande source HTTP, la réponse source et les recommandations sont affichées dans l'onglet Détails dans les espaces de travail Vulnerability Response Réponse aux vulnérabilités .
- La colonne Description est prise en charge dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item].

Modifier les Veracode paramètres d'instance d'intégration

Après l'installation initiale, vous pouvez modifier les Veracode paramètres des intégrations dans l'instance d'intégration Veracode .

Avant de commencer

Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche

Vous pouvez modifier les paramètres d'une intégration à partir de son instance afin de déterminer le type de données que vous ingérez. Pour certains de ces paramètres, vous pouvez également modifier ces paramètres à partir de la page de configuration de l'intégration.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Intégrations**.
2. Sélectionnez **Vulnérabilité de l'application Veracode** dans la colonne Instance source de l'intégration Veracode que vous souhaitez modifier.
3. Sélectionnez l'onglet **Paramètres d'instance d'intégration** et double-cliquez sur un champ dans la colonne Valeur pour modifier les valeurs.

   À partir des versions 19.0 et 4.0 de Réponse aux vulnérabilités , Veracode Vulnerability Integrationvous pouvez configurer les paramètres suivants pour les Veracode intégrations.

   Importer manuel

   Entrez `vrai` pour importer les résultats des tests d'intrusion manuels à partir de Veracode. Vous pouvez également modifier cette valeur à partir de la page de configuration de l'intégration.

   Les tests d'évaluation de pénétration dans le Veracode Vulnerability Integration sont des résultats manuels de Veracode. Ces résultats ne sont pas liés aux demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour en savoir plus sur les demandes de tests de pénétration dans , reportez-vous Configurer les tests de pénétrationà Réponse aux vulnérabilités des applications.

   import_sca

   Entrez `vrai` pour importer les vulnérabilités de l'analyse de la composition logicielle (SCA). Vous pouvez également modifier cette valeur à partir de la page de configuration de l'intégration.

   statut

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Saisissez `Ouvert` ou `Fermé` pour importer les résultats pour les états souhaités. Si vous laissez ce champ vide, l'intégration importe les résultats pour les états Ouvert et Fermé.

policy_sandbox

Entrez une `politique` ou un `bac à sable` pour importer les enregistrements qui correspondent à une politique ou à un bac à sable. Ces enregistrements peuvent être liés à la façon dont les applications sont testées dans votre environnement.

policy_rule_passed

Entrez `vrai` ou `faux` pour importer les enregistrements qui ont réussi une règle de politique. Ces enregistrements peuvent être liés à la façon dont les applications sont testées dans votre environnement.

4. Sélectionnez **Mettre à jour** pour enregistrer vos changements.

Importer manuellement Veracode la vulnérabilité de l'application

Si votre importation initiale a échoué, ou si vous ne souhaitez pas attendre l'importation initiale planifiée, vous pouvez effectuer une importation de données complète indépendamment de la tâche planifiée quotidienne.

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Veracode** > **Intégrations**.
2. Choisissez et intégration, par exemple, l'intégration de liste d'applications Veracode .
3. Cliquez sur **Exécuter maintenant**.

   Remarque : Chacune des intégrations de vulnérabilité d'application Veracode est destinée à fournir la récupération de données la plus complète. Leur mise hors service nécessite ServiceNow une Réponse aux vulnérabilités des applications expertise et peut entraîner des données incomplètes.

   Une fois l'importation terminée, les importations planifiées reprennent.
4. Pour les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation de l'intégration de vulnérabilité de l'application Veracode.
5. Si vous souhaitez modifier d'autres paramètres d'intégration, vous devez accéder à l'instance d'intégration.

Définir les Veracode Vulnerability Integration heures d'importation

Pour vous faciliter la tâche, vous pouvez réinitialiser l'heure de début pour le Veracode Vulnerability Integrationfichier .

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche
Après l'importation initiale, les intégrations de Veracode vulnérabilité procèdent à une importation complète à chaque exécution. Pour plus d'informations sur l'exécution des importations, reportez-vous Importer manuellement Veracode la vulnérabilité de l'application à la section .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Veracode** > **Intégrations**.
2. Choisissez une intégration.
3. Définissez la nouvelle **heure de début**.
   L'heure est calculée en heures dans l'heure locale. L'heure par défaut pour les importations d'intégration de liste d'applications est 00 Veracode :00:00. Les autres intégrations sont **disponibles sur demande** et sont chaînées pour s'exécuter après l'intégration de la liste d'applications Veracode . La modification de **l'heure de début** pour l'un ou l'autre de ces éléments nécessite un niveau avancé ServiceNow et Gestion de la vulnérabilité des applications une expertise.
4. Cliquez sur **Mettre à jour**.
   La nouvelle heure est utilisée pour la prochaine importation planifiée.

Inclure les éléments vulnérables de l'application Veracode fermés

Par défaut, les éléments vulnérables de l'application (AVI) **fermés** ne sont pas créés lors des importations d'intégration Veracode des éléments vulnérables. Si vous souhaitez les créer, vous devez modifier une propriété système.

Avant de commencer

Ils Veracode Vulnerability Integration doivent être installés et en cours d'exécution.

Rôle requis : administrateur

Procédure

1. Dans la zone de texte **Navigateur de filtre** de navigation de gauche, saisissez `sys_properties.list`.
2. Dans la zone de recherche **Nom** de la liste, saisissez `sn_vul.create_closed`.
3. Double-cliquez sur le champ **Valeur** et définissez sur **Vrai**
4. Cliquez sur l'icône en forme de coche pour enregistrer.
   Les enregistrements à l'état **Fermé** lors de l'importation suivante Veracode sont créés en tant qu'AVI dans Réponse aux vulnérabilités des applications.

Rattrapage des Réponse aux vulnérabilités des applications vulnérabilités

La surveillance du rattrapage est un processus qui commence par l'examen de l'état et se termine par la fermeture des éléments vulnérables de l'application (AVIT). Réponse aux vulnérabilités des applications propose des outils et des procédures pour rendre ce processus plus productif et efficace.

Réponse aux vulnérabilités des applications Processus de rattrapage

Le rattrapage des éléments vulnérables de l'application est effectué manuellement.

Voici une vue d'ensemble du processus :

- Connectez-vous à votre instance Réponse aux vulnérabilités des applications.
- Validez le fait que vos règles (recherche de CI, affectation) pour les éléments vulnérables de l'application fonctionnent comme prévu. Pour plus d'informations sur la révision des règles de recherche de CI, reportez-vous à la section Identifier automatiquement les applications dans Réponse aux vulnérabilités des applications. Pour en savoir plus sur les règles d'affectation, reportez-vous à la section Affecter automatiquement les éléments vulnérables de Réponse aux vulnérabilités des applications l'application.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifiez que vos cibles de rattrapage sont correctes. Reportez-vous à la rubrique Automatiser le suivi des cibles de rattrapage dans Réponse aux vulnérabilités des applications pour en savoir plus sur le fonctionnement des règles de cibles de rattrapage et sur la manière de les réviser. Afficher l'état de la cible de rattrapage d'un élément vulnérable de l'application

  Remarque : Les règles de cibles de rattrapage appartiennent aux AVIT. Ces règles sont exécutées lorsque l'AVIT est importé.

- Passez en revue les tableaux de bord ou les rapports. Par exemple, affichez les tableaux de bord qui affichent l'ancienneté des AVIT par états.

  Remarque :

  Lorsque l'application (com.snc.vulnerability.analytics) est activée, les Analyse des performances pour Réponse aux vulnérabilités utilisateurs dotés de certains rôles peuvent afficher les données d'intérêt pour les membres des groupes App-Sec Manager et Security Champion.

  Pour les responsables App-Sec, Analyse des performances pour Réponse aux vulnérabilités contient la vue d'ensemble Réponse aux vulnérabilités des applications , qui peut vous aider à surveiller les domaines de préoccupation. Consultez les solutions d'analyse et de reporting pour letableau de bord Application Vulnerability Response et Application Vulnerability Management [PA].

  À partir de la version 13.0 de l'application Réponse aux vulnérabilités : Pour les champions de sécurité, Analyse des performances pour Réponse aux vulnérabilités contient le tableau de bord Mes vulnérabilités d'application, qui peut vous aider à surveiller vos domaines de préoccupation. Consultez le tableau de bord Mes vulnérabilités d'application.

  À partir de la version 13.0 de l'application Réponse aux vulnérabilités : Pour limiter la quantité de données collectées pour les rapports ou les listes connexes, reportez-vous à la section Définir les classifications de service pour Réponse aux vulnérabilités la génération de rapports et les listes connexes.

- Passez en revue l'état des AVIT, par ordre de priorité, en recherchant ce qui a changé.
- Révisez le risque pour les AVIT, selon les besoins. Consultez Créer un calculateur de vulnérabilité d'application pour plus d'informations.
- Réaffectez l'AVIT à un groupe d'affectation pour le rattrapage, si nécessaire.
- Les nouvelles analyses sont déclenchées automatiquement par le calendrier d'importation tierce.
- Après le nouveau scan, si l'état est **Fixe**, les AVIT sont automatiquement fermés pendant l'importation.
- Après l'analyse, si l'état n'est pas **Fixe**, l'AVIT est rouvert.

Obtenir plus de détails à partir de Veracode

Sélectionnez **Obtenir plus de détails** sur les éléments vulnérables de l'application (AVIT) qui ont Veracode comme source dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item] ou à partir des vues de listes dans les espaces de travail Vulnerability Response pour afficher les données suivantes Veracode .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les détails de la demande source HTTP et de la réponse source pour les analyses de Test dynamique de sécurité des applications (DAST) sont affichés dans la liste connexe Demande/réponse HTTP.
- Les recommandations de solutions de Veracode sont affichées dans la liste connexe Résultats.
- La demande source HTTP, la réponse source et les recommandations sont affichées dans l'onglet Détails dans les espaces de travail Vulnerability Response Réponse aux vulnérabilités .
- La colonne Description est prise en charge dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item].

Afficher les bibliothèques de vulnérabilité

Vous pouvez afficher les données de vulnérabilité importées à partir de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou de tiers pour décider s'il convient d'escalader un groupe de vulnérabilité.

Avant de commencer

Rôle requis : groupe de gestionnaires App-Sec

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > pour **les bibliothèques**.

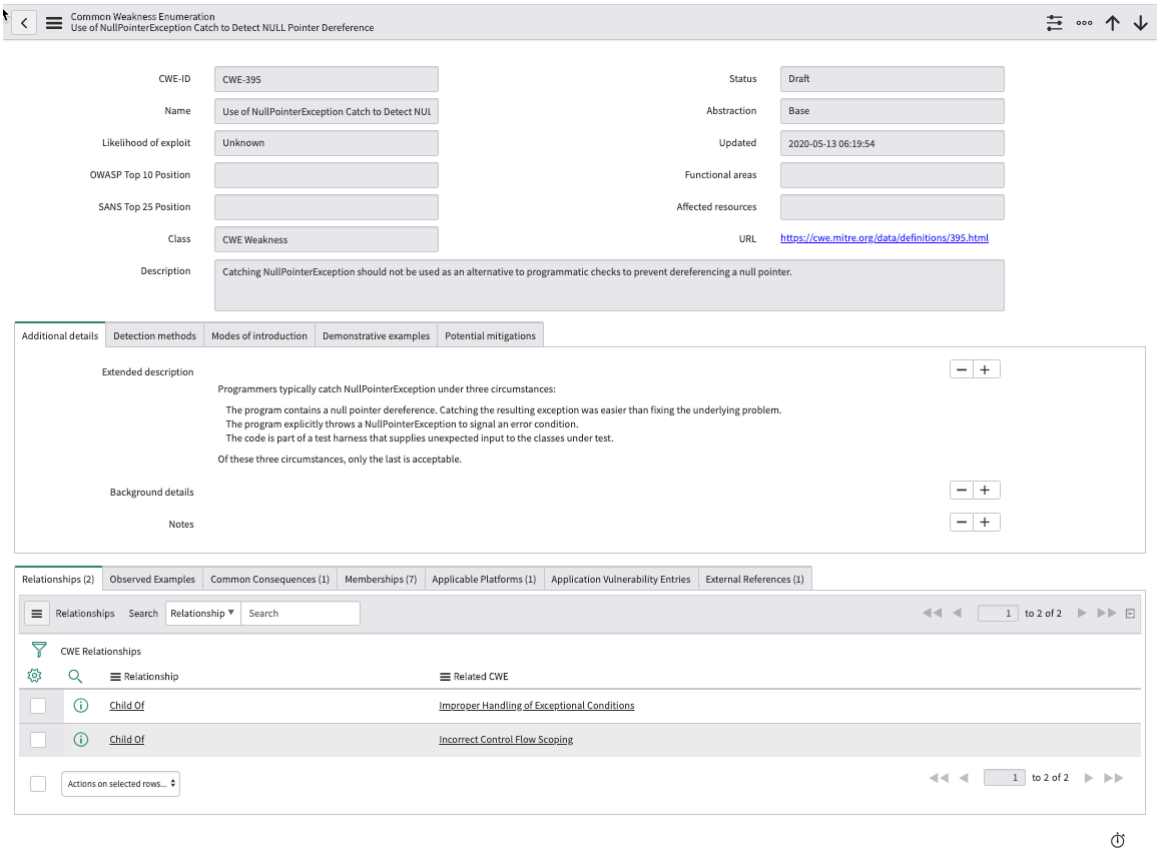
   Les bibliothèques suivantes sont disponibles :

Bibliothèques	Description
NVD	Liste des vulnérabilités détectées par NVD et comprenant des listes de vérification de sécurité, des failles logicielles liées à la sécurité, des erreurs de configuration, des noms de produits et des mesures d'impact, y compris les exploits.
CWE	Liste des types de faiblesses logicielles développés par la communauté. Chaque enregistrement CWE inclut également un article de la base de connaissances associé qui décrit la faiblesse. Vous ne pouvez pas escalader une vulnérabilité à partir de l'écran Common Weakness Enumerations, c'est à titre de référence uniquement.
Tiers	Liste des vulnérabilités tierces importées dans votre instance. Contient une liste de références, d'éléments vulnérables, d'exploits, de CWE et de CVE connexes.

2. Choisissez une bibliothèque pour afficher les vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Pour en savoir plus sur des champs spécifiques, reportez-vous à la section Champs de vulnérabilité de l'application.

Champs de vulnérabilité de l'application

Les vulnérabilités sont créées automatiquement lorsque les enregistrements sont téléchargés à partir de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou d'intégrations tierces. NVD et CWE sont stockés sous **Bibliothèques** dans Réponse aux vulnérabilités ou sous **Vulnérabilités** dans Réponse aux vulnérabilités des applications.

Champs d'entrée de vulnérabilité CWE

Les champs de cette table sont en lecture seule.

Champ	Description
ID CWE	Identificateur de cette entrée de vulnérabilité. Cet identificateur est utilisé à la fois pour les catégories et les faiblesses, et est unique entre les deux jeux de données.
Nom	Nom descriptif affecté à cet ID CWE.
Probabilité d'exploitation	Probabilité que la faiblesse soit exploitée, sur une échelle qualitative. L'un des suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	• Faible • Moyen • Élevé
Position dans le top 10 OWASP	Position numérique de cette vulnérabilité dans la liste des 10 premiers OWASP.
SANS vers 25 positions	Position numérique de cette vulnérabilité dans la liste des 25 premiers SAN.
Classe	Type de faiblesse
Statut	L'un des suivants : • Incomplet • Brouillon • Stable • Déconseillé • Obsolète • Instable
Abstraction	L'un des suivants : • Variante • Classe • Base • Composé
Mis à jour	Dernière mise à jour de l'enregistrement dans l'instance.
Domaines fonctionnels	Liste des domaines fonctionnels concernés. Par exemple, **Traitement des fichiers**. Seulement renseigné pour 24/862 faiblesses.
Ressources affectées	Liste des ressources affectées. Par exemple, **Fichier** ou **Répertoire**. Seulement renseigné pour 51/863 faiblesses.
URL	Article de la base de connaissances associé à cette vulnérabilité.
Description	Description de la vulnérabilité.
Exécution de l'intégration	L'exécution d'intégration dans laquelle cette CWE a été importée.
Sections	
Informations supplémentaires	Descriptions des concepts logiciels qui expliquent plus en détail la faiblesse. Comprend: • Description étendue • Détails en arrière-plan • Notes

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Méthodes de détection	Détails sur la façon dont vous pouvez détecter cette faiblesse dans une application.
Modes d'introduction	Les phases au cours desquelles la faiblesse est introduite, par exemple, **Implémentation**, **Architecture et Conception**, etc.
Exemples démonstratifs	Codez des exemples de la faiblesse avec les descriptions qui les accompagnent.
Atténuations potentielles	Détails sur la façon de prévenir la faiblesse, y compris la phase du cycle de vie de l'application dans laquelle elle se produit et l'efficacité de l'atténuation.
Listes connexes	
Relations	CWE associés à cette vulnérabilité. Répertorie les relations entre cette CWE et d'autres. Peut inclure parent/enfant, suit/précède, requiredby/requires (pour les faiblesses composites), CanAlsoBe, PeerOf, MemberOf.
Exemples observés	Quelques CVE représentatives de cette faiblesse.
Conséquences courantes	Conséquences d'un exploit réussi, en termes de portée et d'impact. Par exemple : Champ d'application : Confidentialité Impact : lire les données de l'application
Adhésions	Adhésions CWE avec cette vulnérabilité.
Plateformes applicables	Plateformes associées à cette vulnérabilité.
Entrées de vulnérabilité de l'application	Autres entrées de vulnérabilité d'application associées à une.
Références externes	Informations sur la vulnérabilité provenant de sources externes.

Champs d'entrée de vulnérabilité de l'application

Les champs de cette table sont en lecture seule.

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Source	Origine de la vulnérabilité : qu'il s'agisse d'un scanner ou d'un test physique.
Sévérité	Degré normalisé de gravité de cette vulnérabilité. Des cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations tierces. Pour plus d'informations sur la création ou l'ajustement de cartes de gravité, reportez-vous à la section Mapper automatiquement la gravité d'un élément vulnérable de l'application.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Version 13.0 : CWE primaire Version 12.1 : entrée CWE	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux. S'il existe plusieurs CWE associées à la vulnérabilité, la CWE primaire est déterminée comme suit : • Correspond au CWE mappé au top 10 OWASP ? Si c'est le cas, utilisez ce CWE. Si ce n'est pas le cas, continuez. • Le CWE est-il mappé au Top 25 des SAN ? Si c'est le cas, utilisez ce CWE. Si ce n'est pas le cas, continuez. • La CWE a-t-elle la gravité la plus élevée ? Si c'est le cas, utilisez ce CWE. Si ce n'est pas le cas, continuez. • Sélectionnez le plus récent de tous les CWE. La dernière CWE est celle qui a la dernière valeur de champ **Mis à jour** dans l'enregistrement CWE.
Nom de catégorie	Classification fournie par l'intégration tierce. Aide à l'affectation.
Détails des vulnérabilités	
Menace	Description de la menace provenant de cette vulnérabilité.
Description de l'atténuation	Description des mesures qui pourraient être prises pour atténuer la vulnérabilité.
Liste connexe	
Version 13.0 : CWE	Liste des CWE associés à cette vulnérabilité. Ne s'applique pas au Veracode Vulnerability Integrationfichier .

Champs d'entrée NVD

Les champs importés dans cette table sont en lecture seule.

Remarque :

Les données NVD ne sont pas utilisées et Réponse aux vulnérabilités des applications les entrées ne représentent Réponse aux vulnérabilités que des données.

Les CWE, qui sont utilisés dans Réponse aux vulnérabilités des applications, peuvent pointer vers des entrées NVD, comme exemples d'une faiblesse, et sont fournis ici à titre informatif uniquement.

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Cote de risque	(Masqué lorsqu'aucun élément vulnérable (VI) n'est Réponse aux vulnérabilités associé à la vulnérabilité) **Score de risque** quantifié séparant les éléments vulnérables en trois catégories : Critique, Élevé, Moyen, Faible et Aucun.
Score du risque	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Quantité calculée de risque que l'élément vulnérable pose à votre environnement.
Sévérité	Degré normalisé de gravité de cette vulnérabilité dans Réponse aux vulnérabilités. Des cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations tierces. Réponse aux vulnérabilités des applications **La gravité** est dérivée de **la gravité source** importée et non NVD. Pour en savoir plus sur le mappage de gravité, reportez-vous Réponse aux vulnérabilités des applications à la section Mapper automatiquement la gravité d'un élément vulnérable de l'application.
Existence de l'exploit	Oui, si au moins un exploit est associé à cette vulnérabilité.
Niveau de compétence de l'exploit	Niveau de compétence le plus bas requis pour exploiter cette vulnérabilité.
Vecteur d'attaque de l'exploit	Vecteur d'attaque le plus vulnérable des exploits pour cette vulnérabilité.
VI actifs	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) Nombre d'éléments vulnérables associés à cette vulnérabilité, dont l'état n'est pas Fermé. Si aucun AVI actif n'est disponible pour cette vulnérabilité, **la cote de risque** et le **score de risque** ne sont pas affichés.
Entrée CWE	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux selon la NVD.
Date de publication	Date de publication de la vulnérabilité.
Dernière modification	Date de la dernière modification de la vulnérabilité.
Résumé	Description de la vulnérabilité.
Détails des vulnérabilités	
CVSS v2	Données CVSS v2 importées
CVSS v3	Données CVSS v3 importées, non disponibles avant 2015.
Solution privilégiée	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) Solution de remplacement la plus élevée de la chaîne, dérivée des solutions référencées dans la vulnérabilité. S'il existe plus d'un remplacement le plus élevé dans la chaîne, aucune valeur n'est fixée. Toute valeur définie manuellement peut être écrasée lors des importations suivantes. La définition manuelle de cette valeur doit être effectuée sur l'élément vulnérable.
État du rattrapage (Masqué lorsqu'aucun VI n'est associé à la vulnérabilité)	

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Exclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables d'applications actifs avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
Inclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité.
Liens connexes	
Avant la version 13.0 : Forcer l'importation de la vulnérabilité logicielle **Remarque :** Supprimé dans la version 13.0	(Déconseillé) Recalcule le mappage des produits en Gestion des actifs logiciels pour ITSM fonction des informations provenant de NVD. Met à jour la bibliothèque de logiciels vulnérables.
Mettre à jour le statut	Affiche la date et l'heure de la dernière mise à jour. Met à jour les éléments suivants : • État du groupe de vulnérabilité • Score et évaluation du risque • Mesures telles que VI actifs, VI totaux de la section État de rattrapage
Listes connexes	
Éléments vulnérables	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) Éléments vulnérables associés à cette vulnérabilité.
Références de vulnérabilité	Informations sur la vulnérabilité provenant de sources externes, citées par NVD.
Exploite	Exploits associés à cette vulnérabilité.
Solutions	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Toutes les Gestion des solutions pour vulnérabilités solutions d'intégration associées à cette vulnérabilité.
Version 13.0 : Faiblesses	Données de faiblesse CWE importées associées à des vulnérabilités et expositions communes (CVE).
Version 13.0 : Logiciel vulnérable	(Masqué lorsqu'aucun VI n'est associé à la vulnérabilité) Données CPE (Common Platform Enumeration) importées associées à la vulnérabilité.

Identifier automatiquement les applications dans Réponse aux vulnérabilités des applications

Lorsque des données sont importées à partir d'une intégration tierce, Réponse aux vulnérabilités des applications utilise automatiquement les données de l'application pour rechercher des correspondances dans le Base de données de gestion des configurations (CMDB)fichier . Pour ce faire, il utilise des **règles de recherche de CI**. Ces règles identifient les applications pour l'enregistrement de l'élément vulnérable de l'application (AVI) afin de faciliter la correction.

Au fur et à mesure que les applications sont importées, une recherche est effectuée sur l'application numérisée [sn_vul_app_scanned _application] ne peut pasutiliser source_app_id et app_name pour trouver des correspondances avec les applications à partir d'importations antérieures. Lorsqu'une correspondance d'ID d'application est trouvée, ses valeurs sont utilisées dans les champs **Application** et **Version de l'application** dans l'enregistrement de l'élément vulnérable de l'application.

Si aucune correspondance n'est trouvée ou si le champ d'ID d'application est vide, les règles utilisent les autres informations d'application pour tenter d'identifier correctement l'application. Si aucune correspondance n'est toujours trouvée, un enregistrement d'application analysée d'espace réservé est créé avec uniquement les champs **Nom de l'application** et **ID de l'application** .

Les règles de recherche ID **d'application source** et **Nom d'application** sont fournies avec le Veracode Vulnerability Integration, par défaut.

Remarque : Les règles Réponse aux vulnérabilités des applications de recherche de CI par défaut ne sont disponibles que pour l'intégration de Veracode vulnérabilité.

Lors de la tentative de correspondance, les règles de recherche sont d'abord évaluées par la valeur **d'ordre** la plus basse. Elles s'arrêtent lorsqu'une règle renvoie un seul CI comme correspondance.

Remarque : Si une règle est créée de telle sorte qu'elle renvoie plusieurs CI, seule la première correspondance est utilisée.

Pour faciliter la recherche de problèmes correspondants, lorsqu'une correspondance est trouvée, la règle de recherche de CI utilisée pour la trouver est ajoutée au champ de **règle de correspondance de CI** pour les applications analysées. Cliquez sur Mettre à jour l'engrenage de la liste personnalisée en haut de la vue de liste Applications numérisées pour l'ajouter à la vue.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les règles, une fois supprimées, ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Les règles de recherche de CI peuvent être séparées par domaine et sont spécifiques à la source. En cas de prise en charge, chaque source peut avoir plusieurs déploiements. Par exemple, l'intégration Veracode de vulnérabilité peut avoir plusieurs déploiements de l'intégration Veracode de vulnérabilité. Chaque déploiement possède son propre ensemble de règles de recherche de CI.

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

L'importation de données de vulnérabilité peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas soigneusement construites. La logique utilisée pour itérer et effectuer une correspondance au sein de peut CMDB entraîner de longs délais de traitement. Pour éviter toute dégradation potentielle des ressources ou toute complication des performances, testez les règles de recherche de CI écrites sur mesure ou les modifications apportées aux **règles de recherche de CI prédéfinies**. Pour plus d'informations sur la prévention des enregistrements orphelins en double, la suppression des données et le nettoyage des données, consultez la rubrique Empêcher les enregistrements dupliqués ou orphelins après l'exécution des règles de recherche de CI d'Application Vulnerability Response .

Information associée

Gestion des configurations et CMDB

Créer une règle de recherche de CI

Le module **Règles de recherche de CI** contient des règles qui définissent les champs qui ont des données correspondantes dans le Base de données de gestion des configurations (CMDB)fichier . Ces règles sont utilisées pour identifier les applications et les versions d'application et les ajouter à l'enregistrement d'élément vulnérable de l'application (AVI) pour faciliter la correction.

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche
La création de règles de recherche de CI nécessite un niveau avancé ServiceNow et Gestion de la vulnérabilité des applications une expertise. Plutôt que de modifier l'une des règles de recherche existantes, envisagez de la copier et de modifier la copie. Lorsque vous êtes convaincu que la nouvelle règle fait ce que vous voulez, désactivez l'originale.

Remarque : Les règles, une fois supprimées, ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **CMDB** > **Règles de recherche de CI**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Règle de recherche de CI

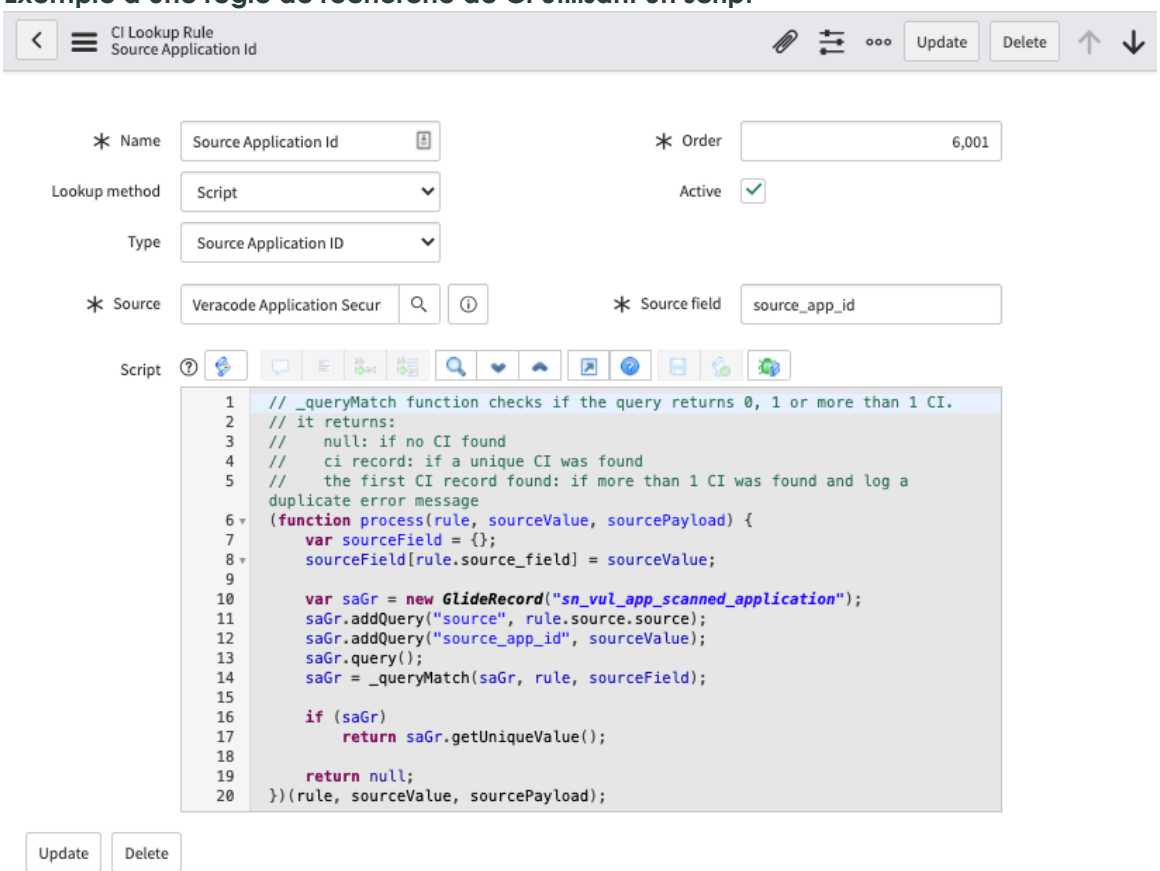
Champ	Description
Nom	Nom de la règle.
Méthode de recherche	Méthode utilisée pour la correspondance. Les choix possibles sont les suivants : ◦ **Script** : script prédéfini ou personnalisé. ◦ **Correspondance de champ** : recherche sur une table ou un champ dans la CMDB.
Type	Type utilisé avec la **méthode Recherche de** script.
Ordre	Ordre de priorité de la règle. Les correspondances avec l'ordre le plus bas sont évaluées en premier.
Actif	Cochez la case pour indiquer si la règle est active ou désactivée.
Source	Source utilisée comme entrée dans cette règle. Une fois choisis, les filtres de condition s'affichent.
Champ source	Champ source utilisé comme entrée à cette règle. Les champs doivent être une chaîne ou un numéro.
Description	Texte décrivant la règle.
V19.0 : cible de recherche	Approche de recherche que vous souhaitez suivre. Sélectionner à partir de : ◦ Élément de configuration ◦ Modèle de produit
Script	Un exemple de script modifiable, basé sur le **type**, est affiché. Implémentez le script personnalisé en fonction des commentaires inclus dans le modèle de la fonction par défaut. **Remarque :** La fonction process comporte trois paramètres : *rule*, *sourceValue* et *sourcePayload*
Rechercher sur la table CI	Table à rechercher dans la CMDB. Utilisé avec la **méthode de recherche** de correspondance de champ.
V19.0 : Recherche sur la table de produits	Si vous choisissez la cible de **recherche Modèle de** produit, la valeur par défaut est Modèle d'application.
Rechercher sur le champ CI	Champ qui contient des informations pouvant être utilisées pour localiser un CI. Utilisé avec la **méthode de recherche** de correspondance de champ. Ce champ peut se trouver sur l'enregistrement CI ou sur un enregistrement connexe, tel qu'une carte réseau.
V19.0 : recherche sur le champ modèle de produit	Si vous choisissez la **cible de recherche Modèle de** produit, la valeur par défaut est Nom.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Envoyer**.

Exemple d'une règle de recherche de CI utilisant un script



Information associée

Champs d'éléments vulnérables d'applications

Réapplication des règles de recherche de CI dans Réponse aux vulnérabilités des applications

Vous pouvez réappliquer vos règles de recherche d'éléments de configuration (CI) pour mettre à jour les CI existants (applications numérisées et modèles de produits) sur les enregistrements d'application détectés.

Réapplication d'une règle de recherche

La réapplication des règles de recherche de CI appliquera toutes les règles activées aux applications détectées existantes. La mise à jour des enregistrements d'application détectés peut prendre du temps.

Pour réappliquer les règles aux applications détectées existantes, accédez à **Tout** > **Security Operations** > **CMDB** > **Règles de recherche** et sélectionnez **Appliquer les modifications**.

Définition de la cible de recherche

Par défaut, la *sn_vul.use_product_model* propriété système est activée (définie sur **true**). Selon la façon dont la propriété système est définie sur les enregistrements de règle de recherche de CI, les enregistrements d'application détectés sont mis à jour de la manière suivante :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si le champ Valeur est défini sur **vrai**, le modèle de produit est la cible de recherche pour les règles de recherche de CI et les applications détectées sont mises à jour avec les modèles de produits.
- Si le champ Valeur est défini sur **faux**, l'élément de configuration (applications analysées) est la cible de recherche et les applications détectées sont mises à jour avec les éléments de configuration (applications analysées).

Pour modifier la *sn_vul.use_product_model* propriété système afin que les éléments de configuration soient utilisés comme cible :

1. En tant qu'utilisateur disposant du rôle sn_vul.app_sec_manager, accédez à **Tout** > **Propriétés système** > **Tout**
2. Localisez *sn_vul.use_product_model*.
3. Ouvrez l'enregistrement.
4. Définissez le champ Type sur **faux**.
5. Sélectionnez **Mettre à jour**.

Si vous réinitialisez cette propriété système, vous devez modifier vos règles afin que les cibles de recherche correspondent au paramètre de propriété système. Par exemple, si vous réinitialisez la propriété système de sorte que vous utilisez l'élément de configuration comme cible, localisez les règles qui ont la cible de recherche comme élément de configuration.

1. Cochez la case Actif pour ces règles, puis sélectionnez **Mettre à jour**.
2. Localisez les règles qui utilisent le modèle de produit comme cible et désactivez-les en désélectionnant la case à cocher Actif, puis en sélectionnant **Mettre à jour**.

Si vous créez une règle de recherche, vous devez définir la cible de recherche de la règle sur le formulaire de règle. Consultez Créer une règle de recherche de CI pour plus d'informations.

Empêcher les enregistrements dupliqués ou orphelins après l'exécution des règles de recherche de CI d'Application Vulnerability Response

Prenez des mesures pour empêcher les enregistrements dupliqués ou orphelins résultant de la mise en correspondance (éléments de configuration (CI) dans le CMDB.

L'importation de données de vulnérabilité peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas soigneusement construites. La logique utilisée pour itérer et effectuer une correspondance au sein de la CMDB peut entraîner de longs délais de traitement. Des tests et un débogage approfondis des scripts de traitement dans les règles permettent d'atténuer le risque de problèmes ultérieurs au cours du processus.

Empêcher les enregistrements en double ou orphelins

- Utilisez de petits sous-ensembles de données spécifiques à la règle de recherche de CI testée.
  - Définissez toutes les **règles de recherche de CI**, autres que celle testée, sur **Inactive**.
  - Analysez les applications et les éléments de configuration importés pour vous assurer que vous observez le comportement attendu et que la correspondance se produit correctement.
- Examinez les états du CI tels que **Mis hors service**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Supprimez les données de test. Une fois que vous commencez à observer le comportement correct ou attendu dans la correspondance CI, recommencez. Cela peut se faire par :
  - Suppression des données utilisées pour les tests : (voir la section **Suppression des données des tables**)
    - Applications numérisées
    - Éléments vulnérables de l'application (AVI)
  - Réexécutez manuellement les intégrations.

.

Suppression des données des tables

Parfois, vous avez importé des données et vous vous rendez compte que quelque chose ne va pas. Si cela se produit dans un environnement de développement ou de performance, vous pouvez vous retirer d'un meilleur environnement, mais ce n'est pas toujours une option.

Remarque : L'exécution de ces actions nécessite une expertise avancée ServiceNow .

Il existe quatre options pour supprimer les données des tables :

- Utilisation de **Supprimer tous les enregistrements** sur **la configuration de table**.
- Configurez le **nettoyeur de table** en accédant à **Purges automatiques** (sys_auto_flush.list) et en créant un nouvel enregistrement **de vidage automatique** .
- Tronquez la gs.truncateTable à l'aide d'un script en arrière-plan.

  Remarque : Ne jamais utiliser *`truncateTable`* dans un environnement de production. Consultez votre représentant du support avant d'effectuer des suppressions importantes dans des environnements de production ou partagés.

- Créez une demande dans HI pour que les données soient supprimées.

Affecter automatiquement les éléments vulnérables de Réponse aux vulnérabilités des applications l'application

Affectez automatiquement des vulnérabilités d'application en fonction des balises d'application, ou de l'un des groupes d'affectation dans l'élément de configuration [cmdb_ci] ou les groupes d'affectation de plateforme, afin de réduire le délai moyen d'affectation.

Affectation automatique des éléments vulnérables de l'application

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

Remarque : La fonctionnalité de recommandation d'affectation dans Réponse aux vulnérabilités n'est pas disponible pour Réponse aux vulnérabilités des applications.

- Groupe d'utilisateurs : cette option vous permet de sélectionner l'un des groupes d'utilisateurs existants Now Platform® .
- Champ de groupe d'utilisateurs : cette option vous permet de choisir n'importe quel champ de groupe d'affectation disponible à l'aide de la table cmdb_ci. Par défaut, les trois champs de groupe suivants s'affichent dans le menu Liste sous **Champ du groupe d'utilisateurs**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Aucun : n'indique aucune valeur par défaut pour ce champ obligatoire
- Élément de configuration : groupe d'approbation
- Élément de configuration : Groupe d'affectation
- Élément de configuration : groupe de support

- Script : cette option vous permet de définir les conditions à l'aide d'un script. Cette option nécessite un codage ou une expertise avancée ServiceNow .

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

Processus d'évaluation des règles d'affectation

Lorsqu'un nouvel AVI est créé, importé ou rouvert après sa fermeture, les règles d'affectation sont évaluées par rapport à celui-ci. Un AVI n'est évalué qu'une seule fois, sauf s'il est rouvert après avoir été fermé. Vous pouvez réappliquer manuellement des règles après les changements.

Le processus suivant est utilisé pour chaque nouvel AVI, mis à jour ou rouvert :

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

Remarque : S'il n'existe pas de règle par défaut, l'AVI n'est pas affecté.

Le type d'affectation, qu'il soit **manuel ou derègle** et **la règle d'affectation** , est disponible dans la zone de sélection Mise en page du formulaire d'élément vulnérable de l'application (AVI). Tout AVI qui a été affecté à l'origine par une règle, mais qui a ensuite été réaffecté manuellement, contient une référence à la règle d'origine. Utilisez la **règle d'affectation** et les informations sur le **type d'affectation** pour identifier les tickets dans lesquels les règles d'affectation n'ont pas trouvé de correspondance correcte pour le destinataire prévu. Ou quelles règles ont eu le plus de réaffectations ?

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

Réapplication des règles d'affectation

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

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Si la *Reapply all vulnerability assignment rules* tâche planifiée n'a pas été exécutée avant la première fois que vous utilisez **l'option Appliquer les changements**, elle exécute toutes les règles d'affectation sur tous les AVI ouverts, à l'exception des AVI qui ont été affectés manuellement. Après cela, toutes les utilisations ultérieures **d'Appliquer les modifications** réexécutent uniquement les règles modifiées et toutes les règles dépendantes. Les changements apportés à une règle peuvent entraîner la mise en correspondance d'un AVI avec une autre règle non modifiée.

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

Créer ou modifier des Réponse aux vulnérabilités des applications règles d'affectation

Vous pouvez créer des règles pour affecter automatiquement les éléments vulnérables de l'application (AVI) en fonction des conditions de filtre. Ces règles affectent les AVI au fur et à mesure qu'ils sont importés ou créés manuellement.

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche
Avec les règles d'affectation, vous définissez la condition d'affectation et l'ordre d'exécution. Une fois qu'un AVI correspond à une condition de règle, la recherche d'affectation s'arrête. Consultez Filtrage au sein de Gestion de la vulnérabilité des applications pour plus d'informations.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Règles d'affectation**.
2. Cliquez sur **Nouveau**.
3. S'il s'agit **d'un nouveau**, renseignez les champs du formulaire comme il convient.

Règle d'affectation de vulnérabilité de l'application

Champ	Description
Nom	Nom de la règle de groupe.
Actif	Indique si la règle d'affectation est active.
Ordre d'exécution	Ordre dans lequel les règles sont évaluées. Les règles de priorité élevée, les éléments qui nécessitent une gestion spéciale, lorsque le risque est critique, ou un AVI qui doit être traité par la conformité réglementaire, doivent être exécutés en premier. Ensuite, exécutez vos règles générales, où aucune manipulation spéciale n'est requise, et vous savez qui doit en être responsable. Enfin, créez une règle par défaut pour affecter les AVI au groupe qui déterminera à quel groupe d'affectation ils doivent appartenir. Ce groupe pourrait ajouter une autre

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	règle pour couvrir ses décisions. Cette règle par défaut s'exécute en dernier.
Description	Description de la règle d'affectation.
Condition	
Champs de condition	Conditions qui doivent être remplies.
Nouveau critère	Ajoute d'autres champs de filtre de condition au choix.
Affecter à l'aide de	Pour automatiser l'affectation des groupes créés en fonction de cette règle, choisissez l'une des options disponibles. ◦ Groupe d'utilisateurs : sélectionnez un groupe d'utilisateurs dans la table de recherche. ◦ Champ de groupe d'utilisateurs : sélectionnez un champ de groupe d'utilisateurs dans le menu Liste. ◦ Script : créer ou modifier un script. **Remarque :** La création ou la modification d'un script nécessite ServiceNow une expertise.

4. Cliquez sur **Envoyer**.
   Les règles nouvelles ou mises à jour sont évaluées lors de l'importation suivante.

Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications

Les calculateurs de vulnérabilité de l'application automatisent le calcul des valeurs de risque initiales pour les champs des éléments vulnérables de l'application (AVI). Les calculs de risque permettent de déterminer clairement comment hiérarchiser le rattrapage. La condition de chaque calculateur est évaluée dans l'ordre, et le premier calculateur correspondant est utilisé.

Calculateurs de vulnérabilité de l'application

Le Réponse aux vulnérabilités des applications système de base comprend deux calculateurs de vulnérabilité qui définissent le **score de risque** de base sur l'élément vulnérable de l'application.

- **Calculateur de risque de base**
- **Calculateur Advanced Risk**

Les calculateurs de vulnérabilité des applications peuvent être conçus pour classer par ordre de priorité et évaluer l'impact des AVI en fonction de n'importe quel critère à l'aide de filtres de condition. Qu'il s'agisse de l'impact sur l'entreprise de la vulnérabilité, de la classe de l'élément de configuration (CI) ou de l'âge de l'AVI, vous pouvez créer des calculateurs de vulnérabilité supplémentaires pour définir d'autres champs sur les AVI. Vous pouvez également personnaliser les calculateurs de vulnérabilité existants. Un calculateur peut être écrit pour refléter n'importe quel ensemble de priorités. Consultez Filtrage au sein de Gestion de la vulnérabilité des applications pour plus d'informations.

Les AVI contiennent la valeur **de score de risque** dérivée des calculateurs de risque.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Un AVI affiche **la gravité de la source** , mais pas la gravité normalisée. La gravité normalisée est utilisée par les calculateurs pour obtenir la valeur **du score de risque** , mais n'est pas affichée sur les AVI.

Chaque calculateur contient une liste de règles de calcul, avec une condition déterminant quand l'appliquer. Lorsque le calculateur est exécuté, la condition de chaque règle de calcul est évaluée dans l'ordre, et la première règle de calcul correspondante est utilisée.

Tous les calculateurs de vulnérabilité activés définissent les champs sélectionnés chaque fois qu'un AVI est créé, lorsqu'un CI associé ou une vulnérabilité change.

Le calculateur **de risque de base** calcule le **score de risque** pour AVI à l'aide de la gravité de vulnérabilité normalisée.

Remarque : Un seul calculateur par champ cible (**score de risque**) peut être actif à la fois.

Le **risque de base** est activé par défaut. Le **calculateur Advanced Risk** est désactivé par défaut.

Règles du calculateur de vulnérabilité de l'application

Le **calculateur de risque de base** du système de base contient des règles de calcul qui attribuent à chaque niveau de gravité (aucun à critique) une valeur (0-100) pour **le score de risque** en fonction de la gravité. **Gravité inconnue** se voit automatiquement attribuer un score de risque de 100. Ces valeurs peuvent être ajustées et, comme **le calculateur Advanced Risk**, de nouvelles règles de calcul ou de nouvelles règles de risque peuvent être créées.

Remarque : À partir de la version 23.0 de Réponse aux vulnérabilités des applications, chaque fois que le score de risque est mis à jour sur un AVIT, la section **Notes** est mise à jour avec les détails suivants :

- Nom du groupe de calculateurs
- Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre parenthèses. Pour modifier ou afficher la base de la règle du calculateur, sélectionnez n'importe quelle règle et cochez la case Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. Si le **modèle** est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si **Script** est sélectionné, vous pouvez ajouter ou mettre à jour le script existant.

Le **calculateur Advanced Risk** du système de base contient une règle de calcul de vulnérabilité spécialisée appelée **règle de risque par défaut**. Il calcule le **score de risque** en fonction de plusieurs valeurs :

- Gravité de la vulnérabilité
- 10 premiers OWASP
- SANS Top 25

Vous pouvez personnaliser les critères de la règle de risque par défaut. Pour plus d'informations, consultez Définir des champs et des poids pour la règle de risque.

Vous pouvez ajuster les valeurs à utiliser dans la **règle de risque par défaut** et le poids à donner à chacune de ces valeurs. Les pondérations sont utilisées pour ajuster l'importance de chaque élément lors de la définition du **score de risque**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chaque règle a un paramètre **d'ordre** . Toutefois, la première à correspondre aux conditions met à jour le champ **Score de risque** dans l'AVI. Les règles de calculateur non scriptées ont généralement moins d'impact sur les performances que les règles de calculateur scriptées.

Poids du score du risque de vulnérabilité

Un score de risque et une évaluation sont attribués à toutes les vulnérabilités en fonction de facteurs tels que la gravité, la criticité, les informations d'exploitation, etc. La règle *`Update Risk Rating from Risk Score`* métier de la table des éléments vulnérables est responsable du calcul de la cote de risque. Chaque fois que le score de risque change, la cote de risque est calculée et renseignée sur les éléments vulnérables. Avant la version 17.1 de l'application Réponse aux vulnérabilités (VR), les évaluations de risque suivantes étaient fournies dans le cadre du script `include VulnerabilityUtils`, qui étaient codés en dur.

Valeur (cote de risque)	Poids (score de risque)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

À partir de la version 18.0 de Réponse aux vulnérabilités,

- Les types de cote de risque sont expédiés dans la table de base en tant que avr_risk_rating. Ces types sont transmis dans le cadre de la règle métier sur chaque table où la cote de risque est calculée.
- Le script est modifié afin que vous puissiez interroger les entrées dans les valeurs de la table Poids du score de risque pour le calcul de la cote de risque.
- Ajoutez des entrées supplémentaires pour un type existant ou créez un nouveau type. Lorsque vous créez un nouveau type, assurez-vous d'ajouter les étiquettes pour la nouvelle cote de risque et de modifier les scripts et règles métier connexes. Vous devez également ajouter un nouveau style pour le nouveau score de risque.
- Modifiez le script pour interroger les enregistrements dans la table de base.

Vous pouvez accéder à la table des poids de score de risque en saisissant sn_sec_cmn_risk_score_weight dans le navigateur de filtre.

En outre, le score de risque est automatiquement recalculé dans les scénarios suivants :

- Lorsqu'un élément de configuration (CI) passe d'un mode non accessible sur Internet à un mode accessible sur Internet.
- Lorsque les vulnérabilités et expositions communes (CVE) ou les entrées tierces (TPE) associées sur les éléments de vulnérabilité (VI) sont liées à une vulnérabilité d'exploitation connue CVE (KEV).

Définir des champs et des poids pour la règle de risque

Personnalisez les paramètres et les pondérations de la règle de risque afin de pouvoir générer des scores de risque qui utilisent les données de vulnérabilité et d'actif propres à votre organisation. En sélectionnant les champs inclus dans la règle de risque, vous pouvez définir un cadre de travail de notation des risques efficace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul.app_manage_risk_score_configuration

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Calculateurs de vulnérabilités**.
2. Sur la page Calculateurs de vulnérabilité, cliquez sur **Calculateur de risque avancé**.
3. Accédez à la **Page Calculateur de vulnérabilité** > **Onglet Règles du calculateur de vulnérabilité** > **Règle sur les risques par défaut**.
4. Facultatif : Dans la section Critères du calculateur de risque de la page Règle de risque de vulnérabilité, définissez la pondération de chaque critère en fonction de son importance dans le calcul du score de risque global.
5. Pour désactiver la règle, vous devez décocher la case **Actif** .
6. Pour ajouter des champs de règle de risque aux critères du calculateur de risque, cliquez sur **Ajouter des critères**.
7. Renseignez les champs du formulaire.

Formulaire de champ de règle de risque

Champ	Description
Choisir la table de référence	Table utilisée pour définir la pondération du score de risque. Vous pouvez sélectionner l'une des options suivantes : ◦ **Élément vulnérable de l'application** : ajoutez des champs directement accessibles par point à partir de l'élément vulnérable (VI). ◦ **Élément vulnérable de l'application : élément de configuration** : ajoutez des champs de remontée pas à pas qui font partie des extensions de table de base, comme la table Matériel. Ces champs ne font pas partie de la table de base (cmdb_ci). ◦ **Élément vulnérable de l'application : vulnérabilité** : ajoutez des champs parcourables par point qui font partie des tables qui étendent la table de base, par exemple, Entrée tierce. Ces champs ne font pas partie de la table de base Entrée de vulnérabilité. ◦ **Table de référence des éléments vulnérables de l'application** : ajoutez des champs qui font partie des tables connexes (m2m) ou des tables qui font référence à l'élément vulnérable. Ces champs ne sont pas directement accessibles par point à partir du VI. ◦ **Table de référence de l'élément de configuration** : ajoutez des champs qui

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	font partie des tables connexes (m2m) de cmdb_ci ou des tables qui font référence à cmdb_ci. Ces champs ne sont pas directement accessibles par point à partir du VI. ◦ **Table de référence de vulnérabilité** : ajoutez des champs qui font partie des tables connexes (m2m) de sn_vul_entry ou des tables qui font référence à sn_vul_entry. Ces champs ne sont pas directement accessibles par point à partir du VI. ◦ **Conditions personnalisées** : utilisez cette option pour affecter des poids à la règle en évaluant la condition. Par exemple, le filtre accessible sur Internet détermine si un élément de configuration (CI) est externe ou interne.
Table	Champ qui n'apparaît que lorsque l'une des options suivantes est sélectionnée dans la table Choisir une référence : ◦ **Élément vulnérable de l'application -> Élément de configuration** ◦ **Élément vulnérable de l'application -> vulnérabilité** ◦ **Table de référence des éléments vulnérables de l'application** ◦ **Table de référence de l'élément de configuration** ◦ **Table de référence de vulnérabilité**
Champ	Champ à utiliser pour le calcul du score de risque pour cette règle.
Agrégation	Champ qui s'affiche uniquement lorsqu'une table de référence est sélectionnée à partir de l'option Choisir une table de référence. Sélectionnez la valeur minimale ou maximale à prendre en compte pour les calculs lorsque le champ est sélectionné dans les tables connexes (m2m).
Poids	Pondération de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
Définir la pondération de la valeur	Composant permettant d'attribuer des poids à chaque valeur de champ. Pour les champs numériques, les valeurs de champ peuvent être définies comme une plage (par exemple, de 1 à 5). Les poids doivent

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	être un nombre entier compris entre 0 et 100. **Remarque :** Ce champ n'apparaît pas si l'option Conditions personnalisées est sélectionnée dans la table Choisir une référence.
Table de condition	Champ qui s'affiche uniquement lorsque Conditions personnalisées est sélectionnée dans la table Choisir une référence. Sélectionnez une condition dans la liste.
Nom de champ	Champ qui s'affiche uniquement lorsque Conditions personnalisées est sélectionnée dans la table Choisir une référence. Saisissez un nom pour les critères de risque.
Condition	Champ qui s'affiche uniquement lorsque Conditions personnalisées est sélectionnée dans la table Choisir une référence. Prévisualisez les éléments de cette table qui correspondent aux conditions définies.

8. Cliquez sur **Envoyer**.
9. Dans la page Règle, activez et réappliquez la règle pour réévaluer le score de risque sur les éléments vulnérables actifs.

Example:
Ajouter la gravité de la source comme critère pour une règle de risque.

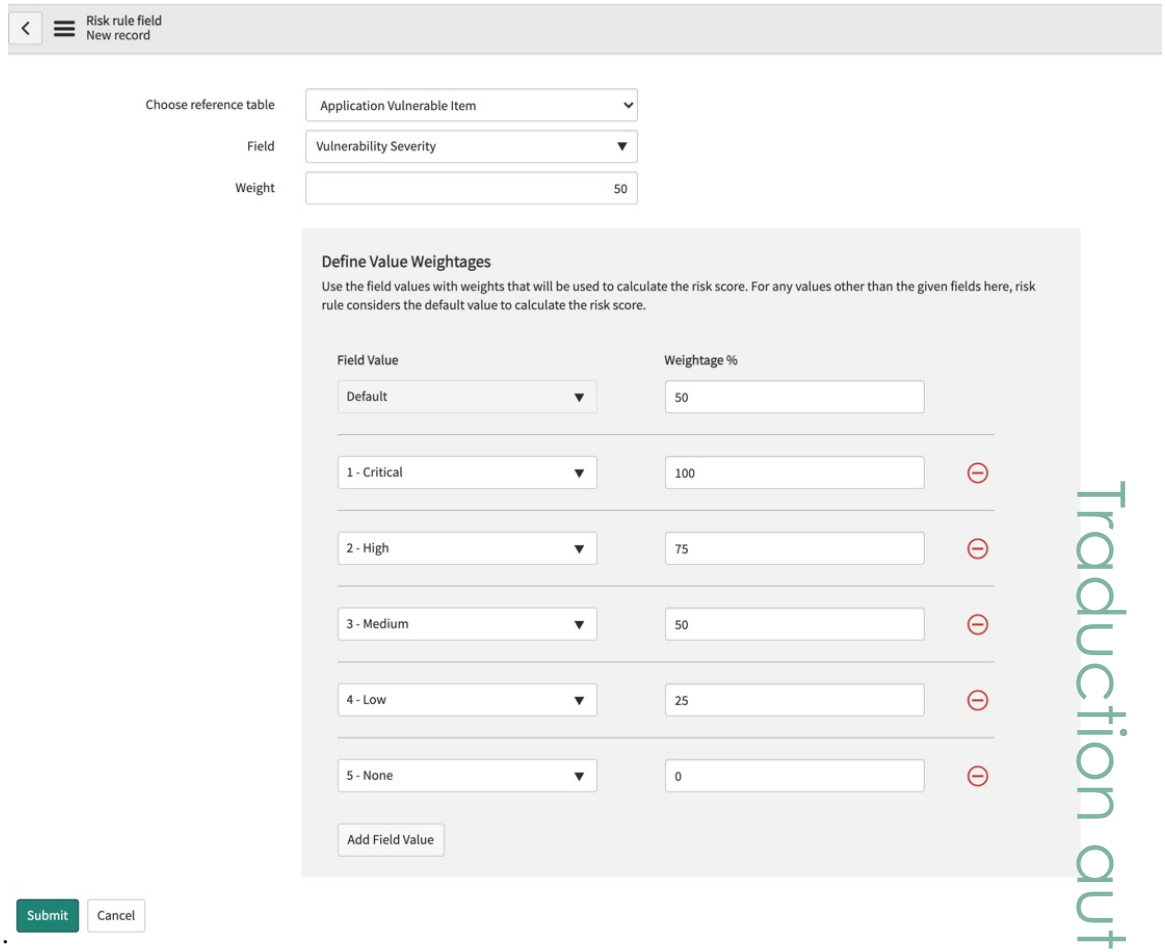
Cas d'utilisation : les fournisseurs tiers, tels que Qualys et Tenable, fournissent leurs propres scores. Ces scores sont renseignés dans le champ **Gravité de la source** de la table sn_vul_entry. Utilisez ce champ pour les calculs de score de risque. Pour utiliser ce score afin de calculer le score de risque, procédez comme suit :

1. Accédez à la page Règle de risque.
2. Pour désactiver la règle, décochez la case **Actif** .
3. Pour ajouter des champs de règle de risque aux critères du calculateur de risque, cliquez sur **Ajouter des critères**.
4. Dans la liste Choisir une table de référence, sélectionnez **Élément vulnérable de l'application**.
5. Dans la liste Champ, sélectionnez **Vulnerability.Severity**.
6. Dans le champ **Poids** , entrez l'importance relative de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Dans la section Définir la pondération des valeurs, ajoutez des valeurs de champ et attribuez-leur une pondération.



8. Cliquez sur **Envoyer**.

Information associée

Calculateurs Vulnerability Response et règles du calculateur de vulnérabilité

Créer un calculateur de vulnérabilité d'application

Un calculateur de vulnérabilité d'application est une formule prédéfinie permettant de calculer un champ cible lorsque certains critères sont remplis. Les calculateurs, qui calculent le **score de risque de l'élément** vulnérable de l'application (AVI), peuvent contenir des **règles de risque**. Les calculs de risque permettent de déterminer clairement les priorités du rattrapage.

Avant de commencer

Rôle requis : groupe de gestionnaires App-Sec

Remarque : Vous remarquerez peut-être une dégradation des performances lors de l'exécution de calculateurs de vulnérabilité d'application contenant des scripts.

Ordonnez à vos règles d'exécuter d'abord les règles les plus simples. Exécuter uniquement des scripts sur les éléments qui ne peuvent pas être gérés avec une condition et une valeur de modèle ou une règle de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Calculateurs de vulnérabilités**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Formulaire du calculateur de vulnérabilité

Champ	Description
Nom	Le nom du calculateur de vulnérabilité de l'application.
Table	Renseigné automatiquement avec le nom de la table AVI.
Application	Rempli automatiquement avec Réponse aux vulnérabilités.
Champ cible	Champ à calculer.
Description	Description textuelle du calculateur.
Actif	Allumez ou éteignez la calculatrice.

4. Cliquez avec le bouton droit de la souris dans l'en-tête pour **enregistrer**.
   La section **Règles du calculateur de vulnérabilité** s'affiche.
5. Créez une règle pour le calculateur en cliquant sur **Nouveau**.

> **Remarque :** Pour le formulaire **Nouvelles règles de risque** (disponible uniquement lorsque le **champ Cible** est **Score de risque**), consultez l'étape 10.

6. Renseignez les champs comme il convient.

Formulaire Règle du calculateur de vulnérabilité

Champ	Description
Nom	Nom de la règle du calculateur.
Ordre	Ordre dans lequel exécuter le calculateur de vulnérabilité. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Renseigné automatiquement avec le parent calculateur.
Actif	Par défaut, la case **Actif** est cochée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Vue avancée	Si cette option est sélectionnée, les conditions et valeurs scriptées peuvent être sélectionnées à partir du **type de condition** et du **type de valeur**.

7. Renseignez les champs de l'onglet **Quand cette condition est remplie** , le cas échéant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Quand cette condition est remplie

Champ	Description
Type de condition	Disponible lorsque vous sélectionnez la **vue avancée**. Les choix sont les suivants : ◦ Filtre : utilise des conditions de filtre. ◦ Groupe de filtres : voir Créer et définir des groupes de filtres pour définir les critères du calculateur. ◦ Script : condition de script utilisée pour déterminer quand appliquer ce calculateur. **Remarque :** Avant d'écrire des scripts pour déterminer quand appliquer les calculateurs, revenez à la liste **des calculateurs de vulnérabilité d'application** . Explorez les enregistrements du calculateur de vulnérabilité expédiés avec le système de base.
Condition	Définit les conditions de filtre de base pour déterminer s'il faut utiliser le calculateur ou non. La sélection du **groupe de filtres** ou des types de conditions de **script** masque ce champ.

8. Cliquez sur l'onglet **Définir ces valeurs** et renseignez les champs du formulaire comme il convient.

Définir l'onglet Définir ces champs

Champ	Description
Type de valeur	Disponible lorsque vous sélectionnez la **vue avancée**. Les choix sont les suivants : ◦ Modèle : définissez les valeurs à définir sur chaque champ. ◦ Script : utilisé pour définir les valeurs de chaque champ.
Valeurs de script	Disponible si vous avez sélectionné le type de valeur **Script** . Définit les valeurs auxquelles appliquer les calculs.
Modèle	Sélectionnez les champs et les valeurs que vous souhaitez utiliser pour le calculateur. La sélection du type **de** valeur de script masque ce champ.

9. Lorsque vous avez rempli toutes les entrées, cliquez sur **Soumettre**.

Remarque : Lorsque vous modifiez un calculateur existant et que vous souhaitez mettre à jour tous les scores existants, vous pouvez utiliser le bouton **Réappliquer le calculateur** . Il passe en revue tous les AVI actifs et, si ce calculateur est utilisé pour définir sa valeur, il recalcule la valeur de ces AVI. Étant donné que la réapplication d'une calculatrice peut prendre beaucoup de temps, une tâche planifiée s'en charge.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

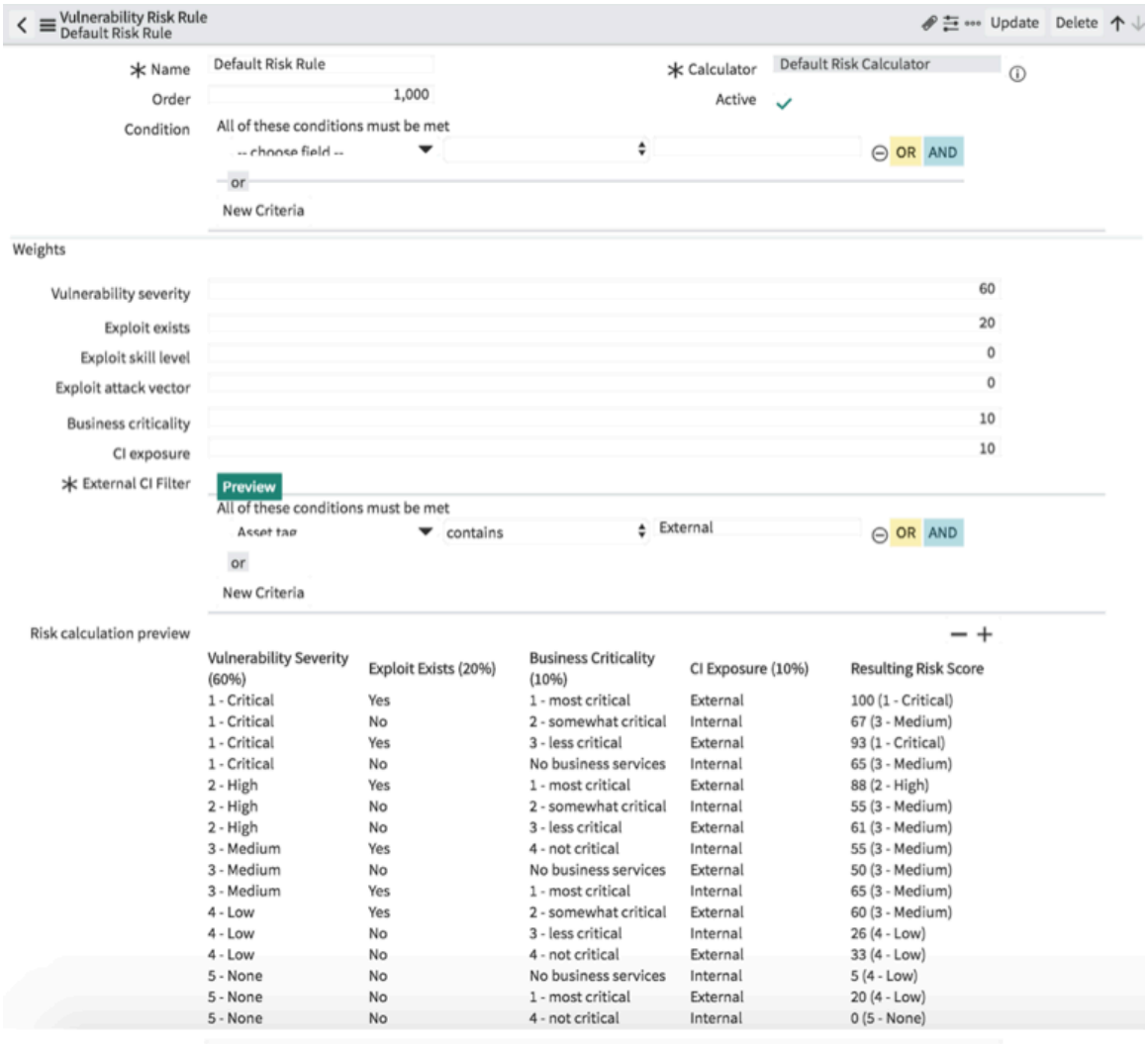
10. Pour le formulaire **Nouvelles règles de risque** , renseignez les champs comme il convient.

Définissez chaque poids en fonction du pourcentage du résultat qui doit provenir de cette valeur. Pour toutes les données que votre scanner ne fournit pas, ou pour les données qui ne doivent pas faire partie du score de risque, définissez le poids sur zéro.

Lorsque vous mettez à jour les pondérations, les scénarios affichent les pondérations restantes, ainsi que les résultats de **score de risque** anticipés.

Champ	Description
Nom	Nom de la règle du calculateur.
Ordre	Ordre dans lequel exécuter le calculateur. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Renseigné automatiquement avec le parent calculateur.
Actif	Par défaut, la case **Actif** est cochée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Condition	Définit les conditions de filtre de base pour déterminer s'il faut utiliser le calculateur. La sélection du **groupe de filtres** ou des types de conditions de **script** masque ce champ.
Pondérations	
Gravité de la vulnérabilité	Pourcentage du résultat qui provient de la gravité.
10 premiers OWASP	Pourcentage du résultat provenant de la présence de la vulnérabilité dans la liste des 10 premiers OWASP. Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.
SANS Top 25	Pourcentage du résultat provenant de la présence de la vulnérabilité dans la liste des 25 premiers SANS Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.
Exécution totale	Totaux des pourcentages calculés automatiquement. Lorsque cette valeur atteint 100, l'aperçu du scénario affiche des exemples de scores de risque dans différents scénarios.
Scénarios d'exemple	Lorsque tous les poids totalisent 100 %, les scénarios de score de risque s'affichent, fournissant un aperçu du score de risque dans certains des scénarios possibles.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



11. Cliquez sur **Envoyer**.

Mapper automatiquement la gravité d'un élément vulnérable de l'application

Réponse aux vulnérabilités des applications Le mappage de gravité transforme les champs de gravité sources tierces en champs reconnaissables dans Réponse aux vulnérabilités.

Avant de commencer

Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche

Réponse aux vulnérabilités des applications Intégrations tierces telles que Fournir Veracode Vulnerability Integration des mappages de gravité à l'installation. Ces cartes peuvent être ajustées en modifiant les champs des cartes existantes.

La création ou la modification d'une carte de gravité est uniquement destinée aux mappages tiers personnalisés ou non standard dans votre environnement et requiert Réponse aux vulnérabilités des applications une ServiceNow expertise.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Mappage de gravité normalisée**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Mappage de champs

Champ	Description
Source	Nom de la source pour le mappage de gravité.
Valeur de la source	Valeur de gravité de la source.
Valeur cible	La valeur de gravité cible. Les choix possibles sont les suivants : ◦ 1 - Critique ◦ 2 : élevé ◦ 3 : moyen ◦ 4 : faible ◦ 5 : aucun

4. Répétez l'étape 3 pour chaque niveau de gravité de la source.
5. Cliquez sur **Envoyer**.

Filtrage au sein de Gestion de la vulnérabilité des applications

Les calculateurs et les règles d'affectation utilisent des conditions pendant l'importation, créées à l'aide du **générateur de conditions**. Les changements apportés à leurs critères peuvent affecter les performances, car chaque enregistrement est évalué à l'aide de ces filtres.

Les règles et les calculateurs fournis avec le système de base sont optimisés en termes de performances. L'édition ou la création de règles ou de calculatrices prend soin et peut nécessiter à la fois ServiceNow une Réponse aux vulnérabilités des applications expertise. Cela dit, des conseils sont disponibles.

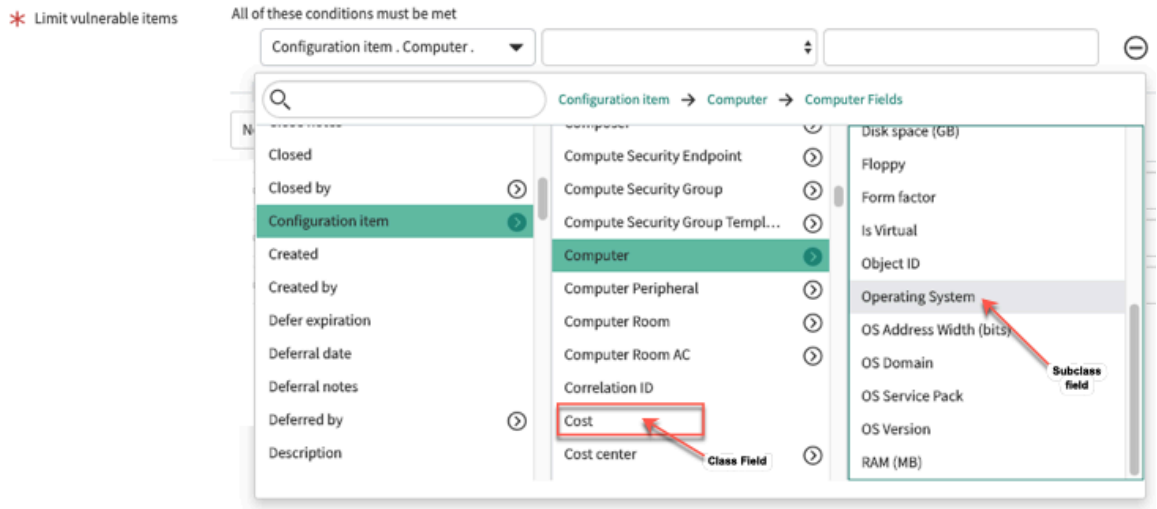
Éviter le filtrage basé sur les champs de sous-classe

Certaines tables prennent en charge l'extension. La table CI [cmdb_ci] CMDB en est un exemple. Les tables telles que cmdb_ci_hardware et cmdb_ci_computer étendent cette table. Si vous filtrez en fonction d'un champ qui n'est pas sur la table parente, ce filtre peut être coûteux à construire et à évaluer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Menu déroulant Filtre de condition



Par exemple, filtrer **ID d'élément de configuration** > **Coût** n'affecterait pas négativement les performances, car **Coût** est un champ de classe et non un champ de sous-classe de **l'élément de configuration**.



ID d'élément de configuration > **Ordinateur**, cependant, est une sous-classe nécessitant une remontée pas à pas vers un autre champ, en l'occurrence **Operating System**. Ce processus peut prendre plusieurs millisecondes, ce qui s'accumule rapidement, lorsque des millions d'éléments vulnérables sont importés, et affecte les performances.



Remarque : L'utilisation de la condition [contains] s'apparente à une recherche par caractères génériques et peut avoir un impact sur les performances. L'utilisation [est], dans la mesure du possible, est plus efficace.

Automatiser le suivi des cibles de rattrapage dans Réponse aux vulnérabilités des applications

Les règles de cibles de rattrapage de l'application définissent le délai attendu pour le rattrapage des éléments vulnérables de l'application (AVI), fournissant un délai pour le rattrapage de la vulnérabilité elle-même. Par exemple, si un élément vulnérable de l'application contient une cote de risque critique, la vulnérabilité de cet élément doit être corrigée dans les 15 jours.

Les gestionnaires App-Sec peuvent créer des règles de cible de rattrapage d'application en définissant :

- La cible de rattrapage.
- La cible de rappel.

Les gestionnaires App-Sec peuvent voir la date cible de rattrapage dans le formulaire AVI et les vues de listes, mais les dates ne sont pas mises à jour pour les AVI à l'état **Différé**, **Résolu** ou **Fermé** .

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

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les AVI qui n'ont pas atteint leur date de notification sont affichés en vert.
- Les AVI approchant de la date cible de rattrapage sont affichés en orange.
- Les AVI au-delà de la date cible de rattrapage sont affichés en rouge.

Règles par défaut

Réponse aux vulnérabilités des applications Livré avec trois règles par défaut qui sont inactives par défaut :

- Règle de cote de risque critique : une cible de rattrapage avec une cote de risque **critique de 1** , une cible de rattrapage de 15 jours et un rappel de **7** jours avant la date cible.
- Règle de cote de risque moyen à élevé : cible de rattrapage avec une cote de risque de **2 à Élevé** ou **3 à Moyen** , une cible de rattrapage de 30 jours et un rappel de **7** jours avant la date cible.
- Règle de cote de risque moins critique : une cible de rattrapage avec une cote **de risque 4-Faible** , une cible de rattrapage de 45 jours et un rappel de **7** jours avant la date cible.

Les règles de cibles de rattrapage peuvent être désactivées ou supprimées

Lorsqu'une règle est désactivée, les dates cibles de rattrapage actuelles pour les AVI auxquels elle a été appliquée sont effacées. Si un AVI satisfait à une règle active, cette règle est appliquée. Sinon, l'AVI n'a pas de règle ou de date cible, et son état est **Aucune cible**.

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

Scénario de la règle de rattrapage

Lorsque plusieurs règles de cible de rattrapage sont appliquées au même AVI, la règle la plus restrictive est appliquée.

Par exemple, si un AVI remplit la condition de deux règles de cible de rattrapage de l'application :

Scénario : AVI ouvert pour la dernière fois le 03/01/2018 à 10:00:00.

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

Dans ce scénario, la règle 2 de la cible de rattrapage de l'application s'applique à l'AVI, car elle contient la date la plus restrictive. 10 jours depuis que l'AVI a été identifiée pour la première fois contre 15 jours.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les cibles de rattrapage des applications sont calculées à partir de la **dernière date d'ouverture** additionnée au nombre de jours (mesurés par incréments de 24 heures). Vous pouvez ajouter ce champ au formulaire AVI à partir de la zone de sélection Mise en page du formulaire. Il s'agit de la date à laquelle l'AVI a été ouvert pour la dernière fois dans votre instance.

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

Remarque : Une fois la règle de cible de rattrapage de l'application définie, les dates de la cible de rattrapage sont calculées par la *Evaluate remediation targets* tâche planifiée ou par le bouton **Appliquer les changements** de la vue de liste Règles de cibles de rattrapage.

À propos de la tâche planifiée Évaluer les cibles de rattrapage

Evaluate remediation targets Fonctionne une fois à 4:00:00 tous les jours.

Evaluate remediation targets parcourt toutes les règles de vulnérabilité actives, en commençant par celles dont la date cible de rattrapage est la plus précoce. Il examine tous les AVI qui :

- ne sont pas dans un état **Fermé**, **Différé** ou **Résolu** .
- N'a pas de date cible de rattrapage.
- Avoir une date cible de rattrapage qui est postérieure à la date indiquée dans la règle de cible de rattrapage de l'application.

Evaluate remediation targets Ajoute une date cible de rattrapage, s'il n'en existe pas, ou si cette règle contient une date antérieure à celle de l'enregistrement, elle met à jour la date cible existante. Enfin, il met à jour les champs **Date cible de rattrapage** et État de **rattrapage** dans le formulaire AVI. Pour les règles inactives, **l'option Évaluer les cibles de rattrapage** efface les champs de rattrapage de l'AVI.

Réapplication des règles de cibles de rattrapage

Lorsque vous modifiez une règle de cible de rattrapage, utilisez le bouton **Appliquer les changements** de la page de liste Règles de cibles de rattrapage pour réexécuter toutes les règles modifiées sur tous les AVI ouverts actifs, à l'exception de ceux à l'état **Fermé**, **Différé** ou **Résolu** .

Remarque :

Si la tâche planifiée est en cours d'exécution *Evaluate remediation targets* , vous ne pouvez pas lancer un processus de nouvelle demande. Toutefois, si un processus de nouvelle demande est déjà en cours d'exécution et que la tâche planifiée est déclenchée, ils s'exécutent en parallèle.

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

Créer ou modifier des règles de cibles de rattrapage d'application

Pilotez le rattrapage des vulnérabilités à haut risque en temps opportun en configurant une règle de cible de rattrapage au niveau de l'élément vulnérable de l'application (AVI).

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le système de base est livré avec trois règles de cibles de rattrapage.

- Règle de cote de risque critique
- Règle de cote de risque moins critique
- Moyen - Élevé Règle d'évaluation des risques

Ces règles sont désactivées par défaut. Si vous choisissez d'en modifier un, plutôt que d'en créer un nouveau, n'oubliez pas de cocher la case**Actif** avant de l'enregistrer.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Administration** > **Règles de cibles de rattrapage**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom de la règle.
Cible (jours)	Spécifiez le nombre de jours pendant lesquels les AVI doivent être corrigés depuis leur dernière ouverture.
V17.1 : (date) à partir de la cible	Date à partir de laquelle les SLA cibles sont calculés. Vous pouvez spécifier uniquement les champs de date ou de type date et heure. La valeur par défaut est Date de dernière ouverture. Pour personnaliser les valeurs de ce champ, reportez-vous à KB1642413 .
Actif	Par défaut, la case **Actif** est sélectionnée, ce qui signifie que la règle de cible de rattrapage est active. Si cette case n'est pas cochée, cette règle ne s'applique pas aux nouveaux AVI créés dans le système.
Notifier (jours avant l'échéance)	Nombre de jours avant l'heure de rattrapage ciblée pour la définition d'un rappel. La date de notification calculée à l'aide de cette valeur est utilisée pour afficher l'état du rattrapage et le code couleur. Si la date est antérieure à la date de notification, l'état du rattrapage est « En cours ». S'il a dépassé la date de notification et avant la date cible de rattrapage, l'état s'affiche comme approchant de la cible. **Remarque :** Si ce champ est défini sur 0, seule une notification **Cible manquée** est définie.
La règle s'applique à	À l'aide du filtre de condition, sélectionnez les critères d'application de la règle aux AVI. Pour éviter tout impact sur les performances, testez vos conditions à l'échelle de la production. Les tests vous permettent de déterminer la durée d'exécution de la tâche **Évaluer les cibles de rattrapage** , compte tenu des conditions et de la taille de votre Base de données de gestion des configurations (CMDB)fichier .
Mettre à jour l'historique	
Activités	Non utilisé pour la création initiale d'une règle. Par la suite, les notes de travail du système sont enregistrées ici.

4. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette règle entre en vigueur lors de la prochaine exécution de la tâche planifiée, *Evaluate remediation targets*. Il en va de même lorsqu'une règle existante est mise à jour ou lors de l'utilisation du bouton **Appliquer les modifications** dans la vue de liste Règles de cibles de rattrapage. Il en va de même lorsqu'une règle existante est mise à jour. Pour plus d'informations sur la tâche planifiée et **l'application des modifications** , reportez-vous à la section Automatiser le suivi des cibles de rattrapage dans Réponse aux vulnérabilités des applications.

Afficher l'état de la cible de rattrapage d'un élément vulnérable de l'application

Lorsqu'un élément vulnérable de l'application (AVI) a presque atteint (ou dépassé) sa date cible de rattrapage, telle que définie par une règle de cible de rattrapage, l'enregistrement AVI est mis à jour avec un état. Ces informations peuvent vous aider à surveiller de manière proactive les activités de rattrapage à venir.

Avant de commencer
Rôle requis : groupe de gestionnaires App-Sec

Pourquoi et quand exécuter cette tâche
La tâche planifiée **Évaluer les cibles de rattrapage** s'exécute une fois par jour pour comparer la date actuelle à la date de rattrapage de l'élément vulnérable spécifiée dans la règle de cible de rattrapage associée. Lorsque la date actuelle tombe dans le nombre de jours avant que le rattrapage ne soit échu, un état de rattrapage est ajouté à l'enregistrement d'élément vulnérable.

Procédure

Accédez à la **Tout** > **Application Vulnerability Response** > **Éléments vulnérables**.
Si la date de rattrapage de l'AVI se situe dans la plage des conditions définies dans la règle de cible de rattrapage, vérifiez les colonnes État de la cible de rattrapage, visibles dans la vue de liste Éléments vulnérables. Si la date cible de rattrapage est passée pour un AVI, une annotation s'affiche sur le formulaire AVI.

Remarque : Pour afficher le nombre d'AVI qui **approchent** de la cible, **en cours**et**qui ont dépassé la cible**, consultez le tableau de bord Gestion de la vulnérabilité des applications [PA].

Information associée

Créer ou modifier des règles de cibles de rattrapage d'application

Fermer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage d'application peut être fermé immédiatement sans autre analyse, vous pouvez utiliser la fonctionnalité **Fermer** . À partir de la version 23.0 de , le bouton **Fermer** a été supprimé pour une tâche de rattrapage d'applicationRéponse aux vulnérabilités.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Dans les Réponse aux vulnérabilités espaces de travail, une tâche de rattrapage passe par les mêmes états qu'une tâche de rattrapage antérieure dans les versions précédentes de Réponse aux vulnérabilités. Lorsque tous les éléments vulnérables (VIT) d'une tâche de rattrapage sont fermés, la tâche de rattrapage passe à l'état Inactif.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Vous pouvez déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre dans leurs enregistrements respectifs sur leurs enregistrements respectifs lorsque la synchronisation d'état est activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement les tâches de rattrapage des états `Fermé` ou `Différé` .

Procédure

1. Ouvrez l'enregistrement pour lequel vous souhaitez demander une révision.
2. Cliquez sur le bouton **Fermer** .
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
État	Sélectionnez l'état Fermé.
Motif	Entrez le motif de la fermeture du problème.
Information supplémentaire	Saisissez toute autre information pertinente.

4. Sélectionnez **Soumettre**.
   La tâche de rattrapage est **marquée comme fermée**.

Test de pénétration

Les tests de pénétration dans Réponse aux vulnérabilités des applications permettent aux propriétaires d'applications d'évaluer la posture de sécurité de leur application. Il s'agit du test manuel d'une application par l'équipe de piratage éthique.

Rôles requis

Le test de pénétration nécessite les rôles suivants :

Gestionnaire de sécurité des applications : contient les gestionnaires de sécurité et les propriétaires d'applications qui gèrent les demandes d'évaluation des tests de pénétration. Il contient les rôles granulaires suivants :

- sn_vul.app_manage_pen_test_request
- sn_vul.app_lecture_tout
- cmdb_read

Hacker éthique : contient les membres de l'équipe de piratage éthique qui effectuent des tests de pénétration des applications. Il comprend les rôles granulaires suivants :

- sn_vul.app_update_assignment_group
- sn_vul.app_update_assigned_to
- sn_vul.app_manage_manual_avits
- sn_vul.app_manage_pen_test_request_config
- itil

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

- sn_vul.app_lecture_tout
- sn_vul.app_manage_pen_test_request
- sn_vul.app_update_state

Pour en savoir plus sur ces rôles, reportez-vous à Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs.

À partir de la version 19.0 de , si vous utilisez , Veracode Vulnerability Integrationles tests d'évaluation Réponse aux vulnérabilitésde pénétration dans le Veracode Vulnerability Integration sont des résultats manuels de Veracode. Elles ne sont pas liées aux demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour plus d'informations sur les évaluations des tests d'intrusion de Veracode, reportez-vous à la Veracode Vulnerability Integrationsection .

Cycle de vie des tests d'intrusion

En tant que propriétaire de l'application, vous pouvez demander à l'équipe de piratage éthique d'évaluer votre application par un test d'intrusion. L'équipe de piratage éthique agit sur cette demande et crée des résultats de test d'intrusion. Ces résultats sont des éléments vulnérables de l'application (AVI) créés manuellement.

Le workflow du test d'intrusion couvre le cycle de vie du test d'intrusion, de l'émission de la demande de test à la résolution des conclusions de l'équipe de piratage éthique.

Demande d'évaluation de test de pénétration

À partir de la version 19.0, vous pouvez créer de nouvelles demandes ou copier des demandes existantes à l'adresse suivante : **Tout** > **Demandes d'évaluation de test de pénétration** > **Tout**.

Avant la version 19.0, en tant que propriétaire de l'application, vous pouvez demander une évaluation de test de pénétration pour votre application à l'aide du catalogue de services ITSM.

Examen de la demande d'évaluation de test de pénétration

L'équipe de piratage éthique examine et évalue l'application et le périmètre de la demande d'évaluation du test d'intrusion, et l'ajoute au backlog existant.

Préparation d'un environnement

L'équipe de piratage éthique envoie ensuite une demande au propriétaire de l'application pour lui fournir un environnement pour commencer les tests. Une fois que l'environnement est prêt, le propriétaire de l'application informe l'équipe de piratage éthique.

Pour plus d'informations sur la configuration des demandes de test, reportez-vous à la section Configurer les tests de pénétration.

Test et communication des résultats du test de pénétration

L'équipe de piratage éthique teste l'application et communique les résultats au propriétaire de l'application. L'équipe de piratage éthique définit également les accords sur les niveaux de service (SLA) pour les résultats du test de pénétration à l'aide de la date cible de correction. Ces résultats sont les AVI créés manuellement. Le propriétaire de l'application examine à son tour les AVI créés par l'équipe de piratage éthique. Il planifie les correctifs et les affecte à l'équipe d'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les règles de cible de rattrapage ne s'appliquent pas aux résultats du test de pénétration.

L'équipe de piratage éthique peut créer une bibliothèque d'entrées de vulnérabilité d'application (AVE) et les réutiliser lors de la génération de rapports sur les AVI. Ils peuvent également suivre l'état des résultats du test d'intrusion.

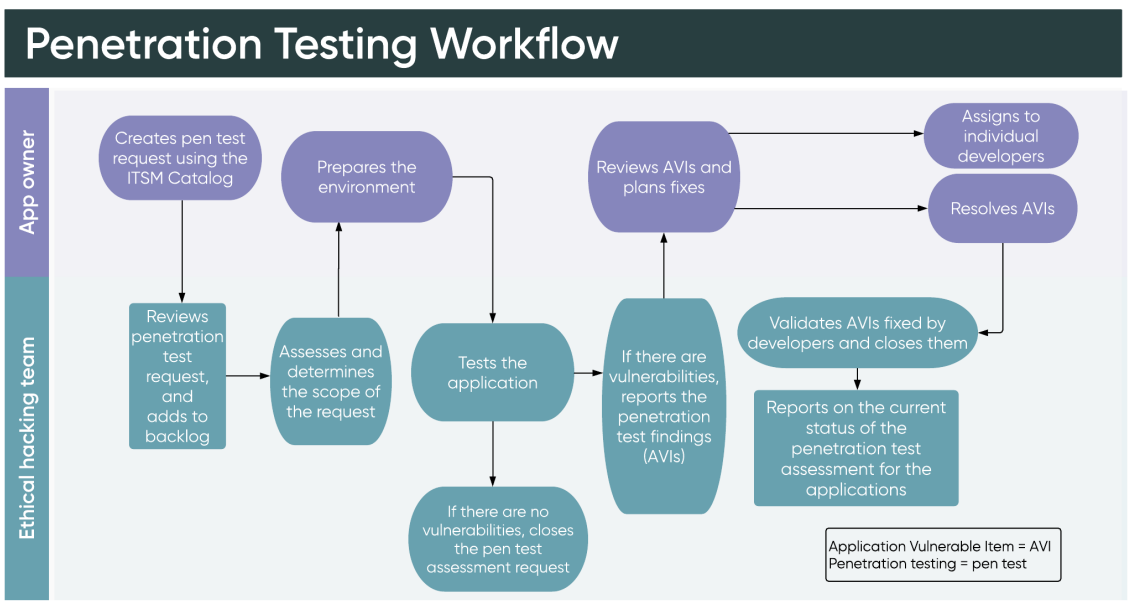
Correction et validation des conclusions du test de pénétration

Une fois que les résultats des tests d'intrusion sont corrigés et résolus par l'équipe d'application, les correctifs sont validés manuellement et fermés par l'équipe de piratage éthique.

Rapports Gestion de la vulnérabilité des applications

Utilisez les rapports disponibles sur le Gestion de la vulnérabilité des applications tableau de bord PA pour suivre les résultats du test de pénétration.

Cycle de vie du test de pénétration



Créer une demande d'évaluation de test de pénétration à partir de demandes existantes (v19.0)

À partir de la version 19.0, vous pouvez créer des demandes d'évaluation de test de pénétration directement à partir de la liste des demandes existantes. Vous pouvez également copier des demandes existantes à l'état Fermé sur cette liste pour créer des demandes.

Avant de commencer

Rôle requis : App-Sec Manager

Pourquoi et quand exécuter cette tâche

À partir de la version 19.0 de , si vous utilisez , Veracode Vulnerability Integrationles tests d'évaluation Réponse aux vulnérabilitésde pénétration dans le Veracode Vulnerability Integration sont des résultats manuels de Veracode. Elles ne sont pas liées aux demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour plus d'informations sur les évaluations des tests d'intrusion de Veracode, reportez-vous à la Veracode Vulnerability Integrationsection .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Demandes d'évaluation de test de pénétration** > **Tout**.
2. Facultatif : Vous pouvez également créer une demande en répliquant les demandes fermées.
   Toutes les valeurs de la demande d'origine sont conservées dans le nouveau formulaire. Les éléments vulnérables de l'application (AVI) actifs sont automatiquement copiés dans la nouvelle demande. Sélectionnez **Copier et créer une demande** à partir d'enregistrements à l'état Fermé.
3. Sélectionnez Nouveau et renseignez les champs.

Formulaire de demande d'évaluation de test de pénétration

Champ	Description
Numéro	Identificateur unique généré pour la demande d'évaluation de test de pénétration.
État	Sélectionnez une valeur en fonction de l'état de la demande.
Demandés par	Personne demandant l'évaluation de la demande.
Groupe d'affectation	Groupe sélectionné pour travailler sur les résultats du test de pénétration. Elles peuvent être ajoutées ou modifiées manuellement par un gestionnaire de sécurité des applications. Pour configurer les groupes, reportez-vous à la section Configurer les tests de pénétration.
Application	Sélectionnez une application à l'aide de l'option de recherche.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur les conclusions du test de pénétration. Elles peuvent être ajoutées ou modifiées manuellement par un gestionnaire de sécurité des applications.
Type d'application	Sélectionnez une option parmi : ◦ Service Web (connu sous le nom d'API avant la version 16.1) ◦ Application Web ◦ Client lourd ◦ Mobile (si vous sélectionnez **Mobile**, l'onglet Mobile s'affiche en bas du formulaire avec des champs supplémentaires)
Sprint	Affiche les sprints avec la bande passante disponible pour prendre en charge la

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	demande d'évaluation en fonction du champ Type d'évaluation sélectionné. Consultez Configurer les sprints pour les tests de pénétration et Configurer les types d'évaluation pour les tests de pénétration pour plus d'informations sur la modification de la capacité de sprint et du périmètre de test.
v19.0 : Taille de l'application	Sélectionnez la taille de l'application que vous souhaitez tester. ◦ Petit ◦ Moyen ◦ Grand ◦ Standard (sélectionnez cette option si vous n'êtes pas sûr de la taille) En savoir plus Configurer les tests de pénétration sur la modification de la capacité de sprint et du périmètre de test avec la taille et la capacité de sprint de l'application.
Créé	Date et heure de création de la demande.
Type d'évaluation	Sélectionner le type d'évaluation dans : ◦ Test de pénétration complet ◦ Test ciblé ◦ Retester Pour plus de détails sur les combinaisons de test et le périmètre du test, reportez-vous à la section Configurer les types d'évaluation pour les tests de pénétration.
Mis à jour	Date et heure de dernière mise à jour de la demande.
Date de la démo	Date à laquelle cette application peut être démontrée.
Déploiement du produit planifié le	Date planifiée pour le déploiement de cette application en production.
Version/mise en production de l'application planifiée pour le déploiement	Version de l'application planifiée pour un déploiement de production.
v19.0 : Application appartenant à un fournisseur tiers ou à un onglet de joint-venture Si vous sélectionnez Oui pour ce champ, l'onglet Informations sur le fournisseur/la société commune s'affiche. Renseignez les champs supplémentaires.	
Existe-t-il une clause qui nous permet d'effectuer un test de pénétration ?	Le terme « clause » peut faire référence à des normes de test qui incluent tous les accords qui existent entre deux ou plusieurs

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	parties que vous souhaitez ajouter. Si vous sélectionnez **Oui**, ajoutez la clause.
La clause citant l'autorisation d'effectuer des tests de pénétration	
Nom juridique complet et adresse du fournisseur	
Système de détection des intrusions	
Contact technique du fournisseur	
Les informations enregistrées ont-elles été examinées pour détecter toute activité malveillante ?	
Application hébergée par un autre fournisseur tiers ?	
Contact du fournisseur qui signera le test de pénétration	
Onglet Détails de l'application	
Objet de l'application	Description de la fonctionnalité de l'application.
Détails des piles de technologies	Pile technologique complète, du front-end au back-end, en passant par les bases de données et d'autres technologies clés.
S'agit-il d'une application tierce ?	Confirme si cette application appartient à un fournisseur tiers.
Types de listes de données sensibles accessibles à partir de l'application	Types de données sensibles accessibles à partir de l'application. Par exemple, les données PII, les données PHI et les données financières telles que les numéros de carte de crédit.
Type d'authentification	Spécifie si cette application utilise LDAP Authentication, sa propre authentification native ou d'autres formes d'authentification.
L'application a-t-elle un impact sur un programme de conformité ?	Spécifie si cette application a un impact sur des programmes de conformité tels que PCI.
Contacts de l'équipe d'application	Les membres de l'équipe d'application doivent être contactés par l'équipe de piratage éthique pour toute question.
Liste des programmes de conformité	
Interfaces ou applications tierces associées	
Adresse IP	
Nombre approximatif d'utilisateurs en production ?	
Existe-t-il un script automatisé ?	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
La version de production de cette application est-elle orientée vers l'extérieur ?	
v 19.0 : Impact sur l'entreprise	
Dommage financier	Sélectionnez-en un dans la liste.
Non-conformité	Sélectionnez-en un dans la liste.
Atteinte à la réputation	Sélectionnez-en un dans la liste.
Violation de la confidentialité	Sélectionnez-en un dans la liste.
Onglet Détails du test	
URL à tester	URL qui doivent être incluses dans les tests de pénétration.
URL à exclure	URL qui doivent être exclues des tests de pénétration.
Cette application a-t-elle été testée précédemment ?	Spécifie si cette application a déjà fait l'objet d'un test de pénétration.
Motif du nouveau test	Motif de demande de réévaluation du test de pénétration si l'application a été testée précédemment.
Quand l'application a-t-elle été testée ?	Délai pendant lequel l'application a fait l'objet d'un test de pénétration.
Détails du compte de test	Détails du compte de test qui peuvent être utilisés par l'équipe de piratage éthique pour les tests d'intrusion.
Rôles d'application	Rôles pris en charge par l'application pour ses utilisateurs.
Rôles les plus utilisés	Rôles les plus couramment utilisés dans l'application.
Onglet Commentaires supplémentaires	
Notes de travail	

Traduction automatique

4. Sélectionnez **Enregistrer** pour enregistrer vos modifications ou **Soumettre** pour lancer la demande.

Créer une demande d'évaluation de test de pénétration (avant la version 19.0)

Lancez une demande d'évaluation de test de pénétration pour vos applications Web ou API. Ces demandes sont soumises à l'équipe de piratage éthique, qui procède ensuite au test de ces applications et signale manuellement les résultats du test d'intrusion.

Avant de commencer

Rôle requis : App-Sec Manager

Pourquoi et quand exécuter cette tâche

Le propriétaire de l'application soumet une demande d'évaluation de test de pénétration pour analyser manuellement son application ou ses API. L'équipe de piratage éthique teste

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'application et crée manuellement les résultats du test d'intrusion. Ces résultats sont des éléments vulnérables de l'application (AVI) créés manuellement.

Le groupe d'affectation par défaut pour le résultat du test de pénétration est le groupe configuré dans le champ « Équipe d'application » de la demande d'évaluation du test de pénétration associée. Le type d'affectation du résultat du test de pénétration est Manuel. Les règles d'affectation ne peuvent pas remplacer l'affectation de ces conclusions de test de pénétration.

À partir de la version 19.0, vous pouvez créer des demandes d'évaluation de test de pénétration directement à partir de la table Demandes d'évaluation de test de pénétration [sn_vul_pen_test_assessment_request_list]. Consultez Créer une demande d'évaluation de test de pénétration à partir de demandes existantes (v19.0) pour plus d'informations.

Procédure

1. Avant la version 19.0, accédez à **Tout** > **Libre-service** > **Catalogue de services** > **Services** > **Demande d'évaluation de test de pénétration**.
2. Facultatif : Vous pouvez également créer une demande en répliquant les demandes fermées.
   Toutes les valeurs de la demande d'origine sont conservées. Les éléments vulnérables de l'application (AVI) actifs sont automatiquement copiés dans la nouvelle demande.
3. Renseignez les champs du formulaire.

Formulaire de demande d'évaluation de test de pénétration

Champ	Description
Numéro	Identificateur unique généré pour la demande d'évaluation de test de pénétration.
Demandés par	Personne demandant l'évaluation de la demande.
Demande d'évaluation parente	Demande d'évaluation de test de pénétration d'origine utilisée pour créer la demande enfant. Elle est créée à l'aide d'une demande d'évaluation fermée. Visible uniquement sur le formulaire de demande d'évaluation de l'enfant.
Application	Sélectionnez une application à l'aide de l'option de recherche.
Type d'application	Sélectionnez une option parmi : ◦ Service Web (connu sous le nom d'API avant la version 16.1) ◦ Application Web ◦ Client lourd ◦ Mobile (si vous sélectionnez Mobile, l'onglet Mobile s'affiche en bas du formulaire avec des champs supplémentaires)
v19.0 : Taille de l'application	Sélectionnez la taille de l'application que vous souhaitez tester.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Petit ◦ Moyen ◦ Grand ◦ Standard (sélectionnez cette option si vous n'êtes pas sûr de la taille)
Type d'évaluation	Sélectionner le type d'évaluation dans : ◦ Test de pénétration complet ◦ Test ciblé ◦ Retester Pour plus de détails, voir Configurer les types d'évaluation pour les tests de pénétration.
Objet de l'application	Description de la fonctionnalité de l'application.
Détails des piles de technologies	Pile technologique complète, du front-end au back-end, en passant par les bases de données et d'autres technologies clés.
S'agit-il d'une application tierce ?	Confirme si cette application appartient à un fournisseur tiers.
Types de listes de données sensibles accessibles à partir de l'application	Types de données sensibles accessibles à partir de l'application. Par exemple, les données PII, les données PHI et les données financières telles que les numéros de carte de crédit.
Type d'authentification	Spécifie si cette application utilise LDAP Authentication, sa propre authentification native ou d'autres formes d'authentification.
L'application a-t-elle un impact sur un programme de conformité ?	Spécifie si cette application a un impact sur des programmes de conformité tels que PCI.
Contacts de l'équipe d'application	Les membres de l'équipe d'application doivent être contactés par l'équipe de piratage éthique pour toute question.
Date de la démo	Date à laquelle cette application peut être démontrée.
Déploiement du produit planifié le	Date planifiée pour le déploiement de cette application en production.
Version/mise en production de l'application planifiée pour le déploiement	Version de l'application planifiée pour un déploiement de production.
v19.0 : application appartenant à un fournisseur tiers ou à une société commune	Si vous sélectionnez Oui pour ce champ, l'onglet Informations sur le fournisseur/ la société commune s'affiche avec des champs supplémentaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Le terme « clause » peut faire référence à des normes de test qui incluent tout accord existant entre deux ou plusieurs parties.
État	Sélectionnez une valeur en fonction de l'état de la demande.
Groupe d'affectation	Groupe sélectionné pour travailler sur les résultats du test de pénétration. Elles peuvent être ajoutées ou modifiées manuellement par un gestionnaire de sécurité des applications.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur les conclusions du test de pénétration. Elles peuvent être ajoutées ou modifiées manuellement par un gestionnaire de sécurité des applications.
Sprint	Affiche les sprints avec la bande passante disponible pour prendre en charge la demande d'évaluation en fonction du champ Type d'évaluation sélectionné.
Créé	Date et heure de création de la demande.
Date de démarrage du test	Date et heure auxquelles le test commence.
Mis à jour	Date et heure de dernière mise à jour de la demande.
Détails du test	
URL à tester	URL qui doivent être incluses dans les tests de pénétration.
URL à exclure	URL qui doivent être exclues des tests de pénétration.
Cette application a-t-elle été testée précédemment ?	Spécifie si cette application a déjà fait l'objet d'un test de pénétration.
Motif du nouveau test	Motif de demande de réévaluation du test de pénétration si l'application a été testée précédemment.
Quand l'application a-t-elle été testée ?	Délai pendant lequel l'application a été testée par pénétration.
Détails du compte de test	Détails du compte de test qui peuvent être utilisés par l'équipe de piratage éthique pour les tests d'intrusion.
Rôles d'application	Rôles pris en charge par l'application pour ses utilisateurs.
Rôles les plus utilisés	Rôles les plus couramment utilisés dans l'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Soumettre**.
   Une notification par e-mail est envoyée à l'équipe de piratage éthique indiquant que la demande a été créée pour l'application concernée.

Répliquer une demande de test de pénétration à l'état Fermé

Créez une demande d'évaluation de test de pénétration en répliquant une demande à l'état Fermé. Les éléments vulnérables de l'application (AVI) actifs sont copiés dans la nouvelle demande.

Avant de commencer
Rôle requis : Équipe d'application

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Demandes d'évaluation de test de pénétration** > **Tout**.
2. Sélectionnez une demande à l'état Fermé.
3. Sélectionnez **Copier et créer une demande**.
   Une nouvelle demande est créée et les AVI actifs sont copiés dans cette demande avec des données mises à jour. Pour afficher l'état d'origine des AVI à partir de la demande parente, accédez à l'onglet **Instantané des conclusions du test de pénétration** .

Créer des conclusions de test de pénétration en fonction des demandes d'évaluation (antérieures à la version 19.0)

Créez des conclusions de test de pénétration basées sur la demande d'évaluation de test de pénétration. Ces résultats sont des éléments de vulnérabilité de l'application (AVI) créés manuellement.

Avant de commencer
Rôle requis : Hacker éthique

Procédure

1. Accédez à la **Tout** > **Libre-service** > **Catalogue de services** > **Services** > **Demandes d'évaluation de test de pénétration**.
2. Pour créer un AVI pour une demande d'évaluation de test de pénétration, sélectionnez la demande pertinente.
3. Dans la section Éléments vulnérables de l'application, sélectionnez **Nouveau**.
4. Renseignez les champs du formulaire.

Formulaire Élément vulnérable de l'application (vue de test de pénétration)

Champ	Description
Numéro	Identificateur AVI généré automatiquement pour cet enregistrement.
Demande d'évaluation	Demande d'évaluation de test de pénétration à laquelle cet AVI est associé.
Vulnérabilité	Vulnérabilité sélectionnée dans la table Entrées de vulnérabilité à l'aide de l'option de recherche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Cote de risque	**Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour en savoir plus sur les évaluations des risques, reportez-vous à Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications. À partir de la version 16.1, par défaut, la valeur est la même que la gravité de la vulnérabilité.
Impacte un programme de conformité ?	Confirme s'il y a un impact sur un programme de conformité. Les choix sont Oui et Non.
Liste des programmes de conformité impactés	Ce champ s'affiche lorsque la valeur alors du champ « Impacte tout programme de conformité » est définie sur *Yes*. Répertorie les programmes de conformité concernés.
Publication/version fixe planifiée	Date limite à laquelle les conclusions du test de pénétration doivent être résolues.
État	La valeur par défaut est **Ouvert** lorsque l'AVI est créé. Pour plus d'informations sur la façon dont les États sont mappés, reportez-vous États des éléments vulnérables de l'application (AVI) à la section .
Groupe d'affectation	Groupe sélectionné pour travailler sur cet AVI. Elles peuvent être ajoutées ou modifiées manuellement par un gestionnaire de sécurité des applications.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cet AVI. Elles peuvent être ajoutées ou modifiées manuellement par un gestionnaire de sécurité des applications.
Cible de rattrapage	Date à laquelle les AVI doivent être corrigés, dès lors qu'ils ont été identifiés pour la première fois. Ce champ n'apparaît que lorsqu'il est applicable. Pour en savoir plus sur les cibles de rattrapage, reportez-vous à Automatiser le suivi des cibles de rattrapage dans Réponse aux vulnérabilités des applications.
Créé	Horodatage de la création de l'élément vulnérable de l'application (AVI).
Mis à jour	Horodatage de la mise à jour de l'élément vulnérable de l'application (AVI).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ouvert par	Utilisateur qui a créé ce résultat du test de pénétration.
Contact de l'équipe de sécurité	Point de contact au sein de l'équipe de piratage éthique.
Description brève	Brève explication du résultat du test de pénétration.
Détails	
Détails techniques	Détails techniques du résultat du test de pénétration.
Impact	Évaluation de l'impact du résultat du test de pénétration.
Étapes à reproduire	Documentez les étapes pour reproduire et examiner le résultat du test de pénétration.
Recommandation	Enregistrez les actions recommandées dans ce champ.
Notes	
Notes de travail	Ajoutez des notes pour communiquer des informations sur les transitions d'états et d'autres mises à jour de champs.
V16.1 : URL affectées	Plus d'informations relatives aux URL affectées.
V16.1 : Paramètres affectés	Plus d'informations relatives aux paramètres affectés.
V16.1 : Fonctionnalités affectées	Plus d'informations relatives aux fonctionnalités affectées.

5. Pour enregistrer le formulaire, sélectionnez **Soumettre**.

Créer une entrée de vulnérabilité de l'application

Créez une entrée de vulnérabilité d'application pour la vulnérabilité spécifiée pour le résultat du test de pénétration. Les vulnérabilités d'application sont des vulnérabilités sur les applications logicielles personnalisées.

Avant de commencer
Rôle requis : Hacker éthique

Pourquoi et quand exécuter cette tâche
Réponse aux vulnérabilités des applications Associe une vulnérabilité à une application pour créer le résultat du test de pénétration. Ces résultats sont des éléments vulnérables de l'application (AVI) créés manuellement. Vous pouvez réutiliser une entrée existante ou en créer une manuellement pour chaque vulnérabilité pendant le test d'intrusion.

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Bibliothèques** > **Tiers**.

2. Sur la page Entrées de vulnérabilité de l'application, sélectionnez **Nouveau**.

3. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire d'entrée de vulnérabilité de l'application (vue de test de pénétration)

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Sévérité	Degré normalisé de gravité de cette vulnérabilité. Des cartes de gravité sont fournies pour NVD et avec les intégrations tierces ServiceNow. Pour plus d'informations sur la création ou l'ajustement de cartes de gravité, reportez-vous à la section Mapper automatiquement la gravité d'un élément vulnérable de l'application.
CVE primaire	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux.
Nom de catégorie	Classification fournie par l'intégration tierce. Aide à l'affectation.
Détails des vulnérabilités	
Vecteur d'attaque	Vecteur d'attaque le plus vulnérable pour cette vulnérabilité.
Complexité de l'attaque	Mesure qui décrit les conditions indépendantes de la volonté de l'attaquant qui doivent exister pour exploiter la vulnérabilité.
Périmètre	Mesure permettant de mesurer la capacité d'une vulnérabilité logicielle à avoir un impact sur les ressources au-delà de ses moyens.
Intégrité	Mesure permettant de mesurer l'impact sur l'intégrité d'une vulnérabilité exploitée avec succès.
Vecteur CVSS	Cadre de travail ouvert pour capturer les caractéristiques et la gravité des vulnérabilités logicielles.
Privilèges requis	Niveau de privilèges qu'un attaquant doit posséder avant d'exploiter avec succès la vulnérabilité.
Interaction de l'utilisateur	Besoin d'interaction humaine pour exploiter avec succès une vulnérabilité.
Confidentialité	Impact sur la confidentialité des ressources d'informations en raison d'une vulnérabilité exploitée avec succès. Ces ressources sont gérées par un composant logiciel.
Graphique des disponibilités	Impact sur la disponibilité du composant impacté résultant d'une vulnérabilité exploitée avec succès.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Score de base CVSS	Représentation numérique (0-10) de la gravité d'une entrée de vulnérabilité de l'application.
Menace	Description de la menace provenant de cette vulnérabilité.
Description de l'atténuation	Description des étapes permettant d'atténuer la vulnérabilité.

4. Pour enregistrer le formulaire, sélectionnez **Soumettre**.

Remarque : Les AVE sont créés dans la table Entrée de vulnérabilité de l'application (sn_vul_app_vul_entry). La table Entrée de vulnérabilité de l'application est un enfant de la table Entrée de vulnérabilité (*sn_vul_entry*). Par conséquent, les AVE créés sont également ajoutés à la table Entrée de vulnérabilité.

Solutions Analyse de la plateforme et Reporting pour Réponse aux vulnérabilités des applications

Solutions Analyse de la plateforme et Reporting contiennent du contenu préemballé Platform Analytics à utiliser avec d'autres Now Platform produits. Cela Solution Analyse des performances et Reporting présente des mesures importantes pour analyser votre processus de gestion de la vulnérabilité des applications.

Vue d'ensemble

Le pack de contenu Analyse des performances pour Vulnerability Response est disponible sur le sous forme ServiceNow® Store d'abonnement distinct. L'application n'est pas automatiquement installée avec l'application Vulnerability Response. Le pack de contenu Application Vulnerability Response fait partie du pack de contenu Performance Analytics pour Vulnerability Response.

Pour plus d'informations sur l'installation, l'installation et la configuration de votre application Analyse des performances pour Vulnerability Response, consultez Installer et configurer l'application Analyse des performances pour Vulnerability Response [PA].

Termes clés

Analyse des performances (PA)

Solution qui crée des tableaux de bord de gestion, des rapports sur les indicateurs clés de performance et les mesures, et répond aux questions commerciales clés pour aider à améliorer la qualité et à réduire les coûts.

Élément vulnérable de l'application (AVI)

Une vulnérabilité d'application signalée par un scanner de vulnérabilité tiers qui est présente sur un élément de configuration (CI).

Indicateur PA

Définit une mesure de performance effectuée à intervalles réguliers d'une activité ou d'un comportement organisationnel, par exemple, 10 principales applications avec les éléments vulnérables les plus critiques de l'application.

Source de l'indicateur PA

Ensembles de données qui filtrent les enregistrements à partir d'une vue de table ou de base de données, par exemple, AVI actif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le tableau de bord Mes vulnérabilités d'application suit le volume, les performances et la progression des vulnérabilités d'application, de l'analyse/détection initiale à l'endiguement ou à la correction.
- Affichez les taux d'atteinte des objectifs de rattrapage et déterminez efficacement quels éléments vulnérables d'application (AVI) présentent le plus de risque pour votre organisation.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur Now Platform (admin) : installer et activer cette solution d'analyse et de génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Administrateur Analyse des performances (pa_admin) : passer en revue les indicateurs, les répartitions, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.

Les tableaux de bord suivants fournissent une vue graphique de l'activité AVI pour aider à déterminer les plans de rattrapage et la progression de l'état. Vous pouvez vous concentrer sur les KPI associés aux applications affectées critiques et aux vulnérabilités à haute visibilité.

- Le tableau de bord Gestion de la vulnérabilité des applications (PA) communique les KPI pour le risque et la prévalence de la vulnérabilité, les applications affectées, les tendances de rattrapage et la progression du rattrapage. La valeur par défaut pour les tendances est de trois mois, mais peut être changée en 7 jours, un mois, 3 mois, 6 mois, cumul annuel, 1 année ou Toutes.
- Le tableau de bord Mes vulnérabilités d'application suit le volume, les performances et la progression des vulnérabilités d'application, de l'analyse/détection initiale à l'endiguement ou à la correction.

> **Remarque :** Le tableau de bord Mes vulnérabilités des applications est un sous-ensemble du tableau de bord Vue d'ensemble et n'est disponible que lorsqu'un membre du groupe d'utilisateurs Champions de sécurité se connecte à une instance. Pour plus d'informations sur le tableau de bord Mes vulnérabilités d'applications, consultez Tableau de bord Mes vulnérabilités d'applications.

Gestion de la vulnérabilité des applications (PA) tableau de bord

Suivez le volume, les performances et la progression des vulnérabilités des applications, de l'analyse initiale et de la détection jusqu'au confinement ou à la correction.

Cas d'utilisation

Utilisateur	Utilisation du tableau de bord
Responsables des vulnérabilités	Grâce au Gestion de la vulnérabilité des applications tableau de bord, la gestion des vulnérabilités peut déterminer quels éléments vulnérables de l'application (AVI) présentent le plus de risques pour son organisation. Ces tableaux de bord fournissent une vue graphique de l'activité AVI pour les aider à déterminer les plans de rattrapage et la

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur	Utilisation du tableau de bord
	progression de l'état. Concentrez-vous sur les KPI associés aux applications affectées critiques et aux vulnérabilités à haute visibilité.

Rôles requis Now Platform , configuration et onglets de tableau de bord

Le tableau de bord Gestion de la vulnérabilité des applications (PA) est inclus dans le pack de contenu Performance Analytics pour Vulnerability Response. Le pack de contenu Analyse des performances pour Vulnerability Response n'est pas automatiquement installé avec l'application Réponse aux vulnérabilités . Il est disponible sur le sous forme d'abonnement ServiceNow® Store séparé.

Pour plus d'informations sur l'installation, l'installation et la configuration de votre application Analyse des performances pour Vulnerability Response, consultez Installer et configurer l'application Analyse des performances pour Vulnerability Response [PA].

Pour afficher le tableau de bord, en tant qu'utilisateur affecté à des groupes d'utilisateurs de champion de sécurité, de gestionnaire de sécurité des applications ou de développeurs, accédez à **Application Vulnerability Response** > **Vue d'ensemble**.

Remarque : Le tableau de bord Mes vulnérabilités des applications est un sous-ensemble du tableau de bord Vue d'ensemble et n'est disponible que lorsqu'un membre du groupe d'utilisateurs Champions de sécurité se connecte à une instance. Pour en savoir plus sur le tableau de bord Mes vulnérabilités d'applications, reportez-vous à la section Tableau de bord Mes vulnérabilités d'applications.

À partir de la version 19.0 de Réponse aux vulnérabilités des applications, ce tableau de bord peut également être consulté dans l'interface utilisateur de la nouvelle expérience. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône**Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités et Vue d'ensemble des tableaux de bord.

Le tableau de bord Vue d'ensemble communique les KPI concernant le risque et la prévalence de la vulnérabilité, les applications affectées, les tendances de rattrapage et l'avancement du rattrapage. La valeur par défaut pour les tendances est de trois mois, mais peut être changée en 7 jours, un mois, 3 mois, 6 mois, cumul annuel, 1 année ou Toutes.

Répartissez les données du Gestion de la vulnérabilité des applications tableau de bord par **type d'analyse**, **application** ou **unité business**. Chacun de ces choix dispose d'un filtre supplémentaire, **Sélectionner des éléments**, pour affiner vos sélections. À partir de la Réponse aux vulnérabilités des applications version 15.0, les applications d'entreprise et CI ont été ajoutées aux choix du filtre **Application** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

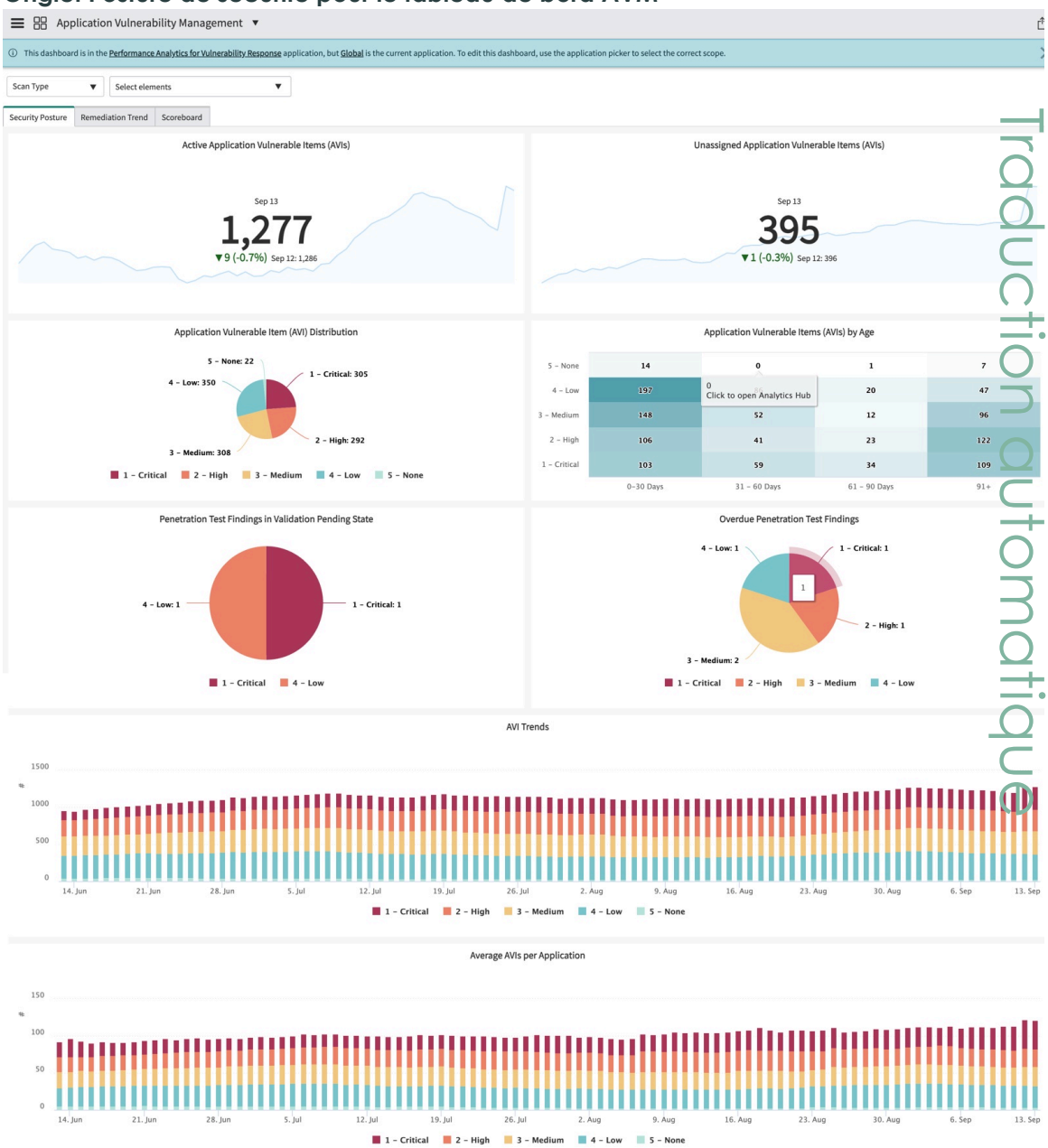
Onglet Posture de sécurité

L'onglet Posture de sécurité vous aide à comprendre votre posture de sécurité et la progression de vos actions de rattrapage.

À partir de la version 15.0, vous pouvez afficher les rapports de résultats des Réponse aux vulnérabilités des applications tests de pénétration. Les conclusions du test de pénétration sont des éléments vulnérables de l'application (AVI) qui sont créés manuellement en fonction des demandes d'évaluation du test de pénétration.

Remarque : Le type d'analyse pour ces widgets est Manuel.

Onglet Posture de sécurité pour le tableau de bord AVM

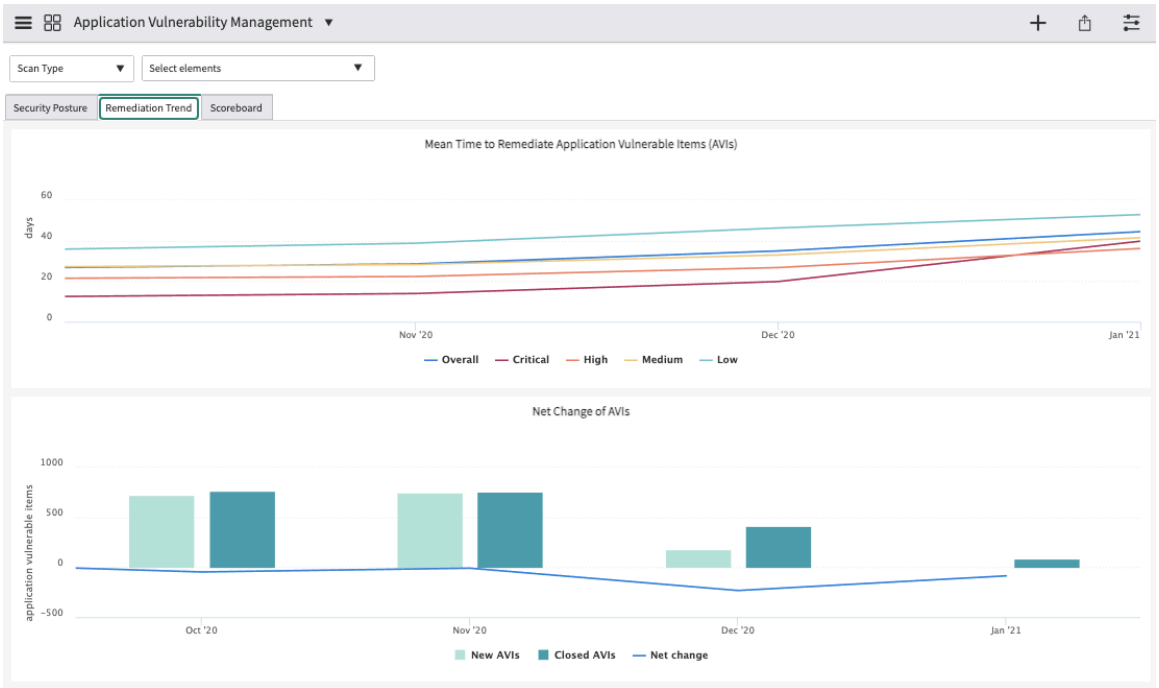


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Tendance de rattrapage

L'onglet Tendance de rattrapage vous aide à comprendre la progression de vos actions de rattrapage.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

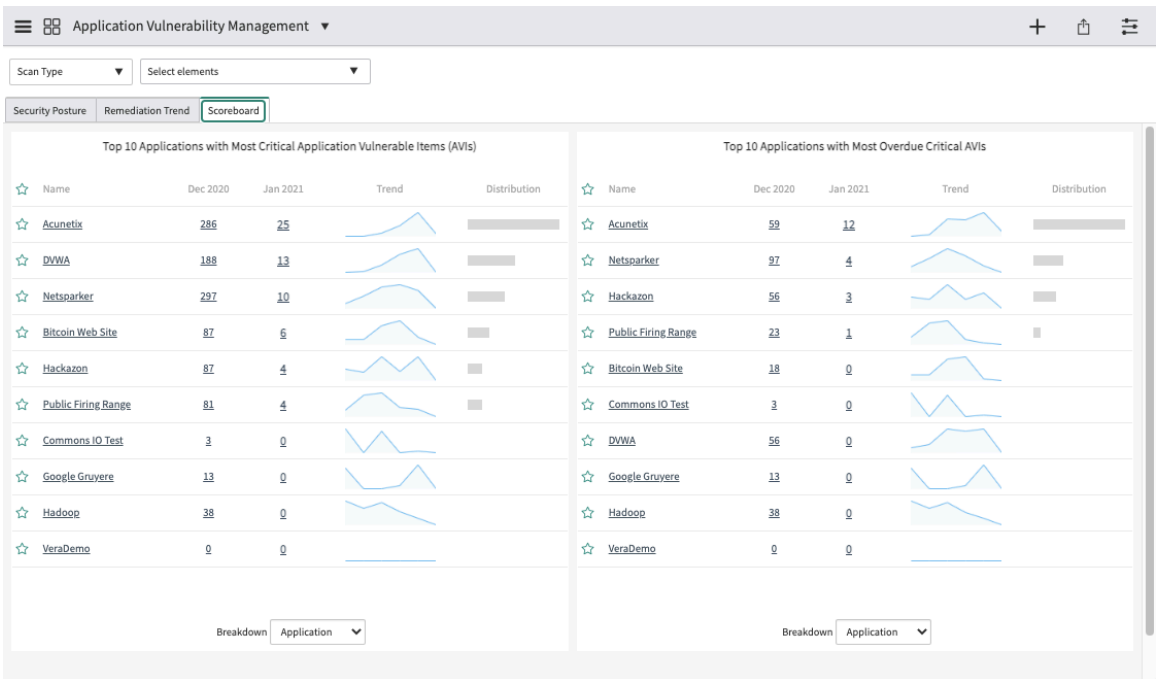
Onglet Tableau des scores

L'onglet Tableau de résultats vous aide à comprendre la progression de vos actions de rattrapage et quels AVI ont le plus besoin d'aide pour leur achèvement.

Éléments de type d'analyse :

- Dynamique : utiliser uniquement les mesures issues de l'importation dynamique de données
- Statique : utiliser uniquement les mesures issues de l'importation de données statiques

Vous pouvez choisir l'un ou l'autre, ou les deux.



Indicateurs

Délai moyen de remédiation des AVI bas

`[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 4 - faible]] / [[Éléments vulnérables de l'application fermée > cote de risque = 4 - faible]]`. L'objectif est de minimiser.

Versions de l'application

Il s'agit du décompte distinct sur les applications d'AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables de l'application

Il s'agit du décompte sur les éléments vulnérables de l'application AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Nombre moyen d'AVI par application

`[Éléments vulnérables de l'application actifs]] / [[Versions de l'application]]`. L'objectif est de minimiser.

VI non affectés

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il s'agit du décompte sur la source de l'indicateur AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Délai moyen de rattrapage des AVI

`[[Durée cumulée des éléments vulnérables de l'application fermée]] / [[Éléments vulnérables de l'application fermée]]`. L'objectif est de minimiser.

Délai moyen de remédiation des AVI élevés

`[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 2 - élevé]] / [[Éléments vulnérables de l'application fermée > cote de risque = 2 - élevé]]`. L'objectif est de minimiser.

Éléments vulnérables d'application clôturés

Il s'agit du décompte sur la source de l'indicateur AVI. Fermé, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de maximiser.

Délai moyen de rattrapage des AVI critiques

`[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 1 - critique]] / [[Éléments vulnérables de l'application fermée > cote de risque = 1 - critique]]`. L'objectif est de minimiser.

Nouveaux éléments vulnérables de l'application

Il s'agit du décompte sur la source de l'indicateur AVI. Nouveau, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Délai moyen de remédiation des AVI moyens

`[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 3 - moyen]] / [[Éléments vulnérables de l'application fermée > cote de risque = 3 - moyen]]`. L'objectif est de minimiser.

Changement net des éléments vulnérables

`[[Nouveaux éléments vulnérables de l'application]] - [[Éléments vulnérables de l'application fermés]]`. L'objectif est de minimiser.

Durée cumulée des éléments vulnérables de l'application fermés

Il s'agit du décompte sur la source de l'indicateur AVI. Fermé, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables d'application critiques en retard

Il s'agit du décompte sur la source de données AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables d'application critiques

Il s'agit du décompte sur la source de l'indicateur Applications avec AVI actifs, qui utilise la table suivante : sn_vul_analytics_app_ci_dept_bu. L'objectif est de minimiser.

Répartitions

- Âge
- Âge clôturé
- Application
- Unité business

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cote de risque
- Type d'analyse

Visualisations des données

Posture de Security

Nom	Type	Description
V15.0 : conclusions du test de pénétration en attente de validation	Graphique à secteurs	Conclusions du test de pénétration à l'état Résolu, mais avec validation en attente, regroupées par cote de risque.
V15.0 : conclusions du test de pénétration en retard	Graphique à secteurs	Conclusions du test de pénétration critiques qui ont manqué leur date cible de rattrapage, regroupées par cote de risque.
Éléments vulnérables de l'application (AVI) actifs	Score unique	Nombre d'éléments vulnérables de l'application (AVI) actifs (non fermés).
Éléments vulnérables de l'application (AVI) non affectés	Score unique	Nombre d'éléments vulnérables d'applications (AVI) actifs sans groupe d'affectation.
Distribution de l'élément vulnérable de l'application (AVI)	Graphique à secteurs	Distribution de tous les éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque.
Éléments vulnérables de l'application (AVI) par âge	Carte thermique	Nombre d'éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque et par âge (en jours).
Tendances AVI	tendance	Tendance des éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque.
Nombre moyen d'AVI par application	tendance	Tendance des éléments vulnérables de l'application (AVI) moyens par application, regroupés par cote de risque.

Tendance des rattrapages

Nom	Type	Description
Délai moyen de remédiation des éléments vulnérables d'application (AVI)	Ligne	Tendance du délai moyen de remédiation pour les éléments vulnérables de l'application (AVI) par cote de risque.
Changement net des AVI	tendance	Tendance des nouveaux éléments vulnérables de l'application (AVI) détectés par rapport à ceux fermés par mois.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau d'affichage

Nom	Type	Description
10 principales applications ayant les éléments vulnérables d'application (AVI) les plus critiques	Carte de score et barre de distribution 	Applications ayant le plus d'éléments vulnérables d'application (AVI) critiques.
10 principales applications ayant le plus d'éléments vulnérables d'application critiques (AVI) en retard	Carte de score et barre de distribution 	Applications ayant le plus grand nombre d'éléments vulnérables d'application (AVI) actifs dont la date cible de rattrapage est dépassée.

Tableau de bord Mes vulnérabilités d'applications

Ce tableau de bord présente des mesures importantes pour analyser votre processus de Gestion de la vulnérabilité des applications, telles que l'affichage des taux d'atteinte des objectifs de rattrapage.

Rôles requis Now Platform et affichage du tableau de bord

Remarque :

- Ce tableau de bord fait partie du pack de contenu Application Vulnerability Response. Le pack de contenu Application Vulnerability Response fait partie du pack de contenu Performance Analytics pour Vulnerability Response.
- Le pack de contenu Analyse des performances pour Vulnerability Response est disponible sur le sous forme ServiceNow® Store d'abonnement distinct.
- Le pack de contenu Analyse des performances pour Vulnerability Response n'est pas automatiquement installé avec l'application Vulnerability Response.

Le tableau de bord Mes vulnérabilités d'application n'est disponible que lorsqu'un membre du groupe d'utilisateurs Champions de sécurité se connecte à une instance. Pour en savoir plus sur le tableau de bord Vue d'ensemble, consultez Tableau de bord Gestion de la vulnérabilité des applications [PA].

Pour afficher le tableau de bord, accédez à **Application Vulnerability Response** > **Mes vulnérabilités d'applications**.

À partir de la version 19.0 de Réponse aux vulnérabilités des applications, ce tableau de bord peut également être consulté dans l'interface utilisateur de la nouvelle expérience. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône**Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités et Vue d'ensemble des tableaux de bord.

Affichez des rapports qui affichent des données de tendance au fil du temps. Consultez régulièrement les tendances des mesures importantes afin d'analyser l'ensemble de vos processus business et d'identifier les domaines d'amélioration.

Le tableau de bord Mes vulnérabilités des applications est inclus dans le pack de contenu Analyse des performances pour Vulnerability Response. Le pack de contenu Analyse

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

des performances pour Vulnerability Response n'est pas automatiquement installé avec l'application Réponse aux vulnérabilités . Il est disponible sur le sous forme d'abonnement ServiceNow® Store séparé.

Cas d'utilisation

Utilisateur	Utilisation du tableau de bord
Les spécialistes informatiques, les responsables du rattrapage ou les analystes qui corrigent les vulnérabilités qui leur sont affectées ou qui sont affectées à un groupe auquel ils appartiennent.	Un champion de sécurité utilise le tableau de bord Mes vulnérabilités d'application pour suivre le volume, les performances et la progression du rattrapage des vulnérabilités d'application. Déterminez efficacement quels éléments vulnérables de l'application (AVI) présentent le plus de risque pour votre organisation. Ces tableaux de bord fournissent une vue graphique de l'activité AVI pour aider à déterminer les plans de rattrapage et la progression de l'état. Vous pouvez vous concentrer sur les KPI associés aux applications affectées critiques et aux vulnérabilités à haute visibilité. Obtenez rapidement un aperçu de votre exposition aux vulnérabilités et de votre posture de sécurité. Effectuez un suivi depuis l'analyse et la détection initiales jusqu'au confinement ou à la correction.

Mes vulnérabilités d'applications [PA] Onglets de tableau de bord

Le tableau de bord Mes vulnérabilités des applications communique les KPI concernant le risque et la prévalence des vulnérabilités, les applications affectées, les tendances de rattrapage et les progrès du rattrapage. La valeur par défaut pour les tendances est de trois mois, mais peut être changée en 7 jours, un mois, 3 mois, 6 mois, cumul annuel, 1 année ou Toutes.

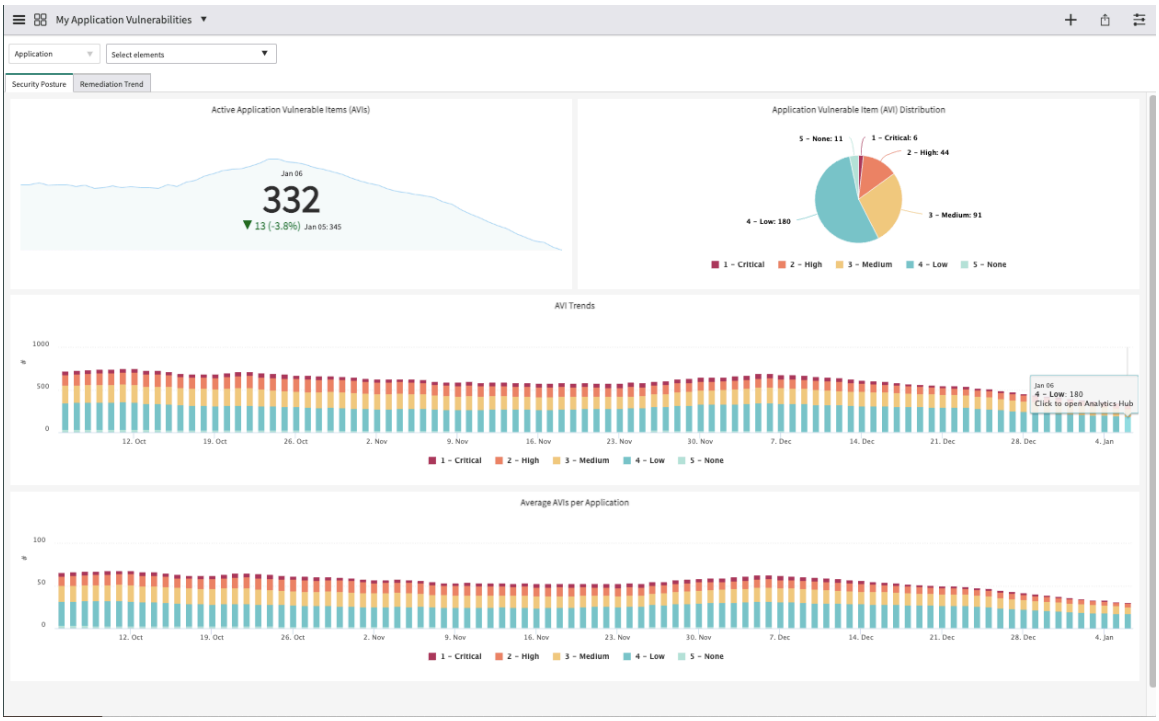
Les données sont ventilées dans le tableau de bord par **application**. Utilisez la liste **Sélectionner des éléments** pour affiner vos sélections.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

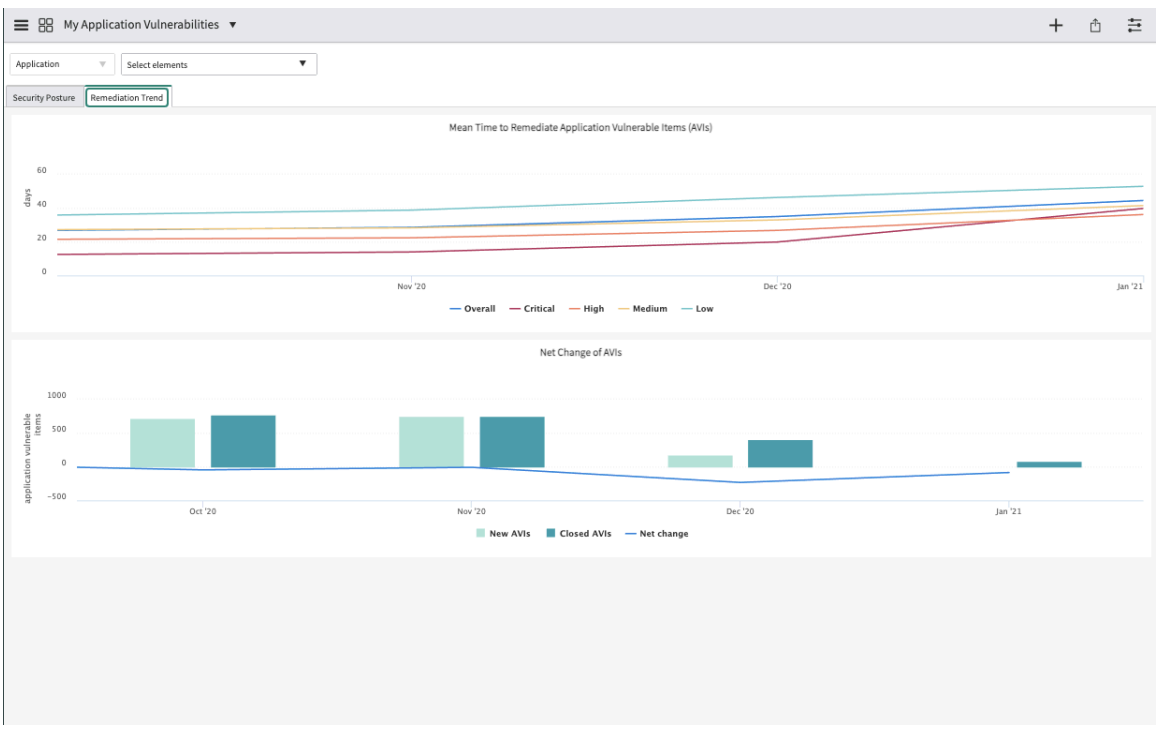
Onglet Posture de sécurité

L'onglet Posture de sécurité vous aide à comprendre votre posture de sécurité et la progression de vos actions de rattrapage. Répartissez les données du tableau de bord Gestion de la vulnérabilité des applications par **type d'analyse**, **application** ou **unité business**. Chacun de ces choix dispose d'un filtre supplémentaire, **Sélectionner des éléments**, pour affiner vos sélections.



Onglet Tendance de rattrapage

L'onglet Tendance de rattrapage vous aide à comprendre la progression de vos actions de rattrapage.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indicateurs

Délai moyen de remédiation des AVI bas

`[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 4 - faible]] / [[Éléments vulnérables de l'application fermée > cote de risque = 4 - faible]]`. L'objectif est de minimiser.

Versions de l'application

Il s'agit du décompte distinct sur les applications d'AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables de l'application

Il s'agit du décompte sur les éléments vulnérables de l'application AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Nombre moyen d'AVI par application

`[Éléments vulnérables de l'application actifs]] / [[Versions de l'application]]`. L'objectif est de minimiser.

VI non affectés

Il s'agit du décompte sur la source de l'indicateur AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Délai moyen de rattrapage des AVI

`[[Durée cumulée des éléments vulnérables de l'application fermée]] / [[Éléments vulnérables de l'application fermée]]`. L'objectif est de minimiser.

Délai moyen de remédiation des AVI élevés

`[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 2 - élevé]] / [[Éléments vulnérables de l'application fermée > cote de risque = 2 - élevé]]`. L'objectif est de minimiser.

Éléments vulnérables d'application clôturés

Il s'agit du décompte sur la source de l'indicateur AVI. Fermé, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de maximiser.

Délai moyen de rattrapage des AVI critiques

`[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 1 - critique]] / [[Éléments vulnérables de l'application fermée > cote de risque = 1 - critique]]`. L'objectif est de minimiser.

Nouveaux éléments vulnérables de l'application

Il s'agit du décompte sur la source de l'indicateur AVI. Nouveau, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Délai moyen de remédiation des AVI moyens

`[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 3 - moyen]] / [[Éléments vulnérables de l'application fermée > cote de risque = 3 - moyen]]`. L'objectif est de minimiser.

Changement net des éléments vulnérables

`[[Nouveaux éléments vulnérables de l'application]] - [[Éléments vulnérables de l'application fermés]]`. L'objectif est de minimiser.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Durée cumulée des éléments vulnérables de l'application fermés

Il s'agit du décompte sur la source de l'indicateur AVI. Fermé, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables d'application critiques en retard

Il s'agit du décompte sur la source de données AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables d'application critiques

Il s'agit du décompte sur la source de l'indicateur Applications avec AVI actifs, qui utilise la table suivante : sn_vul_analytics_app_ci_dept_bu. L'objectif est de minimiser.

Répartitions

- Âge
- Âge clôturé
- Application
- Unité business
- Cote de risque
- Type d'analyse

Visualisations des données

Posture de Security

Nom	Type	Description
Éléments vulnérables de l'application (AVI) actifs	Score unique	Nombre d'éléments vulnérables de l'application (AVI) actifs (non fermés).
Distribution de l'élément vulnérable de l'application (AVI)	Graphique à secteurs	Distribution de tous les éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque.
Tendances AVI	tendance	Tendance des éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque.
Nombre moyen d'AVI par application	tendance	Tendance des éléments vulnérables de l'application (AVI) moyens par application, regroupés par cote de risque.

Tendance des rattrapages

Nom	Type	Description
Délai moyen de remédiation des éléments vulnérables d'application (AVI)	Ligne	Tendance du délai moyen de remédiation pour les éléments vulnérables de l'application (AVI) par cote de risque.
Changement net des AVI	tendance	Tendance des nouveaux éléments vulnérables de l'application (AVI) détectés par rapport à ceux fermés par mois.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cadre de travail pour les rapports agrégés

À l'aide du cadre de travail des rapports agrégés, vous pouvez créer des rapports pour les données qui impliquent des requêtes à la volée complexes et de longue durée pour de meilleures performances.

Le cadre de travail des rapports agrégés améliore les performances en :

- en utilisant moins de ressources et en rendant les rapports plus rapidement,
- l'agrégation des données et la réutilisation des agrégations et des répartitions (Group By) et
- Réduction des requêtes à la base de données

Lorsque vous avez plus d'un million d'éléments vulnérables, utilisez le cadre de travail fourni dans Vulnerability Response Common en plus des rapports standard.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur Now Platform (admin) : installer et activer cette Solution Analyse des performances et Reporting, et apporter les modifications nécessaires aux propriétés système.
- Analyse des performances administrateur (pa_admin) : examinez les agrégations, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.
- Administrateur (sn_vul_cmn.admin) : créer des agrégations.
- VR write(sn_vul_cmn.write) : modifiez les données dans les agrégations et les résultats agrégés.
- Lecture VR (sn_vul_cmn.read) : examinez les données dans les agrégations et les résultats agrégés.
- Analyste de vulnérabilité (sn_vul.vulnerability_analyst) : examiner les résultats agrégés.

Information associée

Configurer une agrégation pour les données sources

Exécuter plusieurs agrégations simultanément

Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Créer un rapport à l'aide d'une agrégation

Configurer une agrégation pour les données sources

Pour analyser les performances d'une facette spécifique d'un processus business enregistré dans une ServiceNow table, créez une agrégation spécifique à la facette et créez un rapport pour cette agrégation.

Avant de commencer

Rôle requis : sn_vul_cmn.admin

Procédure

1. Accédez à la **Tout** > **Rapports agrégés** > **Définitions d'agrégations** > **Tout** et cliquez sur **Nouveau**.
2. Dans le champ **Nom** , donnez à l'agrégation un nom descriptif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans le champ **Description** , décrivez brièvement l'agrégation.
4. Renseignez les champs de l'onglet **Source** .

Champs de l'onglet source

Champ	Description
Table	Table à partir de laquelle vous souhaitez extraire les données pour le rapport. Cette liste déroulante contient uniquement les tables communes de sécurité des applications, app-vul, app-vulc, app-vul-container et de vulnérabilité des applications.
Fonction d'agrégat	Fonction à appliquer à la colonne sélectionnée dans **Champ**. ◦ **Nombre** : nombre d'enregistrements. ◦ **Somme** : somme totale des valeurs de la colonne sélectionnée dans **Champ**. ◦ **Moyenne** : moyenne de toutes les valeurs d'une colonne sélectionnée dans **Champ**. ◦ **Maximum** : valeur maximale dans la colonne sélectionnée dans **Champ**. ◦ **Minimum** : valeur minimale de la colonne sélectionnée dans **Champ**. ◦ **Nombre distinct** : valeurs uniques dans la colonne sélectionnée dans **Champ**.
Champ	Colonne sur laquelle vous souhaitez appliquer la fonction. **Remarque :** Ce champ n'apparaît pas lorsque vous sélectionnez **Nombre** dans le champ **Fonction d'agrégation** .

5. Dans l'onglet **Conditions supplémentaires** , fournissez la condition dans le champ **Conditions** pour sélectionner un ensemble particulier d'enregistrements pour lequel vous souhaitez obtenir les résultats agrégés.
6. Dans l'onglet **Grouper par** , sélectionnez les colonnes de la table selon lesquelles vous souhaitez regrouper ou empiler les données.
   Vous pouvez sélectionner jusqu'à deux répartitions.

   Si vous sélectionnez la colonne **de date** dans n'importe quel champ Grouper par, le champ **Tendance par** s'affiche. Vous pouvez obtenir les résultats d'agrégation classés par semaine, jour, minutes, etc. en sélectionnant les options dans le champ **Tendance par** .
7. Dans l'onglet **Calendrier** , sélectionnez ou créez un calendrier d'agrégation, qui définit la fréquence à laquelle vous pouvez exécuter l'agrégation pour extraire les données.
   Pour créer un calendrier d'agrégation, reportez-vous à Exécuter plusieurs agrégations simultanément.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous ne pouvez pas planifier l'exécution d'agrégation pour une définition d'agrégation inactive.

8. Cliquez sur **Envoyer** pour créer l'agrégation.
   L'agrégation apparaît dans la liste Agrégation. À la fréquence prédéfinie, l'agrégation est exécutée et un enregistrement est créé avec une date et une heure d'exécution dans la liste connexe Exécutions planifiées pour chaque exécution.
9. Accédez à la **Tout** > **Résultats agrégés** et ouvrez votre agrégation pour afficher les résultats agrégés et les exécutions planifiées.
   Les résultats agrégés sont répertoriés dans la liste connexe **Résultats agrégés** . En cas d'échec de l'exécution de l'agrégation, consultez la colonne **Notes** de la liste connexe **Exécutions planifiées** pour plus d'informations.
10. Facultatif : Sélectionnez **Exécuter maintenant** pour collecter les résultats de l'agrégation, quel que soit le calendrier d'agrégation.
    Si vous arrêtez l'exécution planifiée alors qu'elle est en cours, aucune modification n'est apportée aux résultats agrégés. Vous pouvez également supprimer ou désactiver une agrégation.

Que faire ensuite

Créez un rapport à l'aide de votre agrégation. Pour plus d'informations sur la création d'un rapport à l'aide d'une agrégation, reportez-vous à la section Créer un rapport à l'aide d'une agrégation.

Information associée

- Cadre de travail pour les rapports agrégés
- Exécuter plusieurs agrégations simultanément
- Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément
- Créer un rapport à l'aide d'une agrégation

Exécuter plusieurs agrégations simultanément

Vous pouvez planifier l'exécution de plusieurs agrégations à l'aide d'un seul calendrier d'agrégation.

Avant de commencer

Rôle requis : sn_vul_cmn.admin

Pourquoi et quand exécuter cette tâche

Supposons que vous souhaitiez exécuter six agrégations en même temps. Créez un calendrier d'agrégation et ajoutez-y toutes les agrégations. Ces agrégations sont exécutées à la fréquence et à l'heure définies.

Procédure

1. Accédez à la **Tout** > **Rapports agrégés** > **Calendrier**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Calendrier d'agrégation.

Champ	Description
Nom de calendrier	Nom du calendrier d'agrégation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Travail de planification	Exécution de script planifiée qui définit la fréquence à laquelle les agrégations doivent s'exécuter. Vous pouvez créer une tâche planifiée en cliquant sur le bouton **Nouveau** .

4. Sélectionnez **Soumettre**.
   Le calendrier d'agrégation apparaît dans la liste Calendrier d'agrégation.
5. Ouvrez votre calendrier d'agrégation.
6. Sélectionnez **Modifier**, ajoutez les agrégations à la **liste d'agrégation**, puis sélectionnez **Enregistrer**.
   Les agrégations sélectionnées apparaissent dans la liste connexe Agrégations.

   Remarque : Si vous ajoutez une agrégation inactive à un calendrier, l'exécution planifiée ne commencera pas.

7. Sélectionnez **Mettre à jour**.
   Ces agrégations sont exécutées à la fréquence définie dans le calendrier d'agrégation.

Information associée

- Cadre de travail pour les rapports agrégés
- Configurer une agrégation pour les données sources
- Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément
- Créer un rapport à l'aide d'une agrégation

Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Un nouveau processeur ou une tâche en arrière-plan, le processeur Agrégatd Reporting Framework, est fourni avec le système de base, qui exécute les travaux planifiés associés à la table Agrégatd Reports Framework. Cela permet à l'ensemble du sous-système de s'exécuter en arrière-plan et à une meilleure utilisation des ressources système lorsqu'elles sont disponibles.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Configuration de la tâche en arrière-plan – Calculateur de résultat d'agrégation commune de Vulnerability Response**.
2. Définissez le nombre d'agrégations que vous souhaitez exécuter simultanément dans le **champ Nombre maximal de threads simultanés** déposés et sélectionnez **Enregistrer**.
   Par défaut, quatre agrégations sont exécutées simultanément.
3. Accéder à la liste Pools de processeurs de tâches en arrière-plan, **sn_sec_cmn_background_job_processor_pool.list**et sélectionnez **Nouveau** pour créer un processeur de tâches en arrière-plan pour le cadre de travail des rapports agrégés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur la création d'un pool de processeurs de tâches en arrière-plan, consultez Traitement parallèle avancé pour les tâches en arrière-plan dans Vulnerability Response .

Remarque : Le nombre de processeurs de tâches en arrière-plan doit être égal au nombre maximal de threads simultanés fournis dans le formulaire Configuration de la **tâche en arrière-plan – Calculateur de résultats d'agrégation commune de Vulnerability Response** . Reportez-vous à l'étape 2.

Information associée

Cadre de travail pour les rapports agrégés

Configurer une agrégation pour les données sources

Exécuter plusieurs agrégations simultanément

Créer un rapport à l'aide d'une agrégation

Créer un rapport à l'aide d'une agrégation

Pour visualiser et analyser les données spécifiques à une agrégation que vous avez créée, générez un rapport en fournissant une condition pour l'agrégation dans le générateur de conditions.

Avant de commencer

Rôle requis : pa_admin

Procédure

1. Accédez à la **Tout** > **Rapports** > **Créer**.
2. Renseignez les champs de l'onglet **Données** .

Champs de l'onglet Données

Champ	Description
Nom du rapport	Le nom du rapport.
Type de source	Type de la source à partir de laquelle les données sont extraites. Sélectionnez **Table**.
Table	Nom de la table pour laquelle l'agrégation est créée. Sélectionnez la table des résultats agrégés, **Résultat agrégé [sn_vul_cmn_aggregate_result].**

3. Dans le générateur de conditions, définissez la condition de l'agrégation pour laquelle vous souhaitez générer un rapport.

Condition dans le générateur de conditions

Réf.	Description
Champ	Sélectionnez **Agrégation**.
Opérateur	Sélectionnez **est**.
Valeur	Nom de l'agrégation.

4. Dans l'onglet **Données** , cliquez sur **Suivant**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans l'onglet **Types** , sélectionnez la façon dont vous souhaitez visualiser les données et cliquez sur **Suivant**.
   Pour en savoir plus sur les types de rapports, reportez-vous à la section Création de rapports .

   Les visualisations prises en charge sont histogramme, graphique à secteurs et carte thermique. Vous pouvez modifier les graphiques linéaires et d'autres visualisations de tendances pour utiliser les visualisations prises en charge avec un résultat agrégé afin de représenter les mêmes données. La vue de liste n'est pas prise en charge.

6. Renseignez les champs de l'onglet **Configurer** .

Champ	Description
Grouper par	Sélectionnez **Groupé par 1** que vous avez sélectionné dans l'onglet **Grouper par** pour l'agrégation.
Empiler par	Sélectionnez **Groupé par 2** que vous avez sélectionné dans l'onglet **Grouper par** pour l'agrégation.
Agrégation	Appliquer **la fonction Minimum** ou **Maximum** à **la valeur**.

7. Dans l'onglet **Style** , renseignez les champs comme il convient et cliquez sur **Run (Exécuter)**.
   Pour plus d'informations sur les champs des onglets **Configurer** et **Style** , consultez la vidéo Création d'un rapport .
8. Dans le générateur de conditions, définissez la condition de l'agrégation pour laquelle vous souhaitez générer un rapport, puis cliquez sur **Exécuter**.

   Le rapport s'affiche.

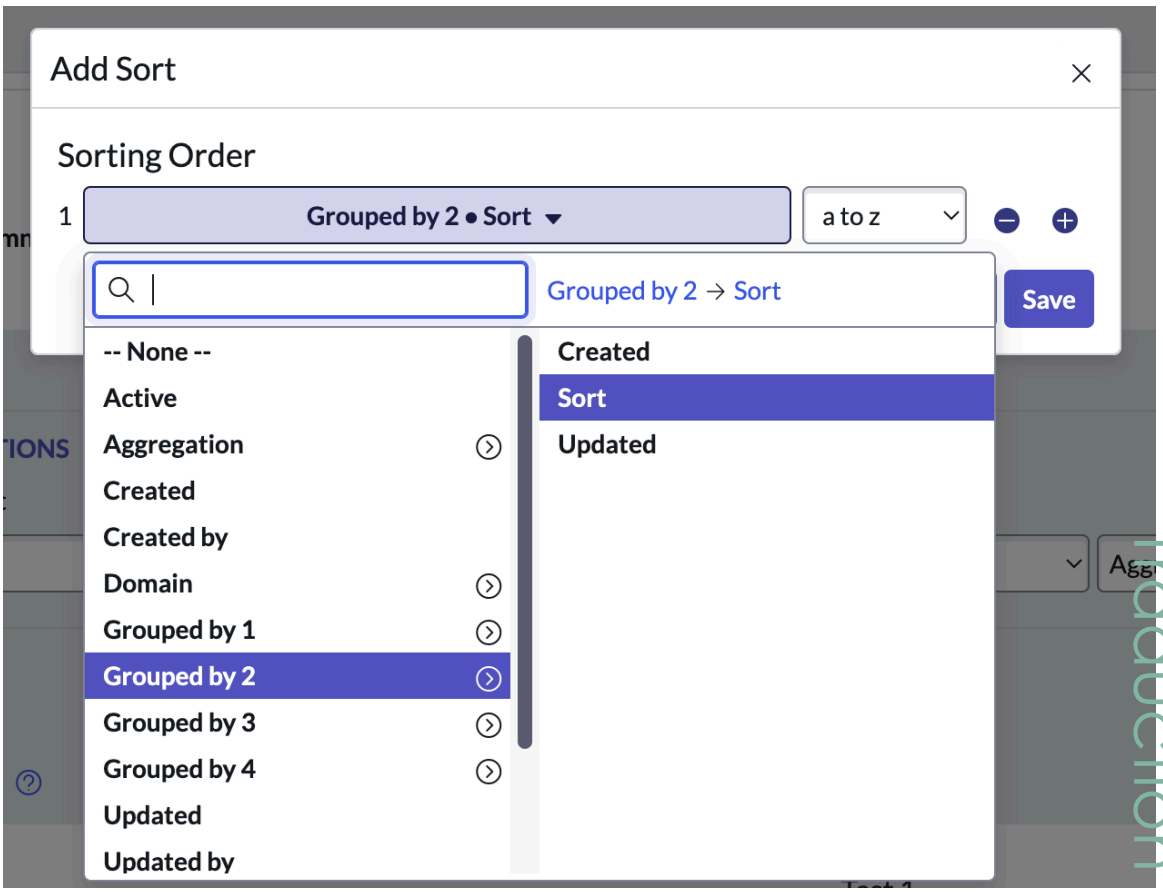
9. Pour trier les valeurs sur l'axe X, sélectionnez **Ajouter un tri**.

   a. Pour les chaînes, indiquez la condition **Groupée par > a-z ou z-a** pour trier les chaînes par ordre alphabétique.

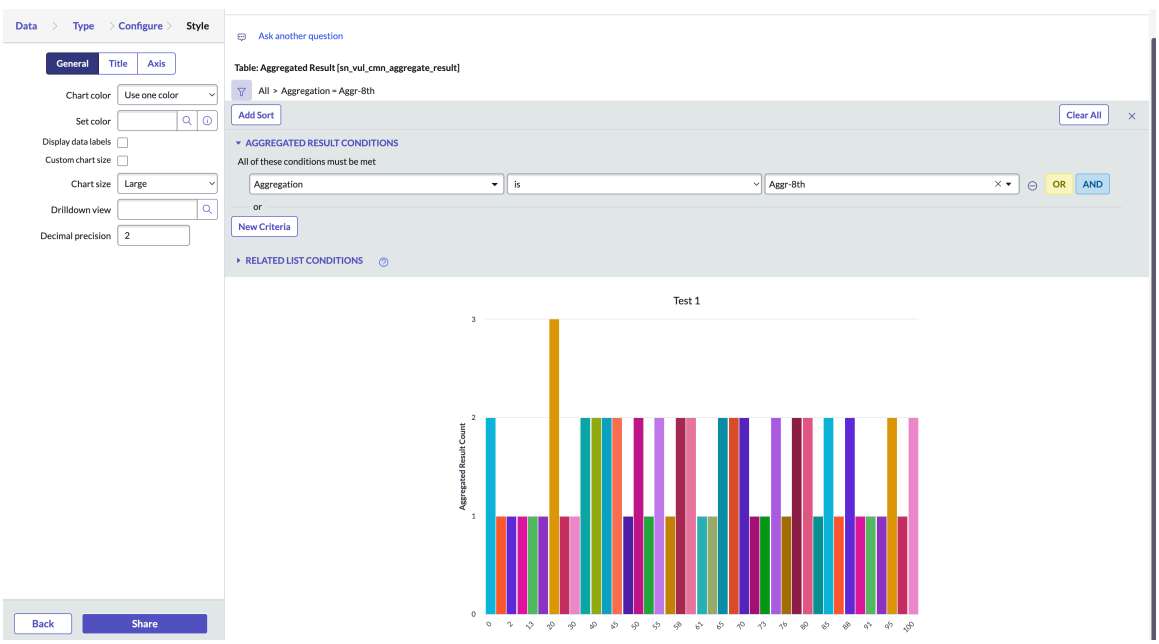
   b. Pour les valeurs de type de données Entier et Date, indiquez la condition sous la **forme Groupé par.trier > a-z ou z-a** pour trier les valeurs par ordre croissant et décroissant respectivement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tri des entiers sur l'axe des X



c. Sélectionnez **Exécuter**.
Les valeurs de nombre entier et de date sont triées sur l'axe X.



10. Cliquez sur **Enregistrer** pour enregistrer votre rapport.
Le rapport généré pour une agrégation s'affiche dans l'onglet **Résultats** du formulaire **d'agrégation** respectif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. Facultatif : Ajoutez votre rapport à un tableau de bord.
    Pour en savoir plus sur l'ajout d'un rapport à un tableau de bord, consultez Ajouter un rapport à un tableau de bord réactif .

    Le tableau **de bord Gestion de la vulnérabilité [agrégé],** composé de rapports créés à l'aide de l'infrastructure de génération de rapports mise en cache, est fourni avec le système de base. Pour afficher ce tableau de bord, accédez à **Tout** > **Analyse des performances** > **Tableaux de bord** > **Tout** > **Gestion de la vulnérabilité [agrégé]**. Les agrégations actives correspondant aux rapports de ce tableau de bord sont expédiées avec le système de base.

12. Partagez votre rapport avec d'autres utilisateurs.
    Pour plus d'informations sur le partage de rapports, voir Distribuer des rapports .

Information associée

Configurer une agrégation pour les données sources

Cadre de travail pour les rapports agrégés

Exécuter plusieurs agrégations simultanément

Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Références de Réponse aux vulnérabilités des applications

Rubriques de référence contenant des informations sur les tables, les rôles et les propriétés installés avec l'application Réponse aux vulnérabilités des applications .

Pour en savoir plus, consultez :

- Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs
- Composants installés avec Réponse aux vulnérabilités des applications
- États des éléments vulnérables de l'application (AVI)
- Champs d'application analysés
- Champs d'éléments vulnérables d'applications
- Champs de vulnérabilité de l'application
- États des tests de pénétration

Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs

Avant de pouvoir corriger avec succès les vulnérabilités avec Réponse aux vulnérabilités des applications (AVR), vous devez affecter des utilisateurs à des groupes d'utilisateurs.

Les rôles définissent ce que vous et vos groupes pouvez voir et faire dans Réponse aux vulnérabilités des applications, Analyse des performances pour Réponse aux vulnérabilités, et les intégrations tierces avec Réponse aux vulnérabilités des applications.

Groupes d'utilisateurs

Les groupes d'utilisateurs par défaut pris en charge Réponse aux vulnérabilités des applicationssont les suivants :

- App-Sec Manager : contient des gestionnaires de sécurité. À partir de la Réponse aux vulnérabilités des applications version 15.0, il contiendra également des propriétaires d'applications qui géreront les demandes d'évaluation de test de pénétration.
- Champion de sécurité : assure la liaison entre le groupe de développement et les responsables de la sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Développeur : contient des contributeurs individuels.
- V15.0 : Hacker éthique : contient les membres de l'équipe de piratage éthique qui effectuent des tests de pénétration des applications.

Le rôle d'administrateur système [admin] est requis pour affecter des utilisateurs aux groupes d'utilisateurs Réponse aux vulnérabilités des applications par défaut, à l'aide du module Administration des utilisateurs.

Remarque :

L'affectation d'utilisateurs AVR aux groupes d'utilisateurs n'est Réponse aux vulnérabilités des applicationsRéponse aux vulnérabilités des applications pas disponible dans la fonctionnalité Assistant de Réponse aux vulnérabilités configuration. Seuls les Réponse aux vulnérabilités rôles y sont affectés.

La table suivante répertorie les groupes d'utilisateurs disponibles Réponse aux vulnérabilités des applications et les rôles qui leur sont associés. Utilisez cette table pour déterminer quels utilisateurs doivent être affectés à quels groupes.

Groupe d'utilisateurs	Rôles dans ce groupe
Champion de la sécurité Les membres de ce groupe peuvent : • Lisez et écrivez les éléments vulnérables de l'application (AVI) qui vous sont affectés. • Affectez un AVI qui vous est affecté à une autre personne ou à un autre groupe. • V20.0 : Créer, mettre à jour, supprimer et annuler (désactiver) des règles d'exception.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_manage_auto_exception_rule
Gestionnaire de sécurité des applications Les membres de ce groupe peuvent : • V20.0 : Créer, mettre à jour, supprimer et annuler (désactiver) des règles d'exception. • Lecture, écriture, suppression et toutes les opérations sur les règles de tâche de rattrapage de l'application. • Lecture et écriture de tous les AVI. • Configurez AVR en créant et en gérant des règles, des calculateurs et des cartes de gravité. • Configurez les intégrations. • Supprimer les AVI. • Affectez AVI à des individus ou à des groupes. • Gérer les applications.	• sn_vul.app_manage_auto_exception_rule • sn_vul.app_manage_group_rules • sn_vul.app_lecture_tout • sn_vul.app_write_all • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_configure_integrations **Remarque :** Par défaut, ce rôle contient des rôles granulaires pour la configuration de l'intégration tierce. Pour définir ou modifier un groupe d'utilisateurs App-Sec Manager par des intégrations uniques ou spécifiques, reportez-vous à la section Réponse aux vulnérabilités Profils et rôles granulaires. • sn_vul.app_manage_assignment_rules

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupe d'utilisateurs	Rôles dans ce groupe
• Permet d'accéder au module d'application. • Planifiez, configurez, exécutez l'intégration. • Lire et exécuter les intégrations. • Affichez les tableaux de bord et les rapports AVR Analyse des performances . • V15.0 : Gérer les demandes d'évaluation de test de pénétration.	• sn_vul.app_manage_remediation_target_rules • sn_vul.app_manage_risk_score_configurations • sn_vul.app_manage_applications • sn_vul.app_manage_app_vul_permissions • sn_vul.app_manage_normalized_severity • Version 13.0 : sn_vul.app_manage_app_sc • Version 12.0 uniquement : sn_vul.app_read_application_release [Supprimé dans la version 12.1. Ne pas utiliser] • sn_sec_int.admin • Version 13.0 : pa_power_user • pa_viewer **Remarque :** À partir de la Réponse aux vulnérabilités version 13.0, pa_viewer est incluse dans pa_power_user et n'est plus nécessaire par elle-même. • V15.0 : sn_vul.app_manage_pen_test_request • V15.0 : sn_vul.app_update_state • V15.0 : cmdb_read
Développeur Les membres de ce groupe peuvent : • Lisez et écrivez les enregistrements AVR qui vous sont affectés. • Affectez un AVI qui vous est affecté à une autre personne ou à un autre groupe.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_pa_sc_view
V15.0 : Hacker éthique Les membres de ce groupe peuvent : • Configurez le groupe d'affectation et le délégataire par défaut pour les demandes d'évaluation de test de pénétration. • Gérez les résultats des tests de pénétration. • Gérer les demandes d'évaluation de test de pénétration.	• V15.0 : sn_vul.app_update_state • V15.0 : sn_vul.app_manage_pen_test_request • V15.0 : itil • V15.0 : sn_vul.app_read_all • V15.0 : sn_vul.app_manage_pen_test_request_config • V15.0 : sn_vul.app_manage_manual_avits

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupe d'utilisateurs	Rôles dans ce groupe
• Affichez les éléments vulnérables de l'application. • Mettre à jour l'affectation des éléments vulnérables de l'application.	• V15.0 : sn_vul.app_update_assigned_to • V15.0 : sn_vul.app_update_assignment_group

Affecter des utilisateurs à des groupes d'utilisateurs dans Réponse aux vulnérabilités des applications

Affectez des utilisateurs à des groupes à l'aide du module Administration utilisateurs de votre instance.

Avant de commencer

Rôle requis : administrateur

Procédure

Pour affecter ou supprimer un utilisateur d'un groupe :

a. Accédez à la **Administration** > **Groupes**.

b. Localisez et ouvrez le groupe approprié, par exemple, **App-Sec Manager**.
L'enregistrement du groupe s'affiche.

c. Sélectionnez l'onglet **Membres de groupe**.
Les membres actuels du groupe s'affichent.

d. Cliquez sur **Modifier**.
Le formulaire Modifier les membres s'affiche.

e. Dans la liste **Collection** , sélectionnez les utilisateurs à ajouter au groupe ou à supprimer.

f. Une fois que tous les utilisateurs ont été ajoutés à la **liste des membres du groupe** ou supprimés, cliquez sur **Enregistrer**.
Vous revenez à l'onglet **Membres du groupe** .

g. Cliquez sur **Mettre à jour** pour enregistrer vos changements et revenir à la liste Groupes.

Information associée

Composants installés avec Réponse aux vulnérabilités des applications

Composants installés avec Réponse aux vulnérabilités des applications

Plusieurs types de composants sont installés avec l'activation de la fonctionnalité, y compris les tables, les rôles d'utilisateur et les Réponse aux vulnérabilités des applications travaux planifiés.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles installés

Les rôles granulaires sont Réponse aux vulnérabilités des applications affectés par défaut à des groupes d'utilisateurs spécifiques.

Remarque : L'utilisation de rôles granulaires en dehors de ces groupes d'utilisateurs nécessite du codage et une expertise avancée Réponse aux vulnérabilités des applicationsServiceNow .

Titre du rôle [name]	Description	Contient des rôles
V20.0 : sn_vul.app_manage_auto_exception_rule	Créer, mettre à jour, supprimer et annuler (désactiver) des règles d'exception.	sn_vul.app_read_auto_
sn_vul.app_manage_group_rules	Lecture, écriture, suppression et toutes les opérations sur les règles de tâche de rattrapage de l'application.	• sn_vul.app_lecture_to • sn_vul.app_read_grou
V20.0 : sn_vul.app_exception_approver	Approuve les règles d'exception et les demandes d'extension des règles d'exception. À partir de la version 20.0, le rôle granulaire sn_vul.app_read_all a été supprimé pour ce rôle afin que vous puissiez accéder aux éléments vulnérables de l'application et aux tâches de rattrapage qui vous sont affectés, à vous et à votre groupe, au lieu de tous les éléments vulnérables de l'application et aux tâches de rattrapage.	sn_vul.app_read_auto_
sn_vul.app_read_assigned	Affichez les éléments vulnérables de l'application (AVI) qui vous sont affectés.	
sn_vul.app_lecture_tout	Afficher tous les AVI et informations connexes.	
sn_vul.app_write_assigned	Mettre à jour les AVI qui vous sont affectés.	
sn_vul.app_write_all	Mettre à jour tous les AVI et les informations connexes.	
sn_vul.app_update_assignment_group	Mettre à jour le groupe d'affectation AVI.	**Remarque :** Lorsq en dehors du group par défaut, sn_vul.c sn_vul.app_write_as

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
sn_vul.app_update_assigned_to	Mettre à jour le délégataire AVI.	**Remarque :** Lorsq en dehors du group par défaut, sn_vul.a sn_vul.app_write_as
sn_vul.app_configure_integrations	Configurez des intégrations tierces.	sn_vul.app_lecture_tout sn_vul.app_read_integra sn_sec_int.admin sn_vul_veracode.config sn_vul.configure_nvd_a **Remarque :** Pour modifier un groupe App-Sec Manager intégrations unique reportez-vous à la s aux vulnérabilités Pr granulaires.
sn_vul.app_read_integrations	Affichez toutes les intégrations tierces.	
sn_vul_veracode.configure_integration	Définir, mettre à jour et supprimer les intégrations Veracode.	
sn_vul.app_manage_assignment_rules	Définissez, mettez à jour et supprimez des règles d'affectation AVI.	sn_vul.app_lecture_tout sn_vul.app_read_assign
sn_vul.app_read_assignment_rules	Affichez les règles d'affectation.	
sn_vul.app_manage_remediation_target_rules	Définissez, mettez à jour et supprimez des règles de cibles de rattrapage AVI.	sn_vul.app_lecture_tout sn_vul.app_read_remed
sn_vul.app_manage_risk_score_configurations	Définir, mettre à jour et supprimer les calculateurs AVR et les règles de risque.	sn_vul.app_lecture_tout sn_vul.app_read_risk_sc sn_sec_cmn.calc.write
sn_vul.app_read_risk_score_configuration	Affichez les calculateurs AVR et les règles de risque.	
sn_vul.app_manage_applications	Affichez, mettez à jour et supprimez des enregistrements d'application.	
sn_vul.app_manage_app_sc	Donne à un champion de sécurité la possibilité de s'ajouter	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	ou de se supprimer de la liste connexe Application analysée.	
sn_vul.app_pa_sc_view	Fournit une vue pertinente au champion de sécurité spécifique.	
sn_vul.app_manage_app_vul_permissions	[interne] Utilisé par sn_vul.app_manage_applications.	
sn_vul.app_manage_normalized_severity	Mettez à jour le mappage sur la gravité normalisée.	sn_vul.app_read_norma
sn_vul.app_read_normalized_severity [Supprimé dans la version 12.1. Ne pas utiliser.]	Affichez les enregistrements de gravité normalisée.	
sn_vul.app_read_application_release	Affichez les enregistrements de version de l'application.	
sn_sec_int.admin	Permet d'accéder aux intégrations.	
pa_power_user	Permet d'accéder aux rapports	pa_viewer
sn_vul.app_sec_manager	Priorise et gère les éléments vulnérables de l'application.	
sn_vul.app_developer	Développeur responsable de la correction des vulnérabilités de l'application.	
sn_vul.app_create_watch_topic	Créez des rubriques de visualisation pour les vulnérabilités d'applications.	
sn_vul.app_read_watch_topic	Lisez les rubriques de surveillance pour les vulnérabilités d'applications.	
sn_vul.app_edit_watch_topic	Modifiez les rubriques de surveillance pour les vulnérabilités d'applications.	
sn_vul_blackduck.configure_integration	Configurez des intégrations tierces.	sn_vul_blackduck.confi

Traduction automatique

Travaux planifiés installés

Pour Réponse aux vulnérabilités les travaux planifiés partagés, Composants installés avec Réponse aux vulnérabilitésreportez-vous à .

Tâche planifiée	Description
Associer les AVI existants à la règle d'exception automatique	Évalue les éléments vulnérables de l'application pour vérifier s'ils correspondent aux règles d'exception.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Renseigner l'entrée et le M2M CVE	Rend les enregistrements existants cohérents avec plusieurs enregistrements CWE. Exécuter une fois après la mise à niveau pour remplir, puis désactiver.
Resynchroniser le CWE primaire	Pour des calculs CWE primaires personnalisés. Exécuter une fois après la mise à niveau pour resynchroniser, puis désactiver.
Déployer les valeurs d'éléments vulnérables d'applications vers la vulnérabilité et le groupe	Calcule les vulnérabilités et les déploiements de groupes pour les éléments vulnérables de l'application. **Remarque :** À partir de la version 23.0 de Réponse aux vulnérabilités des applications, la tâche planifiée est améliorée pour créer des tâches en arrière-plan avec des options de multithreading. Cette mise à niveau implique de segmenter la tâche en plusieurs tâches enfants plus petites, qui sont exécutées en parallèle ou simultanément. Cette modification permet de traiter plusieurs enregistrements simultanément, ce qui accélère considérablement la tâche globale.
Intégration de la liste des projets Black Duck	Extrait et ingère les données dans la table des projets Black Duck.
Intégration de la liste des applications Black Duck	Importe les applications dans la table des applications détectées pour toutes les versions de projet disponibles avec l'intégration de Black Duck dans la table des projets.
Intégration d'élément vulnérable d'application Black Duck	Ingère les éléments vulnérables dans l'application ServiceNow en fonction des vulnérabilités détectées par les analyseurs pour chaque application détectée dans le système.

Tables installées

Table	Description
Version de l'application [sn_vul_app_release]	Contient des informations sur la version de l'application.
Version 13.0 : Champions de sécurité des applications [sn_vul_app_m2m_app_sc]	Contient les enregistrements du Réponse aux vulnérabilités des applications groupe de champions de sécurité.
Entrée de vulnérabilité de l'application [sn_vul_app_vul_entry]	Contient des entrées de vulnérabilité d'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Intégration de vulnérabilité de l'application [sn_vul_app_integration]	Contient des Réponse aux vulnérabilités des applications enregistrements d'intégration.
Emplacement de numérisation de vulnérabilité de l'application [sn_vul_app_vul_scan_location]	Contient des informations d'emplacement d'analyse tierce.
Synthèse de numérisation de vulnérabilité de l'application [sn_vul_app_vul_scan_summary]	Contient des informations récapitulatives d'analyse de tiers.
Élément vulnérable de l'application [sn_vul_app_vulnerable_item]	Contient des enregistrements AVI. À partir de la version 19.0, les colonnes suivantes sont ajoutées pour la nomenclature logicielle : • sn_sbm_config_rule • sn_sbom_component • vex_justification • vex_detail • vex_response • vex_state • sca_type (SBOM-SCA)
Application numérisée [sn_vul_app_scanned_application]	Contient des informations sur l'application.
Mappage d'états [sn_vul_app_state_map]	Contient le mappage d'état des intégrations tierces aux états d'élément vulnérable de l'application (AVI).
CWE de vulnérabilité [sn_vul_m2m_entry_cwe]	Relie les données CVE aux entrées vulnérables de l'application.
Manifeste de tâche de rattrapage d'application sn_vul_app_rt_manifest	Toutes les mises à jour de la tâche de rattrapage sont effectuées à l'aide de cette table de manifestes par travaux planifiés.
Tâche de rattrapage d'application sn_vul_app_vulnerability	Contient des tâches de rattrapage d'applications.
Élément de tâche de rattrapage d'application sn_vul_app_m2m_vul_group_item	Table M2M entre les tâches AVI et de remédiation d'application.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Édition 21.0 : Éléments vulnérables de l'application sn_vul_app_vulnerable_item	Contient des enregistrements AVI.
Édition 21.0 : Package [sn_vul_app_package]	Contient les détails du package d'application.
Édition 21.0 : Licences sn_vul_app_license	Contient des licences d'application.
Édition 21.0 : Tâches de remédiation d'applications sn_vul_app_vulnerability	Contient des tâches de rattrapage d'applications.
sn_vul_blackduck_config	Contient les détails de configuration de l'intégration Black Duck.
sn_vul_blackduck_project	Contient des détails sur les projets de Black Duck.
sn_vul_blackduck_project_import	Table de jeu d'importation pour l'ingestion du projet Black Duck.
sn_vul_blackduck_app_import	Table de jeux d'importation pour l'ingestion d'application Black Duck.
sn_vul_blackduck_avit_import	Table de jeu d'importation pour l'ingestion AVIT de Canard noir.

États des éléments vulnérables de l'application (AVI)

Réponse aux vulnérabilités des applications offre un modèle d'état pour l'état des éléments vulnérables de votre application (AVI), à tout moment. Savoir comment chaque état est lié et s'affecte les uns les autres vous aide à déterminer quand et comment corriger vos AVI.

États des éléments vulnérables de l'application

Comprendre le fonctionnement des états facilite la création ou la modification de règles relatives aux éléments vulnérables de l'application (AVI). Les AVI ont plusieurs états possibles qui sont mappés à partir de l'état de rattrapage importé à partir de l'intégration tierce. Dans un AVI, le champ **État** est en lecture seule.

Réponse aux vulnérabilités des applications Diagramme de flux d'états

État	Description
Ouvrir	État à la création. À partir de cet état, vous pouvez :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Diagramme de flux d'états (suite)

État	Description
	V16 : Obtenir plus de détails Obtenez les informations suivantes sur un AVI importé de Fortify : • Résumé de la vulnérabilité • Explication de vulnérabilité • Recommandation • Références • Demande • Réponse V16 : marquer comme faux positif Marquez un élément comme faux positif si le scanner signale qu'une vulnérabilité existe dans le système, mais qu'en réalité il n'y a pas de vulnérabilité. V16 : Demande d'exception Demandez une exception, une date de réouverture (jusqu'à), un motif et, éventuellement, fournissez des informations supplémentaires. Reporter le rattrapage de l'élément jusqu'à la date jusqu'à laquelle une exception est demandée. V15 : Fermer Sélectionnez l'état Fermé, un motif dans la boîte de dialogue Fermer l'élément vulnérable et fournissez des informations supplémentaires. Ferme l'AVI. V15 : résoudre Marquez un AVI ouvert comme résolu pour le faire passer à l'état résolu. Vous devez ajouter des notes de résolution dans la boîte de dialogue Résoudre l'élément vulnérable de l'application.
Différé	**V15 :** Ceci est déclenché par l'option **Demande d'exception** . Dans le cadre du workflow d'approbation, l'état Différé est en cours de révision et ne peut pas être fermé tant qu'il n'a pas été approuvé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Diagramme de flux d'états (suite)

État	Description
	À partir de cet état, vous pouvez : V16 : Obtenir plus de détails Obtenez les informations suivantes sur un AVI importé de Fortify : • Résumé de la vulnérabilité • Explication de vulnérabilité • Recommandation • Références • Demande • Réponse Rouvrir Fait passer un AVI fermé ou résolu à l'état Ouvert. Fermer Sélectionnez l'état Fermé, un motif et fournissez des informations supplémentaires. Ferme l'AVI.
En cours d'examen	Sélectionnez cette option dans la liste **État** . À partir de cet état, vous pouvez : V20.0 Transitionnez manuellement une tâche de rattrapage ou un enregistrement AVI vers **l'état En attente d'implémentation**. V16 : Obtenir plus de détails Obtenez les informations suivantes sur un AVI importé de Fortify : • Résumé de la vulnérabilité • Explication de vulnérabilité • Recommandation • Références • Demande • Réponse V16 : marquer comme faux positif Marquez un élément comme faux positif si le scanner signale qu'une vulnérabilité existe dans

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Diagramme de flux d'états (suite)

État	Description
	le système, mais qu'en réalité il n'y a pas de vulnérabilité. V16 : Demande d'exception Demandez une exception, une date de réouverture (jusqu'à), un motif et, éventuellement, fournissez des informations supplémentaires. Reporter le rattrapage de l'élément jusqu'à la date jusqu'à laquelle une exception est demandée. V15 : Fermer Sélectionnez l'état Fermé, un motif dans la boîte de dialogue Fermer l'élément vulnérable et fournissez des informations supplémentaires. Ferme l'AVI. V15 : résoudre Marquez un AVI ouvert comme résolu pour le faire passer à l'état résolu. Vous devez ajouter des notes de résolution dans la boîte de dialogue Résoudre l'élément vulnérable de l'application.
En attente d'implémentation	Vous pouvez uniquement faire passer manuellement les enregistrements à cet état en sélectionnant En attente d'implémentation à partir d'AVI et les enregistrements de tâche de rattrapage à l'état En cours d'examen. À partir de cet état, vous pouvez : Ouvrir Fait passer AVI à nouveau à l'état Ouvert. En cours d'examen Obtenez plus d'informations sur la résolution. Transitionne vers En cours d'examen. Résoudre Marquez un AVI ouvert comme résolu pour le faire passer à l'état résolu. Vous devez ajouter des notes de résolution dans la boîte de dialogue Résoudre l'élément vulnérable de l'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Diagramme de flux d'états (suite)

État	Description
	Fermer Sélectionnez l'état Fermé, un motif dans la boîte de dialogue Fermer l'élément vulnérable et fournissez des informations supplémentaires. Ferme l'AVI. Dans cet état, faites passer un enregistrement en En attente d'implémentation lorsque vos recherches et votre travail sur une tâche sont terminés et bien qu'un correctif soit prêt pour l'implémentation, il n'est pas encore disponible. Définissez les champs **Date de l'engagement de rattrapage** et **Plan de rattrapage** . Après l'implémentation, vous résolvez ou fermez les enregistrements.
Résolu	Déclenché à partir du bouton Résoudre. À partir de cet état, vous pouvez : V16 : Obtenir plus de détails Obtenez les informations suivantes sur un AVI importé de Fortify : • Résumé de la vulnérabilité • Explication de vulnérabilité • Recommandation • Références • Demande • Réponse Rouvrir Effectue une transition vers un état **Ouvert** . Fermer Sélectionnez l'état **Fermé** , un motif et fournissez des informations supplémentaires. Ferme le groupe. Les notes et les informations sur la résolution s'affichent sous l'onglet **Notes** .
Fermé	Déclenché à partir du bouton Fermer. À partir de cet état, vous pouvez :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Diagramme de flux d'états (suite)

État	Description
	Rouvrir : revient à l'état Ouvert.

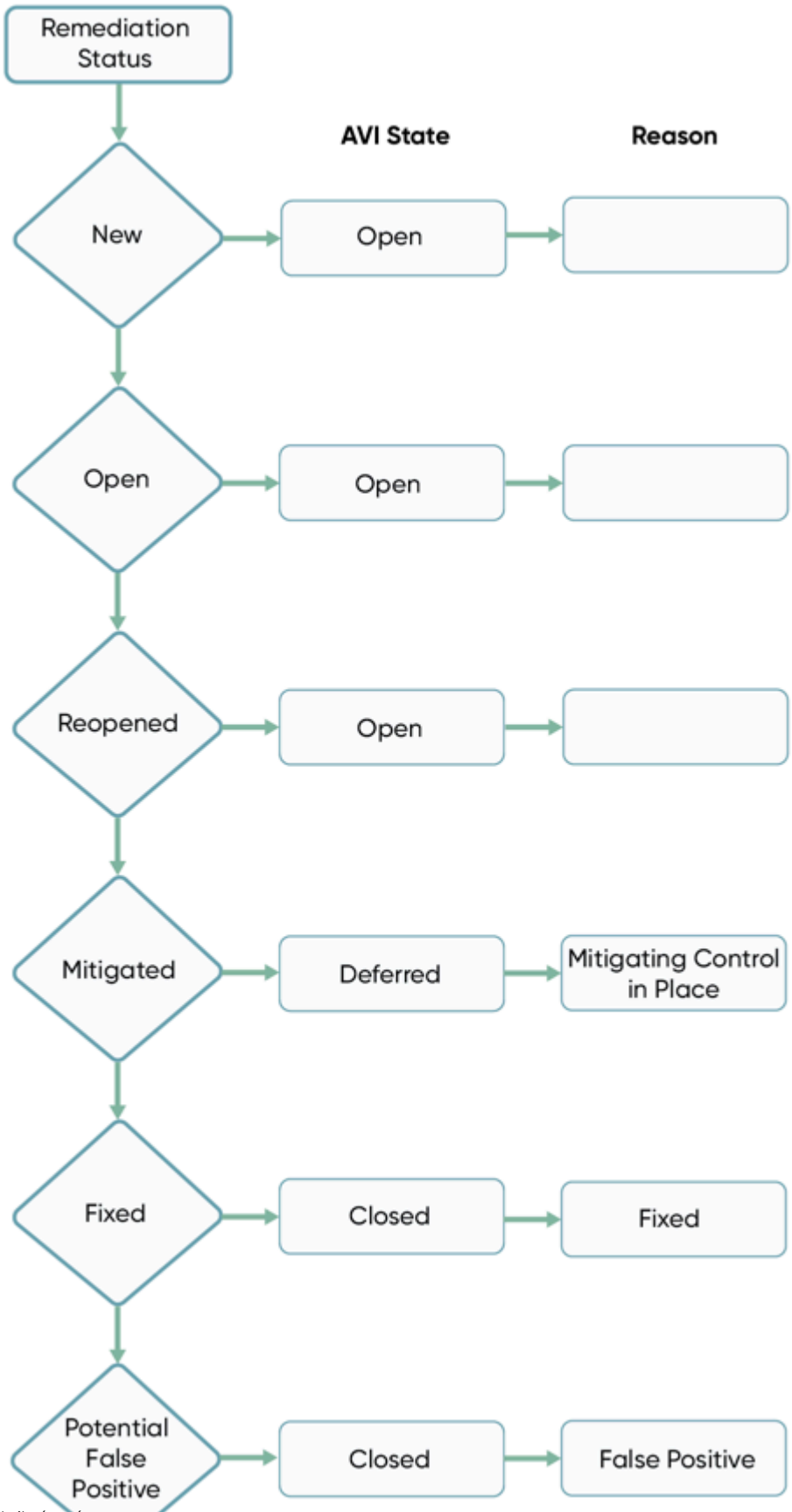
Le mappage des états par intégration est affiché comme suit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de l'état pour Veracode

Remarque : Ce mappage d'état s'applique uniquement lorsque l'option de triage entrant ServiceNow n'est pas sélectionnée.

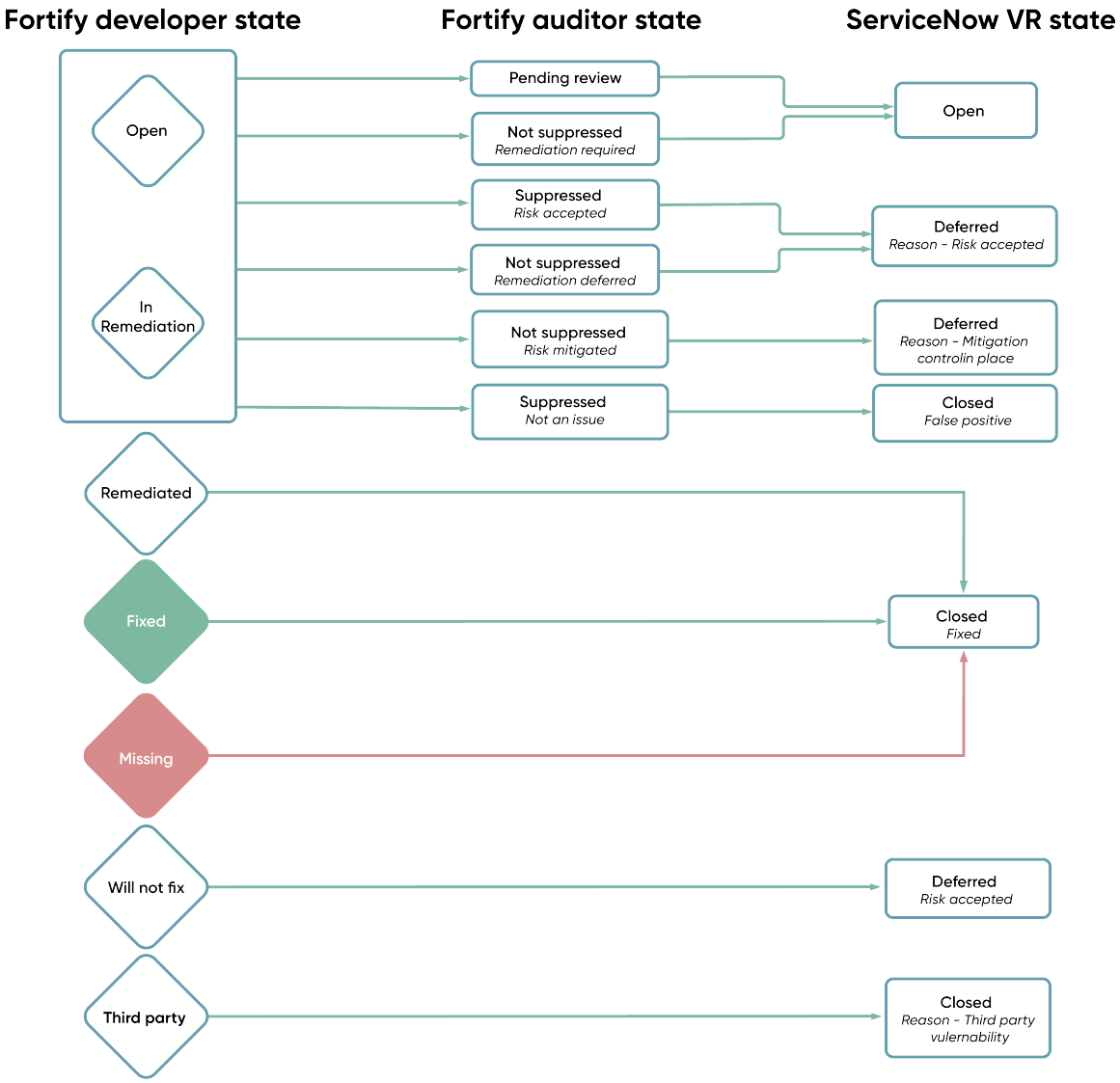


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de l'état pour Fortify

Remarque : Ce mappage d'état s'applique uniquement lorsque l'option de triage entrant ServiceNow n'est pas sélectionnée.



Traduction automatique

Réponse aux vulnérabilités des applications Exemples de règles de tâche de rattrapage

Exemple d'exemple de règle de tâche de rattrapage utilisant le créateur de conditions.

Une règle de tâche de rattrapage utilisant une vulnérabilité, un modèle de produit, une adresse IP et un groupe d'affectation

1. Dans le générateur de conditions d'un nouvel enregistrement, définissez la condition sur **Vulnérabilité** > **est** et entrez une vulnérabilité connue.

   Les vulnérabilités sont importées à partir des intégrations de la base de données de vulnérabilité nation (NVD) et de l'énumération des faiblesses courantes (CWE), comme décrit dans Configurer Réponse aux vulnérabilités des applications.

2. Dans la section Grouper par, sélectionnez **Élément vulnérable de l'application** pour le champ **Regrouper les éléments vulnérables de l'application** .
3. Dans le champ Utilisation, sélectionnez **Groupe d'affectation**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez les règles d'affectation pour définir automatiquement le champ **Groupe d'affectation** à utiliser dans votre règle de tâche de rattrapage. Vous pouvez utiliser une règle fournie avec l'application ou configurer vos propres règles d'affectation. Consultez Affecter automatiquement les éléments vulnérables de Réponse aux vulnérabilités des applications l'application pour plus d'informations.

4. Sélectionnez une autre condition, par exemple, l'élément de configuration de l'élément vulnérable d'application dans le champ **Regrouper l'élément vulnérable d'application de et** l'adresse IP ou le modèle de produit dans le champ **Utilisation** .
5. Dans la section Affectation, pour Affecter une tâche de rattrapage champ par champ, sélectionnez **Grouper par champ**.
6. Dans le champ Grouper par, sélectionnez **Groupe d'affectation**.

   Comme décrit dans cette section, cette sélection affecte des éléments vulnérables à différents groupes en fonction des conditions que vous définissez dans la section Grouper par. Bien que les AVI partagent la vulnérabilité, ils sont affectés à différents groupes en fonction du modèle de produit CI ou par adresse IP.

7. Sélectionnez **Soumettre** pour enregistrer votre règle.

Champs d'application analysés

Les applications sont stockées pendant l'importation sous **Administration** > **Applications** in Réponse aux vulnérabilités des applications.

Champs d'application analysés

Les champs importés dans cette table sont en lecture seule, sauf indication contraire. Les entrées **de département** et de **groupe de support** peuvent être ajoutées ou modifiées manuellement par un gestionnaire App-Sec.

Champ	Description
Nom	Nom importé de l'application.
Version	Version importée de l'application, le cas échéant.
Statut opérationnel	État opérationnel importé de l'application.
Département	Département importé auquel appartient l'application. S'il est vide, il peut être ajouté manuellement.
Unité business	Unité business importée à laquelle appartient le département. Lorsque le champ **Département** est renseigné, il est automatiquement renseigné avec l'unité business à laquelle le département appartient. Dans le cas contraire, il est laissé vide et en lecture seule.
Groupe de support	Groupe de support importé auquel appartient l'application. S'il est vide, il peut être ajouté manuellement.
Description	Description importée de l'application.
Date de dernière vérification de conformité de politique	Date à laquelle l'application a été analysée pour la dernière fois par Veracode pour vérifier sa conformité aux politiques. Il est utilisé dans les intégrations enchaînées de l'intégration de liste d'applications, où la prise en charge de l'ingestion de différentiel pour les applications est disponible, en comparant cette date à l'heure de début de différentiel des intégrations respectives.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Les données sont récupérées pour les applications extraites de Veracode, dont la valeur « Date de la dernière vérification de conformité de la politique » est supérieure ou égale à l'« Heure de début » (delta_start_time) des intégrations chaînées.
Liste connexe (visible uniquement par un gestionnaire de sécurité des applications ou un champion de sécurité)	
Champion de sécurité	Répertorie les applications associées à un champion de sécurité. Les gestionnaires App-Sec peuvent ajouter ou supprimer des membres de la liste.

Champs d'éléments vulnérables d'applications

Les éléments vulnérables de l'application (AVI) sont automatiquement créés lors des importations d'intégration de vulnérabilité tierce.

Champs des éléments vulnérables de l'application

À l'exception des champs **Groupe d'affectation**, **Affecté à** et **Notes**, tous les autres champs de l'AVI sont en lecture seule.

Champ	Description
Numéro	Identificateur AVI généré automatiquement pour cet enregistrement.
Type d'analyse	Type de scanner qui a trouvé cet AVI. Les choix possibles sont les suivants : • Dynamique • Statique • SCA
Cote de risque	**Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour plus d'informations sur les évaluations des risques, reportez-vous à la section Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications.
Score du risque	Quantité calculée de risque que l'AVI pose à votre environnement. Pour plus d'informations, consultez Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications.
Date de l'engagement de rattrapage	Date à laquelle les AVI doivent être rattrapés après leur passage dans **En cours d'examen**. Ce champ s'affiche uniquement si l'AVI est dans **En cours d'examen**.
Cible de rattrapage	Date à laquelle les AVI doivent être corrigés, dès lors qu'ils ont été identifiés pour la première fois. S'affiche uniquement le cas échéant.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Pour en savoir plus sur les cibles de rattrapage, reportez-vous à Automatiser le suivi des cibles de rattrapage dans Réponse aux vulnérabilités des applications.
État du rattrapage	État du rattrapage pour l'AVI. Il est déterminé par l'AVI avec la date d'échéance la plus proche, le cas échéant. Les États sont les suivants : • En cours • Cible presque atteinte • Cible passée
Nom de catégorie	Nom de la catégorie de la vulnérabilité.
Vulnérabilité	ID de la vulnérabilité associée à l'élément vulnérable de cette application.
Version de l'application	Version de l'application.
Module d'application	Application affectée dans l'analyse DAST. Masqué pour les analyses SAST.
Emplacement Version 14.0 : SAST	DAST : Emplacement de l'URL de la vulnérabilité dans l'application. SAST : chemin d'accès et numéro de ligne du fichier de la vulnérabilité dans l'application.
État	Ce champ est défini par défaut sur **Ouvert** lors de sa création. Pour plus d'informations sur la façon dont les États sont mappés, reportez-vous États des éléments vulnérables de l'application (AVI) à la section .
Motif	[Visible uniquement lorsque l'AIV est à l'état **Fermé** .] Explication de l'état.
Groupe d'affectation	Groupe sélectionné pour travailler sur cet AVI. Elles peuvent être ajoutées ou modifiées manuellement par un gestionnaire de sécurité des applications.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cet AVI. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec
Première occurrence trouvée	Date à laquelle la source tierce a trouvé pour la première fois l'élément vulnérable de l'application.
Dernier trouvé	Date à laquelle la source tierce a trouvé l'élément vulnérable de l'application pour la dernière fois.
Fermé	[Visible uniquement lorsque l'AVI est à l'état **Fermé** .] Date à laquelle l'AVI a été fermé.
Fermé par	[Visible uniquement lorsque l'AVI est à l'état **Fermé** .] Entité qui a fermé l'AVI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Résumé	Description importée de la vulnérabilité.
Résultats Données en lecture seule importées d'une intégration tierce.	
ID AVIT source	Identificateur importé pour l'AVI source.
Gravité de la source	Gravité importée de l'application source.
Date de correction de la cible source	Date importée pour laquelle la source s'attend à ce que l'AVI soit corrigé.
État de l'atténuation de la source	État d'atténuation importé de l'application source.
État du rattrapage de la source	État du rattrapage importé à partir de l'application source.
État du résultat de la source	[Visible uniquement lorsqu'il est renseigné] État du problème importé à partir de l'application source.
État SDLC	État du cycle de vie du développement logiciel importé.
Conforme à la politique	État de conformité importé. Si aucun état n'est renseigné, ce champ est défini sur **Non applicable**.
Lien source	URL de l'AVI source.
Notes sources	Notes importées à partir de la source.
Résumé de la vulnérabilité	Résumé importé de la source.
Explication de vulnérabilité	Explication importée de la source.
Recommandation	Recommandation importée à partir de la source.
Références	Références importées de la source.
Demande/réponse HTTP (visible uniquement pour les analyses DAST)	
Demande source	Demande HTTP
Réponse source	Réponse HTTP
Notes	
Plan de rattrapage	Détails sur la façon dont les AVI seront corrigés. Le plan doit être mis en œuvre avant la **date d'engagement d'assainissement**. Ce champ s'affiche uniquement si l'AVI est dans **En cours d'examen**.
Commentaires/ notes de travail supplémentaires	Toute information pertinente. Sélectionnez la zone de texte des notes de travail pour ajouter des informations. À partir de la Réponse aux vulnérabilités version 20.0, vous pouvez ajouter des notes de travail dans la section Notes pour un élément vulnérable différé de l'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des tests de pénétration

Les propriétaires d'applications peuvent demander une évaluation de test d'intrusion pour leurs applications et surveiller les progrès de l'équipe de piratage éthique jusqu'à ce que la demande soit résolue.

La demande d'évaluation de test de pénétration passe par les états de transition suivants jusqu'à ce qu'elle soit résolue.

Étapes de la demande d'évaluation de test de pénétration

Champ	Description
États des tests de pénétration	
Ouvrir	État dans lequel la demande d'évaluation est créée par le propriétaire de l'application.
Définition du périmètre	L'équipe de piratage éthique évalue la demande et le périmètre de l'application.
Préparation de l'environnement	Le propriétaire de l'application crée un environnement avec des rôles et d'autres informations et les fournit à l'équipe de piratage éthique pour qu'elle les teste.
Test en cours	L'équipe de piratage éthique teste manuellement l'application pour identifier les résultats du test d'intrusion.
V16.1 : Test en cours	L'équipe de piratage éthique indique que des tests sont actuellement en cours. Si cet état est sélectionné, l'option **Test en suspens** devient disponible sur le formulaire.
V16.1 : Test en suspens	ce champ n'est affiché que lorsque l'état Test en cours est sélectionné. L'équipe de piratage éthique contrôle les accords sur les niveaux de service (SLA) des demandes d'évaluation de test de pénétration en sélectionnant cet état, si nécessaire. Cela permet de s'assurer que les SLA sont signalés avec précision.
V16.1 : Test en cours de révision	L'équipe de piratage éthique indique que les tests sont terminés et qu'ils sont en cours d'examen par un expert en la matière.
Fermé	L'équipe de piratage éthique ferme les demandes d'évaluation du test d'intrusion une fois que les résultats du test d'intrusion ont été signalés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étapes de la demande d'évaluation de test de pénétration (suite)

Champ	Description
	Remarque : À partir de la version 16.1, vous pouvez utiliser l'option **Copier et créer une demande** du formulaire pour répliquer la demande à l'état Fermé et créer une nouvelle demande. Pour plus de détails, voir Répliquer une demande de test de pénétration à l'état Fermé.
V16.1 : Annulé	Le propriétaire de l'application annule la demande d'évaluation du test de pénétration.
V16.1 : Brouillon	Le propriétaire de l'application crée une demande et l'enregistre en tant que brouillon avant de soumettre la demande.
États des éléments vulnérables de l'application	
Ouvrir	Lorsque l'équipe de piratage éthique identifie et crée les résultats du test d'intrusion, leur statut est Ouvert.
Résolu	Lorsque l'équipe d'application résout les conclusions du test de pénétration, leur état passe à Résolu. **Remarque :** Si le résultat du test d'intrusion a été résolu mais n'a pas encore été validé par l'équipe de piratage éthique, le sous-état est *Validation Pending*.
Fermé	L'équipe de piratage éthique valide que les résultats du test de pénétration ont été résolus et passe l'état à Fermé.

Traduction automatique

Gestion du mappage d'état pour les reports et les faux positifs dans Réponse aux vulnérabilités des applications

Vous pouvez gérer la façon dont les états **source** sur les éléments vulnérables de l'application (AVI) importés par et sont mappés dans votre instance après l'importation Veracode Vulnerability IntegrationFortify Vulnerability Integration .

À partir de la version 20.0 de , vous disposez de Réponse aux vulnérabilitésplus d'options pour trier vos AVI importés avec ServiceNow les workflows.

Lorsque vous Configurez la Fortify Vulnerability Integration. ou le , les pages de configuration de Configurez la Veracode Vulnerability Integration.l'intégration vous offrent deux options pour vous aider à gérer les exceptions et les faux positifs dans votre instance.

- Gérer les exceptions dans ServiceNow
- Gérer les faux positifs dans ServiceNow

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : Gestionnaire App-Sec.

Cas d'utilisation pour la gestion des exceptions

Les AVI sont importés à partir de ces intégrations avec les états **source** . Lors de l'importation, ces états sont mappés aux états **Cible** et **Motif cible** dans votre instance, car dans certains cas, il n'y a pas de correspondance exacte entre les états source de votre scanner et les états utilisés par votre instance.

Par exemple, les états source tels que **Ne corrigera pas**, **Rattrapage différé**, **Risque accepté** et **Risque atténué** de sont Fortify Vulnerability Integration mappés à l'état **Différé** avec un sous-état **Risque accepté** ou **Contrôle d'atténuation en place dans** votre instance.

Les options suivantes s'offrent aux pages de configuration pour ces intégrations :

Option	Case à cocher sélectionnée	Description
Gérer les exceptions dans ServiceNow	Y (par défaut)	Si vous laissez cette option sélectionnée, vous devez demander des exceptions aux enregistrements AVI. Les AVI importés marqués pour l'état **Différé** sont triés avec le ServiceNow workflow de gestion des exceptions. Les AVI dont les états **sources** sont normalement mappés à un état **Différé** sont mappés à l'état **Triage cible à l'étatOuvert** .
	N	Si vous désactivez la case à cocher, vous conservez les états **source** importés à partir de votre scanner. Ces AVI sont mappés à **l'état cibleDifféré** et à un état **Motif cible** dans votre instance. Ils ne sont pas triés par le workflow d'exception, car ils ne sont pas mappés aux états **État de triage cible** et **Motif de triage cible** . L'action **d'interface utilisateur Demande d'exception** n'est pas disponible sur l'enregistrement AVI, car l'enregistrement est déjà dans l'état Cible **différée** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation pour les faux positifs

Par exemple, pour les faux positifs provenant de l'exemple Veracode Vulnerability Integration, les états de la source tels que **Faux positif** ou **Faux positif potentiel** sont mappés à **l'état Ciblefermée** avec un sous-état **Faux positif**.

Option	Case à cocher sélectionnée	Description
Gérer les faux positifs dans ServiceNow	Y (par défaut)	Si vous laissez cette option sélectionnée, vous devez demander un **faux positif** à partir des enregistrements AVI. Les AVI importés marqués pour les **états Faux positif** ou **Faux positif potentiel** sont triés avec le ServiceNow workflow Gestion des exceptions. Les AVI dont les états **sources** sont normalement mappés à un **état ciblefermé** sont mappés à un état de **triage cible** dans **Ouvert**. L'action **d'interface utilisateur Faux positif** est disponible sur l'enregistrement AVI.
	N	Si vous désactivez la case à cocher, vous conservez les états **source** importés à partir de votre scanner. Ces AVI sont mappés à **l'état cibleFermé** et à l'état **Faux positif** de motif **cible** dans votre instance. Ils ne sont pas triés par le workflow de faux positif. L'action **d'interface utilisateur Faux positif** n'est pas disponible sur l'enregistrement AVI, car l'enregistrement est déjà à l'état **Cible fermée** .

Références de Réponse aux vulnérabilités des applications

Les termes suivants sont utilisés dans Réponse aux vulnérabilités des applications.

Éléments vulnérables de l'application (AVI)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appariements d'entrées de vulnérabilité et d'applications potentiellement vulnérables dans votre environnement d'entreprise.

Règles d'affectation

Règles utilisées pour affecter des AVI en fonction des critères que vous avez définis.

Common Platform Enumeration (CPE)

Schéma de dénomination structuré NVD NIST pour les systèmes, logiciels et packages des technologies de l'information.

Vulnérabilités et expositions communes (CVE)

Dictionnaire des vulnérabilités et des expositions en matière de sécurité de l'information connues du public.

Common Weakness Enumeration (CWE)

Liste des types de faiblesses logicielles développés par la communauté.

Intégrations

Travaux planifiés qui extraient les données de rapport de CWE ou d'un système tiers, par exemple Veracode, pour récupérer les données de vulnérabilité.

> **Remarque :** Si l'intégration de la base de données de vulnérabilité nationale du NIST dans Réponse aux vulnérabilités est activée et configurée, l'enrichissement CVE est disponible pour les CWE, mais pas obligatoire. Pour en savoir plus sur l'intégration de la base de données de vulnérabilité nationale du NIST, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces.

Base de données de vulnérabilité nationale (NVD)

Référentiel gouvernemental des États-Unis de données de gestion des vulnérabilités basées sur des normes représentées à l'aide du protocole d'automatisation du contenu de sécurité (SCAP).

Règles de cibles de rattrapage

Règles utilisées pour affecter des dates cibles de rattrapage aux AVI en fonction des critères que vous avez définis.

Calculateurs de vulnérabilités

Calculateurs utilisés pour classer par ordre de priorité et catégoriser les vulnérabilités des applications en fonction des critères que vous avez définis.

Exemple de règle d'exception pour Réponse aux vulnérabilités des applications

Exemple de règle basé sur une vulnérabilité connue pour une règle d'exception.

Champ	Description
Nom	Nom unique pour vous aider à identifier son objectif et à localiser facilement la règle, par exemple, `exception Veracode-1 cwe-22`.
État	Lecture seule : brouillon
Début de validité	Date à laquelle cette règle est active pour différer les AVI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ordre d'exécution	Ordre unique pour chaque règle d'exception. Une valeur inférieure précède une valeur supérieure.
Date de fin de validité	Date à laquelle la tâche de rattrapage cesse d'accepter de nouveaux VI.
Reporté jusqu'à	Date à laquelle les tâches de rattrapage et les AVI sont reportés. À cette date, l'AVUL est fermé, tous les AVI sortent de la tâche et sont rouverts. Les règles de groupe sont réappliquées à ces AVI.
Motif	Raison pour laquelle cette règle d'exception a été créée. Sélectionnez-en un dans la liste, par exemple, **Correctif non disponible**.
Groupe d'affectation	Groupe affecté pour le suivi des VI différés, par exemple, APP Sec Manager.
Information supplémentaire	Informations supplémentaires que le demandeur souhaite fournir à l'approbateur. Ces informations sont renseignées dans le champ de description de la tâche de rattrapage. Dans cet exemple, `différez les AVI avec la vulnérabilité – Veracode-1-22.`
Condition	Conditions de filtre pour spécifier quels AVI correspondent à cette règle. Pour cet exemple, `la vulnérabilité est Veracode-1-22`.
Exécuter sur les données existantes	Option qui vous permet d'exécuter cette règle sur des données existantes la première fois que cette règle est exécutée. Si vous laissez cette option désactivée, votre règle s'exécute quotidiennement par la tâche *`Associate existing AVIs with Auto Exception Rule`* planifiée en commençant par de nouvelles données. Si vous activez l'option Exécuter sur les données existantes, une tâche planifiée s'exécute une seule fois sur les données existantes à la date **de début de validité** .

Vue du produit Réponse aux vulnérabilités des applications

Le produit Application Vulnerability Response (AVR) ingère les faiblesses et les vulnérabilités détectées par vos outils de test de la sécurité des applications et fournit un guichet unique pour comprendre la posture de sécurité de toutes les applications de votre environnement.

AVR vous permet de réduire les risques avec les workflows de rattrapage. L'objectif de cette vue de produit est de vous aider à comprendre comment les entités clés AVR fonctionnent avec le cadre de travail CSDM principal.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise à jour de la terminologie

À partir d'AVR v19.0, les noms de table et de colonne clés suivants ont été mis à jour. Par conséquent, vous verrez des références aux noms plus anciens et plus récents dans la documentation.

Mise à jour de la liste des noms de termes, de tables et de champs pour AVR

Avant AVR v19.0	À partir d'AVR v19.0
Règles de recherche de CI	Règles de recherche
Formulaire Règle de recherche de CI	Formulaire Règle de recherche
Règle de correspondance CI	Règle de correspondance
Rechercher sur la table	Rechercher sur la table CI
Rechercher sur le champ	Rechercher sur le champ CI
Version de l'application	Applications détectées
Table de mise en production de l'application	Table Applications détectées
Criticité pour l'entreprise	Criticité opérationnelle source

Prérequis

Installez les dernières versions des applications suivantes :

- Security Support Common
- Réponse aux vulnérabilités
- Cadre de travail de Security Integration
- Orchestration de support de sécurité
- Intégrations de scanners telles que Veracode et Fortify

AVR et CSDM 4.0

Avant AVR v19.0, lorsque des vulnérabilités d'application étaient ingérées, l'application pour laquelle les vulnérabilités étaient ingérées était recherchée à l'aide des règles de recherche de CI, par rapport aux applications analysées (sn_vul_app_scanned_application). Si l'enregistrement du nom de l'application ne s'y trouvait pas, une entrée serait effectuée.

À partir d'AVR v19.0, pour s'aligner sur le cadre de travail CSDM 4.0, les tables Modèle de produit sont utilisées à la place de la table Applications numérisées. Si l'application dispose de la version, la recherche se fait par rapport à la table Modèle logiciel. S'il n'y a pas de version, la recherche se fait par rapport à la table Modèle d'application. Modèle d'application et Modèle logiciel sont tous deux des tables enfants de la table Modèle de produit, qui est la table de base dans CMDB. La capture d'écran suivante explique le modèle de produit.

Propriété système

Pour utiliser le processus de recherche basé sur un modèle de produit CSDM 4.0, définissez la propriété *sn_vul.use_product_model* système sur *true*.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Considérations relatives aux propriétés système

Nom de la propriété système	Valeur de propriété système	Rechercher une valeur cible	Considérations
sn_vul.use_product_model	VRAI	Sélectionner la valeur **Modèle de produit**	Les nouveaux utilisateurs doivent sélectionner la valeur **Modèle de produit** pour utiliser les règles de recherche de modèle de produit du cadre de travail CSDM 4.0.
	faux	Sélectionner la valeur **Élément de configuration**	Les utilisateurs existants peuvent continuer à utiliser le processus de recherche de CI et les **règles de recherche de CI** existantes.

Remarque : Pour définir la valeur cible de recherche, accédez à la page **Règle de recherche** > **[Règle de recherche d'intégration AVR]** > champ **Cible de recherche** .

Règles de recherche dans AVR

Dans le cadre de travail CSDM 4.0, des règles de recherche basées sur des modèles de produits sont utilisées à la place des règles de recherche de CI pour créer des entrées dans les classes de modèles de produits respectives. De même pour les scripts, vous pouvez définir les règles de recherche dans le cadre du modèle CSDM 4.0.

À partir d'AVR v19.0, lors de la création d'une règle de recherche, vous devez définir si vous souhaitez utiliser l'approche de l'élément de configuration ou du modèle de produit à l'aide du champ **Cible de recherche** . Pour plus d'informations, consultez Créer une règle de recherche de CI.

Applications détectées

Accédez à la **Tout** > **Applications détectées**. La table Applications détectées répertorie les applications ingérées par les scanners. Si la propriété *sn_vul.use_product_model* système est définie sur *true*, vous pouvez voir les modèles de produits correspondants pour les applications.

Considérations relatives à l'AVR

Présence d'enregistrements de CI ou de modèle de produit en double

Vérifiez que la propriété *sn_vul.use_product_model* système a été correctement configurée pour le processus de recherche. Assurez-vous de sélectionner **l'élément de configuration** ou le **modèle de produit** comme cible de recherche lors de la configuration du formulaire de règle de recherche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités pour conteneurs

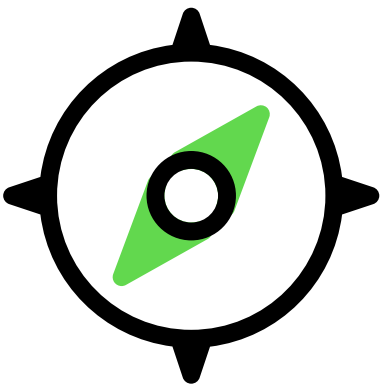
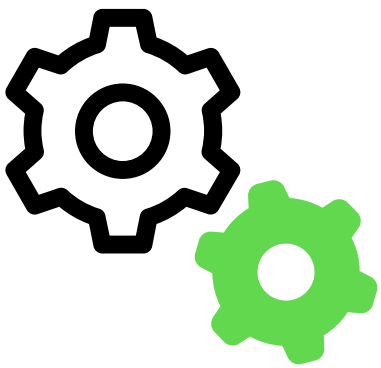
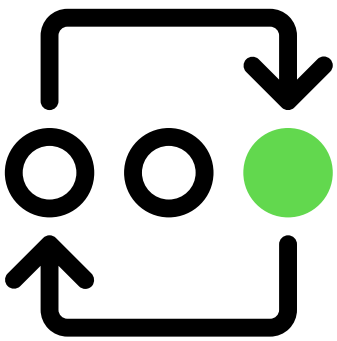
L'application ServiceNow® Réponse aux vulnérabilités pour conteneurs importe les éléments vulnérables du conteneur (CVIT) et, conformément aux règles, vous permet de corriger les vulnérabilités du conteneur. Les données de vulnérabilité sont extraites de sources internes et externes, telles que la base de données de vulnérabilité nationale (NVD) ou des intégrations tierces.

À partir de la version 18.0 de Réponse aux vulnérabilités, vous pouvez surveiller et corriger les CVIT respectivement dans Vulnerability Manager Workspace et IT Remediation Workspace. Pour plus d'informations, consultez Espace de travail du gestionnaire de vulnérabilités et Exploration de l'Espace de travail de remédiation IT.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

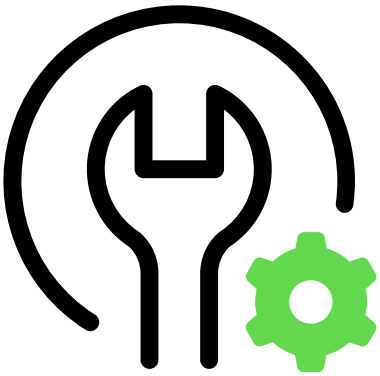
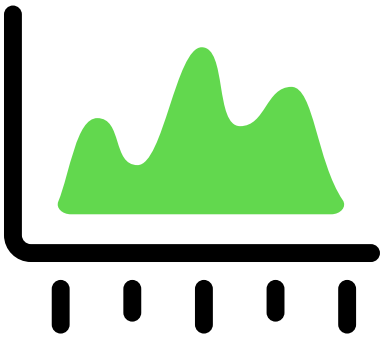
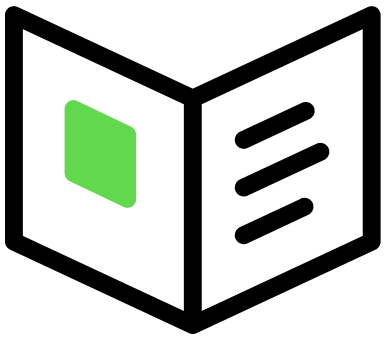
Réponse aux vulnérabilités pour conteneurs

Explorer	Configurer	Intégrer
		
Découvrez les concepts et les fonctionnalités de Container Vulnerability Response.	Configurez Container Vulnerability Response.	Étendez Container Vulnerability Response en l'intégrant à d'autres applications.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités pour conteneurs (suite)

Corriger	Analyse et génération de rapports	Référence
		
Apprenez à corriger les vulnérabilités d'un conteneur.	Afficher l'analyse Vulnerability Response du conteneur	Obtenir des détails sur les composants de Container Vulnerability Response tels que les champs, les tables et les propriétés.

Avantages

L'application Réponse aux vulnérabilités pour conteneurs offre les avantages suivants :

- S'intègre à des produits de sécurité de conteneur tiers, tels que Prisma Cloud Compute de Palo Alto Networks.
- Importe les données de vulnérabilité pour les images déployées pour l'exécution et enrichit les données de vulnérabilité avec des informations contextuelles d'exécution (hôtes, grappes Kubernetes, services et espaces de noms).
- Fournit une liste des références créées à partir des vulnérabilités aux entités Kubernetes pertinentes dans l'utilisation ServiceNow de Base de données de gestion des configurations (CMDB) Kubernetes Découverte.
- Offre un tableau de bord de génération de rapports complet, fournissant des informations sur les tendances de vulnérabilité et de correction.

Fonctionnalités principales

L'application Réponse aux vulnérabilités pour conteneurs gère les vulnérabilités détectées dans les conteneurs. Il offre les fonctionnalités suivantes :

- Pointez vers l'image Docker source à partir de CVIT au lieu d'exécuter des conteneurs.
- Configurez la granularité des CVIT à suivre au niveau de l'image, de la grappe Kubernetes, de l'espace de noms ou du service.
- Suivez les nouvelles versions d'images pour identifier les vulnérabilités corrigées. Toutes les vulnérabilités signalées dans les versions antérieures sont automatiquement résolues lorsque ServiceNow de nouvelles versions d'image sont déployées lors de l'exécution.
- Suivez les CVIT dans les images de base séparément des images d'application pour permettre un rattrapage indépendant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Émettre des demandes d'exception ou des demandes de faux positif, qui peuvent être examinées via un processus d'approbation à plusieurs niveaux.
- Définissez des règles d'exception pour différer automatiquement les CVIT.

Cas d'utilisation

Les conteneurs sont un excellent moyen de déployer et de faire évoluer des applications sur plusieurs environnements avec moins de frais généraux et une portabilité accrue. Toutefois, les vulnérabilités dans les images des conteneurs peuvent présenter un risque pour l'hôte sous-jacent et, en fin de compte, pour l'infrastructure où les conteneurs ont été lancés à partir de ces images. Bien qu'il existe de nombreux produits de sécurité des conteneurs qui analysent les images des conteneurs à la recherche de vulnérabilités, la correction des vulnérabilités présente quelques considérations et problèmes. Réponse aux vulnérabilités pour conteneurs peut aider à résoudre divers problèmes ou cas d'utilisation impliqués dans le rattrapage des vulnérabilités d'images de conteneurs. Découvrez comment tirer parti du Réponse aux vulnérabilités pour conteneurs module :

Contexte d'exécution

Les vulnérabilités dans les images de conteneurs peuvent être découvertes en analysant l'image au cours des étapes suivantes du cycle de vie de l'application.

- Étape 1 : lorsque les images sont en cours de création dans le pipeline CI/CD.
- Étape 2 : quand les images sont publiées dans le registre
- Étape 3 : lorsque les images sont déployées dans l'exécution.

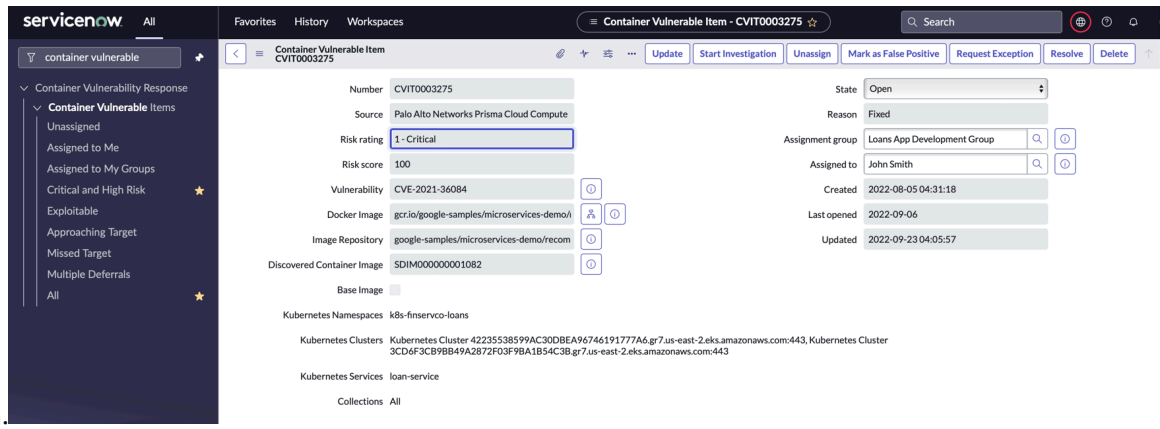
S'il est important d'identifier les vulnérabilités le plus tôt possible aux étapes 1 et 2, il est tout aussi important d'effectuer une analyse sur les images déployées dans un environnement d'exécution. Il offre les avantages suivants :

- identifiant des nouvelles vulnérabilités et expositions courantes (CVE) qui ont été publiées.
- Fournir une visibilité précise sur la posture vis-à-vis du risque des applications déployées.
- Classement par ordre de priorité des vulnérabilités qui doivent être résolues. Le contexte d'exécution en termes de services d'application ou de services d'entreprise impactés en raison d'une vulnérabilité peut aider à établir des priorités.

Réponse aux vulnérabilités pour conteneurs s'intègre aux produits de sécurité de conteneur tels que Prisma Cloud Compute pour Palo Alto Networks extraire les données de vulnérabilité des images déployées pour l'exécution et enrichit les données de vulnérabilité avec les informations contextuelles d'exécution telles que les hôtes, les grappes Kubernetes, les services et les espaces de noms où ces images de conteneur sont déployées. Les clients qui utilisent la ServiceNow détection Kubernetes peuvent voir les références créées à partir des vulnérabilités vers les entités Kubernetes pertinentes dans leur Base de données de gestion des configurations (CMDB)fichier . En plus d'enrichir les métadonnées, ServiceNow offre également un tableau de bord de reporting

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

complet pour fournir des informations sur les tendances de vulnérabilité et de



remédiation.

Identifier la propriété

Prérequis

- **Métadonnées et références Kubernetes** : pour Réponse aux vulnérabilités pour conteneurs renseigner les métadonnées Kubernetes (espace de noms, cluster, entre autres) et les références aux Base de données de gestion des configurations (CMDB) entrées, vous devez implémenter la découverte Kubernetes à partir de Information Technology Operations Management (ITOM). Kubernetes Discovery remplit l'image Docker, les conteneurs Docker en cours d'exécution, les pods, les grappes Kubernetes, entre autres, dans le CMDB. Réponse aux vulnérabilités pour conteneurs identifie l'image Docker en CMDB fonction de l'ID de l'image, puis identifie les entités Kubernetes connexes et renseigne les références à ces entités à partir d'éléments vulnérables.

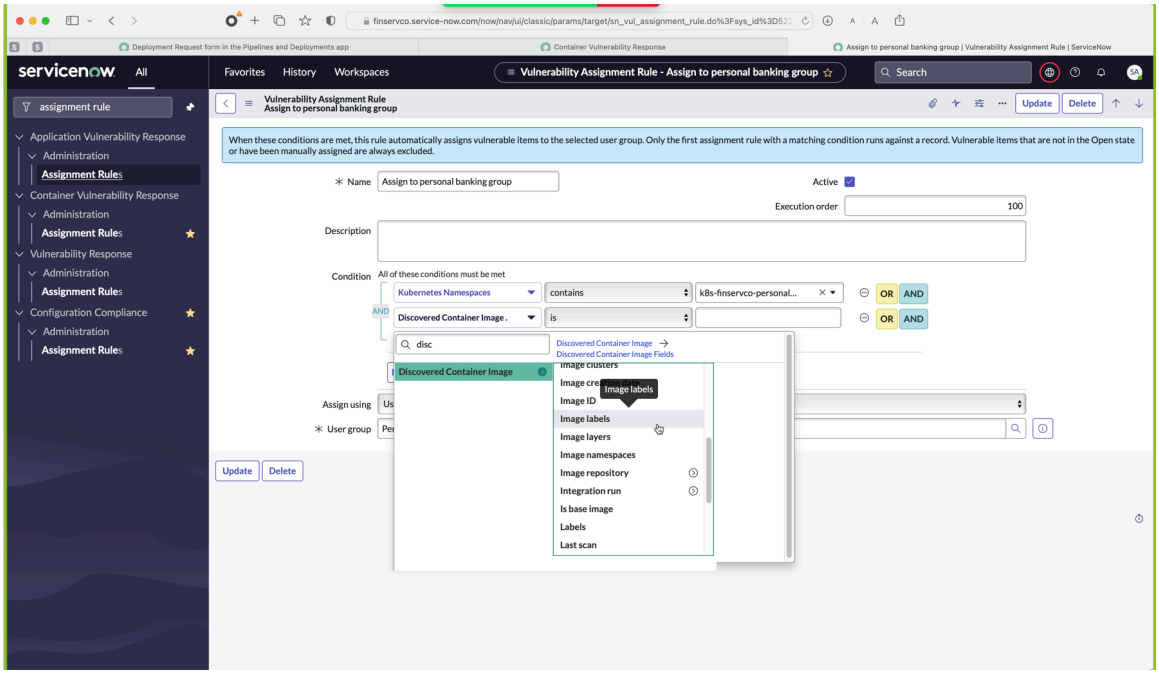
- **Métadonnées dans le cloud et étiquettes d'image Docker** : Réponse aux vulnérabilités pour conteneurs renseigne également les étiquettes d'image Docker, les ID de compte dans le cloud, les régions où une image est déployée. Ces données sont conservées dans l'enregistrement « Image du conteneur détecté » associé à l'élément vulnérable. Il n'y a aucune condition préalable pour que ces données soient renseignées. Réponse aux vulnérabilités pour conteneurs utilise les données renvoyées par les produits de sécurité des conteneurs (par exemple, Palo Alto Prisma Cloud Compute) pour renseigner ces entrées.

La propriété de l'application de correctif d'une vulnérabilité dans une image de conteneur peut varier d'une organisation à l'autre. Ces informations peuvent être capturées à différents endroits. Certaines organisations utilisent des étiquettes d'image Docker pour identifier les équipes d'application propriétaires d'une certaine image de conteneur, tandis que d'autres organisations peuvent utiliser l'espace de noms Kubernetes ou le compte cloud où une image de conteneur est déployée pour identifier le propriétaire du droit.

Réponse aux vulnérabilités pour conteneurs fournit les éléments de modèle de données nécessaires pour pouvoir capturer et utiliser les étiquettes d'image Docker, les métadonnées de cluster/service/espace de noms Kubernetes ou les métadonnées du compte cloud (ID de compte cloud, région, fournisseur, etc.) dans le module « Règles d'affectation » et affecter automatiquement les vulnérabilités à la bonne équipe d'application en fonction des métadonnées de l'image ou de l'environnement d'exécution.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



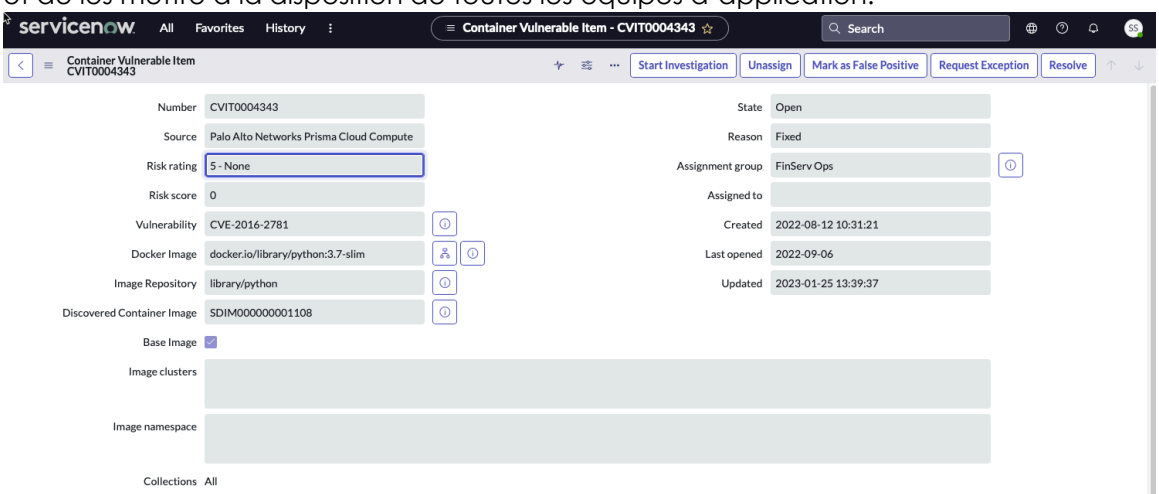
Suivre les vulnérabilités dans les images de base

Prérequis

Pour que la propriété « Image de base » soit renseignée dans Réponse aux vulnérabilités pour conteneurs, les images de base doivent être configurées explicitement dans la Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute console. Pour plus d'informations sur la configuration d'images de base dans Prisma Cloud, consultez https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-compute/vulnerability_management/base_images.

Réponse aux vulnérabilités pour conteneurs Permet de créer des enregistrements de vulnérabilité distincts pour une couche de base afin qu'ils puissent être affectés à une autre équipe.

Suivez les vulnérabilités identifiées dans une image de système d'exploitation de base telle qu'Alpine à partir des vulnérabilités détectées dans d'autres couches de l'image du conteneur. De nombreuses entreprises disposent d'équipes dédiées chargées d'appliquer des correctifs aux images de système d'exploitation de base et de les mettre à la disposition de toutes les équipes d'application.



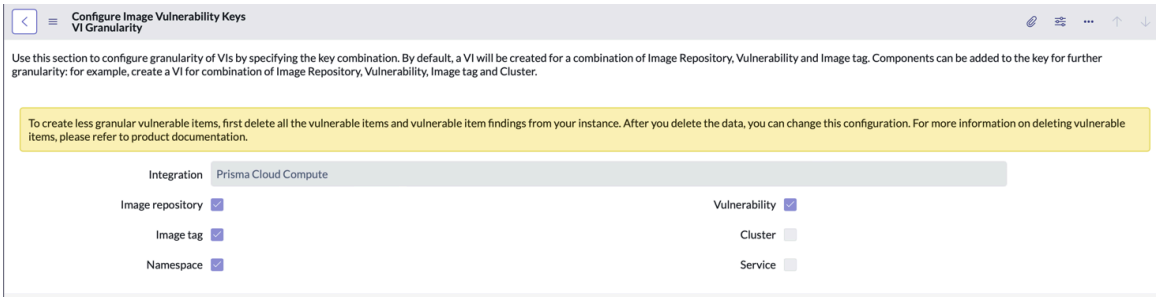
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

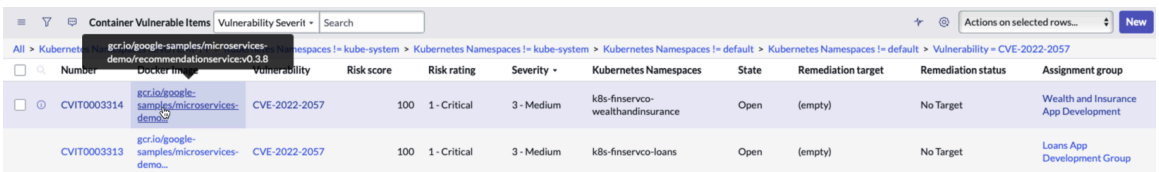
Définir la granularité pour les éléments vulnérables

Prérequis

Configurez la granularité des CVIT en accédant à **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Configurer la granularité VI**.



Par défaut, un élément vulnérable est créé pour chaque combinaison unique de CVE et de la version de l'image Docker (référence + balise). Toutefois, quelques images Docker peuvent être déployées dans plusieurs espaces de noms Kubernetes et chaque espace de noms peut appartenir à différentes unités commerciales ou équipes. Chaque équipe peut suivre sa propre cadence pour déployer de nouvelles versions d'images de conteneurs afin de corriger les vulnérabilités. Pour prendre en charge ce scénario, vous permet de définir la granularité des éléments vulnérables : indique si un élément vulnérable doit être créé pour chaque espace de noms/cluster/service Kubernetes, Réponse aux vulnérabilités pour conteneurs même pour chaque combinaison unique de version et de vulnérabilité de l'image Docker.



Dans l'exemple, vous pouvez voir deux éléments vulnérables créés pour la même combinaison d'image Docker et de CVE. L'un pour l'espace de noms Kubernetes 'k8s-finservco-loans' et l'autre pour 'k8s-finservco-wealthandinsurance'.

Identifier les services impactés à l'aide de l'identification de service basée sur les balises

Prérequis

- Identifiez les différents services dans votre application et définissez les balises/paires clé-valeur qui représentent ces services.
- Déployez des images Docker et des pods Kubernetes avec ces balises ou étiquettes.
- Déployer ITOM Kubernetes Discovery Définissez des « services basés sur les balises » avec les balises ou les étiquettes appropriées.
- Déployer ITOM Kubernetes Discovery
- Définissez des « services basés sur les balises » avec les bonnes balises ou paires clé-valeur.
- Importer des données de vulnérabilité dans l'utilisation ServiceNow de Réponse aux vulnérabilités pour conteneurs

Traduction automatique

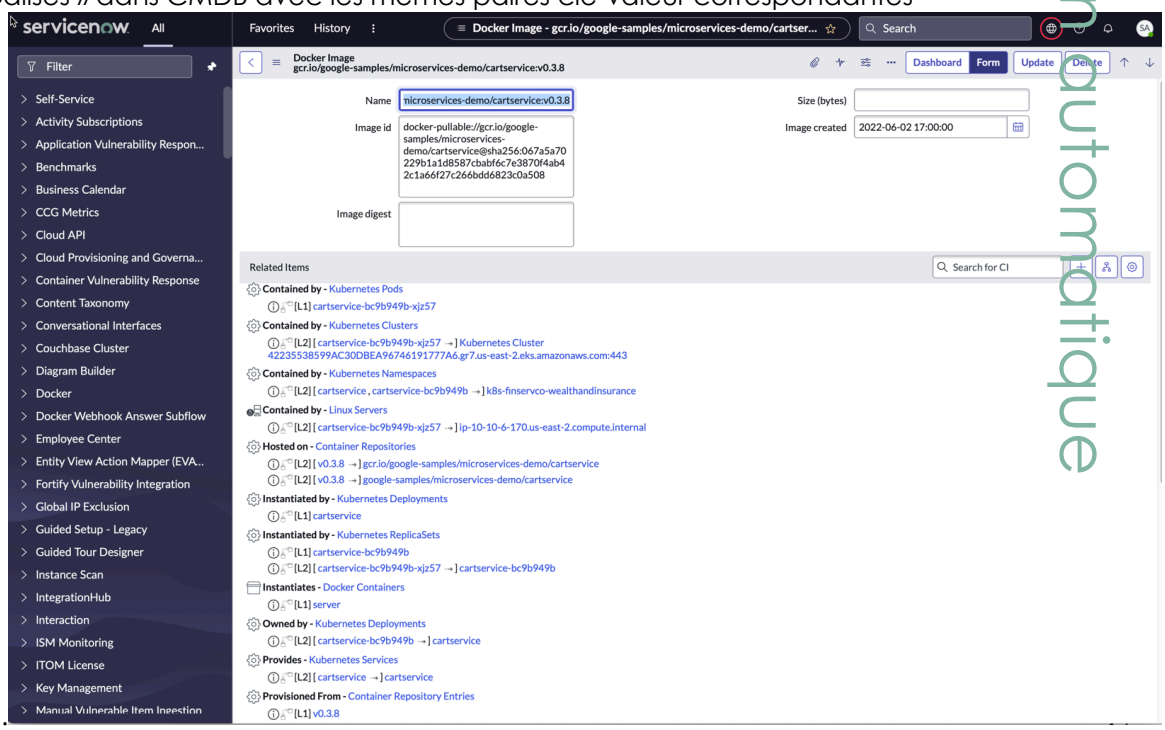
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le calcul du risque pour les éléments vulnérables peut être effectué en examinant le CI (image de Docker) et la criticité des services associés dans CMDB. Toutefois, pour faciliter l'identification des services impactés, Réponse aux vulnérabilités pour conteneurs propose une identification des services basée sur les balises.

Lorsque des pods ou des entités Kubernetes sont publiés avec des clés-valeurs ou des étiquettes correspondant aux clés-valeurs définies dans un « service basé sur les balises » dans ServiceNow, Réponse aux vulnérabilités pour conteneurs établit automatiquement la relation entre une image Docker et le service d'application impacté, et utilise la criticité de ce service d'application dans le calcul du risque.

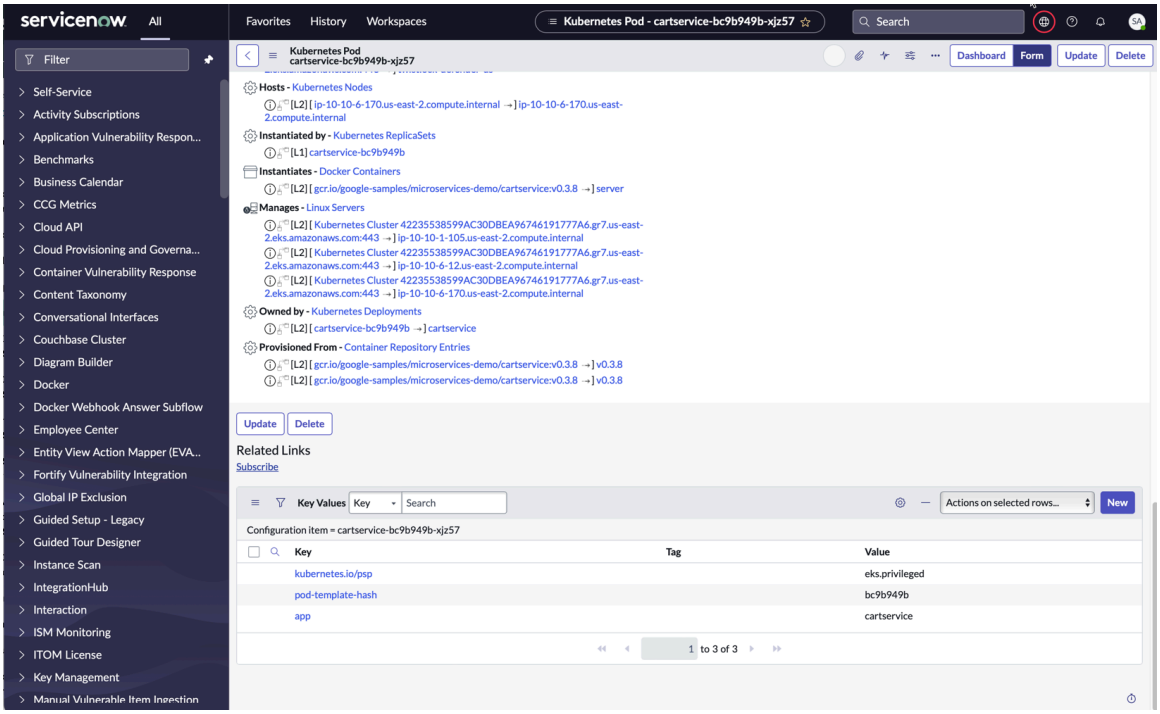
Le flux est le suivant :

1. Réponse aux vulnérabilités pour conteneurs Importe les données de vulnérabilité depuis le produit Security du conteneur.
2. Pour chaque élément vulnérable de conteneur, Réponse aux vulnérabilités pour conteneurs remplit l'image Docker à partir de CMDB laquelle il présente la vulnérabilité.
3. Réponse aux vulnérabilités pour conteneurs examine ensuite les étiquettes d'image Docker ou les étiquettes/clé-valeurs publiées avec les pods Kubernetes où cette image est déployée. Cette image est disponible si la détection Kubernetes est en cours d'exécution CMDB .
4. Réponse aux vulnérabilités pour conteneurs recherche ensuite « Services basés sur les balises » dans CMDB avec les mêmes paires clé-valeur correspondantes définies.

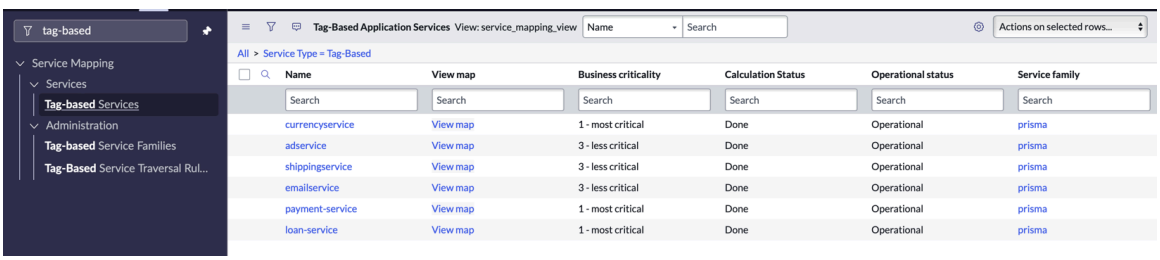


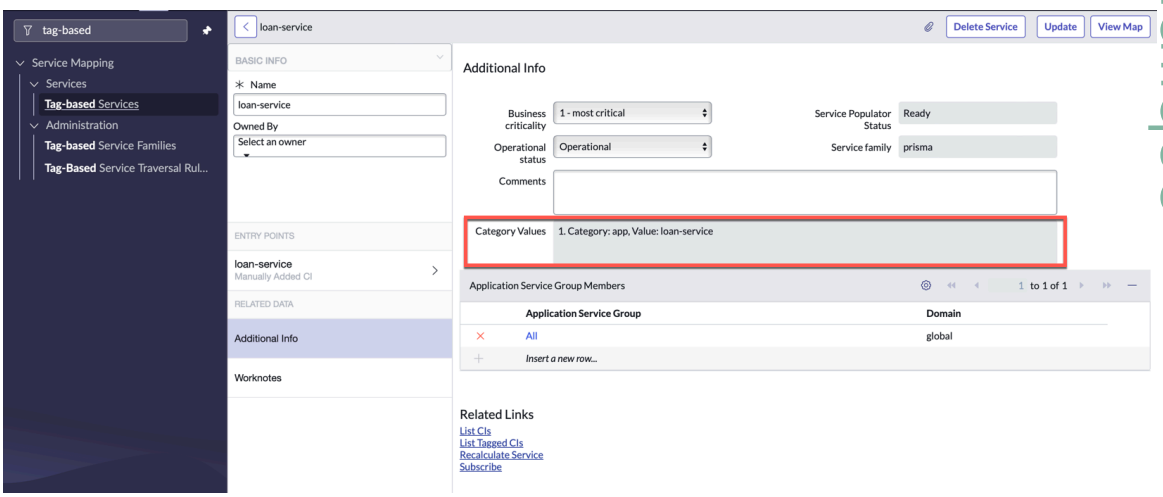
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Réponse aux vulnérabilités pour conteneurs utilise la « criticité opérationnelle » du « service basé sur les balises » correspondant (le cas échéant) pour calculer le risque d'un élément vulnérable du conteneur.





Suivi des vulnérabilités

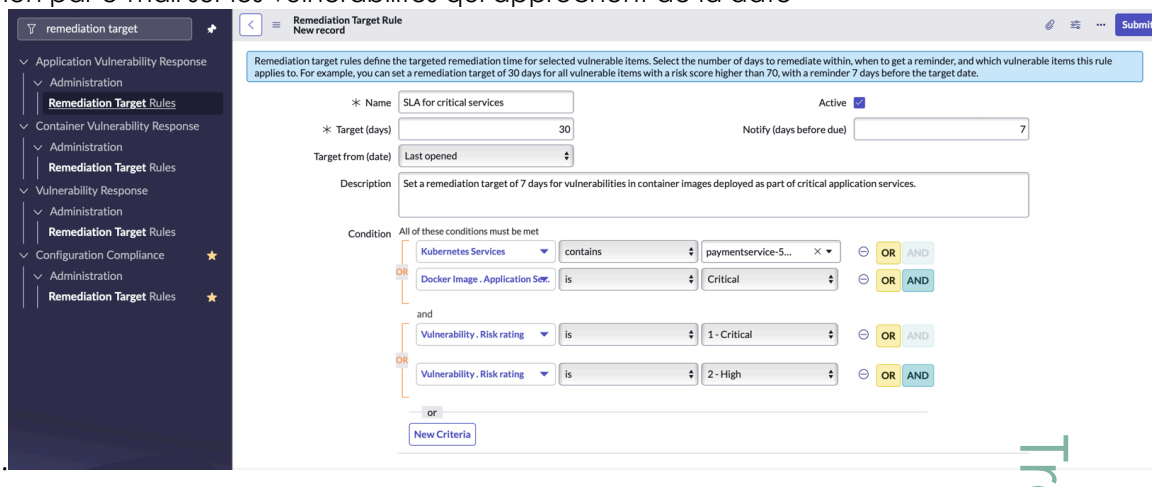
Définition de cibles de rattrapage

ServiceNow permet aux gestionnaires de vulnérabilité de définir des « règles de cibles de rattrapage » pour pouvoir définir des accords sur les niveaux de service (SLA) afin de corriger les vulnérabilités trouvées dans les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

images de conteneurs. La date cible de rattrapage peut être définie en fonction d'une condition/d'un critère sur les métadonnées d'image ou les informations de vulnérabilité. Les propriétaires de rattrapage reçoivent une communication par e-mail sur les vulnérabilités qui approchent de la date d'échéance.



Identification des vulnérabilités corrigées

Contrairement aux vulnérabilités de l'hôte qui peuvent être corrigées en appliquant un correctif sur un hôte, les vulnérabilités des conteneurs ne peuvent pas être corrigées. De nouvelles versions des images de conteneurs doivent être créées et déployées pour remplacer les anciennes versions. Les nouvelles versions ont un identifiant différent (ID d'image) par rapport aux versions précédentes, ce qui rend difficile le suivi des vulnérabilités qui ont déjà été corrigées.

ServiceNow identifie les vulnérabilités qui ont été signalées dans les versions précédentes des images de conteneur mais qui ont été résolues dans la dernière version de l'image et déplace automatiquement ces vulnérabilités vers l'état « Fermé/Corrigé » afin que les équipes de sécurité aient toujours une visibilité précise sur la dernière situation en matière de risque.

Gérer les exceptions

Les équipes d'application ou les propriétaires de la correction des vulnérabilités peuvent avoir besoin de la possibilité de demander une exception pour les raisons suivantes.

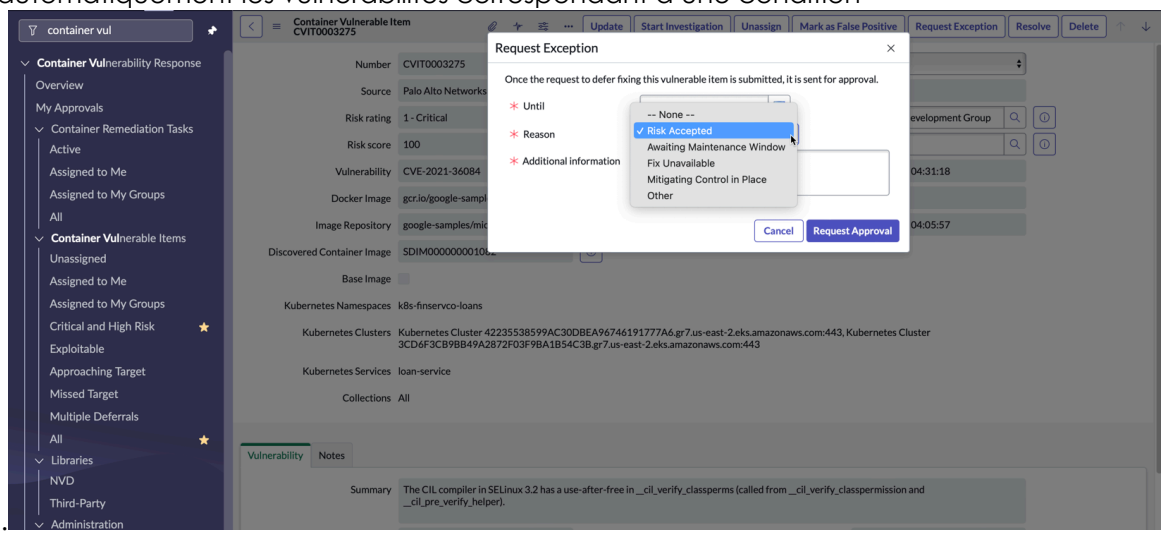
- Un contrôle d'atténuation est déjà en place
- Risque accepté
- En attente d'une fenêtre de maintenance pour transmettre le correctif.

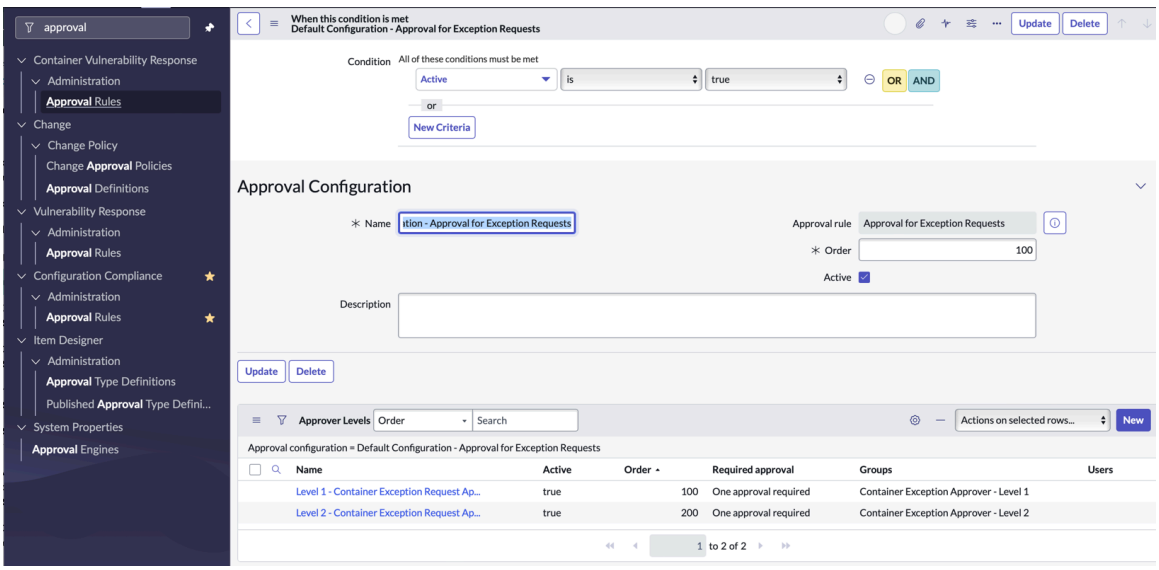
ServiceNow Permet aux administrateurs de sécurité de définir plusieurs niveaux d'approbateurs pour les demandes d'exception. Vous pouvez également définir des règles d'exception automatique qui peuvent être utilisées pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

différer automatiquement les vulnérabilités correspondant à une condition donnée.





Traduction automatique

Nouveautés

Pour en savoir plus sur les nouveautés et les changements apportés à Xanadu, consultez les notes de Xanadu publication.

Premiers pas

- Pour obtenir une vue d'ensemble sur Opérations de sécurité votre Now Platform instance, consultez Présentation des opérations de sécurité.
- Pour plus d'informations sur toutes les Opérations de sécurité applications téléchargeables disponibles à partir de , voir ServiceNow StoreOpérations de sécurité et ServiceNow Store.

Explorer Réponse aux vulnérabilités pour conteneurs

L'application Réponse aux vulnérabilités pour conteneurs importe les éléments vulnérables (CVIT) des conteneurs. Selon les règles, la fonctionnalité vous permet de corriger les vulnérabilités des conteneurs. Réponse aux vulnérabilités pour conteneurs est disponible par le biais d'un abonnement distinct.

Contrairement aux applications traditionnelles, les conteneurs regroupent tous les codes sources des applications ainsi que leurs dépendances dans un fichier binaire appelé image

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de conteneur. L'image est publiée dans un registre pour fournir une option d'exécution de cette image en tant qu'application ou instance de conteneur sur n'importe quelle plateforme. Les étapes d'un cycle de vie de pré-déploiement de conteneur sont les suivantes :

1. Composer l'image du conteneur : l'image du conteneur est composée et pointée vers un code source ou une bibliothèque dépendante.
2. Créer l'image du conteneur
3. Publier l'image du conteneur : le fichier d'image du conteneur est publié dans un registre. Chaque image a son propre identifiant unique basé sur le contenu de l'image. Ces images sont extraites du registre vers l'environnement d'exécution en mode post-déploiement. Les images s'exécutent ensuite en tant qu'instances de conteneur sur l'hôte dans l'environnement de production.

Analyse des images du conteneur

Une image de conteneur peut être analysée à la recherche de vulnérabilités avant ou après le déploiement. Si les images des conteneurs sont analysées pendant la phase de pré-déploiement, vous pouvez recevoir de nombreuses alertes de vulnérabilité qui peuvent ne pas nécessiter votre attention immédiate. Cependant, l'analyse des vulnérabilités pendant la phase post-déploiement offre de plus grands avantages, tels que les suivants :

- Fournir une visibilité sur le risque associé aux applications déployées.
- Fournir une vue focalisée uniquement sur les images de l'environnement de production.
- Identifier et hiérarchiser les vulnérabilités qui doivent être traitées immédiatement.
- Regroupement et affectation des vulnérabilités en fonction des métadonnées de l'image. Par exemple, un référentiel d'images, une étiquette d'image et d'autres attributs associés à l'image du conteneur peuvent être utilisés pour les règles de regroupement et d'affectation.

Chaque image de conteneur possède les composants clés suivants :

- Conteneur ou référentiel d'images : représente l'image Docker avec un référentiel ou un nom donné. Il héberge toutes les versions de l'image.
- Image de Docker : représente une version spécifique de l'image Docker de la version.
- Conteneur Docker : représente une instance en cours d'exécution de l'image Docker. Chaque version a un ID unique et comporte plusieurs instances de conteneurs en cours d'exécution dans l'environnement de production.

Réponse aux vulnérabilités pour conteneurs modules

Le Réponse aux vulnérabilités pour conteneurs module fournit des détails sur les éléments suivants :

Éléments vulnérables de conteneurs

Les éléments vulnérables du conteneur (CVIT) sont regroupés et répertoriés en fonction de leur affectation, de leur criticité, de leur exploitabilité et de l'état de rattrapage.

Bibliothèques

Accédez à la base de données de vulnérabilité nationale (NVD) et à des bibliothèques tierces. Alors que la bibliothèque NVD fournit des informations limitées à l'ID de l'élément de vulnérabilité, la bibliothèque tierce fournit la plupart des détails sur un élément de vulnérabilité. Les informations de l'écran NVD ne sont renseignées que lorsque l'intégration NVD est déclenchée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Administration

Le module Administration fournit des informations sur les règles d'affectation des éléments vulnérables, les règles de cible de rattrapage et les intégrations de vulnérabilité des conteneurs. En outre, vous pouvez également configurer la durée après laquelle un élément vulnérable doit être fermé automatiquement. Vous pouvez utiliser la section Configurer la granularité VI pour configurer la granularité des CVIT en spécifiant les combinaisons de touches. Par défaut, un CVIT est créé pour une combinaison d'un référentiel d'images, d'une balise d'image et d'une vulnérabilité. Vous pouvez ajouter des composants supplémentaires à la clé pour plus de granularité. Par exemple, vous pouvez créer un CVIT pour une combinaison de référentiel d'images, de balise d'image, de vulnérabilité et de grappe.

Versions disponibles

Version	Notes de publication
Réponse aux vulnérabilités pour conteneurs v2.1 Réponse aux vulnérabilités pour conteneurs v2.06 Réponse aux vulnérabilités pour conteneurs v2.0.4	

Réponse aux vulnérabilités pour conteneurs États de la tâche de rattrapage et de l'élément vulnérable du conteneur

Avec l'application Réponse aux vulnérabilités pour conteneurs , vous pouvez utiliser le modèle d'état pour afficher l'état d'une tâche de rattrapage, à tout moment. Savoir comment chaque état est lié et s'affecte les uns les autres vous aide à déterminer quand et comment corriger les éléments vulnérables de votre conteneur (CVIT).

États des tâches de résolution

Des cas d'utilisation complexes peuvent parfois entraîner un élément vulnérable de conteneur dans un état différent de celui de sa tâche de correction. Comprendre le fonctionnement des états permet d'expliquer ce comportement et peut aider à créer des tâches de rattrapage et à créer ou modifier des règles de tâches de rattrapage.

Les tâches de rattrapage ont de nombreux états possibles, comme le montre le diagramme suivant.

Flux d'état de Vulnerability Response du conteneur

Remarque :

- Les éléments vulnérables du conteneur ne peuvent pas être fermés manuellement.
- Chaque formulaire de tâche contient des boutons **Suivre** et **Mettre à jour** qui sont standard pour ServiceNow les tâches.

Configurer Réponse aux vulnérabilités pour conteneurs

Avant de l'exécuter Réponse aux vulnérabilités pour conteneurs dans votre Now Platform instance, vous devez la configurer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer Réponse aux vulnérabilités et Conformité de la configuration pour conteneurs

Avant d'exécuter l'application Réponse aux vulnérabilités et Conformité de la configuration pour conteneurs dans votre Now Platform instance, vous devez obtenir l'autorisation et télécharger l'application à partir du ServiceNow Store. Installez l'application sur votre Now Platform instance et effectuez quelques étapes d'installation dans l'assistant de configuration.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Tâches de configuration	Description
Vérifiez que l'application est installée et activée.	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilitésreportez-vous à la section .
Vérifiez que les rôles requis ServiceNow vous ont été affectés à votre instance.	Le rôle administrateur est requis pour l'installation. S'il n'est pas déjà affecté, l'administrateur système [admin] affecte également le rôle Administrateur de vulnérabilité, sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)].

Rôle requis : administrateur

Procédure

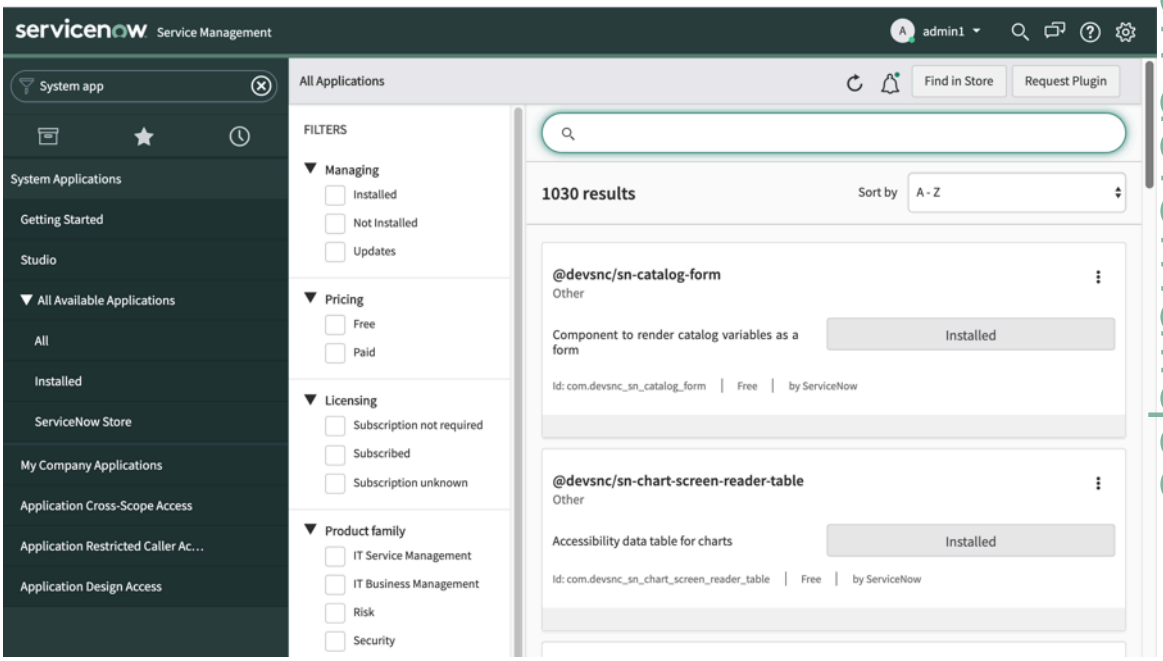
1. Pour obtenir l'autorisation et télécharger l'application Réponse aux vulnérabilités et Conformité de la configuration pour conteneurs , accédez au ServiceNow Store.
2. En haut à droite de la page, cliquez sur **Se connecter**.
3. Dans la barre de recherche, saisissez Réponse aux vulnérabilités et Conformité de la configuration pour conteneurs.
4. Sous Applications et solutions, cliquez sur la Réponse aux vulnérabilités et Conformité de la configuration pour conteneurs vignette.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Demander l'installation**.
6. Connectez-vous à l'instance Now Platform sur laquelle vous souhaitez installer l'application Réponse aux vulnérabilités et Conformité de la configuration pour conteneurs .
7. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tout**.



8. Dans la liste des applications, localisez-la Réponse aux vulnérabilités et Conformité de la configuration pour conteneurs , sélectionnez une version dans la liste et cliquez sur **Installer**. La boîte de dialogue d'installation de l'application s'affiche. Toutes les dépendances installées s'affichent.
9. Cliquez sur **Fermer**.

Définir les Réponse aux vulnérabilités pour conteneurs notifications par e-mail

Configurez des notifications par e-mail pour partager des informations utiles sur les mises à jour et les activités importantes, telles que l'approbation et le rejet des demandes de faux

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

positifs. La création d'une notification par e-mail implique de spécifier quand l'envoyer, qui la reçoit et ce qu'elle contient.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure
1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Modèles d'e-mail**.
2. Sélectionnez **Nouveau**.

   Pour obtenir des instructions détaillées sur la création de notifications par e-mail, reportez-vous à la section Créer une notification par e-mail .

Résultats
À partir de la version 21.0 de , lorsqu'un destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans ou Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT en fonction de Réponse aux vulnérabilitésson rôle.

- Les liens s'ouvrent dans le Pour les Espace de travail du gestionnaire de vulnérabilités utilisateurs ayant les rôles sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin.
- Les liens s'ouvrent dans le Pour les utilisateurs disposant de rôles, sn_vul_container.remediationEspace de travail de remédiation IT_owner.

Si le destinataire n'a aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Créer ou modifier des notifications de cibles de rattrapage

Les administrateurs de vulnérabilité peuvent modifier les notifications de cible de rattrapage ou en ajouter de nouvelles, en spécifiant le moment d'envoi de la notification, qui reçoit la notification et quel contenu contient la notification.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Procédure
1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Notifications**.
2. Sélectionnez l'enregistrement de notification de cible de rattrapage ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Pour plus d'informations sur les champs de formulaire, consultez Créer une notification par e-mail .
4. Sélectionnez **Prévisualiser la notification** pour afficher le message.

Résultats
À partir de la version 21.0 de , lorsqu'un destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans ou Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT en fonction de Réponse aux vulnérabilitésson rôle.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les liens s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs ayant les rôles sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin.
- Les liens s'ouvrent dans le Espace de travail de remédiation IT pour les utilisateurs disposant de rôles, sn_vul_container.remediation_owner.

Si le destinataire n'a aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Configurer la gestion des exceptions pour Réponse aux vulnérabilités pour conteneurs

Limitez la durée d'une demande d'exception et ajoutez un questionnaire à la demande d'exception ou de faux positif à l'aide du Réponse aux vulnérabilités pour conteneurs module. Par défaut, une exception est demandée à l'aide du ServiceNow® Réponse aux vulnérabilités pour conteneurs module. Vous pouvez également demander une exception à l'aide de l'intégration GRC : gestion de la politique et de la conformité .

Avant de commencer

Rôle requis : sn_vul_container.manage_exception_configuration

Pourquoi et quand exécuter cette tâche

Si Réponse aux vulnérabilités pour conteneurs cette option est activée, vous pouvez limiter la durée pendant laquelle une exception peut être demandée. De même, si le GRC : gestion de la politique et de la conformité module est installé, vous pouvez le sélectionner GRC : gestion de la politique et de la conformité sur l'écran de configuration. L'activation de cette option vous permet de demander une exception qui spécifie l'objectif de politique et de contrôle à partir de GRC.

Si vous ajoutez un questionnaire, il est envoyé à la personne qui émet la demande d'exception ou de faux positif. Vous pouvez utiliser le questionnaire par défaut ou en créer un en fonction de vos besoins. .

Il est utile que l'approbateur de l'exception comprenne le motif de la demande d'exception.

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire **Configuration de la gestion des exceptions** , sélectionnez la façon dont vous souhaitez gérer une exception en sélectionnant une option dans la liste **Gérer les exceptions à l'aide** de.
   Vous pouvez sélectionner ou Réponse aux vulnérabilitésGRC : gestion de la politique et de la conformité.
3. Si vous avez sélectionné l'option Réponse aux vulnérabilités , entrez les informations suivantes :

Réponse aux vulnérabilités champs

Champ	Description
Durée	Période pour laquelle une exception peut être demandée.
Unité	Unité de temps pour la période spécifiée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Activer le questionnaire pour demander une exception	Option permettant d'ajouter un questionnaire à la demande d'exception émise.
Questionnaire pour demander une exception	Affiche le questionnaire que vous avez sélectionné pour demander une exception. Le questionnaire d'exceptions est affiché par défaut.

Remarque : Lorsque vous sélectionnez GRC : gestion de la politique et de la conformité, les champs Durée et Unité disparaissent en tant que Gouvernance, risque et conformité gestionnaires de ce flux.

4. Sélectionnez **Enregistrer**.

Configurer les règles d'approbation pour la gestion des exceptions

À partir de la Réponse aux vulnérabilités version 15.0, utilisez le concepteur de flux pour approuver les demandes d'exception pour la gestion des exceptions, les règles d'exception et la gestion des faux positifs. Si vous déployez Réponse aux vulnérabilités (VR) pour la première fois, Flow Designer est activé par défaut.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Pour utiliser le concepteur de flux, créez des règles à l'aide du module Règles d'approbation. À l'aide de ce module, vous pouvez configurer des règles d'approbation pour chacun des workflows de gestion des exceptions suivants.

- Demande d'exception pour les tâches de rattrapage
- Demande d'exception pour les éléments vulnérables du conteneur
- Règle d'exception
- Faux positif pour les tâches de remédiation
- Faux positif pour les éléments vulnérables du conteneur

Vous pouvez également définir des conditions contenant plusieurs niveaux d'approbation au sein d'une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant.

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles d'approbation**.
2. Sur la page Règles d'approbation, sélectionnez le groupe pour lequel vous souhaitez définir la règle d'approbation.
3. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Règle d'approbation

Champ	Description
Nom	Nom de configuration de l'approbation.
Table	Table sur laquelle la règle est appliquée.
Application	La valeur par défaut est Vulnerability Response.
Type de règle	Spécifie le type de règle. Par exemple, gestion des exceptions, faux positif ou règle d'exception.
Actif	Activé par défaut, ce qui signifie que la règle d'approbation est utilisée.
Description	Brève description des règles d'approbation.
Expiration de l'approbation (jours) À partir de la v2.5 de Réponse aux vulnérabilités pour conteneurs	Date jusqu'à laquelle l'approbateur peut approuver la demande.
Notification de l'approbateur (jours) À partir de la v2.5 de Réponse aux vulnérabilités pour conteneurs	Date après laquelle l'approbateur est invité à prendre des mesures.

4. Sélectionnez **Mettre à jour**.
   Dans l'onglet Configurations d'approbation, deux niveaux d'approbateurs sont configurés par défaut. Vous pouvez sélectionner une règle pour définir les conditions en fonction de différents cas d'utilisation au sein d'une règle. Pour plus d'informations, consultez Créer des configurations pour une règle d'approbation.

   Remarque : Dans chaque page de configuration, vous pouvez créer plusieurs niveaux d'approbation. Pour plus d'informations, consultez Créer des niveaux d'approbation pour la gestion des exceptions.

Example:
En fonction des différents cas d'utilisation, vous pouvez définir différents processus d'approbation pour les mêmes vulnérabilités trouvées sur différents éléments de configuration.

Tests de démarrage rapide pour Réponse aux vulnérabilités pour conteneurs

Validez que Réponse aux vulnérabilités pour conteneurs fonctionne toujours après avoir apporté un changement de configuration telle que l'application d'une mise à niveau ou le développement d'une application. Copiez et personnalisez ces tests de démarrage rapide à effectuer lorsque vous utilisez des données spécifiques à votre instance.

La propriété d'exécution du test est désactivée par défaut pour empêcher l'exécution de tests sur un système de production. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production. Pour Exécuter la suite de tests Infrastructure de tests automatisés (ATF) pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités plus d'informations sur la configuration et l'exécution de la suite de tests pour Réponse aux vulnérabilités pour conteneurs.

Les tests de démarrage rapide Réponse aux vulnérabilités pour conteneurs nécessitent l'activation de l'application Réponse aux vulnérabilités pour conteneurs (sn_vul_container).

Tests Réponse aux vulnérabilités pour conteneurs

Test	Description	Version de mise en production
CVR : Règles d'affectation	Déterminez si un exemple d'ensemble de règles d'affectation peut affecter automatiquement des éléments vulnérables de conteneur à un groupe d'affectation à des fins de correction.	Vancouver
CVR : Règle d'exception	Testez les règles d'exception	Vancouver
CVR : Flux Marquer comme faux positif	Vérifiez si le flux Marquer comme faux positif fonctionne sur l'élément vulnérable de conteneur.	Vancouver
CVR : Règles de cibles de remédiation	Créez une règle de cible de rattrapage.	Vancouver
CVR : Flux de demande d'exception	Vérifiez si le flux de demande d'exception fonctionne comme prévu.	Vancouver
VR : Calculateurs de vulnérabilité	Testez les calculateurs de vulnérabilité du conteneur.	Vancouver

Information associée

Tests de démarrage rapide

Exécuter la suite de tests Infrastructure de tests automatisés (ATF) pour Réponse aux vulnérabilités pour conteneurs

Exécutez la suite de tests Infrastructure de tests automatisés (ATF) après avoir installé ou mis à niveau l'application Réponse aux vulnérabilités pour conteneurs .

Avant de commencer

Confirmez que l'installation s'est déroulée correctement et que votre instance fonctionne comme prévu.

La propriété d'exécution du test est désactivée par défaut pour empêcher l'exécution de tests sur un système de production. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production.

- Pour activer le test, procédez comme suit :
  1. Accédez à la **Tout** > **Framework de tests automatisés (ATF)** > **Administration** > **Propriétés**.
  2. Si elle n'est pas cochée, cochez la case **Activer l'exécution du test/de la suite de tests** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Enregistrer**.
4. Si le champ d'application n'est pas défini sur **Conteneur Vulnerability Response** dans l'en-tête, ou s'il n'est pas affiché dans l'en-tête, cliquez sur l'icône des paramètres.
5. Dans la fenêtre Paramètres système, cliquez sur **Développeur**.
6. Si cette option n'est pas sélectionnée, cliquez sur **Afficher le sélecteur d'application dans l'en-tête** et fermez la fenêtre.
7. Dans la liste qui s'affiche en regard de `Administrateur système`, cliquez sur **Conteneur Vulnerability Response** pour le champ.

Rôle requis : admin ou atf_test_admin

Procédure

1. Accédez à la **Tout** > **Framework de tests automatisés (ATF)** > **Tests**.
2. Dans la liste Package, localisez **Vulnerability Response et Configuration Compliance for Containers**.
3. Sélectionnez un test pour ouvrir l'enregistrement.
4. Dans l'enregistrement ouvert, cochez la case **Actif** .
5. Dans la liste connexe Étapes de test, sélectionnez vrai dans la colonne Actif.
6. Cliquez sur **Mettre à jour**.
7. Ouvrez à nouveau le test et cliquez sur **Activer les tests et l'exécution de la suite de tests ici**.
8. Activez les propriétés du test/de la suite de tests et les propriétés de débogage des tests.
9. Cliquez sur **Enregistrer**.
10. Si le bouton **Exécuter le test** ne s'affiche pas, actualisez votre écran, ouvrez à nouveau l'enregistrement et cliquez sur **Exécuter le test** pour lancer le test.
    Au bout de quelques instants, la boîte de dialogue Exécuter le test indique que le test a réussi. Cliquez sur **Accéder au résultat pour plus d'informations** .

Que faire ensuite

Félicitations ! Vous pouvez poursuivre la configuration de Réponse aux vulnérabilités pour conteneurs.

Pour plus d'informations sur les tests automatisés et Réponse aux vulnérabilités pour conteneurs les tests automatisés, les suites de tests et la création de tests automatisés, consultez Infrastructure de tests automatisés (ATF).

Intégrer Réponse aux vulnérabilités pour conteneurs avec d'autres applications

Étendez les options de l'intégration Réponse aux vulnérabilités pour conteneurs avec d'autres applications.

Réponse aux vulnérabilités pour conteneurs S'intègre aux produits de sécurité des conteneurs pour extraire les données de vulnérabilité des images qui sont déployées pour l'exécution. Il enrichit ensuite les données de vulnérabilité avec les informations contextuelles d'exécution telles que les hôtes, les clusters Kubernetes, les services et les espaces de noms où ces images de conteneurs sont déployées. Avec la détection Kubernetes de ServiceNow, vous pouvez voir les références créées à partir des vulnérabilités vers les entités Kubernetes pertinentes dans votre Base de données de gestion des configurations (CMDB). En plus d'enrichir les métadonnées, ServiceNow offre également un tableau de bord de reporting complet pour fournir des informations sur les tendances de vulnérabilité et de correction.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités pour conteneurs fournit des intégrations avec les applications suivantes :

- Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute intégration
- Présentation de l'intégration Atlassian Jira avec Réponse aux vulnérabilités

> **Important :** Dans Vulnerability Manager Workspace, vous pouvez créer manuellement un problème Agile à l'aide de l'action de liste et de l'action de formulaire pour suivre le rattrapage des CVIT et des RT.

Notes supplémentaires pour les intégrations

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 2.1.2 de Réponse aux vulnérabilités pour conteneurs, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

> **Remarque :** Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :
>
> - *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
> - *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute intégration

L'intégration de Prisma Cloud Compute vous permet d'analyser les images de conteneurs pour détecter les vulnérabilités.

À partir de la version 16.1 du Réponse aux vulnérabilités, vous pouvez utiliser le dans l'application Réponse aux vulnérabilités pour conteneurs pour importer des Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute données de vulnérabilité d'image de conteneur pour les conteneurs déployés. Vous pouvez ensuite afficher des rapports sur les vulnérabilités et les éléments vulnérables sur les Réponse aux vulnérabilités tableaux de bord. Ces vulnérabilités peuvent ensuite être classées par ordre de priorité et corrigées.

Si le produit et votre Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud ComputeNow Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID. Pour plus d'informations, reportez-vous à la section Configuration requise pour le Serveur MID .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage des intégrations

Vous pouvez afficher les intégrations qui font partie du Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute. Pour afficher les intégrations, accédez à **Tout** > **Intégration des calculs dans le cloud Prisma** > **Intégrations**.

Les intégrations suivantes sont disponibles.

Exécuter la séquence	Calendrier	Intégration	Description
1	Quotidien	Intégration des images de base de calcul dans le cloud Prisma	Récupère les vulnérabilités pour les images de base à partir de l'API Prisma et signale les vulnérabilités des images de base séparément. Il crée également des résultats d'image et des éléments vulnérables, qui pointent vers les images de base.
2	Quotidien	Intégration des vulnérabilités des calculs dans le cloud Prisma	Récupère les vulnérabilités du conteneur. Crée des résultats et des CVIT ainsi que des images de conteneurs détectées.
3	Sur demande	Intégration des nombres de conteneurs de calcul dans le cloud Prisma	Récupère le nombre de conteneurs pour chaque image non de base.

Configuration de l'image de base dans Prisma

Dans la console Prisma, vous pouvez configurer le registre, puis configurer les images de base à partir de ces registres. Si une vulnérabilité est présente dans l'image de base, lorsque vous exécutez l'intégration des images de base de calcul dans le cloud Prisma, la case Image **de base** est cochée, ce qui indique que les vulnérabilités sont présentes dans l'image de base.

Configurer la granularité VI

Pour configurer la granularité des CVIT, accédez à **Tout** > **Conteneur Vulnerability Response** > **Configurer la granularité VI**et spécifiez les combinaisons de touches. Par défaut, un CVIT est créé pour une combinaison de référentiel d'images, de balise d'image et de vulnérabilité. Vous pouvez ajouter des composants supplémentaires à la clé pour plus de granularité. Par exemple, vous pouvez créer un CVIT pour une combinaison de référentiel d'images, de balise d'image, de vulnérabilité et de grappe.

Processus d'intégration Prisma

Lorsqu'il Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute est exécuté, il vérifie s'il existe une vulnérabilité et une exposition communes (CVE) dans la table Base de données de vulnérabilité nationale (NVD). Si elles sont déjà présentes, les informations existantes sont utilisées. Toutefois, si le CVE est introuvable, des enregistrements d'espace réservé sont générés dans la table NVD. Lors de la création de ces enregistrements NVD d'espace réservé, dans un premier temps, seuls le CVE et son nom sont renseignés. D'autres détails ne sont pas renseignés en supposant que l'intégration NVD

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

renseigne ces détails ultérieurement. Si le paramètre *update_nvd* d'instance d'intégration est défini sur vrai, il met à jour les enregistrements NVD de l'espace réservé. Par défaut, le paramètre d'instance est défini sur false. Toutefois, au moins jusqu'à ce que l'intégration NVD s'exécute et renseigne ces détails, une certaine compréhension des CVE, telles que leur gravité ou des informations de base sur le problème, est nécessaire. Pour répondre à cette exigence, les champs **Exploit exists (L'exploit existe**) et **Notes de rattrapage** sont renseignés avec les détails obtenus auprès de Prisma. De plus, cette configuration est personnalisable, ce qui vous permet de spécifier tous les autres champs que vous souhaitez renseigner dans l'entrée NVD en fonction des informations fournies par Prisma.

Se préparer à la Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute

Vous pouvez vous y préparer en Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute effectuant des tâches de configuration.

Avant de commencer

Pour installer et configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute , vous pouvez imprimer la liste de vérification suivante. Vérifiez que les éléments répertoriés sont terminés avant d'installer l'application et d'importer les données de vulnérabilité dans votre Now Platform® instance.

Liste de vérification de la préparation de l'intégration

Tâche	Description
☐	Vérifiez que vous disposez des ensembles d'informations suivants : • URL de base de l'API • Nom d'utilisateur et mot de passe. Ces informations d'identification sont utilisées pour extraire les vulnérabilités de l'intégration des calculs dans le cloud Prisma. Pour plus d'informations, voir https://pan.dev/compute/api/ **Remarque :** MID Server est facultatif. Les informations d'identification de l'utilisateur utilisées pour l'intégration des calculs dans le cloud Prisma ont besoin d'une autorisation pour surveiller les images. Consultez le code suivant : `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Si elle n'est pas déjà installée et activée, installez l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour en savoir plus sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 16.1 ou Réponse aux vulnérabilités ultérieure.
☐	Obtenez des autorisations et téléchargez l'application Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute sur votre Now Platform® instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
☐	Estimez le nombre d'éléments vulnérables que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance ou si vous avez besoin d'aide, contactez ServiceNow le support technique.
☐	Vérifiez que vous disposez des groupes ou utilisateurs suivants pour gérer les intégrations et corriger les éléments vulnérables : administrateur Installez l'application Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute. Si elle n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité de conteneur (sn_vul_container.vulnerability_admin) et d'autres rôles. sn_vul_container.vulnerability_admin Termine la configuration de l'intégration Prisma Cloud Compute. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités pour conteneurs (CVR) et à ses enregistrements. Cet administrateur configure les intégrations et les règles dans Réponse aux vulnérabilités pour conteneurs. Groupe Vulnerability Response Par défaut, le groupe Vulnerability Response est disponible. Les utilisateurs affectés au groupe Vulnerability Response héritent des sn_vul.read_all, sn_vul_container.read_all. Groupe de propriétaires de rattrapage de conteneurs Par défaut, le groupe de propriétaires de rattrapage de conteneurs est disponible. Les utilisateurs affectés à ce groupe héritent du sn_vul_container.remediation_owner. Le propriétaire de rattrapage de conteneur corrige les vulnérabilités de conteneurs qui lui sont affectées ou qui sont affectées à un groupe auquel il appartient. Analyste de vulnérabilité Les utilisateurs affectés au groupe d'analystes de vulnérabilité de conteneur héritent de sn_vul.vulnerability_analyst. L'analyste des vulnérabilités surveille le rattrapage de tous les éléments vulnérables. Si ce n'est pas déjà fait, vous pouvez créer des groupes supplémentaires et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance. Pour plus d'informations, consultez Créer un groupe d'utilisateurs .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
☐	Installez l'intégration Réponse aux vulnérabilités à NVD et exécutez l'API NIST National Vulnerability Database Integration (CVE uniquement).

Vous êtes prêt à Configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute.

Installer Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que le produit Prisma Cloud Compute s'intègre correctement à Réponse aux vulnérabilités pour conteneurs. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Rôle requis : administrateur

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez l'installer Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute .
2. Accédez au ServiceNow Store.
3. Dans le , recherchez Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute l'applicationServiceNow Store.
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Lisez les sections **Autres exigences** et **Dépendances** , si nécessaire.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Mettez à jour le **nom de l'instance** et **le motif pour les champs de l'instance** , puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Votre application est automatiquement installée sur votre instance.

Que faire ensuite
Configurez le Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute pour votre environnement. Consultez Configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute.

Configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute

Installez et configurez l'application Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Compute . Importez des données à partir de Prisma Cloud Compute. Vous pouvez utiliser les données importées pour classer par ordre de priorité et corriger les vulnérabilités de vos images Docker.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Ouvrez l'e-mail que vous avez reçu au sujet de ServiceNow l'intégration.
2. Connectez-vous à votre instance en tant qu'administrateur.
3. Suivez les instructions contenues dans l'e-mail pour obtenir le Intégration de Réponse aux vulnérabilités à Palo Alto Networks Prisma Cloud Computefichier .
4. Accédez à la **Tout** > **Intégration des calculs dans le cloud Prisma** > **Administration** > **Configuration**.
   Renseignez les champs du formulaire Configuration des calculs dans le cloud Prisma. Pour plus d'informations, consultez Formulaire Configuration des calculs dans le cloud Prisma.
5. Dans la liste Projets, sélectionnez **Tous les projets** ou **Projets spécifiques** pour configurer respectivement tous les projets ou les projets sélectionnés.
   Si vous sélectionnez **Projets spécifiques**, vous pouvez sélectionner les projets dans la liste Disponibles.
6. Terminez la configuration en cliquant sur **Terminer** ou sur **Enregistrer et tester les informations d'identification**.
   - Si vous avez configuré un projet, cliquez sur **Terminer**.
   - Si vous n'avez pas configuré de projet, cliquez sur **Enregistrer et tester les informations d'identification**
7. Affichez l'instance nouvellement créée en naviguant vers **Intégration des calculs dans le cloud Prisma** > **Administration** > **Instances d'intégration**.
8. Affichez les projets que vous avez configurés précédemment en cliquant sur **Paramètres d'instance d'intégration**.
9. Exécutez l'instance d'intégration nouvellement créée pour importer les données suivantes :
   - Images Docker : répertorie les images Docker, qui sont créées à l'aide d'un moteur d'identification et de rapprochement (IRE). Chaque image Docker fournit également des informations sur la relation entre les référentiels et les versions installées.
   - Images de conteneurs détectées : le module Images de conteneurs détectées fournit des informations sur l'ID d'image, l'image Docker et le référentiel d'images. Il stocke également les informations de la couche et les associe à l'image détectée. Vous pouvez également afficher les projets et le nombre de conteneurs ici. Pour une image de conteneur détectée, vous pouvez afficher les métadonnées dans le cloud telles que

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le fournisseur dans le cloud, la région dans le cloud, l'ID de compte dans le cloud et les ID de ressources dans le cloud.

- Packages d'images de conteneurs : fournit des informations sur les packages où se trouvent les vulnérabilités. Les détails du package binaire sont également fournis sous forme de valeurs séparées par des virgules.
- Couches d'images de conteneurs : cet écran affiche l'enregistrement de chaque couche d'image.
- Conclusions de l'image du conteneur : cet écran affiche la liste des résultats ainsi que des informations sur les vulnérabilités associées, la couche d'image, l'image Docker, le référentiel d'images et l'image détectée. Actuellement, les informations sur la vulnérabilité sont limitées à l'ID. Des informations supplémentaires sont renseignées lorsque l'intégration NVD est déclenchée.
- Éléments vulnérables du conteneur : chaque résultat a une vulnérabilité correspondante. Les CVIT sont ensuite créés en fonction de la granularité.

10. Configurez la granularité d'un élément vulnérable.

a. Accédez à la **Intégration des calculs dans le cloud Prisma** > **Configurer les clés de vulnérabilité de l'image**

b. Configurez la granularité des CVIT en cochant les cases requises.
Les éléments vulnérables sont créés en fonction des clés sélectionnées lors de l'importation suivante.

> **Remarque :** Par défaut, un CVIT est créé pour une combinaison de référentiel d'images, de vulnérabilité et de balise d'image. Vous pouvez ajouter des composants à la clé pour plus de granularité. Par exemple, vous pouvez créer un CVIT pour une combinaison de référentiel d'images, de vulnérabilité, de balise d'image et de grappe. Une fois que les éléments vulnérables ou les résultats d'éléments vulnérables sont créés, les cases à cocher ne sont plus modifiables.

Résolution des vulnérabilités du conteneur

Le rattrapage de surveillance est un processus qui commence par l'examen de l'état et se termine par la fermeture des éléments vulnérables du conteneur (CVIT). Réponse aux vulnérabilités pour conteneurs propose des outils et des procédures pour rendre ce processus plus productif et efficace.

Réponse aux vulnérabilités pour conteneurs Règles de calcul

Les calculateurs de vulnérabilité automatisent le calcul des valeurs initiales pour les champs des éléments vulnérables du conteneur. La condition de chaque calculateur est évaluée dans l'ordre, et le premier calculateur correspondant est utilisé.

Pour afficher et créer des calculateurs de vulnérabilité, accédez à **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Calculateurs de vulnérabilités**.

Le Réponse aux vulnérabilités pour conteneurs système de base comprend deux calculateurs de vulnérabilité qui définissent le score de risque de base sur l'élément vulnérable du conteneur. Les groupes de calculateurs suivants sont disponibles dans le système de base :

- Gravité de la vulnérabilité : calcule le score de risque pour les éléments vulnérables en utilisant la gravité de vulnérabilité normalisée.
- Calculateur de risque par défaut : il est basé sur la règle de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 2.10 de Réponse aux vulnérabilités pour conteneurs, en cas de :

- **Règle du calculateur de risque par défaut** : chaque fois que le score de risque d'un élément vulnérable du conteneur (CVIT) change, les détails suivants sont documentés dans la section Notes du CVIT :
  - Nom du groupe de calculateurs
  - Nom du calculateur
  - Valeurs de champ ayant une pondération supérieure à 1 et leur contribution au score de risque.
  - Score de risque final
- Règle de risque **de gravité** de la vulnérabilité : chaque fois que le score de risque est mis à jour sur un CVIT, la section **Notes** est mise à jour avec les détails suivants :
  - Nom du groupe de calculateurs
  - Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre parenthèses. Pour modifier ou afficher la base de la règle du calculateur, sélectionnez n'importe quelle règle et cochez la case Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. Si le **modèle** est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si **Script** est sélectionné, vous pouvez ajouter ou mettre à jour le script existant.

Poids du score du risque de vulnérabilité

Un score de risque et une évaluation sont attribués à toutes les vulnérabilités en fonction de facteurs tels que la gravité, la criticité, les informations d'exploitation, etc. La règle *`Update Risk Rating from Risk Score`* métier de la table des éléments vulnérables du conteneur est responsable du calcul de la cote de risque. Chaque fois que le score de risque change, la cote de risque est calculée et renseignée sur les éléments vulnérables du conteneur. Avant la version 17.1 de l'application Réponse aux vulnérabilités (VR), les évaluations de risque suivantes étaient fournies dans le cadre du script `include VulnerabilityUtils`, qui étaient codés en dur.

Valeur (cote de risque)	Poids (score de risque)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

À partir de la version 18.0 de Réponse aux vulnérabilités,

- Les types d'évaluation des risques sont envoyés dans la table de base Poids du score de risque [sn_sec_cmn_risk_scorew_weights] sous forme de cvr_risk_rating. Ces types sont transmis dans le cadre des règles métier ou des includes de script sur chaque table où la cote de risque est calculée.
- Le script est modifié afin que vous puissiez interroger les entrées dans les valeurs de la table Poids du score de risque pour le calcul de la cote de risque.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Ajoutez des entrées supplémentaires pour un type existant ou créez un nouveau type. Lorsque vous créez un nouveau type, assurez-vous d'ajouter les étiquettes pour la nouvelle cote de risque et de modifier les scripts et règles métier connexes. Vous devez également ajouter un nouveau style pour le nouveau score de risque.
- Modifiez le script pour interroger les enregistrements dans la table de base.

Vous pouvez accéder à la table des poids de score de risque en saisissant sn_sec_cmn_risk_score_weight dans le navigateur de filtre.

En outre, le score de risque est automatiquement recalculé dans les scénarios suivants :

- Lorsqu'un élément de configuration (CI) passe d'un mode non accessible sur Internet à un mode accessible sur Internet.
- Lorsque les vulnérabilités et expositions communes (CVE) ou les entrées tierces (TPE) associées sur les éléments de vulnérabilité (VI) sont liées à une vulnérabilité d'exploitation connue CVE (KEV).

Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.

Réponse aux vulnérabilités pour conteneurs Règles d'affectation

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

Pour créer et afficher des règles d'affectation pour les éléments vulnérables de conteneur. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles d'affectation**. Lorsque vous créez une règle d'affectation, vous pouvez définir les conditions. Lorsque ces conditions sont remplies, la règle affecte automatiquement les éléments vulnérables du conteneur au groupe d'utilisateurs sélectionné. Seule la première règle d'affectation avec une condition correspondante s'exécute sur un enregistrement.

Remarque : Les éléments vulnérables de conteneur qui ne sont pas à l'état Ouvert ou qui ont été affectés manuellement sont toujours exclus.

Pour plus d'informations, consultez Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

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

Réponse aux vulnérabilités pour conteneurs Règles de cibles de rattrapage

Les règles de cibles de rattrapage définissent le délai prévu pour le rattrapage d'un élément vulnérable du conteneur (CVIT). Ces règles sont similaires à la façon dont les SLA fournissent un délai pour corriger la vulnérabilité elle-même.

Pour créer et afficher des règles de cible de rattrapage pour les vulnérabilités du conteneur, accédez à **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles de cibles de rattrapage**.

Les règles de cible de rattrapage définissent le délai de rattrapage cible pour les éléments vulnérables du conteneur (CVIT) sélectionnés. Définissez une date limite pour le rattrapage

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de la vulnérabilité en sélectionnant le nombre de jours pour le rattrapage. Définir un rappel pour le rattrapage et définir les éléments vulnérables de conteneur auxquels la règle s'applique. Vous pouvez définir une cible de rattrapage pour les jours pendant lesquels elle doit être corrigée et définir un rappel avant d'approcher de la date cible. Pour plus d'informations, consultez Réponse aux vulnérabilités Règles de cibles de rattrapage.

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

Gestion des exceptions dans Réponse aux vulnérabilités pour conteneurs

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive de sécurité ou de gestion des vulnérabilités publiée, vous pouvez demander une exception. La gestion des exceptions implique de demander, examiner, approuver ou rejeter des exceptions à un élément vulnérable du conteneur (CVIT) qui ne peut pas être corrigé conformément à la politique.

Certaines vulnérabilités de conteneur (CVIT) peuvent ne pas disposer d'un correctif, d'un correctif ou d'une solution existante. Lorsqu'une exception est approuvée, cela signifie également que vous acceptez un risque, car vous reconnaissez et acceptez les conséquences de ne pas corriger la vulnérabilité.

Cycle de vie d'une exception

Définition d'une exception

Une exception est une demande de report du rattrapage d'un CVIT ou d'un RT pour une période spécifiée. Par exemple, en tant que propriétaire du rattrapage, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine.

Demande d'une exception

En tant que propriétaire du rattrapage, vous pouvez demander une exemption pour un CVIT ou un RT en utilisant le processus de gestion des exceptions. Une fois que l'approbateur d'exceptions a approuvé cette demande, le CVIT ou le RT passe à un état **Différé** .

Approuver une demande d'exception

Les CVIT ou les RT qui ne peuvent pas être corrigés immédiatement sont examinés par des analystes de vulnérabilité, évalués pour le risque et approuvés pour le report jusqu'à ce qu'ils puissent être corrigés. L'approbation d'une demande d'exception peut être un workflow à deux niveaux. Si seul l'approbateur de premier niveau est présent, l'exception peut être demandée et approuvée. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Consultez Ajouter un approbateur d'exception pour plus d'informations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

À partir de la Réponse aux vulnérabilités version 15.0, si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas le repasser en workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et des faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Une fois qu'une demande d'exception pour un CVIT ou un RT est approuvée, vous pouvez effectuer les actions suivantes :

- Rouvrir
- Supprimer
- Mettre à jour les champs **Affectation à** ou **Groupes d'affectation**

Suivi d'une demande d'exception

Après avoir émis l'exception, vous pouvez suivre son état à l'aide de l'onglet **Approbations de changement d'état** du CVIT ou du RT. Si une action est effectuée sur un RT, vous ne pouvez pas suivre l'état des CVIT individuels dans ce RT.

Expiration d'une demande d'exception

Lorsqu'une demande d'exception pour un CVIT ou un RT particulier expire, le CVIT ou le RT impacté revient à son état **Ouvert** .

Si une seule CVIT ou toutes les CVIT d'une RT passent à l'analyse suivante, les CVIT et, le cas échéant, le champ **État** de la RT basculent sur **Fermé** avec le sous-état **Fixe**.

Configurer les règles d'approbation

Affichez et configurez des règles d'approbation en accédant à **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles d'approbation**. Demandez une exception pour les CVIT qui ne peuvent pas être corrigés ou différés immédiatement, en identifiant les vulnérabilités impactées, les éléments de configuration (CI) ou les CVIT. Automatisez le processus de report du CVIT. Différez les CVIT correspondants en fonction de ces règles lorsque le système identifie ces CVIT.

Les règles d'approbation suivantes sont expédiées par défaut :

- Approbation des demandes d'exception : une configuration par défaut avec deux niveaux d'approbation est fournie dans le système de base. Chaque fois qu'il y a une demande d'exception sur un élément vulnérable, la demande d'approbation est envoyée aux utilisateurs ou groupes présents au niveau 1. Une fois approuvée par les approbateurs de niveau 1, elle est envoyée aux approbateurs de niveau 2.

Remarque : Vous pouvez modifier les niveaux par défaut et les modifier si nécessaire. À partir de la Réponse aux vulnérabilités pour conteneurs version 2.0.6, vous pouvez utiliser les propriétés système fournies dans le système de base pour les approbations d'exceptions via le workflow dans la table Propriétés système [sys_properties]. Ainsi, lorsqu'une demande d'exception ou de faux positif est émise via le workflow, elle est envoyée pour approbation aux ID de groupe définis dans la propriété système. Accédez à la **Tout** > **Propriétés système** et sélectionnez *sn_vul_container.container_exception_approver_L1*, *sn_vul_container.container_exception_approver_L2*ou *sn_vul_container.container_false_positive_approver_group* pour modifier la valeur de la propriété.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Approbation des règles d'exception : elle n'a pas de configuration mais deux niveaux d'approbation.
- Approbation des faux positifs : elle comporte une configuration avec un niveau d'approbation.

Remarque : À partir de la version 2.5 de Réponse aux vulnérabilités pour conteneurs, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable du conteneur passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage du conteneur revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

La demande et l'approbation d'une exception dans Réponse aux vulnérabilités pour conteneurs

Vous pouvez demander à différer le rattrapage d'un élément vulnérable du conteneur (CVIT) pendant une période spécifiée. Par exemple, en tant que développeur, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine. Les approbateurs qui y ont accès peuvent approuver les demandes d'autres utilisateurs.

Pour demander ou approuver une exception, consultez :

- Demander une exception pour un élément vulnérable de conteneur
- Demander une exception pour les vulnérabilités du conteneur à l'aide de GRC : gestion de la politique et de la conformité

Remarque :

Des notifications par e-mail sont envoyées à chaque étape de la gestion des exceptions, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'une exception est demandée, le demandeur reçoit un e-mail confirmant que la demande est émise. L'approbateur reçoit également un e-mail l'informant qu'une exception a été demandée. À partir de la version 2.5 de Réponse aux vulnérabilités pour conteneurs, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable du conteneur passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage du conteneur revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Demander une exception pour un élément vulnérable de conteneur

Demandez une exception pour un élément vulnérable de conteneur (CVIT) qui ne peut pas être corrigé immédiatement. Par exemple, en tant que propriétaire du rattrapage, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine.

Avant de commencer

Rôle requis : groupe de développeurs

Pourquoi et quand exécuter cette tâche

Vous pouvez demander une exception pour plusieurs CVIT simultanément à l'aide de la fonction de modification en bloc du Espace de travail du gestionnaire de vulnérabilités. Pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

plus d'informations, consultez Demander une exception en bloc dans Vulnerability Manager Workspace.

Procédure

1. Accédez à la **Conteneur Vulnerability Response** > **Éléments vulnérables de conteneurs** > **Tout**.
2. Sélectionnez l'élément pour lequel vous souhaitez demander une exception. L'élément sélectionné doit être à l'état Ouvert ou En cours d'examen.
3. Sur le formulaire Élément vulnérable de conteneur, cliquez sur **Demande d'exception**.

4.a. Renseignez les champs du formulaire.

Formulaire Demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée sélectionnée dans le **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Gestion des exceptions** écran. Lorsque la demande d'exception expire, le groupe revient à son état Ouvert. **Remarque :** À partir de la version 1.2 de Réponse aux vulnérabilités pour conteneurs, si un élément vulnérable a été différé pour correction à l'aide de la fonctionnalité de gestion des exceptions, la date de report définie sur la vulnérabilité persistera au cas où il serait rouvert par l'analyseur. Pour activer cette fonctionnalité, définissez la valeur de la propriété *sn_vul.container.auto_defer_cvit_in_active_e* système sur vrai. De plus, la date de fin de report persiste même après la fermeture du CVIT ou l'expiration de l'exception. Le rôle requis est sn_vul_container.manage_exception_configuration pour la lecture et l'écriture.
Motif	Raison de l'exception. Les choix sont les suivants : ▪ Risque accepté ▪ En attente de fenêtre de maintenance ▪ Correctif non disponible ▪ Contrôle d'atténuation en place ▪ Autre

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à la section Définir un mappage de motif de politique.
Informations supplémentaires	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ doit être mis à jour par le propriétaire du rattrapage.

b. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**. L'état de l'élément vulnérable du conteneur passe à En cours de révision. Utilisez l'onglet **Approbation de changement d'état** pour suivre l'état de la demande d'exception.

Demander une exception pour une tâche de rattrapage de conteneur

Demandez une exception pour différer une tâche de rattrapage de conteneur pendant une période spécifiée si elle ne peut pas être résolue immédiatement.

Avant de commencer

Vous pouvez demander des exceptions à partir Réponse aux vulnérabilités des espaces de travail. Consultez Demander une exception dans le Espace de travail de remédiation IT.

Rôle requis :

sn_vul.remediation_owner, sn_vul.app_security_champion ou sn_vul_container.remediation_owner.

Vous pouvez également demander des exceptions pour les tâches de rattrapage de conteneurs dans l'environnement classique.

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Tâches de rattrapage** > **Tout**.
2. Sélectionnez le groupe pour lequel vous souhaitez demander une exception. La tâche sélectionnée doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Dans l'enregistrement de tâche de rattrapage de conteneur, sélectionnez **Demande d'exception**.
4. Renseignez les champs du formulaire.

Formulaire Demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée d'exception définie dans la configuration.
Motif	Justification de la demande d'exception.
Informations supplémentaires	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	doit être mis à jour par le propriétaire du rattrapage.

5. Cliquez sur **Demander l'approbation**.

Demander une exception pour les vulnérabilités du conteneur à l'aide de GRC : gestion de la politique et de la conformité

Demandez des exceptions de politique à l'aide de l'option GRC de gestion des exceptions de politique de l'application à partir de .Gestion de la politique et de la conformitéRéponse aux vulnérabilités pour conteneurs

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions de politique, vous devez télécharger l'application GRC : gestion de la politique et de la conformité à partir du ServiceNow Store.

Rôle requis : sn_vul.remediation_owner

Vous pouvez également demander des exceptions dans l'interface utilisateur classique :

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Éléments vulnérables de conteneurs** (ou **Tâches de rattrapage**)>**Tous**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.
   L'élément ou le groupe sélectionné doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Sur le formulaire sélectionné, cliquez sur **Demande d'exception**.

   Remarque : Si GRC : gestion de la politique et de la conformité cette option est sélectionnée dans l'écran Gestion des exceptions, renseignez les champs du formulaire Demande d'exception. Pour plus d'informations sur les champs de formulaire, consultez Formulaire Demande d'exception.

   a. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**.
   L'état des éléments vulnérables passe à En cours de révision et une exception de politique est créée. Utilisez l'onglet **Approbation de changement d'état** pour suivre l'état de la demande d'exception.

   b. Affichez l'exception de politique en cliquant sur la liste connexe Exceptions de politique.

   c. Cliquez sur le numéro d'exception de politique.

   d. Dans le champ **Approbateur** , sélectionnez le nom de l'approbateur.

   e. Cliquez sur l'onglet Source et sélectionnez un objectif de contrôle dans le champ **Objectif de contrôle** .

   f. Cliquez sur l'onglet Évaluation des risques et sélectionnez l'évaluation des risques dans le champ **Évaluation des risques** .

   g. Enregistrez le formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

h. Cliquez sur l'onglet **Contrôles concernés** .

i. Ajoutez les contrôles en cliquant sur **Ajouter**.

j. Enregistrez le formulaire.

Remarque : Vous pouvez soumettre un examen de conformité en cliquant sur **Demander un examen de conformité**.

Le formulaire d'approbation est envoyé à l'approbateur.

L'approbateur peut approuver la demande en cliquant sur **Approuver** ou demander une approbation supplémentaire en cliquant sur **Demander une approbation supplémentaire**.

L'état de l'enregistrement devient Différé. Le motif indiqué est celui que vous avez sélectionné lors de l'émission de la demande d'exception. L'onglet **Report** fournit des notes supplémentaires sur l'enregistrement.

Remarque : Si la demande est rejetée, l'enregistrement passe à son état précédent.

3. Cliquez sur **Envoyer**.
Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez la configuration facultative de Gestion de la politique et de la conformité .

Définir un mappage de motif de politique

Définissez les choix de motifs afin qu'ils soient disponibles pour tout utilisateur qui demande une exception.

Avant de commencer

Rôle requis : sn_vul.compliance.manager et sn_vul_container.manage_exception_configuration

Procédure

1. Accédez à la **Tout** > **Politique et Conformité** > **Exceptions de politique** > **Registre d'intégration**.

Remarque : Vous pouvez sélectionner un motif parmi les choix de motifs disponibles dans la table Choix du motif ou ajouter un nouveau motif.

2. Cliquez sur le registre d'intégration de Container Vulnerability Response - CVIT.
3. Dans la liste Choix du motif, cliquez sur **Nouveau**.
4. Cliquez sur l'icône de la loupe.
5. Ajoutez un choix de motif existant pour en créer un nouveau.
   - Si vous souhaitez ajouter un choix de motif existant, sélectionnez un motif.
   - Si vous souhaitez ajouter un nouveau choix de motif à la table Choix du motif, cliquez sur **Nouveau** et renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de liste de choix de motifs

Champ	Description
Étiquette	Étiquette unique pour ce choix.
Valeur	Valeur unique pour ce choix. Cette valeur est mappée dans la table de mappage des motifs de politique pour les applications respectives. Pour accéder à cette table, saisissez `sn_vul_policy_reason_mapping. LIST` dans le navigateur de filtre.
Ordre	Ordre pour ce choix. Les motifs sont classés en fonction de ce nombre.
Par défaut	Option pour indiquer que ce choix de motif sera disponible chaque fois qu'une exception de politique sur demande est demandée. Si le registre d'intégration ne contient pas de choix spécifiques à l'application, tous les choix de motif pour lesquels le champ **Par défaut** est sélectionné sont disponibles.
Actif	Option permettant d'afficher le choix dans la liste des choix de motifs.

6. Cliquez sur **Envoyer**.

Résultats

Le choix du motif est ajouté. Le choix du motif est disponible dans le champ **Motif** du formulaire de demande d'exception de politique pour l'application sélectionnée.

Approuver une demande d'exception dans Réponse aux vulnérabilités pour conteneurs

Approuvez les demandes d'exception pour les éléments vulnérables de conteneurs ou les tâches de rattrapage qui ne peuvent pas être corrigés immédiatement. Vous devez évaluer les risques de ces demandes, puis approuver leur report jusqu'à ce qu'elles puissent être corrigées.

Avant de commencer

Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche

Vous pouvez approuver les demandes d'exception et de faux positif dans le Espace de travail du gestionnaire de vulnérabilités. Consultez Approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilités.

Vous pouvez également approuver les demandes d'exception dans l'environnement classique :

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Différer un élément vulnérable de conteneur dans Réponse aux vulnérabilités pour conteneurs

Si vous déterminez que le problème associé à un élément vulnérable de conteneur (CVIT) présente un risque faible et peut être différé immédiatement sans analyse supplémentaire, vous pouvez utiliser la fonctionnalité **Différer** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Une tâche planifiée s'exécute tous les jours pour vérifier les éléments vulnérables différés qui ont atteint leur date de réouverture. Le jour où le report du CVIT doit expirer, le dossier est rouvert.

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Éléments vulnérables de conteneurs**.
2. Ouvrez un élément vulnérable.
3. Cliquez sur **Demander une exception**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Jusqu'à	Sélectionnez la date à laquelle l'état Différé expire et à laquelle la tâche de rattrapage est réactivée. **Remarque :** À compter de la version 18.0 de Réponse aux vulnérabilités pour conteneurs, si un élément vulnérable de conteneur différé (CVIT) est fermé et rouvert par un scanner avant l'expiration de la fenêtre d'exception, l'état du CVIT revient à l'état Différé, honorant la fenêtre d'exception active. Pour activer cette fonctionnalité, définissez la valeur de la propriété *sn_vul.container.auto_defer_cvit_in_active_ex* système sur vrai. De plus, la date de fin de report persiste même après la fermeture de l'élément vulnérable ou l'expiration de l'exception. Le rôle requis est sn_vul_container.manage_exception_configuration pour la lecture et l'écriture. Une fois l'enregistrement soumis, si des notifications par e-mail sont définies, les membres du groupe reçoivent un e-mail lorsque la Réponse aux vulnérabilités pour conteneurs date d'expiration est inférieure à une semaine. Lorsque la date de report

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	expire, l'élément vulnérable est remis en état Ouvert et une deuxième notification par e-mail est envoyée.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Faux positif ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Informations supplémentaires	Saisissez toute autre information pertinente.

5. Cliquez sur **Envoyer**.
   Le groupe est marqué **comme En cours de révision**. Un lien **connexe Rouvrir** s'affiche. La date et le motif de réouverture apparaissent dans les notes de travail sous l'onglet **Approbations de changement d'état** .

   À partir de la Réponse aux vulnérabilités pour conteneurs version 2.3, vous pouvez ajouter des informations pertinentes dans le champ Notes de travail de la section Notes pour un élément vulnérable de conteneur différé.

Demander une extension pour un élément vulnérable de conteneur différé

Demandez une extension pour un élément vulnérable de conteneur différé avant qu'il n'atteigne sa date de report jusqu'à échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche
Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités.

Procédure
1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Éléments vulnérables de conteneurs**.
2. Ouvrez un élément vulnérable de conteneur différé.
3. Sélectionnez **Demande d'extension**.

   Remarque : Le bouton Demande d'extension n'est visible que lorsque l'état de l'élément vulnérable du conteneur est Différé.

4. Renseignez les champs du formulaire comme il convient.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle l'élément vulnérable de conteneur différé doit être prolongé pour le rattrapage.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Informations supplémentaires	Saisissez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Un e-mail est déclenché lors de l'envoi de la demande et de l'action ultérieure de l'approbateur.

   Remarque :

   - La demande passe par deux niveaux d'approbation.
   - Si un élément vulnérable de conteneur différé est à nouveau étendu, le nombre de reports d'extension augmente dans le back-end.

6. Une fois la demande approuvée, les notes Jusqu'à, Motif et Report sont mises à jour.

Utiliser une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Vous pouvez demander une exception pour les éléments vulnérables de conteneurs (CVIT) qui ne peuvent pas être corrigés ou différés immédiatement. En automatisant le processus de report des VI, vous pouvez différer les CVIT correspondants en fonction de la règle lorsque le système les identifie.

Vous pouvez effectuer les tâches suivantes pour une règle d'exception :

- Créer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs
- #unique_626
- L'activation d'une règle d'exception dans Réponse aux vulnérabilités pour conteneurs
- Rouvrez une règle d'exception dans Réponse aux vulnérabilités pour conteneurs
- Mettre à jour une règle d'exception approuvée dans Réponse aux vulnérabilités pour conteneurs
- Supprimer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs
- Différer un élément vulnérable de conteneur dans Réponse aux vulnérabilités pour conteneurs

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 2.5 de Réponse aux vulnérabilités pour conteneurs, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable du conteneur passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage du conteneur revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Créer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Créez une règle pour demander automatiquement une exception pour une condition spécifique pour un groupe d'éléments vulnérables de conteneurs (CVIT), telle qu'une règle avec une condition basée sur la gravité de vulnérabilité de ces CVIT. Avec cette règle, vous pouvez différer automatiquement les CVIT nouveaux et existants s'ils correspondent à la condition de règle approuvée.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
La règle s'applique à partir de la date « Valide à partir de » jusqu'à la date « Valide jusqu'à ». La tâche de rattrapage (VUL) est créée lorsque la règle est approuvée. La méthode de regroupement de cette vulnérabilité est connue sous le nom de règles d'exception. La vulnérabilité est créée à l'état Différé. Vous ne pouvez pas fermer, rouvrir ou supprimer ce VUL. Les CVIT nouveaux et rouverts sont différés et ajoutés à cette VUL à partir de la date de début de validité jusqu'à l'expiration du groupe à la date de fin de validité.

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de la règle d'exception. Ces e-mails fournissent l'état et d'autres détails d'une demande. Par exemple, lorsqu'une règle d'exception est demandée, le demandeur reçoit un e-mail qui confirme que la demande est envoyée.

Remarque : Si la règle est rejetée, vous pouvez la rouvrir à l'état Brouillon, la mettre à jour, puis la soumettre à nouveau pour approbation.

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles d'exception**.
2. Sur la page d'enregistrement Nouvelle règle d'exception, cliquez sur **Nouveau** pour créer une règle.
3. Renseignez les champs du formulaire Règle d'exception.

   Remarque : Pour plus d'informations sur les champs de formulaire, consultez Formulaire Règle d'exception.

4. Ajoutez le groupe d'affectation lors de la création de la règle.
5. Envoyez le formulaire pour approbation.
   L'état de la demande passe à En cours de révision. Tant que vous n'avez pas soumis la règle d'exception, elle reste à l'état Brouillon.
6. Pour afficher et créer un groupe afin de gérer les règles d'exception :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Tout** > **Administration utilisateurs** > **Groupes**.

b. Dans une règle d'exception, cliquez sur l'onglet **Approbations demandées** pour afficher l'état de la demande.
Une tâche planifiée est exécutée quotidiennement, qui exécute les règles d'exception sur les données existantes. Tous les éléments vulnérables qui correspondent à la condition passent à l'état Différé. Si une règle d'exception approuvée est supprimée, tous les éléments vulnérables différés reviennent à leur état précédent. Pour plus d'informations, consultez Utilisation d'une règle d'exception.

L'activation d'une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Une règle est activée à sa date de début de validité. Après activation, il automatise le processus d'exception pour les éléments vulnérables du conteneur (CVIT).

La règle d'exception suit le cycle de vie suivant :

1. Les nouveaux CVIT que vous créez ou rouvrez et qui remplissent la condition spécifiée sont reportés. Si vous activez l'option Exécuter sur les données existantes lors de la première exécution de la règle d'exception, tous les CVIT actifs et non différés qui correspondent à la condition de la règle d'exception sont déplacés vers la tâche de rattrapage (RT) nouvellement créée et son état passe à Différé.
2. Si un CVIT nouvellement créé correspond à la condition de la règle d'exception, il est déplacé vers le RT différé qui est associé à la règle et la règle de groupe n'est pas exécutée dessus.
3. À la date de début de validité, les CVIT existants sont ajoutés si vous activez l'option Exécuter sur les données existantes.
4. Le RT cesse d'accepter de nouveaux CVIT lorsque la règle expire à la date de fin de validité. Le RT reste en vigueur jusqu'à la date « Différé jusqu'à ».
5. La règle d'exception expire à la date de fin de validité.

Rouvrez une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Rouvrez une règle d'exception qui a été rejetée, mais que vous souhaitez soumettre à nouveau. La réouverture de la règle la fait passer à l'état Brouillon.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Vous pouvez ensuite mettre à jour et soumettre à nouveau la règle pour approbation.

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles d'exception**.
2. Recherchez la règle que vous souhaitez rouvrir et cliquez sur **Rouvrir**.
3. Mettez à jour le formulaire et soumettez-le à nouveau pour approbation.

Mettre à jour une règle d'exception approuvée dans Réponse aux vulnérabilités pour conteneurs

Annulez une règle approuvée pour pouvoir la mettre à jour. Par exemple, avant de pouvoir modifier des dates ou ajouter une condition à une règle approuvée, vous devez l'annuler

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

afin que la tâche de rattrapage (VUL) soit supprimée et que les éléments vulnérables du conteneur (CVIT) passent à l'état Ouvert.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Les règles de groupe sont réappliquées à ces CVIT. Soumettez la règle après avoir apporté les modifications afin qu'elle passe à nouveau par le processus d'approbation.

Procédure
1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles d'exception**.
2. Ouvrez la règle d'exception que vous souhaitez annuler, puis cliquez sur **Annuler**.
3. Dans la boîte de dialogue Annuler la règle, cliquez sur **Annuler la règle**.
   La règle revient à l'état Brouillon et le VUL associé est supprimé. Les CVIT connexes sont rouverts et des règles de groupe sont appliquées aux CVIT individuelles.

Supprimer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Supprimez une règle d'exception qui n'est plus requise. Par exemple, vous pouvez supprimer une règle si vous ne souhaitez pas différer un élément vulnérable de conteneur (CVIT) pendant l'ingestion.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
La suppression d'une règle annule la tâche de rattrapage associée (VUL). Les CVIT connexes sont rouverts et des règles de groupe sont appliquées aux CVIT individuelles.

Procédure
1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles d'exception**.
2. Ouvrez la règle d'exception que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue Supprimer la règle, cliquez sur **Supprimer la règle** pour supprimer la règle sélectionnée.
   La tâche de rattrapage associée est également supprimée. Les CVIT connexes sont rouverts et des règles de groupe sont appliquées aux CVIT individuelles.

Demander une prolongation pour une tâche de rattrapage différée dans Réponse aux vulnérabilités pour conteneurs

Demandez une prolongation pour une tâche de rattrapage différée (VUL) avant qu'elle n'atteigne sa date de report jusqu'à l'échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche
Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Tâches de remédiation**.
2. Ouvrez une tâche de rattrapage différée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date à laquelle l'état Différer expire et à laquelle l'élément vulnérable du conteneur est réactivé.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Informations supplémentaires	Saisissez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les changements apportés à la tâche de rattrapage sont également étendus aux éléments vulnérables du conteneur, qui font partie de la tâche de rattrapage. Toutefois, les éléments vulnérables du conteneur doivent être dans l'état Différé et leur date actuelle jusqu'à ce que les données précèdent la date de fin de mise à jour. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure de l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une tâche de rattrapage différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

Demander une extension pour une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Demandez une prolongation pour une règle d'exception différée avant qu'elle n'atteigne sa date de report jusqu'à échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.exception_approver

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités.

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Règles d'exception**.
2. Sélectionnez une règle d'exception différée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle la règle d'exception doit être prolongée.
Motif	Entrez le motif du report de la règle d'exception. Les choix sont les suivants : ◦ Risque accepté ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Contrôle d'atténuation en place ◦ Autre
Informations supplémentaires	Saisissez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les champs Différé jusqu'à, Motif et Informations supplémentaires sont mis à jour sur la règle d'exception et les éléments vulnérables du conteneur. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure de l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une règle d'exception différée est à nouveau étendue, le nombre de reports prolongés augmente dans le back-end.

Marquage et approbation d'un élément de vulnérabilité de conteneur faux positif

Les éléments vulnérables de conteneurs (CVIT) et les tâches de remédiation (VUL) peuvent être marqués comme faux positifs. Les approbateurs ayant un accès en écriture peuvent approuver ces demandes de la part d'autres utilisateurs.

- Marquer comme faux positif dans Réponse aux vulnérabilités pour conteneurs
- Approuver un faux positif

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de faux positif, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'un CVIT ou une tâche de rattrapage est marqué comme faux positif, le demandeur reçoit un e-mail de confirmation. Simultanément, l'approbateur reçoit un e-mail indiquant qu'un CVIT ou une tâche de rattrapage a été marqué comme faux positif. À partir de la version 2.5 de Réponse aux vulnérabilités pour conteneurs, vous pouvez configurer les délais d'approbation des faux positifs et des exceptions, ainsi que des notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable du conteneur passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage du conteneur revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Important : En tant qu'analyste de vulnérabilité et propriétaire du rattrapage, vous pouvez demander et approuver des faux positifs à partir de l'espace de travail du gestionnaire de vulnérabilité et de l'espace de travail de rattrapage informatique respectivement.

Marquer comme faux positif dans Réponse aux vulnérabilités pour conteneurs

Marquez un élément vulnérable du conteneur (CVIT) ou une tâche de rattrapage comme faux positif si l'avertissement donné par le scanner n'est pas réellement un problème. Par exemple, si un CVIT a été mis hors service, mais que le scanner soulève toujours un problème qui lui est lié, marquez-le comme faux positif.

Important : En tant qu'analyste de vulnérabilité et propriétaire de la correction, vous pouvez demander des faux positifs à partir de l'espace de travail du gestionnaire de vulnérabilité et de l'espace de travail de remédiation informatique respectivement.

Avant de commencer

Rôle requis : propriétaire de la résolution

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response (ou tâches de remédiation)** > **Tout**.
2. Ouvrez le CVIT que vous souhaitez marquer comme faux positif et cliquez sur **Marquer comme faux positif**.
   Le CVIT doit avoir l'état **Ouvert** .
3. Sur le formulaire Faux positif, saisissez les détails dans **Informations supplémentaires** et cliquez sur **Demander l'approbation**.
   La demande est envoyée pour approbation et l'état du CVIT passe à **En cours de révision**.
   Le demandeur et l'approbateur sont informés par e-mail.

Approuver un faux positif

En tant qu'approbateur de faux positif, vous pouvez approuver les demandes de faux positif d'autres utilisateurs.

Important : Vous pouvez approuver ou rejeter des demandes de faux positif dans le Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : false_positive_approver
Vous pouvez également approuver les demandes d'exception et de faux positif dans l'environnement classique :

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

> **Remarque :** Un faux positif peut être limité dans le temps. Seul l'approbateur peut définir la date de fin.

Vue d'ensemble des tâches de remédiation et des règles de tâche de Container Vulnerability Response

Configurez les tâches de rattrapage (CVUL) pour aider les analystes et les spécialistes du rattrapage à organiser les éléments vulnérables du conteneur (CVIT) et à les analyser en bloc. Les critères selon lesquels les tâches de rattrapage sont formées sont configurés de telle sorte que les CVIT soient automatiquement affectés à des tâches de rattrapage. Les tâches de rattrapage vous permettent de surveiller la progression et de piloter le processus de rattrapage plus efficacement.

Suivi des nombres de reports pour les éléments vulnérables de conteneurs et les tâches de rattrapage

Suivez le nombre de fois où un élément vulnérable, un élément vulnérable d'application, un élément vulnérable de conteneur ou une tâche de rattrapage est différé. La tâche planifiée Définir les nombres de reports s'exécute quotidiennement pour publier les nombres des enregistrements qui sont différés plus d'une fois dans la colonne Nombre de reports. Les enregistrements s'affichent dans les modules Reports multiples pour VR, AVR et CVR.

Présentation des règles de tâche de rattrapage

Les règles de tâche de rattrapage vous permettent de définir la manière dont les éléments vulnérables des conteneurs sont automatiquement regroupés et affectés. Une règle par défaut **La vulnérabilité** est incluse dans le système de base qui recueille les CVIT en fonction de leurs vulnérabilités. Toutefois, vous pouvez effectuer un regroupement par n'importe quel autre ensemble de valeurs dans des colonnes accessibles à partir du CVIT. Ces valeurs peuvent inclure l'élément de configuration (CI), l'entrée de vulnérabilité, etc.

Il existe des règles de tâche pour Container Vulnerability Response qui sont incluses dans l'application Vulnerability Response disponible lorsque vous l'activez.

Vous pouvez créer plusieurs conditions à l'aide du Créateur de conditions. Dans la section Grouper par, une fois que vous avez défini une paire de champs, une autre ligne apparaît. Vous pouvez avoir jusqu'à six **sélections Grouper par** . Vous pouvez également automatiser l'affectation de groupe.

Par exemple, vous pouvez regrouper vos éléments vulnérables de conteneur par élément de configuration ou par modèle de produit. Vous pouvez avoir une règle de tâche pour les vulnérabilités de faible gravité ou les CI à faible risque. Vous pouvez avoir une autre règle de tâche pour les serveurs critiques et les vulnérabilités qui exposent l'entreprise à plus de risques. Consultez Créer, modifier et supprimer des règles de tâche de rattrapage de Container Vulnerability Response pour plus d'informations sur les options qui s'offrent à vous.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un ensemble différent de règles peut être utilisé pour les éléments vulnérables du conteneur qui exposent la société à davantage de risques. Le nom de la tâche de rattrapage est ajouté à la règle de la tâche de rattrapage **Grouper par** valeurs pour créer la description brève du nouvel enregistrement.

Lorsqu'un nouvel élément vulnérable de conteneur est créé, importé ou rouvert après avoir été fermé, les règles sont évaluées en fonction de celui-ci. Une CVIT n'est évaluée qu'une seule fois, automatiquement, à moins qu'elle ne soit rouverte après avoir été fermée ou que les règles ne soient réappliquées manuellement.

Le processus suivant est utilisé pour chaque CVIT nouvelle ou rouverte :

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

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

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

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

Plusieurs règles de tâche de rattrapage peuvent être définies pour regrouper différents types de vulnérabilités. Étant donné que chaque vulnérabilité est comparée aux conditions de règles de tâche de rattrapage avant de la placer dans une tâche de rattrapage, un trop grand nombre de règles peut avoir un impact sur les performances. Configurez vos règles de tâche afin que les conditions vous aident à éviter de créer des tâches de rattrapage en double.

Par défaut, les règles de tâche de rattrapage utilisent le groupe d'affectation défini par les **règles d'affectation** sur le CVIT lors du regroupement des éléments et affectent la tâche de rattrapage pour qu'il corresponde aux CVIT.

Dans le cadre de la règle de tâche par défaut, l'affectation de ces tâches de rattrapage est contrôlée par les règles du module **Règles d'affectation** . Pour plus d'informations sur les règles d'affectation, consultez Vue d'ensemble des règles d'affectation de Vulnerability Response.

Lorsqu'une règle de tâche est supprimée du formulaire ou de la vue de liste, vous avez la possibilité de supprimer toutes les tâches ouvertes créées par cette règle. Les tâches qui ne sont pas dans l'état **ouvert** sont exclues.

Réapplication des règles de tâche de rattrapage

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

Réappliquer vérifie uniquement les tâches de rattrapage existantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois que vous avez sélectionné **Réappliquer**, le message suivant s'affiche : La réapplication de cette règle de tâche de rattrapage supprimera et recréera les tâches de rattrapage pour cette règle. Les tâches de rattrapage qui ne sont pas dans l'état ouvert ne sont pas supprimées.

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

Règles de tâche de rattrapage et création et mise à jour de CVIT

Si un CI d'une analyse est associé à une vulnérabilité connue, une CVIT est créée. Une fois créé, le CVIT est évalué par rapport aux conditions des règles de tâche de rattrapage d'une correspondance. S'il existe une correspondance avec une tâche de rattrapage existante, le CVIT est ajouté. Si aucune tâche de rattrapage correspondante n'est trouvée, une tâche est créée pour le CVIT.

Si une propriété capturée dans les conditions de filtrage de la tâche de rattrapage est mise à jour ou modifiée dans un CVIT, l'AVI mis à jour est également évalué par rapport aux règles de la tâche de rattrapage pour une correspondance. S'il existe une correspondance avec une tâche de rattrapage existante, le CVIT est ajouté. Si aucune tâche de rattrapage correspondante n'est trouvée, une tâche est créée pour le CVIT.

Déploiement d'état et déploiement

Si vous mettez à jour une tâche de rattrapage sur Ouvert, ou d'Ouvert à En cours d'examen, le nouvel état s'étend à tous les CVIT associés. La restauration d'état se produit immédiatement après la modification de l'état.

Le déploiement d'état des CVIT vers la tâche de rattrapage ne se produit que si tous les CVIT de la tâche sont à l'état **Différé** ou **Fermé (fixe**). Le déploiement s'effectue avec le déploiement des valeurs d'éléments vulnérables de conteneur vers la vulnérabilité et une tâche planifiée par le groupe, qui s'exécute toutes les 15 minutes. L'état n'est pas déployé tant que la tâche n'est pas exécutée. Pour qu'un état se déploie entre les CVIT et la tâche de rattrapage, toutes les CVIT doivent être dans le même état.

Créer, modifier et supprimer des règles de tâche de rattrapage de Container Vulnerability Response

Vous pouvez créer des règles pour regrouper automatiquement les éléments vulnérables du conteneur (CVIT) dans des tâches de remédiation (CVUL) en fonction des conditions de filtre. Ces règles regroupent automatiquement les CVIT au fur et à mesure qu'elles sont importées ou créées manuellement.

Avant de commencer

Si vous créez une nouvelle règle, elle ne s'applique pas aux données existantes. Une fois que vous l'avez soumis, il est exécuté par rapport aux nouvelles importations.

Rôle requis : App-Sec Manager

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles de tâche de rattrapage.**.
2. Ouvrez la règle ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire ou modifiez-les.

Règle de la tâche de rattrapage

Champ	Description
Nom	Nom de la règle de tâche.
Actif	Indique si la tâche est active.
Description	Description de la règle.
Sensible à la casse	Détermine si une condition est sensible à la casse ou non. **Remarque :** La valeur par défaut n'est pas sensible à la casse.
Condition	Conditions de filtre facultatives pour la règle. Par défaut (case **sensible à la casse** non cochée), le texte de recherche que vous saisissez dans le générateur de conditions sur les enregistrements et formulaires de règles de tâche n'est pas sensible à la casse. Vous pouvez activer les recherches sensibles à la casse sur les enregistrements de tâches et les formulaires. Voici un exemple de condition **Vulnérabilité** > **est** > **VULNENT123451** (une vulnérabilité importée connue). Tous les CVIT présentant cette vulnérabilité correspondent à cette condition.
Grouper par (jusqu'à six ensembles de conditions sont disponibles)	
Regrouper les éléments vulnérables de conteneurs à partir de	Table que la règle utilise pour regrouper les CVIT. Sélectionner les éléments de l'arborescence : ◦ Élément vulnérable de conteneur [sn_vuln_vulnerable_item] ◦ Élément vulnérable de conteneur : image de Docker ◦ Élément vulnérable de conteneur : vulnérabilité de conteneurs

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si vous choisissez une table étendue, le **champ Utilisation** n'est appliqué qu'aux éléments vulnérables de l'application qui utilisent cette table étendue.
Utilisation du champ	Champ de la table que la règle utilise pour regrouper les CVIT. Sélectionnez des conditions dans l'arborescence.
Affectation	
Affecter la tâche de rattrapage par	Lors de l'affectation automatique des tâches de rattrapage, le choix Affectation est utilisé en plus des choix **Grouper par** pour regrouper les éléments vulnérables. De nouvelles tâches sont créées, selon les besoins, de sorte que chaque CVIT est placé dans une tâche avec un ensemble de groupes d'affectation correspondants. Pour automatiser l'affectation des tâches créées en fonction de cette règle, choisissez l'une des options disponibles. ◦ Regrouper par champ : si vous avez sélectionné un champ de groupe d'utilisateurs à partir des valeurs du **champ Utilisation** dans la section **Grouper par** , il apparaît dans le menu déroulant. ◦ Groupe d'utilisateurs : utilisez la liste de recherche pour sélectionner un groupe d'utilisateurs statique.

Remarque : Si vous supprimez une règle de la vue de formulaire ou de la vue de liste, vous avez la possibilité de supprimer toutes les tâches de rattrapage ouvertes créées par cette règle. Les groupes qui ne sont pas dans l'état Ouvert sont exclus.

4. Sélectionnez **Soumettre** pour de nouvelles règles.
   Une fois que vous avez sélectionné **Soumettre**, votre règle s'affiche dans la liste Règles de tâche de rattrapage [sn_vul_grouping_rule]. Les situations suivantes initient votre règle.
   - Lorsque de nouveaux CVIT sont créés.
   - Lorsque vous sélectionnez **Réappliquer**. Vous sélectionnez **Réappliquer** pour évaluer les règles de tâche sur les tâches de rattrapage existantes uniquement.
   - Lorsque les CVIT sont mis à jour, soit par vous, soit par le système.

     Si un CVIT est mis à jour, les règles de tâches sont évaluées pour vérifier leur correspondance avec les tâches de rattrapage existantes. Voici quelques mises à jour courantes qui déclenchent une vérification des règles :
     - Lorsque l'état passe de Fermé à Ouvert, ou de Fermé à En cours d'examen.
     - L'élément de configuration (CI) est modifié.
     - La vulnérabilité est modifiée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le système vérifie que toutes les règles de tâches ne correspondent pas au CVIT mis à jour. Si les conditions d'une règle correspondent aux conditions d'une tâche de rattrapage, les CVIT correspondants lui sont affectés.

Si aucune correspondance n'est trouvée, une nouvelle tâche de rattrapage est créée.

Pour plus d'informations sur le déploiement d'état des CVIT vers les tâches de remédiation et sur le déploiement de l'état des tâches de rattrapage vers les CVIT, consultez Vue d'ensemble des tâches de remédiation et des règles de tâche de Container Vulnerability Response.

Pour obtenir un exemple de règle de tâche de rattrapage, consultez Exemples de règles de tâche de rattrapage d'Application Vulnerability Response.

5. Pour supprimer une règle de tâche, sélectionnez-la dans la liste Règles de tâche de rattrapage, puis sélectionnez Supprimer.
Le message suivant s'affiche : `La règle de tâche de rattrapage sélectionnée a créé n tâches de rattrapage. Parmi les tâches de rattrapage, n sont à l'état Ouvert.`

Option	Description
Case à cocher désactivée (par défaut).	Supprimez uniquement la règle. Les tâches qui ne sont pas dans l'état ouvert sont exclues.
Case à cocher.	Inclure les tâches de rattrapage dans l'état Ouvert lorsque vous supprimez la règle de tâche de rattrapage. Supprimez la règle et toutes les tâches de rattrapage à l'état Ouvert.

6. Choisissez une option et sélectionnez **Supprimer**.

Créer des règles de fermeture automatique

Utilisez les règles de fermeture automatique pour fermer automatiquement les CVIT plus anciens en fonction des conditions de filtre que vous définissez.

Avant de commencer
Rôle requis : sn_vul.app_manage_auto_close_rules

Procédure

1. Accédez à la **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles de fermeture automatique**.

   Le système de base fournit les règles de fermeture automatique suivantes : **Dernières vulnérabilités du conteneur analysées** : les vulnérabilités non signalées au cours des 90 derniers jours passent à l'état Périmé.

2. Sélectionnez **Nouveau** pour créer une règle de fermeture automatique.
3. Renseignez les champs du formulaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Nom	Nom de la règle de fermeture automatique.
Actif	Option permettant d'activer la règle. Si elle est activée, elle ferme automatiquement toutes les détections qui correspondent à ses critères de filtrage.
Ordre d'exécution	Valeur unique pour l'exécution de la règle de fermeture automatique. Cette valeur détermine l'ordre d'exécution. La valeur par défaut est 100.
Type d'intégration	Intégration de vulnérabilité de l'application
Description	Description de la règle de fermeture automatique.
Condition	Conditions de filtre utilisées pour identifier les détections qui doivent être fermées.

4. Sélectionnez **Soumettre**.
   Les travaux planifiés **des règles de fermeture automatique** s'exécutent de nuit. Il identifie les CVIT en fonction des conditions spécifiées et fait passer celles qui correspondent à l'état **Périmé** . Dans les cas où il y a des CVIT avec à la fois des statuts « Fermé » et « Périmé », le CVIT est fermé avec le sous-état défini sur « Fixe ».

Fermer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage d'application peut être fermé immédiatement sans autre analyse, vous pouvez utiliser la fonctionnalité **Fermer** . À partir de la v2.10 de , le bouton **Fermer** a été supprimé pour une tâche de rattrapage de Réponse aux vulnérabilités pour conteneursconteneur.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Dans les Réponse aux vulnérabilités espaces de travail, une tâche de rattrapage passe par les mêmes états qu'une tâche de rattrapage antérieure dans les versions précédentes de Réponse aux vulnérabilités. Lorsque tous les éléments vulnérables (VIT) d'une tâche de rattrapage sont fermés, la tâche de rattrapage passe à l'état Inactif.

Important : Vous pouvez déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre dans leurs enregistrements respectifs sur leurs enregistrements respectifs lorsque la synchronisation d'état est activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement les tâches de rattrapage des états `Fermé` ou `Différé` .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez l'enregistrement pour lequel vous souhaitez demander une révision.
2. Cliquez sur le bouton **Fermer** .
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
État	Sélectionnez l'état *Fermé*.
Motif	Entrez le motif de la fermeture du problème.
Informations supplémentaires	Saisissez toute autre information pertinente.

4. Sélectionnez **Soumettre**.
   La tâche de rattrapage est **marquée comme fermée**.

Gestion des opérations informatiques et détection de modèles

Lorsque Discovery est activé, les informations sont reçues de l'équipe Information Technology Operations Management (ITOM). Si la ITOM détection est activée, vous pouvez voir les espaces de noms Kubernetes, les grappes Kubernetes et les services Kubernetes lorsque vous ouvrez un élément vulnérable de conteneur (CVIT). Sinon, vous pouvez voir les informations de charge utile Prisma.

Les étiquettes d'image des charges utiles Prisma sont stockées en tant que paires de valeurs clés sous l'image Docker. Les étiquettes d'une charge utile Prisma sont stockées dans la table cmdb_key_value. Pour activer cette fonctionnalité, une règle d'identification est envoyée pour cmdb_ci_docker_image par l'équipe ITOM. Ouvrez l'image Docker pour afficher la liste des éléments connexes. La plupart des éléments sont renseignés par l'équipe ITOM . L'entrée d'identification d'une image de Docker est expédiée pour afficher les valeurs sous forme de paires de valeurs clés.

La criticité opérationnelle est déterminée en fonction des informations de criticité de service reçues de l'équipe ITOM . Une tâche planifiée est exécutée pour extraire les données de tous les services associés à une image. Il calcule la criticité opérationnelle en fonction du mappage des services. Comme le score de risque peut dépendre de la criticité opérationnelle, le score de risque est également calculé en fonction de celle-ci.

Solutions d'analyse et de reporting pour Réponse aux vulnérabilités pour conteneurs

Il Solution Analyse des performances et Reporting contient du contenu préemballé Platform Analytics à utiliser avec d'autres Now Platform produits. Cela Solution Analyse des performances et Reporting fournit une exposition sur la façon dont les vulnérabilités sont gérées à travers les différents graphiques.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur Now Platform (admin) : installer et activer cette solution d'analyse et de génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Administrateur Platform Analytics (pa_admin) : passer en revue les indicateurs, les répartitions, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Information associée

Solutions d'analyse et de génération de rapports

Tableau de bord de Réponse aux vulnérabilités pour conteneurs

Les solutions d'analyse et de génération de rapports comportent un contenu Analyse des performances et Reporting pré-paramétré pour être utilisé avec d'autres produits Now Platform. Cela Solution Analyse des performances et Reporting vous permet de suivre le volume, les performances et la progression des vulnérabilités, de l'analyse initiale et de la détection au confinement ou à la correction. Vous pouvez filtrer les rapports par groupe d'affectation, exploits, cote de risque ou état.

Rôles Now Platform requis

- Administrateur Now Platform (admin) : installer et activer cette solution d'analyse et de génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Administrateur Analyse des performances (pa_admin) : passer en revue les indicateurs, les répartitions, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.

Accéder au tableau de bord Réponse aux vulnérabilités pour conteneurs

Pour ouvrir le tableau de bord, accédez à **Tout** > **Conteneur Vulnerability Response** > **Vue d'ensemble**.

Important :

À partir de la version 2.2 de Réponse aux vulnérabilités pour conteneurs, ce tableau de bord peut également être consulté dans l'interface Next Experience utilisateur. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et sélectionnez l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, sélectionnez la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités et Vue d'ensemble des tableaux de bord.

Remarque :

- Si vous êtes un nouvel utilisateur, vous pouvez afficher les tableaux de bord uniquement à partir des espaces de travail.
- Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

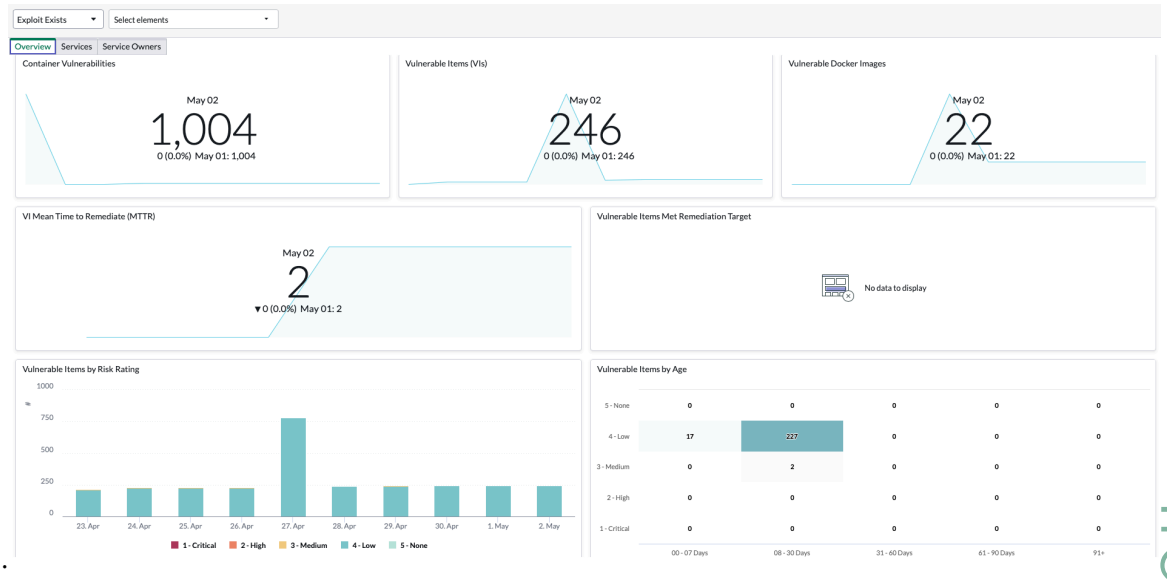
Onglets Gestion de la vulnérabilité du conteneur

Ce tableau de bord vous permet de voir les vulnérabilités présentes dans les conteneurs. Vous pouvez afficher les vulnérabilités et leurs données connexes par région, âge, services et autres répartitions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'onglet **Vue d'ensemble** fournit l'état global de la gestion de la vulnérabilité des conteneurs dans le

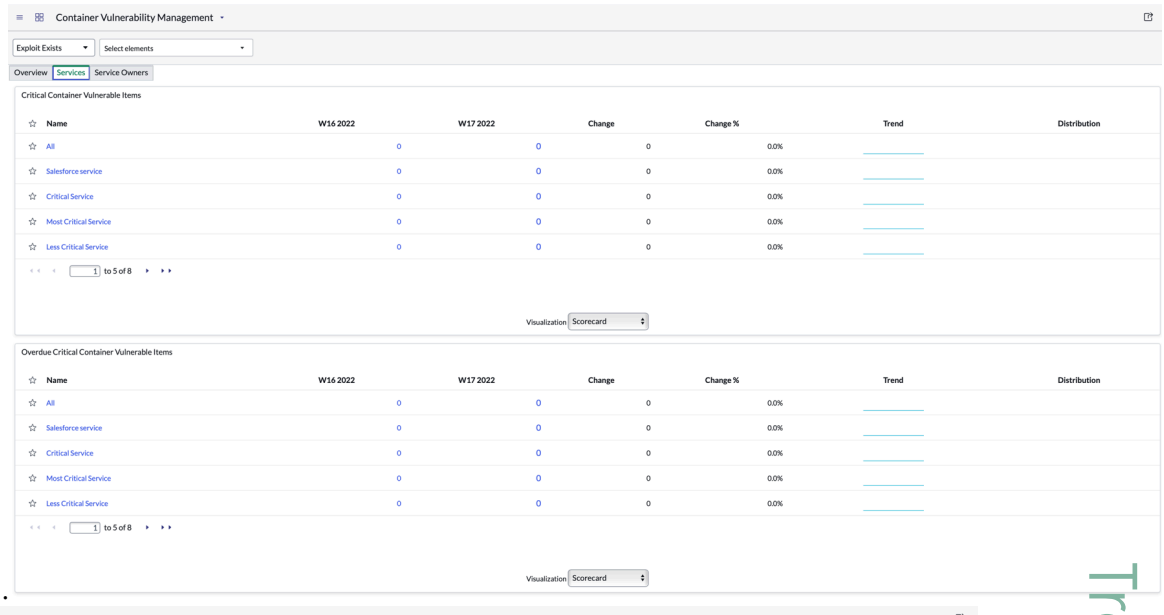


système.

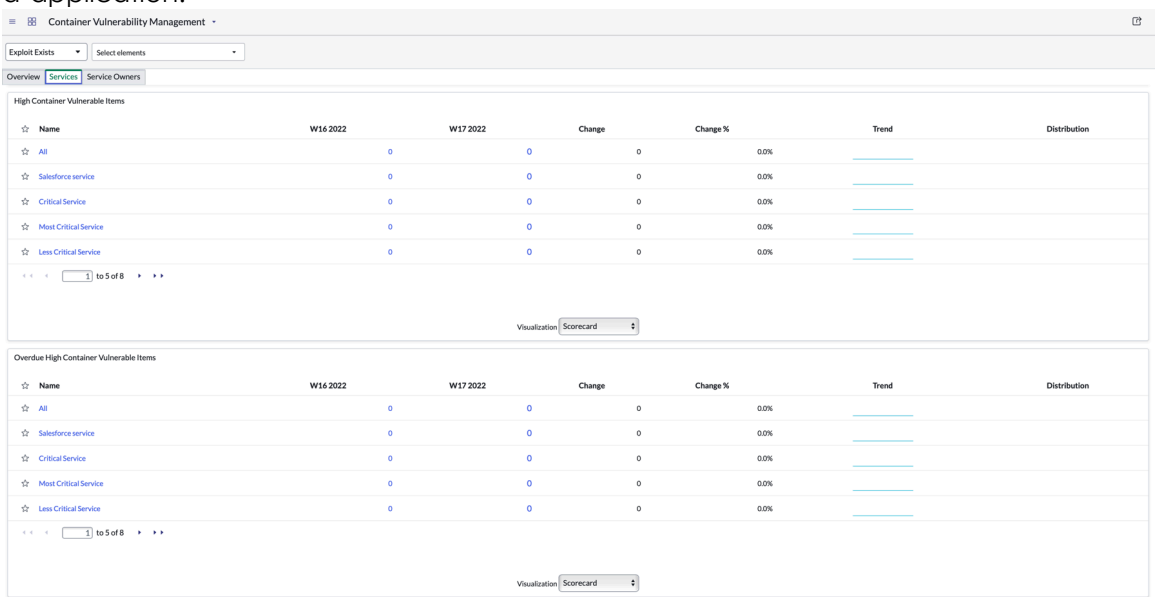
L'onglet **Services** affiche les éléments vulnérables de conteneurs ayant un impact sur les services

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



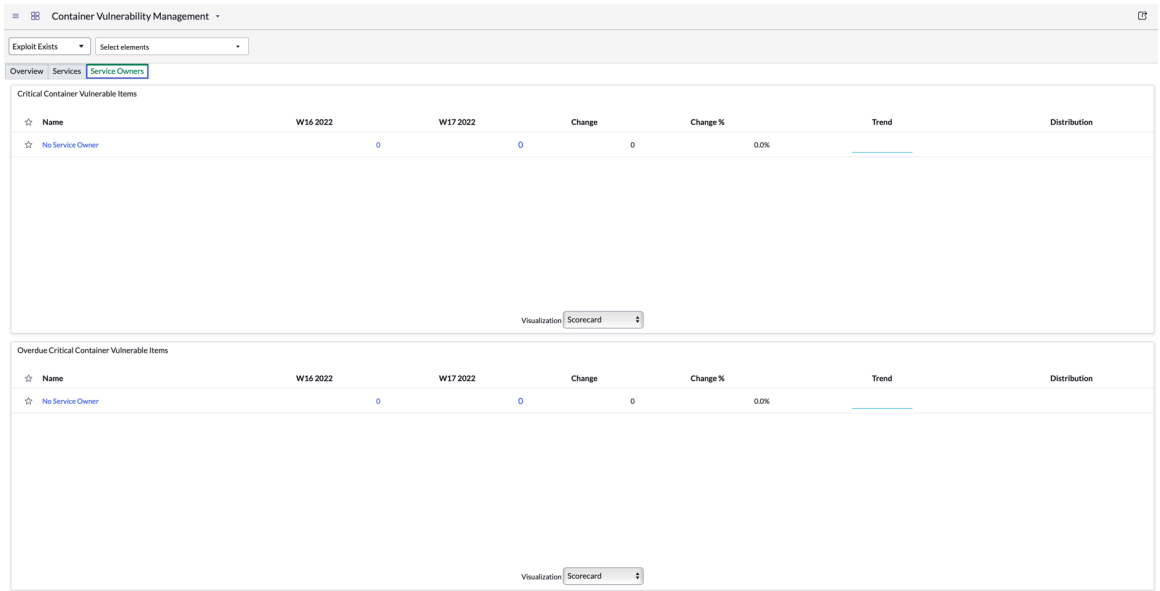
d'application.



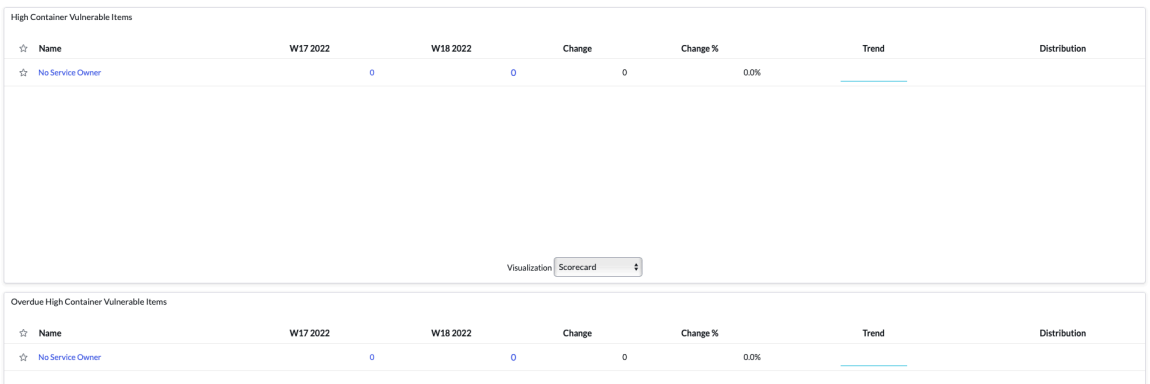
L'onglet **Propriétaires de service** affiche les éléments vulnérables de conteneurs ayant un impact sur les propriétaires de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



service.



Répartitions

- Un exploit existe
- Vecteur d'attaque de l'exploit
- Niveau de compétence de l'exploit
- État de la cible de la remédiation
- Cote de risque
- État
- Groupe d'affectation

Traduction automatique

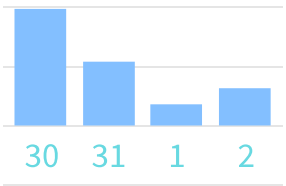
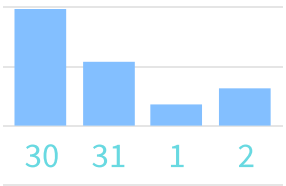
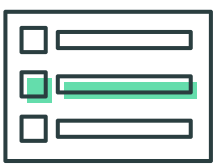
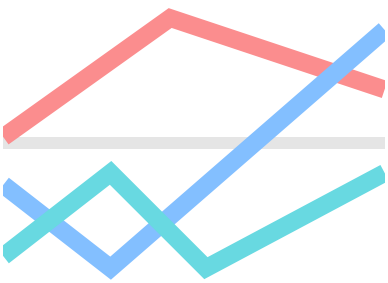
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations des données

Nom	Type	Description
Vulnérabilités du conteneur	Score unique 	Nombre de vulnérabilités de conteneur associées à un ou plusieurs éléments vulnérables de conteneur actifs.
Éléments vulnérables (VI)	Score unique 	Nombre d'éléments vulnérables actifs (non fermés) de conteneur.
Images Docker vulnérables	Score unique 	Nombre d'images docker associées aux éléments vulnérables des conteneurs actifs.
Délai moyen de rattrapage (MTTR) du VI	Score unique 	Le délai moyen de rattrapage (fermeture) d'un élément vulnérable, affiché comme moyenne d'exécution de 30 jours.
Éléments vulnérables ayant atteint la cible de rattrapage	Score unique 	Pourcentage d'éléments vulnérables de conteneur fermés qui ont atteint leur date cible de rattrapage au cours des trimestres actuels et précédents. Les cibles de rattrapage sont calculées à partir de la dernière date

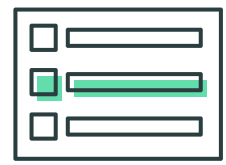
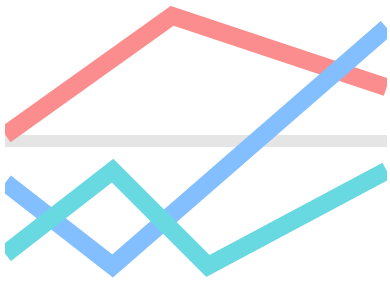
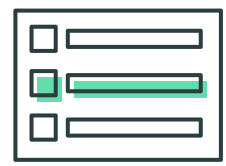
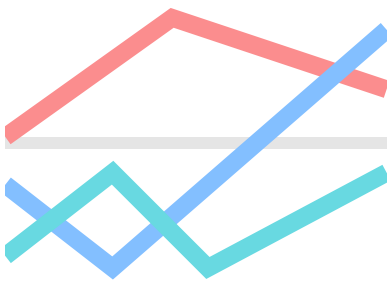
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
		d'ouverture additionnée au nombre de jours.
Éléments vulnérables par cote de risque	Bar 	Nombre d'éléments vulnérables de conteneur actifs regroupés par cote de risque au cours de la période sélectionnée.
Éléments vulnérables par âge	Bar 	Nombre d'éléments vulnérables de conteneur actifs regroupés par cote de risque et par âge (en jours).
Éléments vulnérables du conteneur critiques	Liste et   ligne	Nombre d'éléments vulnérables de conteneur actifs ayant une cote de risque critique, regroupés par service.

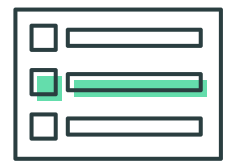
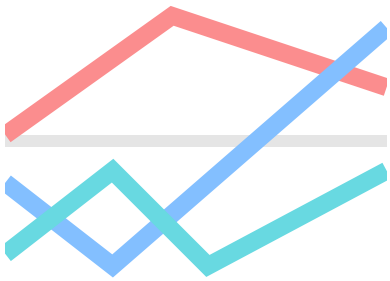
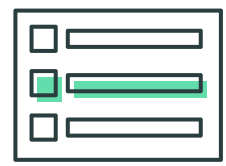
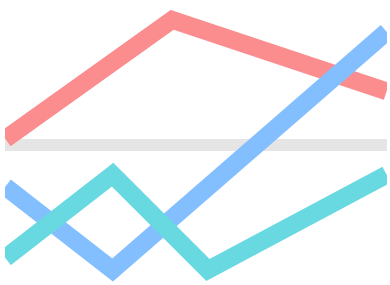
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Éléments vulnérables du conteneur critiques en retard	Liste et ligne  	Nombre d'éléments vulnérables de conteneur actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par service.
Éléments du conteneur hautement vulnérables	Liste et ligne  	Nombre d'éléments vulnérables de conteneurs actifs ayant une cote de risque élevée, regroupés par service.

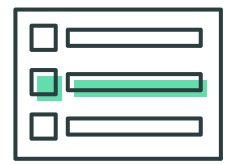
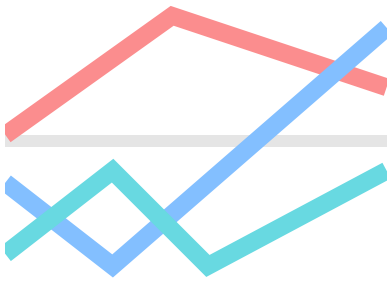
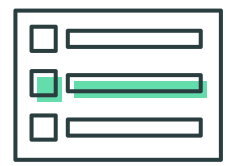
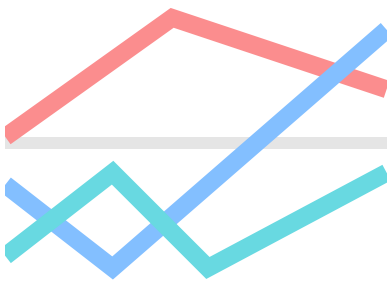
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Éléments hautement vulnérables du conteneur en retard	Liste et ligne  	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée et dépassant leur date cible de rattrapage, regroupés par service.
Éléments vulnérables du conteneur critiques	Liste et ligne  	Nombre d'éléments vulnérables de conteneur actifs ayant une cote de risque critique, regroupés par propriétaire de service.

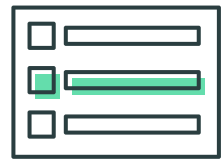
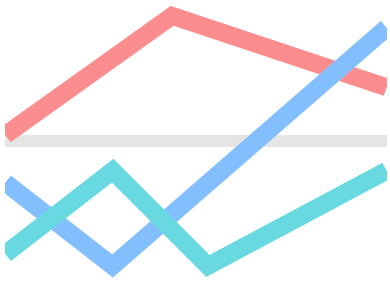
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Éléments vulnérables du conteneur critiques en retard	Liste et ligne  	Nombre d'éléments vulnérables de conteneur actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par propriétaire de service.
Éléments du conteneur hautement vulnérables	Liste et ligne  	Nombre d'éléments vulnérables de conteneur actifs ayant une cote de risque élevée, regroupés par propriétaire de service.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Éléments hautement vulnérables du conteneur en retard	Liste et ligne  	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée et dépassant leur date cible de rattrapage, regroupés par propriétaire de service.

Référence Réponse aux vulnérabilités pour conteneurs

Rubriques de référence contenant des informations sur les tables, les rôles et les propriétés installés avec le Réponse aux vulnérabilités pour conteneurs.

Composants installés avec Réponse aux vulnérabilités pour conteneurs

Plusieurs types de composants sont installés lors de l'activation de l'application Réponse aux vulnérabilités pour conteneurs, notamment des tables, des rôles d'utilisateur et des tâches planifiées.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

Rôles installés avec Réponse aux vulnérabilités pour conteneurs

Des rôles sont ajoutés avec l'activation de Réponse aux vulnérabilités pour conteneurs.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Si vous êtes un client de mise à niveau, l'accès des utilisateurs et des groupes que vous avez affectés avec les autorisations sn_vul.vulnerability_read et sn_vul.vulnerability_write avant la version 10.3 n'a pas changé. Ces rôles restent affectés aux utilisateurs et aux groupes jusqu'à ce que vous les changiez. Toutefois, à partir de la version 10.3, vous préférerez peut-être affecter des rôles granulaires pour plus de contrôle sur ce que les utilisateurs et les groupes peuvent faire et voir dans l'application Réponse aux vulnérabilités . Pour une vue d'ensemble et plus d'informations sur la gestion de ces rôles, consultez Réponse aux vulnérabilités Profils et rôles granulaires et Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Titre du rôle [name]	Description
V2.10 : sn_vul_container.delete	Supprime les enregistrement Contient les rôles sn_vul_cm sn_vul_container.delete_vi.
sn_vul_container.ci_manager	Gère la reclassification des configuration (CI) dans corre
sn_vul_container.configure_integrations	Configure les intégrations d
sn_vul_container.configure_vi_granularity	Configure la granularité des vulnérables de conteneur.
sn_vul_container.create_vi	Peut créer manuellement d vulnérables de conteneur.
sn_vul_container.delete_vi	Peut supprimer les éléments de conteneur créés manue
sn_vul_container.exception_approver	Approuve les exceptions, le les fermetures des éléments du conteneur. À partir de la version v2.3, le granulaire sn_vul_container a été supprimé pour ce rôle vous puissiez accéder aux é vulnérables du conteneur e de rattrapage qui vous sont vous et à votre groupe, au les éléments vulnérables et rattrapage du conteneur.
sn_vul_container.false_positive_approver	Approuve ou rejette la ferm éléments vulnérables du co tant que faux positif.
sn_vul_container.manage_assignment_rules	Définit et met à jour les règl d'affectation des éléments de conteneur.
sn_vul_container.manage_auto_close_stale_vi	Configurer la fermeture aut des éléments vulnérables d périmé
sn_vul_container.manage_auto_exception_rule	Gérer (créer/lire/mettre à jo supprimer) les règles d'exce

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description
sn_vul_container.manage_normalized_severity	Peut mettre à jour le mappa normaliser la gravité.
sn_vul_container.manage_permissions	Peut affecter des rôles de V Response de conteneur aux
sn_vul_container.manage_remediation_targ...	Définit et met à jour les règl de rattrapage de conteneu
sn_vul_container.manage_risk_score_confi...	Définit et met à jour les calc de score de risque, les règle et les calculateurs de déplo de vulnérabilité pour les élé vulnérables du conteneur.
sn_vul_container.read_all	Peut afficher tous les éléme vulnérables du conteneur e informations connexes.
sn_vul_container.read_assigned	Peut afficher les éléments v conteneurs qui me sont affe sont affectés à mes groupe
sn_vul_container.read_assignment_rules	Peut afficher les éléments v conteneur et les règles d'af
sn_vul_container.read_auto_exception_rule	Règles d'exception en lectu
sn_vul_container.read_discovered_image	Peut afficher les éléments d
sn_vul_container.read_integrations	Peut afficher les résultats de d'intégration.
sn_vul_container.read_normalized_severity	Peut afficher le mappage d normalisé.
sn_vul_container.read_remediation_target...	Peut afficher les règles de c rattrapage.
sn_vul_container.read_risk_score_configu...	Peut afficher les calculateu score de risque, les règles d et les calculateurs de déplo de vulnérabilité pour les élé vulnérables du conteneur.
sn_vul_container.remediation_owner	Lit et écrit les éléments vuln conteneurs qui leur sont affe enregistrements de vulnéra également lisibles par un ut disposant de ce rôle.
sn_vul_container.update_assigned_to	Peut mettre à jour l'affecta éléments vulnérables de co Nécessite sn_vul_container. sn_vul_container.write_assig
sn_vul_container.update_assignment_group	Peut mettre à jour le groupe d'affectation pour les élém vulnérables de conteneur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description
	Nécessite sn_vul_container. sn_vul_container.write_assig
sn_vul_container.update_state	Peut mettre à jour l'état des vulnérables. Nécessite sn_vul_container. sn_vul_container.write_assig
sn_vul_container.vulnerability_admin	Configure toutes les règles, etc., pour le Réponse aux v pour conteneurs produit.
sn_vul_container.vulnerability_analyst	Surveille le rattrapage de to éléments vulnérables du co
sn_vul_container.write_all	Peut mettre à jour tous les é vulnérables et tâches de ra conteneurs.
sn_vul_container.write_assigned	Peut mettre à jour des élém vulnérables de conteneurs tâches de rattrapage affec ou à mes groupes.
sn_vul_container.read_watch_topic	Peut lire les rubriques de sur pour les vulnérabilités de co
sn_vul_container.create_watch_topic	Peut créer des rubriques de pour les vulnérabilités de co
sn_vul_container.edit_watch_topic	Peut modifier les rubriques d surveillance pour les vulnéra conteneur.
sn_vul_container.manage_exception_configuration	Peut gérer les configuration des exceptions.

Tables installées avec Réponse aux vulnérabilités pour conteneurs

Les tables sont ajoutées avec l'activation de Réponse aux vulnérabilités pour conteneurs (CVR).

Table	Description
Recherche d'image de conteneur sn_vul_container_image_findings	Stocke des informations sur les vulnérabilités associées, la couche d'image, l'image Docker, le référentiel d'images et l'image détectée.
Couche d'image du conteneur sn_vul_container_image_layer	Contient les informations de chaque couche d'image. Une image est un fichier statique avec du code exécutable qui peut créer un conteneur sur un système informatique.
Package d'images du conteneur sn_vul_container_image_package	Fournit des informations sur les packages dans lesquels se trouvent les vulnérabilités. Les détails du package binaire sont également

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	fournis sous forme de valeurs séparées par des virgules.
Élément vulnérable de conteneur sn_vul_container_image_vulnerable_item	Contient les détails de chaque résultat et la vulnérabilité correspondante.
Image du conteneur détectée sn_vul_container_image	Fournit des informations sur l'ID d'image, l'image Docker et le référentiel d'images. Il stocke également les informations de la couche et les associe à l'image détectée.
Recherche de mappages sn_vul_container_finding_m2m_vul_item	Relation M2M entre les résultats de l'image du conteneur et les éléments vulnérables (CVIT) du conteneur.
Éléments vulnérables à fermeture automatique sn_vul_container_image_auto_close_config	Contient les informations sur la façon de fermer les résultats d'image du conteneur périmés et de déployer l'état jusqu'aux CVIT.
Clés de vulnérabilité de l'image du conteneur sn_vul_container_image_vulnerability_keys	Contient la configuration de granularité pour la création de CVIT à partir des résultats de l'image du conteneur.
Services associés au Doker sn_vul_container_m2m_ci_services	Contient tous les services d'entreprise associés à une image de conteneur.
Nombres de conteneurs VR sn_vul_container_vr_container_counts	Contient la moyenne mobile des instances de conteneur dérivées d'une image de conteneur au cours des 90 derniers jours.
Élément de tâche de rattrapage de conteneur sn_vul_container_m2m_vul_group_item	Table M2M entre les tâches CVIT et Container Remediation.
Tâche de rattrapage de conteneur sn_vul_container_vulnerability	Contient des tâches de rattrapage de conteneurs.
Manifeste de tâche de rattrapage de conteneur sn_vul_container_rt_manifest	Toute mise à jour de la tâche de rattrapage sera effectuée à l'aide de cette table de manifestes par les travaux planifiés.

Tâches planifiées installées avec Réponse aux vulnérabilités pour conteneurs

Des tâches planifiées sont ajoutées à l'activation d'Réponse aux vulnérabilités pour conteneurs.

Tâche planifiée	Description
Associer les VI de conteneurs existants à la	Associe automatiquement la règle d'exception automatique aux éléments vulnérables du conteneur (CVIT) existants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
règle d'exception automatique	
Vérifier l'expiration du report de l'élément vulnérable du conteneur	Envoie des notifications si des éléments vulnérables du conteneur ou des vulnérabilités du conteneur ont expiré (et s'ils expirent dans une semaine).
Nombre de conteneurs de Vulnerability Response (Application - Vulnerability Response et Configuration Compliance pour les conteneurs)	S'exécute quotidiennement pour remplir la table sn_vul_container_vr_container_counts qui calcule la moyenne mobile de 90 jours pour les conteneurs.
Fermer automatiquement les CVIT	Ferme automatiquement les éléments de vulnérabilité de conteneur qui correspondent à la condition définie dans la configuration de fermeture automatique. Leur statut passe à « Corrigé ».
Calculer la criticité opérationnelle pour la CVIT	Traite tous les CVIT actifs et met à jour le champ Criticité opérationnelle, en fonction des services affectés de l'image Docker du CVIT.
Fermer les CVIT d'annulation qui n'ont pas d'image Docker associée	Expire automatiquement les CVIT qui n'ont pas de CI associé. Leur état est défini sur Fermé et le sous-état sur Annulé.
Calculer les nombres de VI connexes pour la tâche de rattrapage de conteneurs	Calcule les nombres sur les enregistrements de tâches de rattrapage de conteneurs.
Déployer les valeurs d'éléments vulnérables de conteneur vers la vulnérabilité et le groupe	Calcule les vulnérabilités et les déploiements de groupes pour les éléments vulnérables du conteneur. **Remarque :** À partir de la version 2.10 de Réponse aux vulnérabilités pour conteneurs, la tâche planifiée est améliorée pour créer des tâches en arrière-plan avec des options de multithreading. Cette mise à niveau implique de segmenter la tâche en plusieurs tâches enfants plus petites, qui sont exécutées en parallèle ou simultanément. Cette modification permet de traiter plusieurs enregistrements simultanément, ce qui accélère considérablement la tâche globale.

Réponse aux vulnérabilités pour conteneurs glossaire

Découvrez les termes et concepts propres à Réponse aux vulnérabilités pour conteneurs.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Termes clés

Conteneur

Unité logicielle qui empaquette le code et toutes ses dépendances de sorte que l'application s'exécute de manière transparente et fiable d'un environnement informatique à un autre.

Image du conteneur

Un fichier statique avec du code exécutable qui peut créer un conteneur sur un système informatique. Une image de conteneur ne peut pas être modifiée et peut donc être déployée de manière cohérente dans n'importe quel environnement.

Grappe

Ensemble d'ordinateurs de travailleur, appelés nœuds, qui exécutent des applications conteneurisées.

Docker

Logiciel pour créer, déployer et gérer des conteneurs d'applications sur les serveurs et dans le cloud.

Image de Docker

Fichier de modèle qui contient le code, les bibliothèques requises, les configurations, etc. Le fichier est utilisé pour lancer des instances de conteneur. Il s'agit d'une union de systèmes de fichiers superposés.

Fichier Dockerfile

Fichier texte contenant des instructions pour créer des images de conteneur en ajoutant plusieurs couches. Par exemple, la superposition du code de base Ubuntu, Nginx et App.

Composition de Docker

Un outil pour définir et exécuter des applications complexes avec Docker. Avec Compose, vous pouvez définir une application multi-conteneurs dans un seul fichier.

Conteneur Docker

Un conteneur Docker est une instance d'exécution lancée à partir d'une image Docker.

Couche d'image

Un calque est une modification apportée à une image. Il est représenté par une instruction dans le Dockerfile. Les calques sont appliqués en séquence à l'image de base pour créer l'image finale.

Référentiel d'images

Une collection d'images Docker avec différentes balises ou versions.

Étiquettes d'image

Ensemble de paires clé-valeur stockées avec l'image en tant que métadonnées.

Espace de noms

Une abstraction utilisée par Kubernetes pour prendre en charge l'isolation de groupes de ressources au sein d'un seul cluster.

Pod

Un ensemble de conteneurs en cours d'exécution (une autre abstraction au-dessus d'un conteneur).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Registre

Service hébergé contenant des référentiels d'images.

Service

Une manière abstraite d'exposer une application s'exécutant sur un ensemble de pods en tant que service réseau.

Balises

Une balise est une étiquette appliquée à une image Docker dans un référentiel d'images donné. Les balises permettent de distinguer les différentes images d'un référentiel les unes des autres.

Formulaire Configuration des calculs dans le cloud Prisma

Le formulaire Configuration des calculs dans le cloud Prisma est accessible depuis le module Intégration des calculs dans le cloud Prisma.

Pour afficher le formulaire Configuration des calculs dans le cloud Prisma, naviguez vers **Tout** > **Intégration des calculs dans le cloud Prisma** > **Administration** > **Configuration**.

Configuration des calculs dans le cloud Prisma

Champ	Description
Instance d'intégration	Nom de la nouvelle instance d'intégration. Vous pouvez créer une instance ou cliquer sur l'icône de recherche pour sélectionner une instance existante.
URL de base de l'API	URL à intégrer à Prisma Cloud Compute.
Nom d'utilisateur	Nom d'utilisateur permettant d'accéder à Prisma Cloud Compute.
Mot de passe	Mot de passe pour accéder à Prisma Cloud Compute.
MID Server	Une application Java qui s'exécute en tant que service Windows ou démon UNIX sur un serveur de votre réseau local. Le serveur MID permet la communication et le mouvement de données entre une instance et des ServiceNow applications, sources de données et services externes.
Utiliser des projets	Option permettant de configurer les projets. Lorsque vous cochez la case, vous pouvez sélectionner des projets dans la page de configuration et exécuter les intégrations en fonction des projets configurés pour renseigner les détails spécifiques au projet. **Remarque :** Si cette case est cochée, l'onglet **Configurer les projets** est activé. Cliquez sur **Suivant** pour poursuivre la configuration des projets.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Demande d'exception

Demandez des exceptions de politique à l'aide de l'option GRC de gestion des exceptions de politique de l'application à partir de .Gestion de la politique et de la conformitéRéponse aux vulnérabilités pour conteneurs

Pour afficher le formulaire Configuration des calculs dans le cloud Prisma, naviguez vers **Tout** > **Conteneur Vulnerability Response** > **Éléments vulnérables de conteneurs** (ou **Tâches de rattrapage**)>**Tous**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.

Formulaire Demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si aucune politique n'est sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date du jour. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et à laquelle l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert. **Remarque :** Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale (jours) de l'exception** que vous avez définie pour la politique dans Politique et conformité. Pour plus d'informations, reportez-vous à la section Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ doit être renseigné par le propriétaire du rattrapage.

Formulaire Règle d'exception

Créez une règle pour demander automatiquement une exception pour une condition spécifique pour un groupe d'éléments vulnérables de conteneurs (CVIT), telle qu'une règle avec une condition basée sur la gravité de vulnérabilité de ces CVIT. Avec cette règle, vous pouvez différer automatiquement les CVIT nouveaux et existants s'ils correspondent à la condition de règle approuvée.

Pour afficher le formulaire Règle d'exception, accédez à **Tout** > **Conteneur Vulnerability Response** > **Administration** > **Règles d'exception**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Règle d'exception

Champ	Description
Nom	Nom de la règle d'exception.
Début de validité	Date à partir de laquelle cette règle est active pour différer les CVIT.
Date de fin de validité	Date à partir de laquelle la tâche de rattrapage cesse d'accepter de nouveaux CVIT.
Motif	Raison pour laquelle cette règle d'exception a été créée.
Groupe d'affectation	Groupe auquel la tâche de rattrapage créée pour le suivi des CVIT différés est affectée.
Informations supplémentaires	Informations supplémentaires que le demandeur souhaite fournir à l'approbateur. Ces informations sont renseignées dans le champ de description de la tâche de rattrapage.
Condition	Condition de filtre pour les CVIT qui peut être définie lors du traitement des CVIT.
Exécuter sur les données existantes	Option qui vous permet d'exécuter cette règle sur des données existantes la première fois que cette règle est exécutée.
Étape du workflow	État d'approbation actuel de la règle d'exception.
État	État de la règle d'exception.
Ordre d'exécution	Ordre unique pour chaque règle d'exception.
Reporté jusqu'à	Date jusqu'à laquelle les VUL et les CVIT sont reportées. À cette date, la vulnérabilité créée est fermée, tous les CVIT sont retirés du groupe et les règles de groupe sont réappliquées.

Traduction automatique

Conformité de la configuration

Il ServiceNow® Conformité de la configuration s'agit d'une application SCA (Secure Configuration Assessment) qui regroupe les résultats d'analyse issus d'intégrations avec des applications d'analyse de configuration tierces. Vous pouvez classer par ordre de priorité les problèmes de conformité de la configuration à l'aide de votre Base de données de gestion des configurations (CMDB). Conformité de la configuration s'intègre étroitement au processus de gestion des changements informatiques pour corriger vos configurations non conformes.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

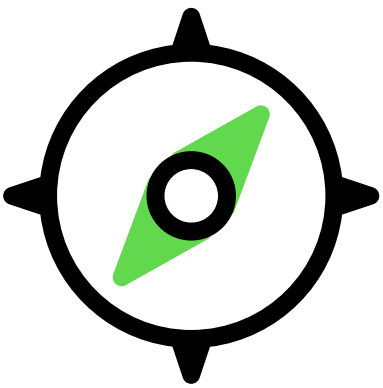
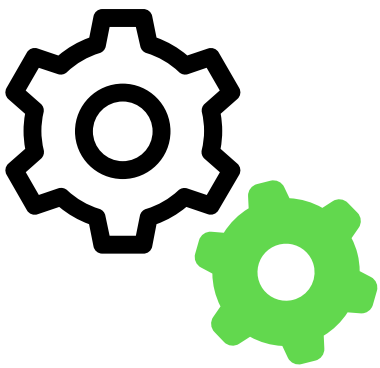
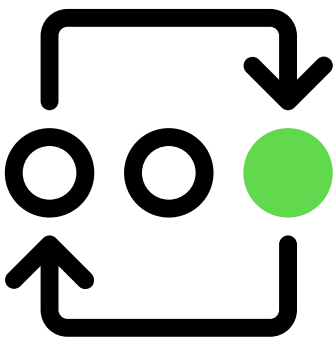
Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

À partir de la version 18.0 de , vous pouvez surveiller et corriger les problèmes de Réponse aux vulnérabilitésconfiguration dans et respectivement Espace de travail de remédiation ITEspace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Conformité de la configuration

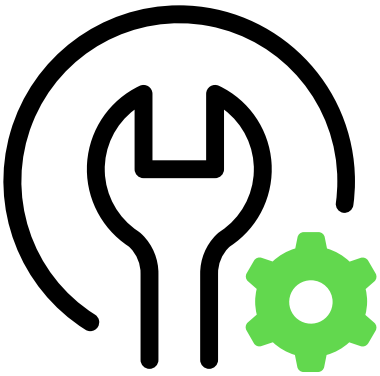
Explorer	Configurer	Intégrer
		
Découvrir les concepts et les fonctionnalités de Configuration Compliance	Configurer Configuration Compliance	Étendre la conformité de la configuration en l'intégrant à d'autres applications

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

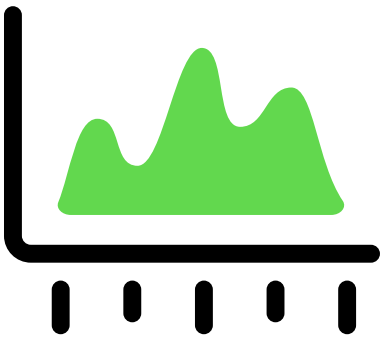
Conformité de la configuration (suite)

Corriger



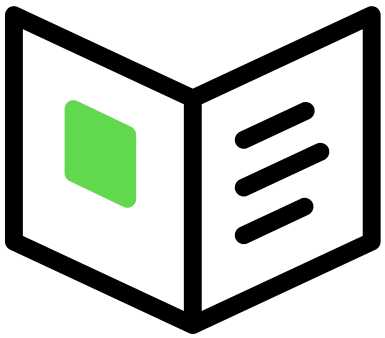
Découvrez comment corriger vos actifs non conformes avec Configuration Compliance

Analyses et rapports



Afficher les rapports et les tableaux de bord dans Configuration Compliance

Référence



Obtenir des détails sur les composants de Configuration Compliance tels que les champs, les tables et les propriétés

Explorer Conformité de la configuration

Utilisez les résultats des tests obtenus à partir d'intégrations tierces de Secure Configuration Assessment (SCA) pour vérifier la conformité aux politiques de sécurité ou d'entreprise. Identifiez, hiérarchisez et corrigez les éléments de configuration non conformes.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

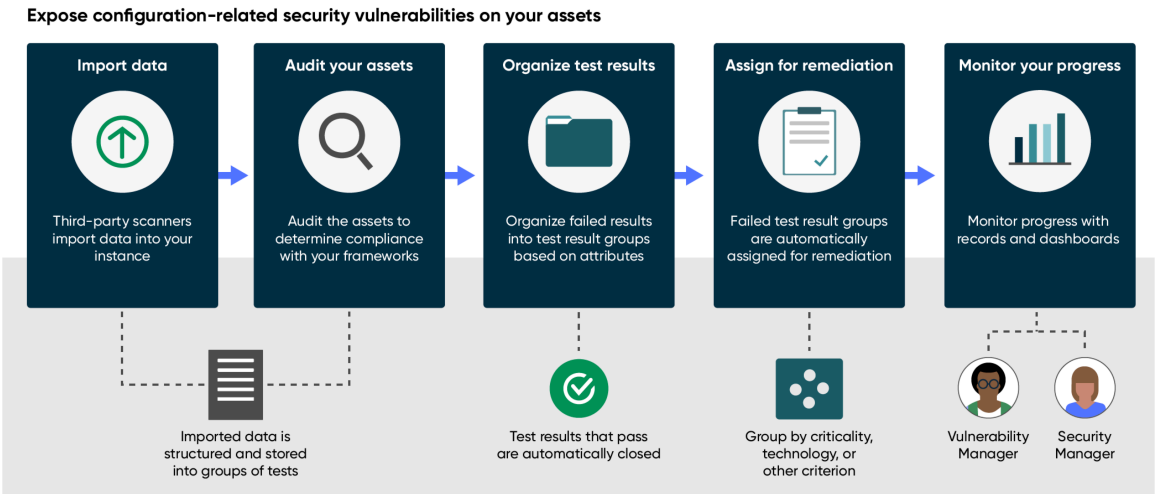
Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Qu'est-ce que Conformité de la configuration ?

L'application ServiceNow® Conformité de la configuration vous permet de hiérarchiser et de corriger rapidement et efficacement les vulnérabilités les plus critiques liées à la configuration dans votre environnement. Conformité de la configuration est disponible par abonnement dans le ServiceNow® Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Fonctionnalités principales de Conformité de la configuration

Utilisez le dans votre Now Platform® pour vous aider à exposer et à corriger vos vulnérabilités de sécurité les plus critiques liées à la Base de données de gestion des configurations (CMDB) configuration. Concentrez vos ressources de rattrapage sur les activités présentant la plus grande réduction des risques. Rationalisez le processus de rattrapage entre les personnes concernées par la sécurité, le service informatique et vos processus business. L'application Conformité de la configuration comprend les fonctionnalités clés suivantes :

- Grâce aux intégrations tierces prises en charge, importez automatiquement des politiques, des tests, des sources de référence et des technologies. Consultez la rubrique Intégrations de Conformité de la configuration pour plus d'informations sur les intégrations prises en charge.
- Corrélez les politiques et les tests aux éléments de configuration (actifs) pour identifier les vulnérabilités liées à la configuration et vous aider à vérifier que vos actifs sont conformes à vos politiques et contrôles.
- Unifiez l'évaluation, l'affectation et le rattrapage de la configuration sur l'ensemble de vos actifs.
- Le contenu de l'analyse de configuration peut être importé à partir des principales applications d'intégration de l'écosystème SCA (Secure Configuration Assessment).
- Les résultats de configuration, les échecs de test, peuvent être regroupés et acheminés automatiquement en fonction des compétences et des domaines de responsabilité des spécialistes du rattrapage. Des workflows intelligents et une intégration étroite avec la gestion des changements permettent un transfert fluide des tâches entre les groupes.
- Lorsqu'ils sont utilisés avec l'application (GRC), les ServiceNow Gouvernance, risque et conformité tests de configuration peuvent Conformité de la configuration être déployés sur leurs contrôles GRC correspondants.
- Grâce à la gestion des changements améliorée, créez des demandes de changement préremplies pour le service informatique directement à partir de afin de vous aider dans vos tâches de Conformité de la configuration rattrapage nécessitant des ressources supplémentaires.
- Grâce aux tableaux de bord, affichez les mesures d'état de rattrapage sur la tâche de rattrapage, le test de conformité et les enregistrements de politique.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Qui utilise Conformité de la configuration

Conformité de la configuration Les activités peuvent impliquer de nombreux niveaux de gestion.

- Administrateurs système
- Administrateurs de vulnérabilité
- Responsables des vulnérabilités
- Analystes de vulnérabilités
- Administrateurs de la conformité

Conformité de la configuration Les tâches impliquent les rôles suivants.

- sn_vulc.admin : peut lire, écrire, supprimer
- sn_vulc.write — peut lire et écrire
- sn_vulc.remediation_owner — Peut lire et mettre à jour les enregistrements affectés

  Remarque : Le rôle sn_vulc.remediation_owner est également automatiquement attribué lorsqu'un utilisateur se voit attribuer le rôle itil.

- sn_vulc.read : peut lire

Conformité de la configuration et Opérations de sécurité

Lorsque les et les Tenable Vulnerability Integration sont installés, l'accès Qualys Vulnerability Integration à Réponse aux vulnérabilités devient disponible. Vous pouvez avoir plusieurs déploiements de ces intégrations. Les données provenant de chaque déploiement sont identifiées et disponibles dans une instance unique de GRC.

Versions disponibles pour Xanadu

Version	Notes de publication
Conformité de la configuration v14.7, v14.8, v14.9, v14.10, v14.11, v14.12	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Conformité de la configuration Données importées

L'application Conformité de la configuration importe les politiques, les tests, les sources de référence et les résultats des tests à partir d'intégrations tierces et les stocke dans des modules pour consultation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Intégrations prises en charge

Les intégrations tierces importent dans l'application les résultats de l'évaluation de configuration, les groupes de tests, les tests, les technologies, les sources de référence et les Conformité de la configuration résultats des tests. Les gestionnaires de vulnérabilité ou les analystes de vulnérabilité peuvent utiliser ces données pour identifier et répondre aux vulnérabilités liées à la configuration sur vos actifs.

Pour en savoir plus sur les intégrations prises en charge, reportez-vous à la section Intégrations de Conformité de la configuration.

Groupes de tests

Les groupes de tests sont associés à des documents et des enregistrements de test faisant autorité. Un groupe de tests de configuration définit les groupes de tests. Les groupes de tests s'alignent généralement sur une classe de technologie, par exemple, Windows, les bases de données Oracle, Cisco IOS, et sont souvent dérivés de la norme principale du secteur. Les groupes de tests peuvent être modifiés pour répondre aux besoins de l'organisation. Un seul test de configuration peut appartenir à plusieurs groupes de tests.

Intégration	Description
Qualys Vulnerability Integration	Les groupes de tests sont récupérés et les ID de contrôle sont renseignés par la tâche planifiée, **Qualys PC Policies** à 1h00 du matin. Vous pouvez afficher la tâche planifiée en accédant à **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Politiques de PC Qualys**. **Remarque :** Si vous choisissez d'exécuter l'intégration manuellement, exécutez d'abord **Qualys PC Policies** .
Tenable Vulnerability Integration	L'intégration des résultats de conformité de la tâche Tenable.io planifiée importe les politiques. Si vous choisissez d'exécuter les intégrations manuellement, exécutez-les dans l'ordre suivant jusqu'à ce que vous rapprochiez tous les actifs ignorés avec les données d'évaluation :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
	• Tenable.io Intégration des actifs • Tenable.io Intégration des résultats de conformité • Tenable.io Intégration du remplissage des résultats de conformité • Tenable.io Intégration des actifs • Tenable.io Intégration du remplissage des résultats de conformité Pour afficher l'enregistrement de politique, accédez à **Tout** > **Configuration Compliance** > **Groupes de tests**. Pour identifier et créer correctement les enregistrements des groupes de test, les informations d'audit des groupes de tests sont importées et affichées dans le champ **Brève description** .

Tests

Les tests sont des bibliothèques d'enregistrements de données qui organisent les analyses des ressources informatiques. Les tests de configuration définissent la manière dont une classe d'actifs technologiques doit être gouvernée.

Un Conformité de la configuration test est le mécanisme utilisé par les applications d'intégration tierces pour regrouper les actifs par type de vulnérabilité. Certaines solutions d'analyse VA tierces, telles que Qualys, disposent de très grandes bibliothèques de tests (jusqu'à 8 000) qui sont mappées à des politiques et à des « cadres » de sources faisant autorité.

Un test peut avoir plusieurs valeurs, un-à-plusieurs, attendus et réels, etc. Un test est tout ce qui peut être utilisé pour identifier une classe d'actifs logiciels ou matériels non conformes. Par exemple, un numéro de version ou de matériel.

Intégration	Description
Qualys Vulnerability Integration	La tâche planifiée, **Qualys PC Controls**, récupère les tests. Vous pouvez afficher la tâche planifiée en accédant à **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Contrôles de PC Qualys**. **Remarque :** Si vous choisissez d'exécuter l'intégration manuellement, exécutez **Qualys PC Controls** après **Qualys PC Policies**.
Tenable Vulnerability Integration	L'intégration des résultats de conformité de la tâche Tenable.io planifiée importe les tests de configuration (Tests).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
	Si vous choisissez d'exécuter les intégrations manuellement, exécutez-les dans l'ordre suivant jusqu'à ce que vous rapprochiez tous les actifs ignorés avec les données d'évaluation : • Tenable.io Intégration des actifs • Tenable.io Intégration des résultats de conformité • Tenable.io Intégration du remplissage des résultats de conformité • Tenable.io Intégration des actifs • Tenable.io Intégration du remplissage des résultats de conformité Pour afficher l'enregistrement du test de configuration, accédez à **Configuration Compliance** > **Tests**. Sur l'enregistrement, les données importées s'affichent dans le champ **Brève description** et dans les onglets État du rattrapage, Description et Rattrapage. Les données sont également affichées dans les liens connexes **Citation**,**Politiques** et **Résultats des tests** .

Technologies

L'une des techniques utilisées par les analyseurs de vulnérabilité tiers pour créer des groupes de test d'éléments de configuration logiciels et matériels à des fins d'analyse consiste à les organiser par technologie. Les technologies sont une bibliothèque importée de systèmes d'exploitation, d'appareils réseau, de bases de données et d'applications associés à des stratégies. Les tests ont plusieurs implémentations pour différentes technologies. L'assainissement est également spécifique à la technologie.

Vous pouvez afficher les technologies applicables pour un test, afin de mieux comprendre à quels types de ressources logicielles ou matérielles le contrôle peut être appliqué. Parmi les exemples de technologies pouvant être appliquées aux contrôles, citons CentOS 7.x, Windows 8.1, Windows 2016 Server, etc. La liste des technologies est en lecture seule et correspond aux technologies définies dans l'application Qualys Cloud Platform .

Les technologies sont importées uniquement pour les évaluations de configuration liées aux bases de données. Le *db_type* (s'il n'est pas vide) dans l'importation est utilisé pour créer une technologie. Affichez les technologies renseignées dans la section Technologies sur les enregistrements de tests de configuration, les enregistrements de résultats des tests, les enregistrements de politiques et à **Configuration Compliance** > **Données associées** > **Technologies**.

Sources de référence

Conformité de la configuration utilise des sources de référence et des citations lors de la génération d'alertes de vulnérabilité pour les tests. Les sources faisant autorité renvoient généralement à des sections de normes industrielles publiées, telles que « NIST 800-53 version 3 (2009) 3 : 2009, SA-4 ».

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Dans le Qualys Vulnerability Integration, cette combinaison est appelée framework.

Les sources de référence et les citations (également appelées mandats) sont importées à partir des analyseurs de vulnérabilité tiers.

Les enregistrements sources faisant autorité contiennent des références à des informations sur des problèmes connus de configuration logicielle et matérielle provenant d'experts dans le domaine de la sécurité informatique. Ils définissent les exigences en matière de politiques et de procédures de sécurité. Les tests de configuration peuvent référencer plusieurs sources faisant autorité par le biais de citations. Les sources de référence peuvent rendre compte de la conformité à une norme donnée en vue d'un audit.

Intégration	Description
Qualys Vulnerability Integration	La tâche planifiée, **Qualys PC Policies Detail**, récupère les sources de référence et les citations. Vous pouvez afficher cette tâche planifiée en accédant à **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Détail des politiques de PC Qualys**. **Remarque :** Si vous choisissez d'exécuter l'intégration manuellement, exécutez le **détail des politiques informatiques Qualys** après **les politiques informatiques Qualys**.
Tenable Vulnerability Integration	La tâche Tenable.io planifiée Intégration des résultats de conformité importe des sources de référence dans le cadre des données de citation. Si vous choisissez d'exécuter les intégrations manuellement, exécutez-les dans l'ordre suivant jusqu'à ce que vous rapprochiez tous les actifs ignorés avec les données d'évaluation : • Tenable.io Intégration des actifs • Tenable.io Intégration des résultats de conformité • Tenable.io Intégration du remplissage des résultats de conformité • Tenable.io Intégration des actifs • Tenable.io Intégration du remplissage des résultats de conformité Les données sont affichées sur le lien connexe **Citations** dans les enregistrements de test de configuration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats des tests

Conformité de la configuration ne calcule pas les résultats des tests, mais les importe dans le cadre d'une intégration tierce. Une fois visibles dans Conformité de la configuration, ils sont corrigés à l'aide de **tâches de rattrapage**. Consultez Conformité de la configuration corrélation pour plus d'informations.

Intégration	Description
Qualys Vulnerability Integration	Vous pouvez récupérer les résultats des tests de l'une des façons suivantes : • La tâche planifiée, **Résultats Qualys PC**, récupère les résultats des tests. Vous pouvez afficher cette tâche planifiée en accédant à **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Résultats de l'ordinateur Qualys**. **Remarque :** Si vous choisissez d'exécuter l'intégration manuellement, exécutez les **résultats de Qualys PC** après **les Politiques de PC Qualys et ledétail des politiques de PC Qualys**. L'importation des **résultats Qualys PC** utilise le *Start Time* paramètre de l'onglet Détails de l'intégration. Toutes les autres Conformité de la configuration importations apportent toutes les données disponibles, indépendamment de *Start Time*. Lorsque l'importation des **résultats Qualys PC** est terminée, un événement est déclenché pour déclencher les calculs de fin d'importation. Pour plus d'informations, reportez-vous à la section Conformité de la configuration États. • Alternativement, à partir de la version 14.5, vous pouvez également exécuter les intégrations suivantes pour récupérer les résultats des tests :

Nom de l'intégration	Description
Qualys Intégration de l'hôte de la politique PCRS	Récupère les ID d'hôte pour chaque politique. Pour afficher cette tâche planifiée, accédez à : Intégration de vulné-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
	<table><tr><th>Nom de l'intégration</th><th>Description</th></tr><tr><td></td><td>rabilité Qualys > Intégrations principales > Intégration de l'hôte de politique Qualys PCRS. **Remarque :** Si vous choisissez d'exécuter l'intégration manuellement, exécutez Qualys PCRS Policy Host Integration après Qualys PC Policies et Qualys PC Policies Detail. Une fois cette tâche planifiée terminée, elle déclenche automatiquement l'intégration des résultats des tests Qualys PCRS.</td></tr><tr><td>Qualys Intégration des résultats des tests PCRS</td><td>Récupère les résultats des tests pour chaque ID d'hôte. Pour afficher cette tâche planifiée, accédez à Intégration de vulnérabilité Qualys > Intégrations principales > Intégration des résultats des tests Qualys PCRS.</td></tr></table>

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

<table>
<tr><th>Intégration</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Nom de l'intégration</th><th>Description</th></tr>
<tr><td></td><td>Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez l'intégration des résultats des tests Qualys PCRS après Qualys PC Policies, Qualys PC Policies Detail et Qualys PCRS Policy Host Integration.

Cette intégration utilise le paramètre Heure de début dans l'onglet Détails de l'intégration.</td></tr>
</table>
</td></tr>
<tr><td>Tenable Vulnerability Integration</td><td>L'intégration des résultats de conformité de la tâche Tenable.io planifiée importe les résultats des tests.

Si vous choisissez d'exécuter les intégrations manuellement, exécutez-les dans l'ordre suivant jusqu'à ce que vous rapprochiez tous les actifs ignorés avec les données d'évaluation :
• Tenable.io Intégration des actifs
• Tenable.io Intégration des résultats de conformité
• Tenable.io Intégration du remplissage des résultats de conformité
• Tenable.io Intégration des actifs
• Tenable.io Intégration du remplissage des résultats de conformité

Pour afficher l'enregistrement du test de configuration, accédez à Configuration Compliance > Résultats des tests. Sur</td></tr>
</table>

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
	l'enregistrement, les données importées s'affichent dans les champs**Test** et **Élément de configuration** . Les données sont également affichées dans les **onglets Expected Values (Valeurs attendues**), **Actual Values (Valeurs réelles**) et **Remédiation (Remédiation**). Les liens connexes **Tâches de rattrapage** et **Historique des résultats des tests** sont renseignés.

Détection de Conformité de la configuration

Conformité de la configuration les données sont importées à partir d'applications de scanner SCA tierces. Ils structurent les groupes de tests logiciels et matériels en enregistrements de données afin d'accélérer la réalisation des évaluations.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Lorsqu'une importation est terminée, un événement est envoyé pour indiquer les actions de fin d'importation. Pour chaque tâche de rattrapage active, les actions suivantes sont effectuées :

- Les groupes résolus avec des résultats ayant échoué reviennent à l'état **En attente d'implémentation** .
- Les tâches de rattrapage pour lesquelles tous les résultats ont été transmis sont **fermées**.
- L'état des résultats des tests dans les tâches de rattrapage actives est mis à jour.
- Le marqueur indiquant si un résultat fait partie d'une tâche de rattrapage active est mis à jour.

Conformité de la configuration corrélation

Conformité de la configuration assure la hiérarchisation et le regroupement des résultats des tests (dans la tâche de rattrapage) pour faciliter la correction des problèmes de non-conformité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Priorisation centrée sur les actifs

Les analyses de configuration peuvent produire un grand nombre de résultats. Classer les résultats par ordre de priorité pour une réduction maximale des risques. La priorité inclut à la fois la criticité des tests de configuration et la criticité des actifs. La priorité des résultats des tests de configuration est exprimée sous la forme d'un score de risque sur une échelle de 0 à 100. Les groupes de calculateurs calculent le score de risque et peuvent être personnalisés.

Lorsque l'importation tierce est terminée, Conformité de la configuration envoie un événement pour indiquer les actions de fin d'importation. Pour chaque groupe de résultats actif, les actions suivantes sont effectuées :

- Les tâches de rattrapage résolues avec des résultats ayant échoué reviennent à l'état **En attente d'implémentation** .
- Les tâches de rattrapage pour lesquelles tous les résultats sont **transmis sont fermées**.
- L'état des résultats des tests dans les tâches de rattrapage actives est mis à jour.
- Le marqueur indiquant si un résultat fait partie d'une tâche de rattrapage active est mis à jour.

Ordre de priorité des tâches de remédiation

Lorsque les résultats des tests appartiennent à plusieurs tâches de rattrapage, **l'état** d'un résultat de test est dérivé selon un ordre de priorité.

Les champs **État** et **Résolution** du formulaire **Test de configuration** et le champ **Résultat** du formulaire **Résultat** du test sont calculés selon cet ordre de priorité.

Remarque :

La priorité d'appartenance au groupe s'applique uniquement aux éléments pour lesquels l'élément n'a pas réussi le test de configuration. **Les éléments réussis** sont toujours à l'état **Fermé-Fixe** .

La valeur **Résultat** détermine l'état. Nous ignorons les tâches de rattrapage à l'état **Fermé-Corrigé** et **Fermé-Annulé** . L'état de l'élément est calculé à partir des états de toutes les autres tâches de rattrapage auxquelles il appartient ou est défini sur **Ouvert**, si aucune autre tâche de rattrapage n'existe pour l'élément.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

Création de tâches de remédiation

Conformité de la configuration Les tâches de rattrapage sont créées manuellement.

Il existe deux façons de créer et de remplir des **tâches de rattrapage**.

- À partir du module **Tâches de remédiation** et à l'aide de filtres qui remplissent automatiquement l'onglet **Résultats des tests** .

  Cette méthode est utile lorsque vous savez quel filtrage vous souhaitez utiliser. Par exemple, la capture de tous les résultats des tests ayant échoué avec une criticité modérée et élevée affecte l'infrastructure Windows et s'applique uniquement à l'application de chaîne d'approvisionnement SAP.

- En sélectionnant les résultats des tests dans la liste **Résultats des tests** et en créant une tâche de rattrapage à partir du menu **Actions sur les lignes sélectionnées...**

  Cette méthode est idéale pour les résultats qui ne sont pas facilement filtrés ou pour les situations dans lesquelles vous souhaitez spécifier des résultats de test pour le rattrapage. Par exemple, des valeurs aberrantes qui n'ont rien en commun.

Remarque : Si vous créez une tâche de rattrapage à partir de la liste **Résultats des tests** et que vous décidez ultérieurement d'utiliser un filtre pour cette tâche de rattrapage, vos entrées d'origine sont supprimées et remplacées par les résultats du filtre.

Résultats des tests dégroupés

Les résultats des tests dégroupés contiennent tous les résultats des tests non réussis qui ne sont pas membres d'une tâche de rattrapage active (non **fermée**). Ce module est mis à jour après chaque importation et chaque fois que des résultats de tests sont ajoutés ou supprimés d'une tâche de rattrapage.

Éléments détectés pour Conformité de la configuration

Les actifs sont automatiquement mis en correspondance avec des éléments de configuration (CI) à l'aide des règles de recherche de CI, lorsqu'ils sont importés à l'aide de l'intégration des résultats des tests et de l'hôte. Les éléments détectés vous donnent une visibilité sur la façon dont l'identification des actifs est mappée aux CI dans le CMDB.

Les éléments détectés sont considérés comme **correspondants**, **sans correspondance** ou **reclassés**. Les CI identifiés sont dans l'état **En correspondance** .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour faciliter la recherche de problèmes de correspondance potentiels, la règle de recherche de CI correspondant au CI apparaît dans le champ **Règle de correspondance de CI** .

Remarque : La prise en charge du champ **de règle de correspondance CI** n'est disponible que pour l'intégrationQualys.

Si aucune correspondance n'a été trouvée, un CI est créé dans la classe *`CI sans correspondance`*`[sn_sec_cmn_unmatched_ci]`,`[cmdb_ci_unclassed_hardware]` ou `[cmdb_ci_incomplete_ip]` du CMDB. Si le CI sans correspondance d'origine a été reclassé, les enregistrements d'éléments détectés sont mis à jour pour refléter cet état. Pour plus d'informations, consultez CI sans correspondance et Afficher et reclasser les éléments de configuration sans correspondance pour plus d'informations.

Par défaut, l'option **Security Operations** > **CMDB** > **Éléments détectés** Liste les éléments de configuration sans correspondance. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour obtenir une description des champs dans Éléments détectés, consultez la section Champs du formulaire Éléments détectés.

Changements de CI pour les éléments détectés pour Conformité de la configuration

La valeur par défaut de la propriété `sn_sec_cmn.update_on_ci_change` est `vrai`. Ainsi, lorsque l'élément de configuration (CI) d'un élément détecté est mis à jour, les résultats des tests sont également mis à jour.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

L'ID externe du résultat du test est mis à jour et le score de risque, les règles d'affectation, les règles de tâche de rattrapage et la règle de cible de rattrapage sont réévalués. Si un résultat de test existe avec le même test et le même CI, les résultats du test sont mis à jour avec le résultat de test existant et le résultat du test actuel est fermé avec le sous-état `invalidCI`. Des notes de travail sont ajoutées en conséquence.

Si vous ne voulez pas mettre à jour le CI pour le résultat de test existant, définissez la propriété sur false. Dans ce cas, si un CI change, un nouveau résultat de test est créé et le résultat existant est fermé en tant que `CI non valide`.

Rapprocher les éléments détectés sans correspondance pour Conformité de la configuration

Créez une tâche planifiée pour rapprocher les éléments détectés sans correspondance Lorsqu'un résultat de test est créé, l'élément de configuration (CI) qui lui a été ajouté au moment de la création peut être obsolète.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Si les informations contenues dans la CMDB changent, les informations de CI sans correspondance ne sont pas rapprochées. Pour le rapprochement, appliquez des règles de recherche de CI sur les résultats des tests qui sont dans un état sans correspondance lorsque la CMDB est mise à jour avec les derniers CI.

Une tâche planifiée est exécutée à la demande pour réappliquer la règle de correspondance CI pour les éléments détectés dans un état sans correspondance. Si le CI change après réapplication des règles de recherche, les éléments détectés sont mis à jour avec le nouveau CI. Les résultats des tests concernés sont également mis à jour. Pour plus de détails, voir Changements de CI pour les éléments détectés pour Conformité de la configuration.

Procédure

1. Accédez à la **Tout** > **Security Operations > rapprocher les éléments détectés sans correspondance**.
2. Sur la page Tâches en arrière-plan, cliquez sur **Créer une tâche de rapprochement**.
3. Renseignez les champs du formulaire.

Remarque : Vous ne pouvez modifier que le champ Paramètres.

Tâche en arrière-plan

Champ	Description
Numéro	Numéro de tâche unique.
Créé par	Utilisateur qui a créé la tâche.
Paramètres	Paramètres permettant de rapprocher les éléments détectés sans correspondance : ◦ limit : nombre maximal d'éléments détectés à rapprocher. Si vous ne saisissez pas de valeur, 10 000 éléments détectés sont rapprochés. ◦ firstDiscovereditem : premier élément détecté qui doit être rapproché. Si vous ne saisissez pas de valeur, le processus de rapprochement commence à partir du premier élément détecté.
État	État actuel de la tâche en arrière-plan.
Description d'état	Description de l'état actuel de la tâche en arrière-plan.
Type de tâche	Type d'emploi. La valeur est **Rapprocher les éléments détectés sans correspondance**.
Démarré à	Heure de début de la tâche.
Heure de fin	Heure à laquelle la tâche a été terminée.
Durée de la tâche	Temps total nécessaire à l'achèvement de la tâche.
Sous-état	Sous-état de l'état sélectionné.
Notes	Nombre d'enregistrements traités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Envoyer**.

Remarque :

- Pour arrêter l'exécution de la tâche, cliquez sur **Annuler**.
- Vous ne pouvez pas rapprocher les CI sans correspondance ni réappliquer des règles de recherche de CI lors de l'importation d'hôtes ou de résultats de tests.

Réappliquer des règles de recherche de CI sur les éléments détectés sélectionnés pour Conformité de la configuration

Réappliquez les règles de recherche d'éléments de configuration (CI) sur les éléments détectés sélectionnés à partir des actions de sélection de la vue de liste des éléments détectés. L'administrateur peut être amené à modifier ou à mettre à jour une règle de recherche pour plusieurs raisons. Si la règle de recherche change, ils peuvent l'appliquer à nouveau sur les éléments détectés.

Avant de commencer

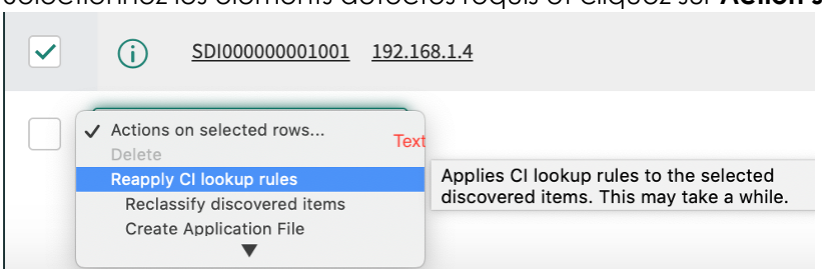
Rôles requis :

Pourquoi et quand exécuter cette tâche

Si le CI change après la réapplication des règles de recherche de CI, les éléments détectés sont mis à jour avec le nouveau CI et les résultats des tests. Pour plus d'informations, consultez Changements de CI pour les éléments détectés pour Conformité de la configuration.

Procédure

1. Accédez à la **Tout** > **Opérations de sécurité** > **CMDB** > **Éléments détectés**.
2. Sélectionnez les éléments détectés requis et cliquez sur **Action sur les lignes sélectionnées**.



3. Sélectionnez **Réappliquer les règles de recherche de CI** dans la liste.

   Les règles sont réappliquées sur ces éléments détectés.

L'option Tenable Vulnerability Integration avec Conformité de la configuration

Produit Tenable.io des politiques d'importation Tenable Vulnerability Integration , des contrôles (résultats des tests) et des tests de configuration pour le traitement dans l'application Conformité de la configuration .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Tenable.io

Le Tenable Vulnerability Integration est pris en charge.

Vous pouvez utiliser les données importées pour :

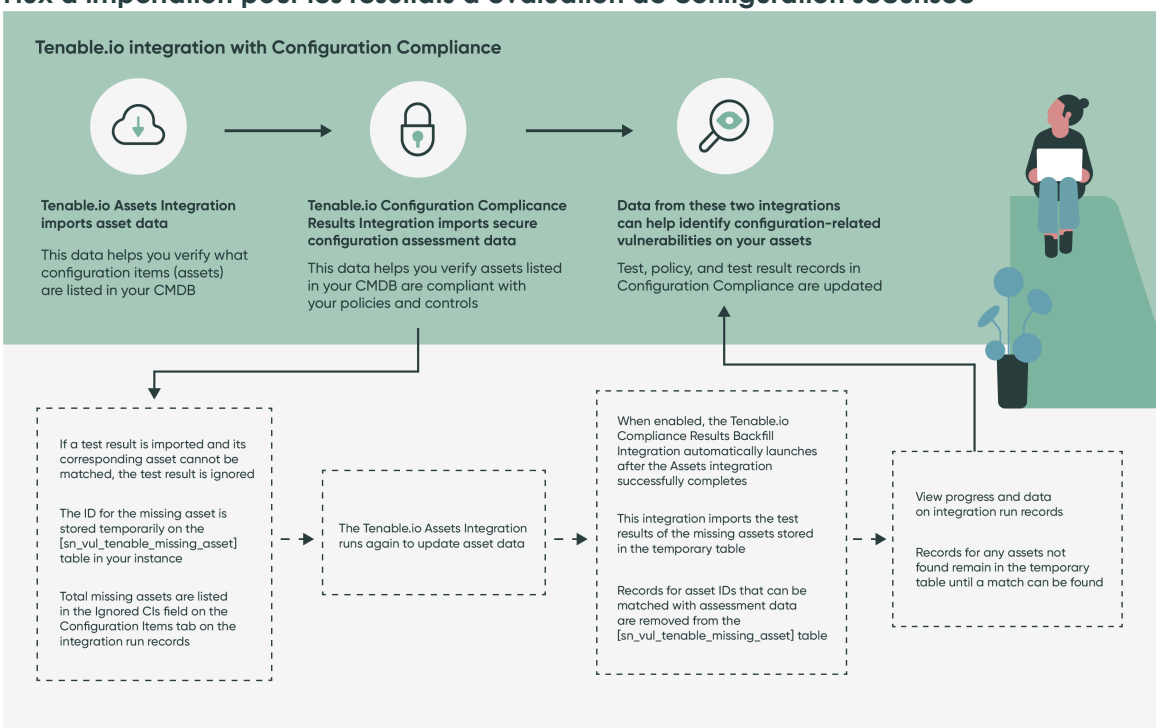
- Identifiez les vulnérabilités liées à la configuration sur vos actifs répertoriés dans votre Base de données de gestion des configurations (CMDB)
- Vérifiez que vos actifs sont conformes à vos politiques et contrôles.

Les données des actifs, les politiques, les contrôles (résultats des tests) et les tests de configuration sont importés avec les intégrations suivantes :

- Tenable.io Intégration des actifs
- Tenable.io Intégration des résultats de conformité
- Tenable.io Intégration du remplissage des résultats de conformité

L'image suivante illustre la façon dont les intégrations fonctionnent ensemble pour importer des données d'évaluation des actifs et des configurations et rapprocher tous les CI ignorés lors d'une importation.

Flux d'importation pour les résultats d'évaluation de configuration sécurisée



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les données sont importées, mises à jour et affichées sur les enregistrements de résultats des tests, de politique et de test de configuration dans l'application Conformité de la configuration .

Dans certains cas, le nombre d'éléments de configuration (CI) importés est différent pour l'intégration des actifs et l'intégration Tenable.io des résultats de conformité Tenable.io . Lorsque cela se produit, des enregistrements temporaires sont créés et stockés pour les ID d'actifs ignorés. Ces enregistrements peuvent être mis en correspondance ultérieurement avec les données d'évaluation importées par importations à partir de l'intégration du remplissage des résultats de conformité.

Par exemple, supposons que l'intégration des actifs importe 80 actifs lors d'une exécution d'intégration, mais que l'intégration des résultats de conformité en importe 100.

Remarque : Vous pouvez vérifier le nombre de CI ignorés lors des exécutions d'intégration en accédant à **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**. Cliquez sur le nom d'une intégration pour ouvrir l'enregistrement. Sur le lien connexe **Exécutions de l'intégration de vulnérabilité** , ouvrez un enregistrement d'exécution de l'intégration et sélectionnez l'onglet **Éléments** pour afficher la valeur dans le champ **CI ignorés** . Ce champ suit le total des actifs ignorés (manquants) de l'importation.

En comparant les valeurs des champs **CI ignorés** de chaque enregistrement d'exécution d'intégration, on obtient une différence de 20 CI ignorés. Par conséquent, l'intégration de remplissage s'exécute automatiquement, comme illustré dans l'image précédente. Cette intégration importe les informations d'évaluation de la configuration pour les 20 actifs supplémentaires trouvés par l'intégration des résultats de conformité, mais manqués par l'intégration des actifs. Étant donné que les données d'évaluation des actifs manquants ne sont pas importées, l'intégration Tenable.io du remplissage des résultats de conformité importe jusqu'à 200 ID d'actifs par exécution d'intégration pour rapprocher les actifs manquants avec leurs données d'évaluation correspondantes. Tous les enregistrements créés pour les actifs manquants ou ignorés et répertoriés dans la table temporaire sont supprimés une fois que ces actifs et leurs données sont mis en correspondance.

Remarque : plusieurs exécutions de ces intégrations peuvent être nécessaires pour importer tous les actifs ignorés.

Pour en savoir plus sur l'activation et la configuration de l'intégration Tenable.io des actifs, reportez-vous à la section Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration. Consultez Présentation de l'intégration Tenable Vulnerability pour plus d'informations sur l'intégration.

L'intégration Tenable.io des résultats de conformité et l'intégration du remplissage des Tenable.io résultats de conformité sont inactives par défaut.

Pour les activer :

1. Accédez à la **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.
2. Dans la liste Intégrations Tenable, cliquez sur un nom d'intégration pour ouvrir l'enregistrement et cochez la case **Actif** pour l'activer. Vous préférerez peut-être conserver les paramètres de calendrier dans leurs valeurs par défaut pour que ces intégrations démarrent.

Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Conformité de la configuration vulnérabilité tierces

Lorsque les données sont importées à partir d'une intégration tierce, Conformité de la configuration utilise automatiquement les données de l'hôte pour rechercher des

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

correspondances dans le Base de données de gestion des configurations (CMDB)fichier . Pour ce faire, il utilise des **règles de recherche de CI**. Ces règles sont utilisées pour identifier les éléments de configuration (CI) et les ajouter à l'enregistrement des résultats des tests pour faciliter le rattrapage.

Au fur et à mesure que les actifs sont importés, une recherche est d'abord effectuée sur la liste **des éléments détectés** à l'aide d'ID tiers pour trouver des correspondances avec des éléments de configuration (CI) à partir d'importations précédentes. Lorsqu'une correspondance d'ID d'hôte est trouvée, elle est utilisée comme champ **d'élément de configuration** dans l'enregistrement des résultats du test.

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

Un nouvel élément détecté est créé et mappé à ce CI.

Remarque : Les règles de recherche de CI ne sont disponibles que pour l'intégration Qualys pour Security Operations.

Les règles de recherche de CI peuvent être séparées par domaine et sont spécifiques à la source. Chaque source peut avoir plusieurs déploiements. Qualys peut avoir plusieurs déploiements de l'intégration Qualys. Chaque déploiement possède son propre ensemble de règles de recherche de CI.

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

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

Remarque : Pour éviter toute correspondance sur des éléments de réseau de bas niveau, si un CI correspondant est l'un des `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic` ou `cmdb_ci_ip_address`, le CI parent est renvoyé.

Une propriété système permettant d'exclure les classes CI est disponible. Cette propriété n'est pas disponible avec la mise à niveau. Consultez la section Ignorer les classes CI pour obtenir des informations sur la mise à niveau et des instructions sur la définition de la propriété.

Pour faciliter la recherche de problèmes correspondants, lorsqu'une correspondance est trouvée, la règle de recherche de CI utilisée pour la trouver est ajoutée à l'enregistrement d'élément détecté dans le champ **Règle de correspondance de CI** . Les règles de recherche sont évaluées en fonction de la valeur **d'ordre** la plus basse en premier.

Voici quelques-unes des Qualys règles de recherche de CI fournies avec le système de base :

- ID D'HÔTE QUALYS
- FQDN

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- NetBIOS
- DNS
- IP

Voici quelques-unes des règles de recherche de CI Microsoft Defender fournies avec le système de base :

- Catégorie S3
- Nom
- ID de ressource

Voici quelques-unes des règles de recherche de CI Palo Alto Prisma Cloud fournies avec le système de base :

- Catégorie S3
- Nom
- ID de ressource

L'importation des données des résultats des tests peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas construites avec soin. La logique utilisée pour itérer et effectuer une correspondance au sein de peut CMDB entraîner de longs délais de traitement. Pour éviter toute dégradation potentielle des ressources ou toute complication des performances, testez les règles de recherche de CI écrites sur mesure ou les modifications apportées aux **règles de recherche de CI prédéfinies**. Pour plus d'informations sur la prévention des enregistrements orphelins en double, la suppression des données et le nettoyage des données, consultez la rubrique Étapes pour empêcher les enregistrements en double ou orphelins après l'exécution de Réponse aux vulnérabilités règles de recherche de CI .

Réapplication des règles de recherche de CI mises à jour

Lorsque vous modifiez une règle de recherche de CI, cliquez sur **Appliquer les changements** sur la page de liste Règles de recherche de CI pour réexécuter toutes les règles sur les éléments détectés qui :

- Ont été appariés par les règles mises à jour
- Ne sont assortis à aucune règle

Si l'élément de configuration (CI) change après la réapplication des règles de recherche, les éléments détectés sont mis à jour avec le nouveau CI. Les résultats des tests sont également mis à jour. Pour plus d'informations, consultez Changements de CI pour les éléments détectés pour Conformité de la configuration.

Déduplication des éléments de configuration existants pour Conformité de la configuration

Le correcteur de CI en double pour les tâches de déduplication est mis à jour avec la propriété `sn_sec_cmn_src_ci.cmdb_ci` .

Chaque fois qu'une tâche de déduplication est utilisée pour mettre à jour les éléments de configuration (CI), elle met également à jour les éléments détectés associés à ces CI. Par conséquent, les résultats des tests sont mis à jour avec le CI. Pour plus de détails, voir Changements de CI pour les éléments détectés pour Conformité de la configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Création de CI pour Conformité de la configuration l'utilisation du moteur Identification et Réconciliation

À partir de la Conformité de la configuration version 11.1, vous pouvez créer des éléments de configuration (CI) dans l'API Base de données de gestion des configurations (CMDB) du moteur Identification et rapprochement (IRE). En utilisant l'API IRE pour créer des CI, vous pouvez empêcher la création de CI en double et vous pouvez rapprocher les attributs de CI en autorisant uniquement les sources de données de référence à écrire vers CMDB.

Une classe CI (table) est le nom de table d'origine dans la base de données de l'instance. CMDB contient des classes système de base qui stockent des données sur les CI.

Utilisation d'IRE pour la création de CI

Avant la version 11.1, si un CI correspondant n'était pas trouvé dans la liste des éléments détectés ou CMDB, un CI était créé dans la classe CI sans correspondance (`sn_sec_cmn_unmatched_ci`).

Pour plus d'informations, consultez CI sans correspondance.

À partir de la version 11.1, vous pouvez utiliser l'API IRE pour créer des CI dans CMDB. Au lieu d'utiliser la classe de CI sans correspondance, un CI est créé dans la classe Matériel non classé ou Appareil identifié IP incomplète.

CMDB Classes CI

Remarque : Pour utiliser les nouvelles classes, activez le module d'extension Modèles de CMDB classes CI. Dans le cas contraire, les CI sont créés dans la classe CI sans correspondance.

À partir de la version 11.1, si l'hôte que vous avez importé à partir d'un scanner tiers est introuvable dans la liste des éléments détectés ou CMDB, il est stocké dans l'une des nouvelles CMDB classes CI suivantes.

CMDB Classes CI

CMDB **Classe CI**	**Description**
Adresse IP incomplète de l'appareil identifié (`cmdb_ci_incomplete_ip`)	Le CI est créé dans cette table si seule l'adresse IP est disponible dans les informations d'hôte reçues de l'analyseur.
Matériel non classé (`cmdb_unclassed_hardware_ci`)	Le CI est créé dans cette table si l'une des informations suivantes est disponible dans les informations de l'hôte reçues du scanner : • Nom d'hôte • Adresse IP • DNS • NETBIOS • Adresse MAC

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

CMDB Classes CI (suite)

CMDB **Classe CI**	**Description**
	Remarque : Si l'adresse MAC est disponible, l'entrée de la carte réseau est créée et associée au CI matériel non classé. Si les adresses IP et MAC sont disponibles, le CI d'adresse IP est également créé et associé au CI matériel non classé.

Le système utilise automatiquement une classe CI sans correspondance si l'une des situations suivantes se produit :

- Le CMDB module d'extension Classe CI n'est pas activé.
- IRE lève une exception lors de la création d'un nouveau CI.

Information associée

Application de stockage CMDB CI Class Models

Moteur Identification et réconciliation (IRE)

Conformité de la configuration Vue d'ensemble des règles d'affectation

Définissez les critères selon lesquels les résultats des tests sont automatiquement affectés à un groupe d'affectation pour le rattrapage.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Une règle d'affectation par défaut, **Affecter au groupe de support CI**, est incluse dans l'affectation des résultats des tests au **groupe de support** CI par le système de base. Inactif par défaut.

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

Affectation automatique des résultats des tests

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

- Groupe d'affectation : cette option vous permet de sélectionner l'un des groupes d'utilisateurs existants Now Platform®.
- Champ de groupe d'affectation : cette option vous permet de choisir n'importe quel champ de groupe d'affectation disponible à l'aide de la table cmdb_ci. Par défaut, les trois champs de groupe suivants s'affichent :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Aucun : n'indique aucune valeur par défaut pour ce champ obligatoire
- Élément de configuration : groupe d'approbation
- Élément de configuration : Groupe d'affectation
- Élément de configuration : groupe de support

- Script : cette option vous permet de définir les conditions à l'aide d'un script. Cette option nécessite un codage ou une expertise avancée ServiceNow® .

Pour plus d'informations sur la création de règles d'affectation, reportez-vous Créer ou modifier des Conformité de la configuration règles d'affectation à la rubrique

Le rôle sn_vulc.remediation_owner vous permet d'afficher et de mettre à jour les résultats des tests et les tâches de rattrapage qui leur sont affectés ou qui sont affectés à leurs groupes d'affectation. Pour afficher les modules, accédez à **Tout** > **Configuration Compliance** > **Résultats des tests** > **Mes résultats des tests ouverts**ou **Configuration Compliance** > **Tâches de remédiation** > **Mes tâches ouvertes**.

Le rôle sn_vulc.remediation_owner peut être affecté directement à un utilisateur ou il est automatiquement attribué lorsque vous affectez le rôle itil à un utilisateur.

Processus d'évaluation des règles d'affectation

Lorsqu'un nouveau résultat de test est importé ou rouvert après sa fermeture, les règles d'affectation sont évaluées par rapport à ce résultat. Les règles d'affectation sont évaluées après la correspondance des CI et les calculs de score de risque. Un résultat de test n'est automatiquement évalué qu'à l'importation initiale et lorsqu'une règle est modifiée, sauf si elle est rouverte après avoir été fermée. Vous pouvez réappliquer manuellement des règles après les changements.

Le processus suivant est utilisé pour chaque nouveau résultat de test ou rouvert :

- Pour chaque règle d'affectation des résultats des tests, le résultat du test est comparé au filtre d'affectation, en commençant par la règle d'ordre le plus bas.
- Lorsque la condition est remplie, un groupe d'affectation est affecté au résultat du test. La recherche s'arrête.
- Si les conditions ne trouvent pas de correspondance entre toutes les règles, le résultat du test n'est pas affecté.

Réapplication des règles d'affectation

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

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

La tâche planifiée [*Reapply all assignment rules*] est inactive par défaut. Lorsqu'elle est activée, elle évalue tous les résultats des tests ouverts par rapport à toutes les règles actives, à l'exception de celles affectées manuellement. Il peut fonctionner quotidiennement, hebdomadairement, mensuellement, périodiquement, une fois ou sur demande.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

Règles d'affectation et affectation de tâche de rattrapage

En règle générale, vous affectez votre tâche de rattrapage (RT) au même groupe d'affectation que les résultats du test. C'est ce que font les règles de tâche de rattrapage par défaut.

Par exemple, si vos groupes de tâches de rattrapage par classe d'éléments de configuration, la tâche de rattrapage créée peut être répartie par les différents groupes d'affectation. Un TRG de base de données Oracle peut être affecté au groupe 1 et un TRG de base de données Oracle affecté au groupe 2.

Lorsque le groupe d'affectation est modifié au niveau de la tâche de rattrapage, tous les résultats des tests de cette tâche de rattrapage qui ont le même groupe d'affectation sont mis à jour vers le nouveau groupe d'affectation. Les résultats des tests sont marqués comme affectés manuellement et ne peuvent pas faire l'objet d'une évaluation de règle plus poussée.

Suppression des affectations des tâches de Conformité de la configuration rattrapage

Vous pouvez effacer les champs Affecté à et **Groupe d'affectation** sur les tâches de rattrapage (RT) et leurs résultats des tests associés directement à partir des enregistrements TRG qui, selon vous, pourraient être incorrectement affectés à vous ou à vos groupes.

Vue d'ensemble

À partir de la version 14.3 de l'application, les propriétaires de rattrapage peuvent mettre à jour les enregistrements en vue d'une réaffectation à l'aide du Conformité de la configuration bouton **Annuler l'affectation** .

Cas d'utilisation pour sn_vulc.remediation_owner

Si vous déterminez que les RT et leurs résultats des tests associés ne sont pas dans votre champ d'application pour le rattrapage, ou si vous pensez que les enregistrements ont été affectés de manière incorrecte à vous ou à vos groupes, vous pouvez vous retirer, vous ou vos groupes, des champs **Affecté à** et **Groupe d'affectation** sur ces enregistrements de tâche de rattrapage.

Désaffecter le module

Le bouton **Annuler l'affectation** s'affiche sur les enregistrements RT dans n'importe quel état autre que l'état ou Fermé ou Résolu.

Si vous sélectionnez **Annuler l'affectation**, vous êtes invité à indiquer que tous les résultats des tests associés au groupe sont réaffectés et passent au type **d'affectation Non affecté** .

Tous les enregistrements que vous mettez à jour à l'aide du bouton d'interface utilisateur ou manuellement s'affichent dans le module Non affecté sous Conformité de la configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour savoir comment réaffecter des enregistrements à l'aide de l'action d'interface utilisateur, reportez-vous à la *Unassigned* section Supprimer les affectations des tâches de rattrapage pour vous ou vos groupes.

Propriété système et notifications

Si vous êtes un administrateur disposant du rôle sn_vulc.vulnerability_admin, lorsque vous sélectionnez **Annuler l'affectation** d'un enregistrement, par défaut, la propriété *sn_vulc.unassign_test_result_group.approval_required* système déclenche l'enregistrement Approbation de changement d'état et l'enregistrement Approbation demandée. En outre, la demande s'affiche dans la liste Mes approbations de l'approbateur.

Remarque : En tant qu'administrateur de vulnérabilité, vous pouvez définir la *sn_vulc.unassign_test_result_group.approval_required* propriété système sur **false** pour désactiver le processus d'approbation.

- Si l'approbateur approuve votre demande, par défaut, la propriété *sn_vulc.default_assignment_group* système efface les champs Affecté à et Groupe d'affectation et renseigne le champ Type d'affectation avec **Non affecté.** En tant qu'administrateur de vulnérabilité, vous pouvez modifier la valeur de la *sn_vulc.default_assignment_group* propriété système afin que les champs d'affectation soient effacés et qu'un groupe spécifique soit ensuite affecté. Par exemple, si un utilisateur sélectionne **Annuler l'affectation** d'un enregistrement et que vous souhaitez le rediriger vers un groupe spécifique pour révision, vous pouvez ajouter un ID système pour le groupe de votre choix dans le champ Valeur de la propriété système.
- Si l'approbateur rejette votre demande, le motif du rejet s'affiche dans l'onglet **Notes** .

S'il *sn_vulc.default_assignment_group* n'est pas configuré pour un groupe spécifique, par défaut, les utilisateurs que vous ajoutez au groupe d'utilisateurs de notification Annuler l'affectation sont avertis lorsque les enregistrements ne sont pas affectés. La propriété *sn_vulc.default_notification_group* système détermine les notifications à ce groupe.

Le type d'affectation, qu'il soit **manuel**, **de règle** ou **non affecté,** est disponible dans les enregistrements RT et la vue de liste. Le type **d'affectation non affecté** s'affiche une fois que les champs **Affecté à** et **Groupe d'affectation** sont effacés par la propriété système de la fonctionnalité.

Surveillance de vos règles d'affectation avec la tâche planifiée pour cette fonctionnalité

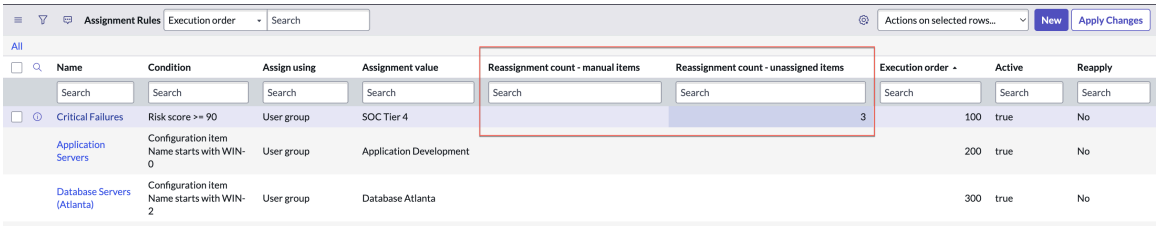
Une tâche planifiée quotidienne compte les enregistrements lorsqu'ils passent au type **d'affectation Non affecté.** Grâce à ce nombre, les analystes de vulnérabilité peuvent surveiller et ajuster toutes les règles d'affectation qui pourraient ne pas être performantes en fonction des règles d'affectation qui ont un nombre plus élevé de RT non affectés.

La *Reassignment count for assignment rules* tâche planifiée s'exécute quotidiennement et publie le nombre total de RT qui ne sont pas affectés par cette fonctionnalité pour une règle d'affectation particulière.

La tâche compte également tous les enregistrements qui ne sont pas affectés manuellement. Les décomptes manuels et les décomptes collectés par cette fonctionnalité sont publiés dans la liste Règles d'affectation de vulnérabilité dans deux colonnes : *Reassignment count - manual items* et *Reassignment count - unassigned items*.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



1. En tant qu'administrateur de vulnérabilité, vous pouvez afficher ces nombres en accédant à **Configuration Compliance** > **Administration** > **Règles d'affectation**.
2. Sélectionnez l'icône d'engrenage dans le coin supérieur droit de la liste, puis sélectionnez le **nombre de réaffectations : éléments manuels** et le **nombre de réaffectations : éléments non affectés** à afficher.
3. Tout RT qui a été affecté à l'origine par une règle, mais qui a ensuite été réaffecté automatiquement ou manuellement, contient une référence à la règle d'origine dans la vue de liste.

Conformité de la configuration Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage

Créez automatiquement des tâches de rattrapage (RT) pour analyser les résultats en bloc à l'aide des règles de tâche de rattrapage. Les critères de formation des groupes sont configurés de manière à ce que vous n'ayez pas à affecter manuellement les résultats des tests aux groupes.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Présentation des tâches de rattrapage

Les tâches de rattrapage représentent un ensemble de résultats des tests à corriger. Le regroupement des résultats des tests présente de nombreux avantages. Vous pouvez déplacer les résultats des tests d'un état de rattrapage à un autre, les marquer comme étant en cours d'examen, les différer, les marquer comme résolus en bloc à l'aide de groupes. Vous pouvez créer des conditions pour regrouper automatiquement tous les résultats avec des résultats, des technologies, des scores de risque et toutes les autres données associées aux résultats des tests. Les résultats des tests peuvent appartenir à plusieurs tâches de rattrapage, ce qui vous donne la possibilité de travailler activement avec une tâche de rattrapage et d'en surveiller une autre. Tout dépend de vos besoins organisationnels. Par exemple, vous pouvez regrouper par affectation et créer une tâche de rattrapage contenant des technologies.

Les tâches de rattrapage sont créées comme suit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Manuellement, à l'aide de l'une des deux options, pour ajouter des résultats des tests à la tâche de rattrapage.
  - **Manuel** : crée une tâche de rattrapage sans entrées. Les résultats des tests doivent être ajoutés manuellement.
  - **Filtre** : crée une tâche de rattrapage et utilise des conditions pour y ajouter automatiquement des résultats des tests.

  Remarque : Les résultats des tests ajoutés manuellement ne sont pas automatiquement supprimés des tâches de rattrapage par les règles de tâche de rattrapage ou les conditions de tâche de rattrapage.

- Automatiquement, à l'aide des règles de tâche de rattrapage. Cette option est l'option la plus simple. Une fois configurées, les règles de tâche de rattrapage créent toutes les tâches de rattrapage souhaitées.

À partir d'une tâche de rattrapage, le groupe de résultats des tests peut être affecté à un utilisateur, reporté à plus tard, utilisé pour créer une **demande de changement**, etc.

Remarque :

Avec le rôle sn_vulc.remediation_owner, vous pouvez afficher et mettre à jour les résultats des tests et les tâches de rattrapage qui vous sont affectés ou qui sont affectés à vos groupes d'affectation. Pour afficher les modules, accédez à **Tout** > **Configuration Compliance** > **Résultats des tests** > **Mes résultats des tests ouverts**ou **Configuration Compliance** > **Tâches de remédiation** > **Mes tâches ouvertes**.

Lorsqu'il est déterminé qu'un nouveau résultat de test peut être ajouté à une tâche de rattrapage, le résultat du test est inclus dans la liste **connexe Résultats des tests** de la tâche de rattrapage.

Lors de la mise à jour de l'état d'une tâche de rattrapage, l'état des résultats des tests associés peut être mis à jour pour correspondre à cette tâche de rattrapage. Pour plus d'informations sur les changements d'état, reportez-vous à Conformité de la configuration États.

Présentation des règles de tâche de rattrapage

Les règles de tâche de rattrapage vous permettent de définir la manière dont les résultats des tests sont automatiquement regroupés et affectés. Une règle par défaut, **Groupe d'affectation, Test**, est incluse dans le système de base regroupant les résultats des tests en fonction d'un **groupe d'affectation** de résultats des tests et du champ **Test** . Cette règle est désactivée par défaut. Vous pouvez effectuer un regroupement selon n'importe quel autre ensemble de valeurs dans des colonnes accessibles à partir du résultat du test. Vous pouvez utiliser jusqu'à six clés et n'importe quel nombre de conditions. Pour plus d'informations, consultez Créer ou modifier Conformité de la configuration des règles de tâche de rattrapage.

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

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, vous pouvez regrouper les résultats de vos tests par groupe d'affectation ou par technologie et élément de configuration (CI). Un ensemble différent de règles peut être utilisé pour les résultats des tests qui exposent l'entreprise à plus de risques. Vous pouvez avoir une règle de tâche de rattrapage pour les CI de faible gravité ou de faible risque. Consultez la rubrique Champs Résultats des tests pour plus d'informations sur les champs disponibles.

Lorsqu'un nouveau résultat de test est importé ou rouvert après sa fermeture, les règles de la tâche de rattrapage sont évaluées par rapport à celui-ci. Un résultat de test n'est évalué qu'une seule fois, sauf s'il est rouvert après avoir été fermé.

Les règles de tâche de rattrapage sont évaluées après la correspondance des CI, les calculs de score de risque et les règles d'affectation.

Le processus suivant est utilisé pour chaque nouveau résultat de test ou rouvert :

- Pour chaque règle de tâche de rattrapage, le résultat du test est comparé au filtre de condition.
- Pour chaque règle dans laquelle la condition de règle correspond, elle extrait les données des colonnes de clé de groupe sur le résultat du test. La règle vérifie s'il existe une tâche de rattrapage **ouverte** correspondante affectée au même groupe d'affectation que le résultat du test.

  Si la tâche de rattrapage est trouvée, le résultat du test est ajouté à la tâche de rattrapage existante à l'état **Ouvert** .

- Si aucune tâche de rattrapage à l'état **Ouvert** n'est trouvée, la règle crée une tâche de rattrapage, l'affecte en fonction du **groupe d'utilisateurs** ou de la valeur **de clé** dans la règle et y place le résultat du test.

Plusieurs règles de résultats de test peuvent être définies pour regrouper différents types de résultats. Étant donné que chaque résultat est comparé aux conditions de la règle avant de le placer dans une tâche de correction, un trop grand nombre de règles peut avoir un impact sur les performances.

Lorsqu'une règle de tâche de rattrapage est supprimée, vous avez la possibilité de supprimer toutes les tâches de rattrapage ouvertes créées par la règle. Cela s'applique à la fois à la vue de formulaire de règle et à la vue de liste.

Lorsqu'une affectation de tâche de rattrapage est faite ou modifiée, les champs **Groupe d'affectation** et **Affecté à** sont déployés sur tous les résultats des tests, à l'exception de ceux pour lesquels le groupe d'affectation du résultat des tests est différent de celui du RT. Pour en savoir plus sur les règles d'affectation, reportez-vous à Conformité de la configuration Vue d'ensemble des règles d'affectation. Ces affectations sont utilisées automatiquement pour ce groupe lors de l'importation suivante.

Suivre les nombres de reports pour les résultats des tests et les tâches de rattrapage

À partir de la version 14.3, suivez le nombre de fois où un résultat de test ou une tâche de rattrapage est différé dans le module Reports multiples. Une tâche planifiée, **définissez les nombres de reports**, s'exécute quotidiennement pour publier les nombres d'enregistrements qui sont différés plus d'une fois dans la colonne Nombre de reports dans les enregistrements répertoriés dans le module Plusieurs reports.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration des groupes de calculateurs et des calculateurs pour Conformité de la configuration

Les calculateurs de Configuration Compliance sont utilisés pour mettre à jour les valeurs d'enregistrement lorsque des conditions prédéfinies sont remplies. Les calculateurs sont regroupés en fonction des critères utilisés pour déterminer comment les enregistrements sont mis à jour.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Calculateurs de Configuration Compliance

L'application Configuration Compliance comprend deux types de calculateurs : les calculateurs de risque et les calculateurs de déploiement de score de risque. Ces groupes de calculateurs sont activés par défaut.

Le groupe de calculateurs de score de risque a été renommé Calculateurs de risque.

Les calculateurs de déploiement de score de risque comprennent des calculateurs de déploiement pour les tests de configuration et les tâches de rattrapage.

La configuration des calculateurs de risque et de déploiement pour le rattrapage des résultats des tests et des tâches de rattrapage comprend les tâches suivantes :

- Créer un calculateur de risque
- Créer un calculateur de déploiement de score de risque

Une fois que vous avez créé un calculateur de risque, il est disponible pour les calculs avec l'ingestion de données suivante. Après l'avoir créé, vous pouvez également préférer l'appliquer à la demande.

Pour plus d'informations sur les calculateurs et les groupes de calculateurs, reportez-vous à la section Conformité de la configuration Groupes de calculateurs.

Conformité de la configuration Vue d'ensemble de la gestion des exceptions

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive de sécurité ou de gestion des vulnérabilités publiée, vous pouvez demander une exception. La gestion des exceptions implique de demander, examiner, approuver ou rejeter des exceptions pour une tâche de rattrapage qui ne peut pas être corrigée conformément à la politique.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Certaines vulnérabilités peuvent ne pas disposer d'un correctif, d'un correctif ou d'une solution existante. Lorsqu'une exception est approuvée, cela signifie également que vous acceptez un risque, car vous reconnaissez et acceptez les conséquences de ne pas corriger la vulnérabilité liée à la configuration.

Cycle de vie d'une exception

Une exception est une demande de différer le rattrapage d'une tâche de rattrapage pour une période spécifiée.

Le cycle de vie d'une exception est le suivant :

- Demande d'une exception
- Approuver une demande d'exception
- Suivi d'une demande d'exception
- Expiration d'une demande d'exception

Demande d'une exception

En tant que propriétaire du rattrapage, vous pouvez demander une exemption pour une tâche de rattrapage à l'aide du processus de gestion des exceptions. Pendant le processus d'approbation, la tâche de rattrapage reste dans l'état **En cours de révision** . Une fois que l'approbateur d'exceptions a approuvé cette demande, la tâche de rattrapage passe à un état **Différé** .

Approuver une demande d'exception

Les tâches de rattrapage qui ne peuvent pas être corrigées immédiatement sont examinées, évaluées pour le risque et approuvées pour le report jusqu'à ce qu'elles puissent être corrigées. L'approbation d'une demande d'exception peut être un workflow à deux niveaux. Si seul l'approbateur de premier niveau est présent, l'exception peut être demandée et approuvée. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Consultez Ajouter un approbateur d'exception pour Conformité de la configuration pour plus d'informations.

Remarque :

À partir de la Conformité de la configuration version 13.0, si vous déployez l'application CC pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas le repasser en workflow.

Une fois qu'une demande d'exception pour une tâche de rattrapage est approuvée, vous pouvez effectuer les actions suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Rouvrir
- Fermer
- Supprimer

Remarque : Les commentaires sur le rejet sont affichés dans les notes de travail d'une tâche de rattrapage. Si une demande d'exception est rejetée, cette tâche de rattrapage revient à son état précédent.

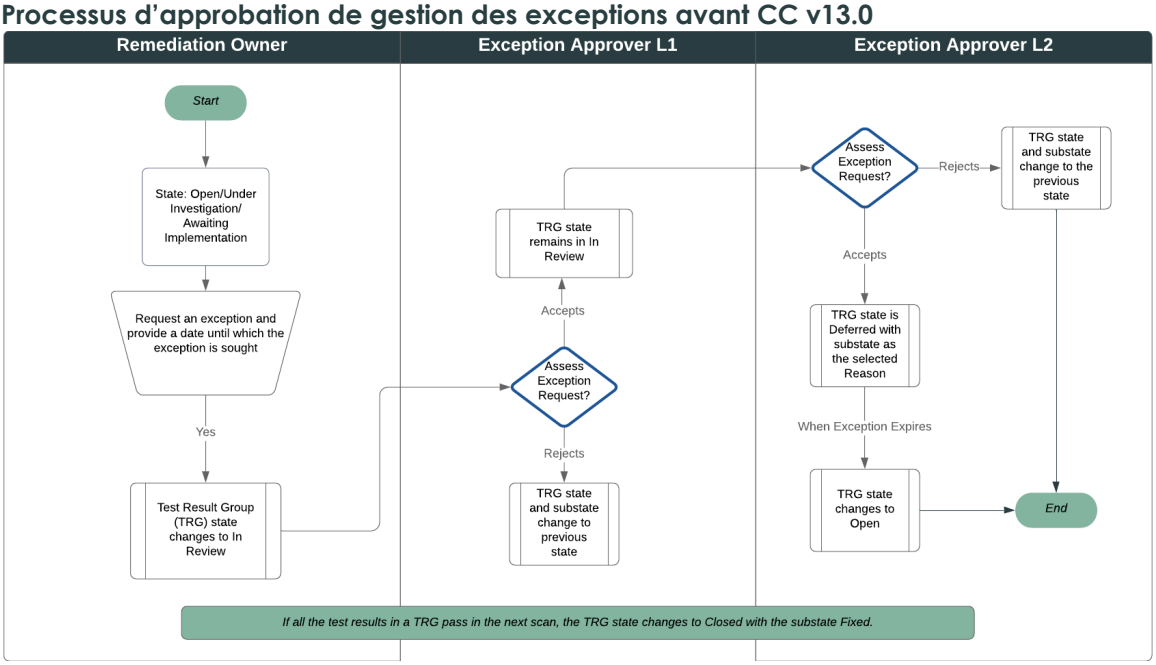
Suivi d'une demande d'exception

Après avoir déclenché l'exception, vous pouvez suivre son état à l'aide de l'onglet **Approbations de changement d'état** de la tâche de rattrapage. Si une action est effectuée sur une tâche de rattrapage, vous ne pouvez pas suivre l'état des résultats des tests individuels dans cette tâche de rattrapage.

Expiration d'une demande d'exception

Lorsqu'une demande d'exception pour une tâche de rattrapage expire, la tâche de rattrapage revient à son état **Ouvert** .

Processus d'approbation de gestion des exceptions avant CC v13.0



Conformité de la configuration Gestion des changements

En tant que propriétaire de rattrapage informatique, vous pouvez créer et gérer les demandes de changement (CHG) directement à partir des tâches de rattrapage (RT) dans l'application Conformité de la configuration .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Les demandes de changement et le Conformité de la configuration workflow

Les demandes de changement et la gestion des changements font partie du processus de rattrapage du Conformité de la configuration workflow. Au cours de cette phase de rattrapage, vous pouvez utiliser des demandes de changement pour vous aider à hiérarchiser, suivre et corriger les résultats des tests.

L'application Conformité de la configuration fonctionne avec le processus de Now Platform® gestion des changements informatiques pour vous aider à corriger les logiciels et les technologies non conformes dans votre environnement.

Avec Change Management dans l'application Conformité de la configuration , vous pouvez associer des résultats de tests à des demandes de changement existantes, ou diviser une tâche de rattrapage et créer une nouvelle tâche de rattrapage uniquement pour les résultats des tests sélectionnés.

Pour plus d'informations, consultez Créer une demande de changement dans Conformité de la configuration.

Termes clés

Tests

Les tests sont des bibliothèques d'enregistrements de données qui organisent les analyses des ressources informatiques. Les tests de configuration définissent la manière dont une classe d'actifs technologiques doit être gouvernée. Un test est tout ce qui peut être utilisé pour identifier une classe de logiciels ou un actif matériel non conforme.

Résultats des tests

Les résultats des tests sont importés par des intégrations tierces. Une fois visibles dans Conformité de la configuration, ils sont corrigés à l'aide de **tâches de rattrapage**. Les groupes sont affectés au rattrapage conformément aux règles d'affectation.

Remarque : À partir de la version 14.9 de , le résultat des Conformité de la configurationtests est étiqueté Résultat.

Tâche de rattrapage

Les résultats des tests sont regroupés en tâches de rattrapage en fonction des règles d'affectation et affectés automatiquement aux propriétaires de rattrapage pour le rattrapage.

Remarque : À partir de la version 14.9 de , le résultat du test est étiqueté Tâche de Conformité de la configurationrattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupes de tests

Les groupes de tests sont associés à des documents et des enregistrements de test faisant autorité. Un groupe de tests de configuration définit un groupe de tests.

Demandes de changement

Les demandes de changement vous aident à implémenter des processus contrôlés pour le rattrapage. Vous pouvez utiliser des demandes de changement avec des tâches de rattrapage pour Conformité de la configuration vous aider à identifier, suivre et résoudre les actifs non conformes (éléments de configuration) qui nécessitent des ressources supplémentaires ou que vous pouvez cibler pour le report.

Pour en savoir plus sur les résultats des tests et les tâches de rattrapage, reportez-vous à Conformité de la configuration Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage.

Quand utiliser les demandes de changement dans Conformité de la configuration

Les demandes de changement vous permettent de lancer et de suivre des activités de rattrapage sur vos résultats des tests. Lorsque les propriétaires de rattrapage ont un grand nombre de résultats des tests ou d'éléments de configuration non corrigés, ils peuvent utiliser des demandes de changement pour identifier les résultats des tests devant être reportés. Ils peuvent également identifier et regrouper les résultats des tests et les éléments de configuration qui nécessitent plus de ressources que celles initialement identifiées dans la tâche de rattrapage initiale.

Créer des demandes de changement à partir d'une tâche de rattrapage

Créez une demande de changement directement à partir d'une tâche de rattrapage pour tous les résultats des tests de la tâche de rattrapage, ou utilisez le filtrage pour identifier uniquement les résultats des tests qui correspondent à des critères spécifiques. Créez une demande de changement avec des informations pré-remplies pour accélérer votre examen des résultats des tests qui nécessitent une intervention manuelle.

Diviser une tâche de rattrapage

À partir d'une tâche de rattrapage existante, identifiez un sous-ensemble de résultats des tests que vous souhaitez déplacer vers une nouvelle tâche de rattrapage. En créant un nouveau TRG, vous pouvez utiliser un groupe spécifique de résultats des tests sans affecter la tâche de rattrapage d'origine.

Associer les résultats des tests à une demande de changement existante

Associez les résultats des tests aux tâches existantes pour éviter de créer des demandes de changement en double pendant que vous résolvez vos tâches de rattrapage. En associant une tâche de rattrapage à une demande de changement déjà disponible dans votre instance, vous pouvez utiliser une liste de tâches existante.

Types de demandes de changement pour une tâche de rattrapage

Vous pouvez créer, approuver, implémenter, examiner et fermer des demandes de changement directement à partir des tâches de rattrapage qui vous sont affectées. Vous pouvez créer trois types de demandes de changement avec des informations pré-remplies à partir d'une tâche de rattrapage :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Standard. Un changement pré-autorisé à risque faible, relativement commun et qui suit une procédure ou une instruction de travail spécifique.
- Normal. Les demandes de changement normal suivent un processus prescriptif qui requiert deux niveaux d'approbation avant leur implémentation, revue et fermeture.
- Urgence. Un changement pour résoudre un incident majeur.

Installation, installation et configuration de l'application Conformité de la configuration

Avant d'exécuter l'application dans votre Now Platform® instance, vous devez d'abord télécharger et installer l'application Conformité de la configuration à partir du ServiceNow® Store. Cette application est disponible sous forme d'abonnement distinct.

Suivez les étapes suivantes de la liste de vérification de configuration répertoriées dans le tableau suivant avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Pour plus d'informations sur les versions mises en production de l'application Conformité de la configuration , ainsi que sur les applications tierces et ServiceNow compatibles avec elle, consultez l'article Matrice de compatibilité de Vulnerability Response et Changements de schéma de mise en production [KB0856498] dans la base de connaissances HI.

Pour plus d'informations sur l'obtention d'autorisations pour les applications du Store, reportez-vous à la section .

Configurer les tâches de la liste de vérification

Tâches de configuration	Description
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte le rôle d'administrateur de Configuration Compliance [sn_vulc.admin]. • L'administrateur Configuration Compliance [sn_vulc.admin] supervise la configuration et vérifie les résultats attendus. • Le propriétaire du rattrapage [sn_vulc.remediation_owner] lit et met à jour les enregistrements affectés. Le rôle sn_vulc.remediation_owner est également automatiquement attribué lorsqu'un utilisateur se voit attribuer le rôle itil.
Intégrations prises en charge	Avant de pouvoir Conformité de la configuration corriger des éléments de configuration, vous devez installer une intégration de scanner tiers et effectuer au moins une analyse réseau.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les tâches de la liste de vérification (suite)

Tâches de configuration	Description
	Vérifiez que l'application Réponse aux vulnérabilités est installée et activée avant de configurer les intégrations tierces prises en charge. Consultez Installer Réponse aux vulnérabilités. Pour vérifier que les applications d'intégration sont installées et activées, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Pour en savoir plus sur les intégrations tierces et obtenir la liste des produits pris en charge, reportez-vous Intégrations de Conformité de la configurationà .

Qualys Vulnerability Integration

- Si le Qualys Vulnerability Integration est déjà installé sur votre système et que vos informations d'identification d'API sont différentes de celles que vous souhaitez utiliser pour Conformité de la configuration, accédez à l'Assistant de configuration (dans Réponse aux vulnérabilités) et affectez-les à chaque intégration **Qualys PC** .
- Accédez à la **Intégration de vulnérabilité Qualys** > **Intégrations principales** et modifiez le champ **Informations d'identification de l'API Qualys** sous l'onglet **Détails REST Qualys** .

Pour plus d'informations sur le Qualys Vulnerability Integration, reportez-vous à la section Présentation de Qualys Vulnerability Integration.

Vous êtes maintenant prêt à installer l'application Conformité de la configuration . Consultez Installer Conformité de la configuration.

Installer Conformité de la configuration

Avant d'exécuter Conformité de la configuration dans votre Now Platform® instance, vous devez d'abord télécharger et installer l'application Conformité de la configuration à partir du ServiceNow Storefichier . Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Voir pour les Installation, installation et configuration de l'application Conformité de la configuration tâches de configuration. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

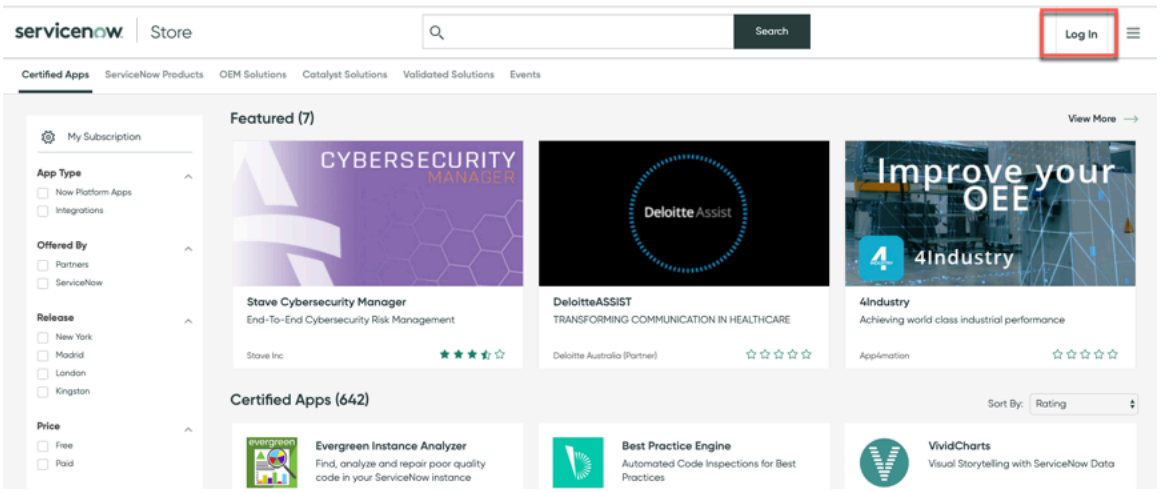
Rôle requis : administrateur

Traduction automatique

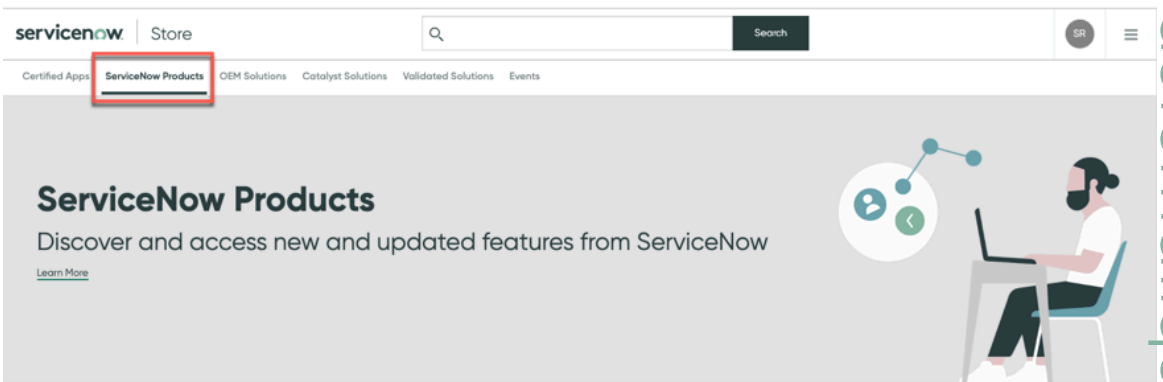
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Pour obtenir une autorisation et télécharger l'application Conformité de la configuration principale, accédez ServiceNow Storeau .
2. En haut à droite de la page, cliquez sur **Se connecter**.



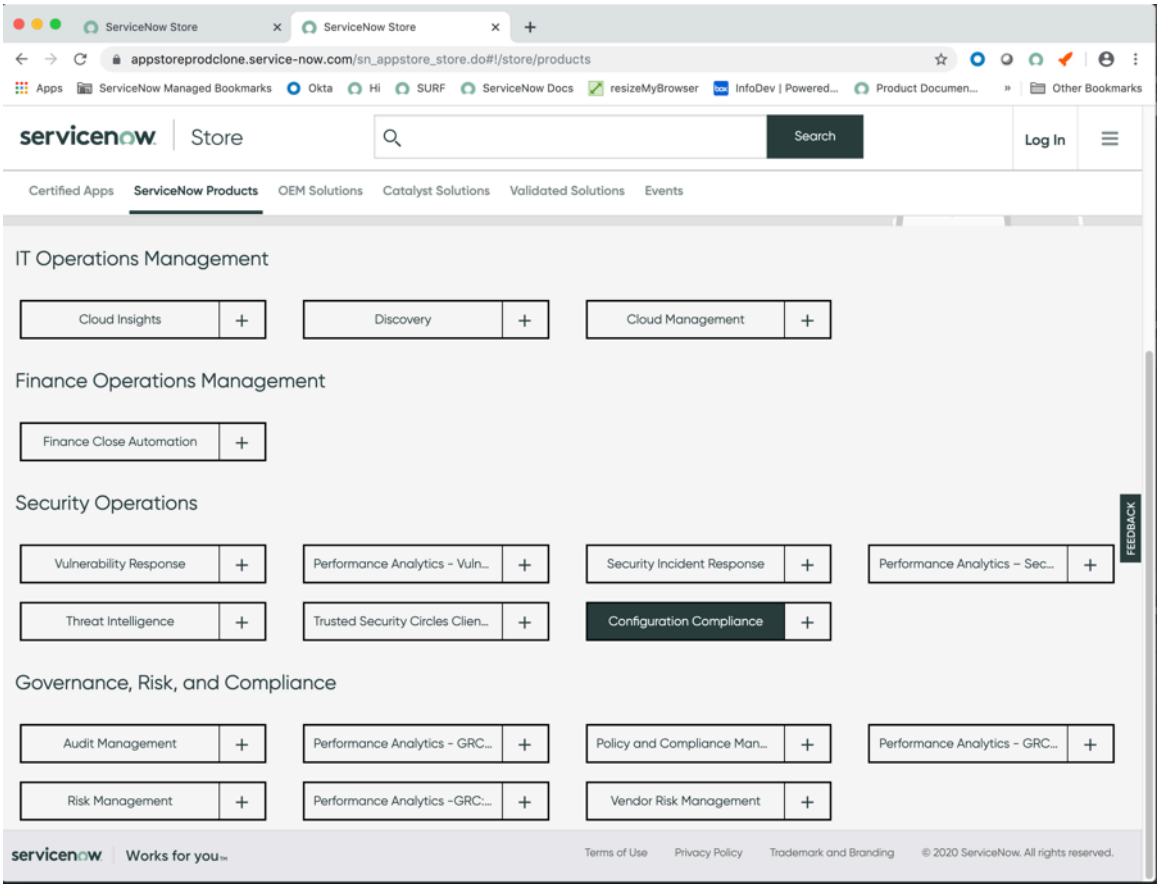
3. Dans la boîte de dialogue qui s'affiche, saisissez vos informations d'identification HI et cliquez sur **Connexion**.
4. Sur la page qui s'affiche, si elle n'est pas sélectionnée, cliquez sur l'onglet **Produits ServiceNow** .



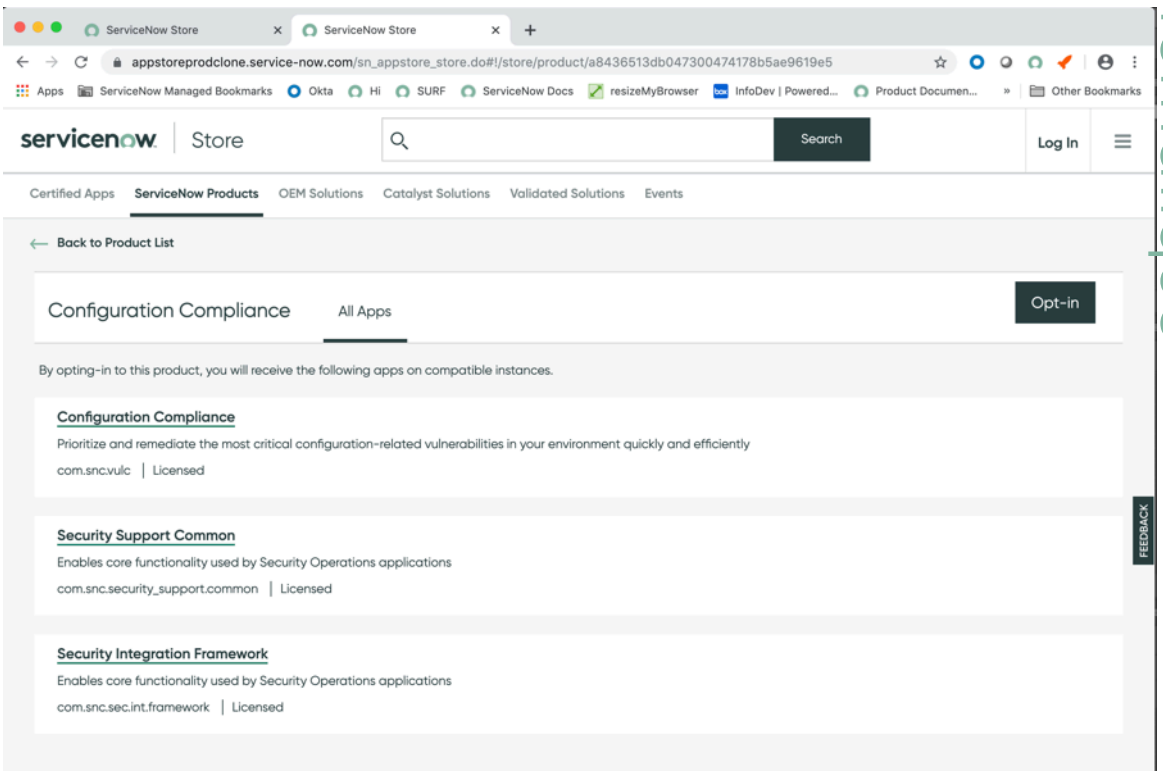
5. Pour afficher les applications associées auxquelles vous êtes éligible avec l'application, sur la page de liste des Conformité de la configuration produits, cliquez sur le produit **Configuration Compliance** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La page qui s'affiche répertorie toutes les applications auxquelles vous êtes éligible si vous optez. Pour plus d'informations sur une application, cliquez sur un lien.

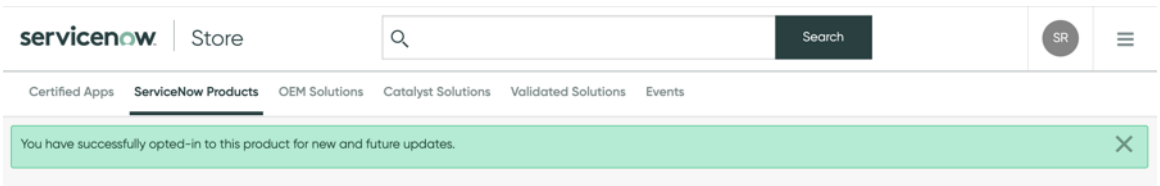


6. Pour obtenir l'application Conformité de la configuration , cliquez sur **S'abonner**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Pour accepter les termes et conditions, à l'invite, cochez la case et cliquez sur **Accepter**. Un message s'affiche qui indique que vous avez adhéré avec succès à l'application.



Lorsque l'onglet ServiceNow Produits est sélectionné dans la liste des produits, une coche verte remplace le signe plus à droite de l'application Conformité de la configuration , comme illustré dans la figure suivante.

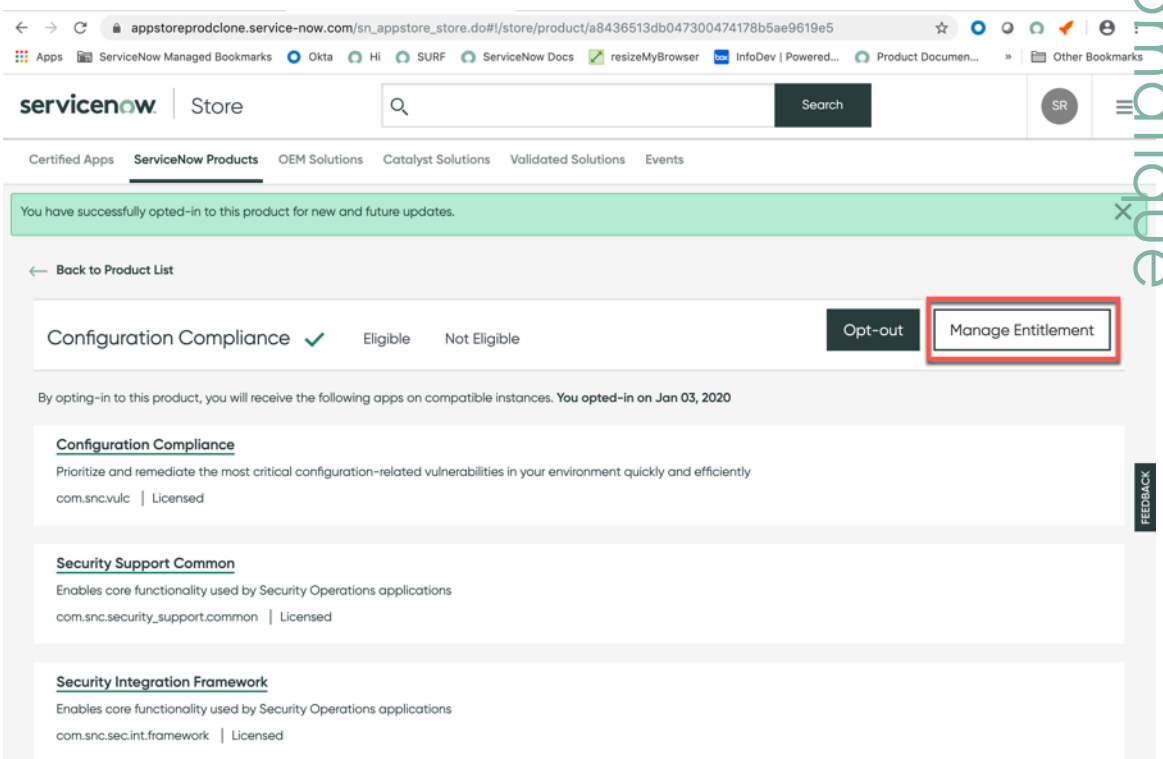


Une fois que vous avez accepté les termes et conditions et les autorisations gérées pour l'une des applications de l'onglet **Produits ServiceNow** , sur la page Liste des produits, vous pouvez cliquer sur le signe plus (+) pour obtenir l'autorisation et l'adhésion aux autres applications de cette page en un seul clic.

8. Passez à l'étape 10 pour installer l'application sur votre Now Platform instance.
9. Facultatif : Si vous souhaitez gérer votre autorisation pour l'application Conformité de la configuration sur d'autres Now Platform instances, suivez également les étapes suivantes.

   a. Si le bouton Gérer l'autorisation n'est pas affiché, cliquez sur l'application Conformité de la configuration dans la liste de produits pour l'afficher.

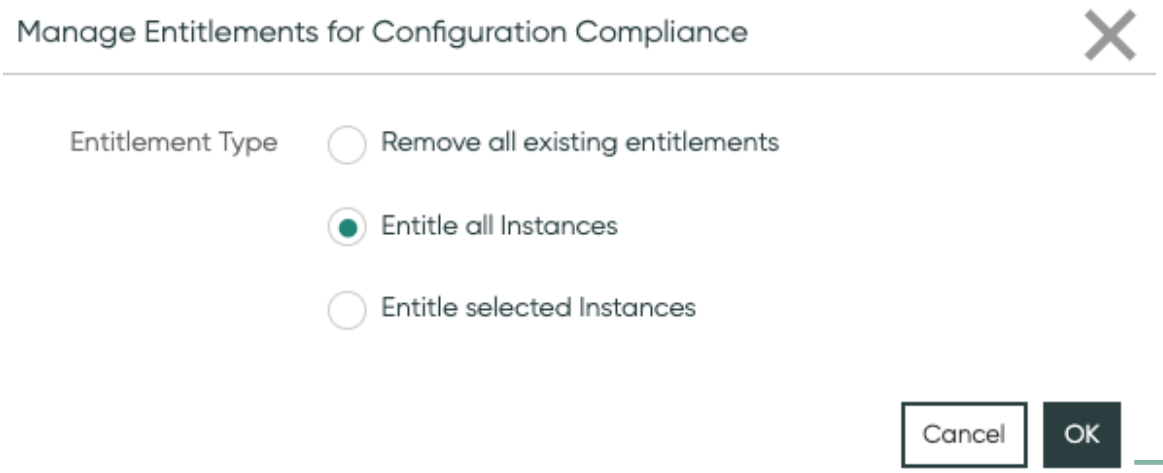
   b. Cliquez sur **Gérer les autorisations**.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Dans la boîte de dialogue Gérer les autorisations pour Configuration Compliance qui s'affiche, choisissez l'une des options suivantes :

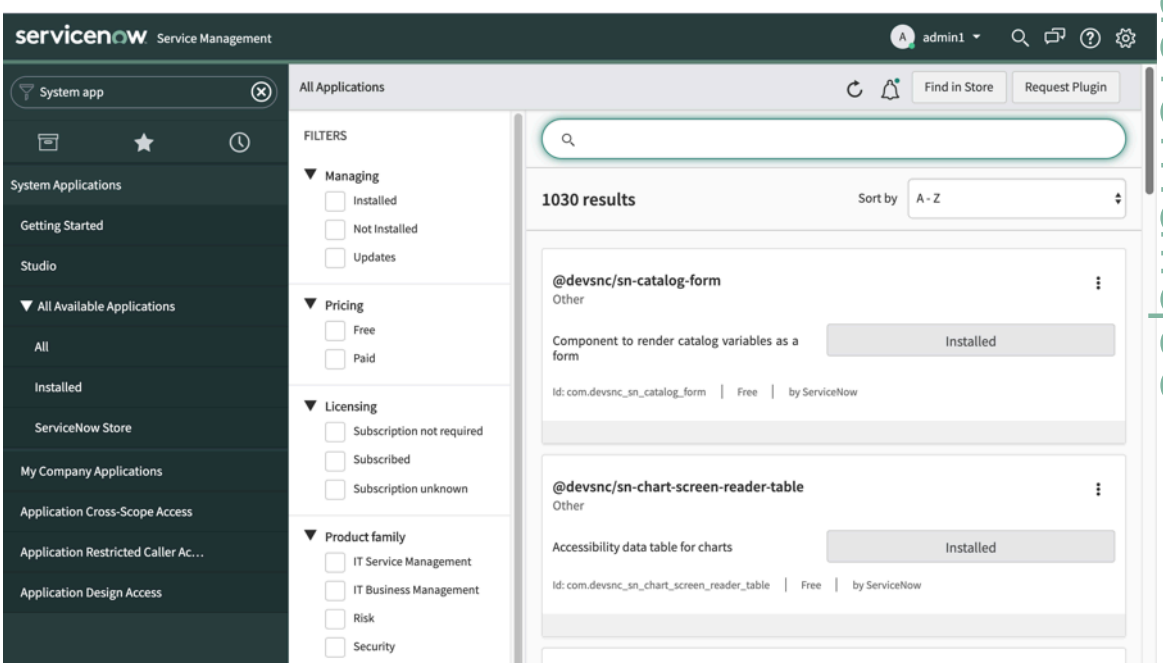


d. Cliquez sur **OK** ou **Annuler** pour continuer.

Vous êtes prêt à activer les modules d'extension et à installer l'application sur votre ou vos Now Platform instances.

10. Connectez-vous à l'instance Now Platform sur laquelle vous souhaitez installer l'application Conformité de la configuration .

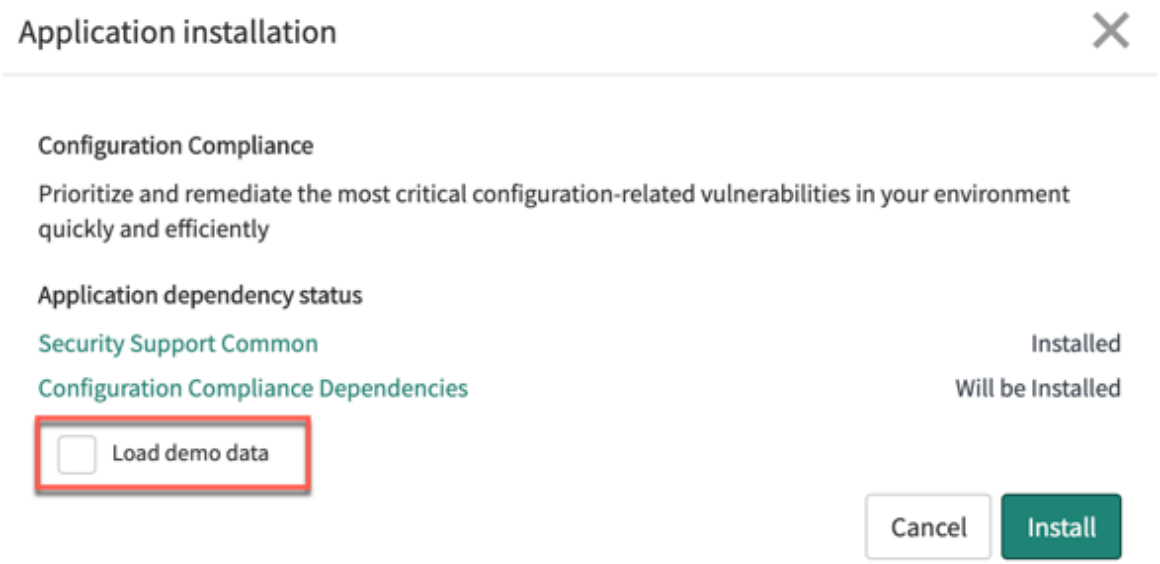
11. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tout**.



12. Dans les applications répertoriées, localisez l'application Conformité de la configuration (sn_vulc) et cliquez sur **Installer**.
La boîte de dialogue d'installation de l'application s'affiche. Toutes les dépendances qui seront installées sont affichées.

Traduction automatique

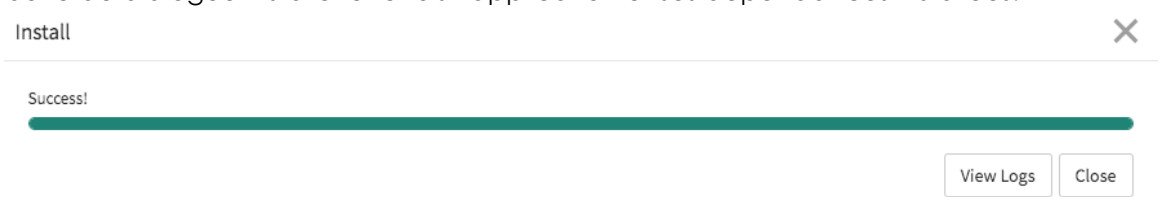
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



13. Si vous souhaitez des données de démonstration, cochez la case Charger les données de démonstration et cliquez sur **Installer**.

> **Remarque :** Si vous ne cochez pas la case **Charger les données de démonstration** , les données de démonstration ne peuvent pas être installées ultérieurement à partir d'Application **Manager** . Pour plus d'informations sur l'installation ou la réinstallation de données de démonstration après l'installation initiale, consultez l'article Solution de contournement pour installer des données de démonstration si l'application est déjà installée [KB0722909] dans la base de Now Support connaissances.

Cette installation peut prendre un certain temps. Un message s'affiche dans la boîte de dialogue Installer une fois l'application et ses dépendances installées.



14. Cliquez sur **Fermer**.

Des modules d'extension SCA tiers distincts acquièrent et transforment des données au format Conformité de la configuration. Avant de pouvoir Conformité de la configuration corriger des éléments de configuration, vous devez installer une intégration de scanner tiers et effectuer au moins une analyse réseau.

Pour en savoir plus sur l'installation d'intégrations tierces pour , reportez-vous à Conformité de la configurationla section Intégrations de Conformité de la configuration.

Composants installés avec Conformité de la configuration

Plusieurs types de composants sont installés avec l'activation du module d'extension Conformité de la configuration, y compris les tables et les rôles d'utilisateur.

> **Remarque :** La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les données de démonstration sont disponibles pour cette fonctionnalité.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Afficher les listes filtrées pour les composants installés avec une application

Filtrez la table Fichiers d'applications afin que seuls les rôles, les travaux planifiés et les tables installés avec une application s'affichent. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés sur l'instance et dans la table de métadonnées. Procédez comme suit pour afficher les listes filtrées à partir de la table Fichiers d'applications.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application. Par exemple : **Application** > **est** > **Réponse aux vulnérabilités**.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, sélectionnez **ET**, puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
Administrateur Configuration Compliance [sn_vulc.admin]	Capable de modifier la propriété de l'application, la configuration, les règles de mise à jour, les intégrations de l'application Conformité de la configuration . À partir de la version 15.0, un utilisateur administrateur ne peut pas supprimer	sn_vulc.write **Remarque :** Hérite des rôles requis pour l'administration des enregistrements de l'application Configuration Compliance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	d'enregistrements sources tels que des expliots, des CVE, etc.	
lu [sn_vulc.read]	Lisez les listes et les enregistrements dans Configuration Compliance.	sn_sec_cmn.calc_read
write [sn_vulc.write]	Écrire des listes et des enregistrements dans Configuration Compliance.	• sn_vulc.read • sn_vulc.remediation_owner
Écrire l'affectation [sn_vulc.write_assignment	Écrire dans les champs d'affectation du résultat de test.	Contenu dans le rôle sn_vulc.remediation_owner.
Propriétaire de la résolution sn_vulc.remediation_owner	Affichez et mettez à jour l'autorisation pour les résultats des tests affectés à vous ou à votre groupe.	Contenu dans le rôle itil. Contient : • sn_sec_cmn.read • sn_vulc.write_assignment
CC.Système sn_vulc.import_admin	Exécute tous les travaux planifiés dans l'application Configuration Compliance. **Remarque :** Cet utilisateur est l'utilisateur d'exécution par défaut pour chaque tâche planifiée dans Configuration Compliance.	• sn_vulc.write • import_admin • sn_vul_tenable.read_integration
VRCommon.Système sn_vul_cmn.admin	Exécuter en tant qu'utilisateur par défaut pour tous les travaux planifiés dans l'application commune	• sn_vul_cmn.write • sn_sec_cmn.admin • report_admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	Vulnerability Response.	
SecCommon.System sn_sec_cmn.admin	Exécuter en tant qu'utilisateur par défaut pour tous les travaux planifiés utilisés pour l'option de tâches en arrière-plan dans l'application commune d'assistance de sécurité	• sn_sec_cmn.int_write • sn_sec_cmn.write • workflow_admin • sn_sec_cmn.calc_write • sn_sec_core.read_dictionary • sn_sec_cmn.manage_approval_rules • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.gérer_les_règles_de_classification • sn_sec_cmn.manage_background_job
V14.7 : sn_vulc.edit_watch_topic	Modifiez les rubriques de surveillance pour Configuration Compliance.	sn_vulc.read_watch_topic
V14.7 : sn_vulc.read_watch_topic	Lisez les rubriques de surveillance de Configuration Compliance.	cmdb_read
V14.7 : sn_vulc.create_watch_topic	Créez des rubriques de surveillance pour Configuration Compliance.	sn_vulc.read_watch_topic
sn_vulc.auditeur	Autoriser la lecture pour tous les modules Configuration Compliance	sn_vulc.read sn_vulc.advanced_read
sn_vulc.advanced_read	Autoriser la lecture pour tous les modules d'administration de Configuration Compliance	sn_vulc.read_auto_close_rules sn_vulc.read_exception_configuration sn_vulc.read_assignment_rules sn_vulc.read_task_rules sn_vulc.read_auto_exception_rule sn_vulc.read_notifications sn_vulc.read_risk_score_configuration sn_vulc.read_test_criticality_mapping

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
		sn_sec_cmn.read_approval_rules sn_vulc.read_auto_delete sn_vulc.read_remediation_target_rules
sn_vulc.read_test_criticality_mapping	Autoriser la lecture pour le mappage de criticité de test	
sn_vulc.read_task_rules	Autoriser la lecture pour les règles de tâche de rattrapage	
sn_vulc.read_assignment_rules	Autoriser la lecture pour les règles d'affectation	
sn_vulc.read_risk_score_configuration	Autoriser la lecture pour la configuration du score de risque	
sn_vulc.read_auto_close_rules	Autoriser la lecture pour la configuration de fermeture automatique	
sn_vulc.false_positive_approver	Permet d'approuver/ de rejeter la fermeture des tâches de rattrapage en tant que faux positif	
V15.0 : sn_vulc.delete	Supprime les enregistrements sources.	

Traduction automatique

Travaux planifiés installés

Tâche planifiée	Description
V15.0 : Mettre à jour le groupe de tests sur les tests de configuration	Met à jour le groupe de tests sur les tests pour les sources Tenable et Microsoft Defender. Il s'agit d'un travail ponctuel.
V15.0 : renseigner les champs de résultats des tests existants	Met à jour les valeurs dans les colonnes nouvellement ajoutées (telles que Âge, Âge fermé, Actif, etc.) dans la table des résultats des tests, les filtres enregistrés et les modules. Il s'agit d'un travail ponctuel.
V15.0 : remplir la table CI vulnérables, supprimer et remplir	Renseigne le nombre total d'enregistrements dans la table CI vulnérables. Il s'agit d'un travail ponctuel.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
à nouveau pour les résultats des tests	
Édition 12.0 Calculer les mesures de rattrapage pour tous les groupes de résultats des tests	Calcule et met à jour les valeurs des mesures d'état sur les enregistrements de tâches de rattrapage.
Version 12.0 : Calculer les mesures de rattrapage pour tous les résultats des tests	Calcule et met à jour les valeurs des mesures d'état dans les enregistrements de résultats des tests.
Version 12.0 : Synchronisation de l'état de la demande de changement	Tâche à la demande qui synchronise les états de toutes les tâches de rattrapage (RT) existantes avec les demandes de changement (CHG). Au fur et à mesure qu'une demande de changement avance dans son cycle de vie, elle déplace automatiquement les états de toutes les tâches de rattrapage connexes. Active la synchronisation d'état à partir de maintenant.
Version 11.1 : Vérifier le report des groupes de résultats des tests Expiration	Envoie des notifications si les tâches de rattrapage ont expiré (et si elles expirent dans une semaine).
Nombre de CI Configuration Compliance	Renseigne le nombre d'éléments de configuration (CI) distincts et la moyenne mobile de 90 jours dans la table Nombre d'éléments de configuration [sn_vulc_cc_configuration_item_count].
Version 11.1 : Évaluer et notifier les cibles de rattrapage	Définit ou met à jour les dates cibles de rattrapage sur tous les résultats des tests. Détermine l'état des dates cibles de rattrapage par rapport aux règles. Envoie des notifications
V14.7 : Insérer des groupes de résultats des tests dans une tâche de rattrapage unifiée	Tâche planifiée unique pour insérer toutes les tâches de rattrapage créées dans l'interface utilisateur classique dans la tâche de rattrapage unifiée (sn_vul_remediation_task).
Version 12.0 : Renseigner CR-TRG m2m pour CR et CR-Parent	Remplit les demandes de changement sur les tâches de rattrapage.
Supprimé dans la version 11.1 : réouverture des groupes de résultats des tests différés	Rouvre les groupes différés lorsque la date d'échéance est passée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Remarque : Obsolète pour les versions antérieures à la version 11.1. Ne pas utiliser.	
Réappliquer toutes les règles d'affectation	Réapplique toutes les règles d'affectation.
Version 14.3 : Nombre de réaffectations pour les règles d'affectation	S'exécute quotidiennement et publie le nombre total de résultats des tests et de tâches de rattrapage non affectés par cette fonctionnalité pour une règle d'affectation particulière.
Réévaluer l'état des groupes de résultats des tests	Réévalue l'état des tâches de rattrapage pour les entrées où **assess_state** est faux. S'exécute toutes les 15 minutes.
Déployer le score de risque du résultat de test au groupe de résultats de test et au test de configuration	S'exécute toutes les heures et calcule les scores de déploiement pour les tests de configuration et les tâches de rattrapage modifiés. • Calcule le score de risque de déploiement pour tous les tests en sn_vulc_test_manifest et supprime l'enregistrement de manifeste une fois l'opération terminée. • Calcule le score de risque de déploiement pour tous les tests en sn_vulc_result_group_manifest et supprime le manifeste une fois l'opération terminée.
Version 12.0 : Mettre à jour les mesures de rattrapage de la politique	À partir de la version 15.0 de , cette tâche planifiée a été renommée Mettre à jour les mesures de Conformité de la configurationrattrapage. • Calcule et met à jour les valeurs des mesures d'état dans les enregistrements de politique. • Calcule le % de conformité des résultats des tests d'un CI sur l'élément détecté.
Version 14.3 : Définir les nombres de reports	Collecte le nombre de fois où un résultat de test ou une tâche de rattrapage est reporté.
Mettre à jour la cote de risque pour les résultats des tests	Met à jour la cote de risque pour les résultats des tests.
Mettre à jour le score de risque de déploiement pour tous les groupes de résultats et tous les	Met à jour le score de risque de déploiement pour tous les groupes de résultats et Conformité de la configuration tous les tests non fermés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
tests de configuration non fermés.	

Tables installées

Table	Description
Règle d'affectation [sn_vulc_assignment_rule]	Contient l'ensemble des règles évaluées pour définir le groupe d'affectation sur les résultats des tests.
Source de référence [sn_vulc_auth_src]	Stockez les sources de référence importées.
Calculateur [sn_vulc_calculator_risk_score]	Contient le calculateur qui définit certains champs de résultat de test lorsque certaines conditions sont remplies.
Nombre d'éléments de configuration CC [sn_vulc_cc_configuration_item_count]	Contient le nombre total d'éléments de configuration.
Version 12.0 : Association de demandes de changement [sn_vulc_action_associate_cr]	Table intermédiaire utilisée pour associer des demandes de changement à des tâches de rattrapage.
Version 12.0 : création de demandes de changement [sn_vulc_action_create_cr]	Table intermédiaire utilisée pour créer des formulaires de demande de changement.
Version 12.0 : formulaire de demande de changement [sn_vulc_cr_form]	Table de base pour la gestion des demandes de changement.
Contenu source d'autorité [sn_vulc_citation]	Contient le contenu des documents de référence importés
Test de configuration [sn_vulc_test]	Contient les données de test de configuration importées.
Manifeste de test de configuration [sn_vulc_test_manifest]	Contient les tests de configurations pour lesquels le score de risque de déploiement doit être calculé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Version 12.2 Table d'actifs manquante [sn_vul_missing_asset]	Contient des enregistrements d'actifs temporaires pour les données d'évaluation de Configuration Compliance importées avec des actifs sans correspondance.
Technologie de test de la configuration [sn_vulc_test_technology]	Contient les technologies de test de configuration importées.
Règle de groupe [sn_vulc_grouping_rule]	Contient les règles qui définissent les critères avec lesquels les groupes sont automatiquement créés pour un ensemble de résultats des tests.
Politique [sn_vulc_policy]	Contient les politiques importées.
Test de configuration de la politique [sn_vulc_policy_test]	Contient les données de test de configuration de politique importées.
Règle de cible de rattrapage [sn_vulc_ttr_rule]	Définit le délai prévu pour corriger un résultat de test.
Calculateurs de risque [sn_vulc_calculator_group]	Contient le groupe de Conformité de la configuration calculateurs. L'ordre du groupe de calculateurs détermine quel groupe est évalué en premier, et dans chaque groupe, un calculateur au maximum est utilisé.
Calculateur de déploiement des scores du risque [sn_vulc_risk_score_rollup]	Contient les configurations du calculateur de cumul.
Diviser le groupe de résultats des tests [sn_vulc_action_split_trg]	Table intermédiaire utilisée pour diviser les tâches de rattrapage.
Approbation de changement de l'état [sn_vulc_state_change_approval]	Contient les données du processus d'état d'approbation.
Technologie [sn_vulc_technology]	Contient les technologies importées.
Tester le mappage de criticité	Contient des données de mappage de criticité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vulc_test_criticality_map]	
Résultat de test [sn_vulc_result]	Contient les résultats des tests importés.
Groupe de résultats des tests [sn_vulc_result_group]	Contient les tâches de rattrapage importées.
Version 12.0 : Demandes de changement de groupe de résultats de test	Contient des demandes de changement pour les tâches de rattrapage.
Manifeste de groupe de résultats de test [sn_vulc_result_group_manifest]	Contient les tâches de rattrapage pour lesquelles le score de risque de déploiement doit être calculé.
Groupes de résultats des tests [sn_vulc_m2m_result_result_group]	Contient les données de la tâche de rattrapage.
Historique des résultats des tests [sn_vulc_result_history]	Contient l'historique des résultats des tests importés.
État de rattrapage des résultats des tests	État du résultat du test par rapport à la règle de cible de rattrapage appliquée la plus proche.
V14.7 : Nombres de tests de rubriques de surveillance [sn_vulc_wt_test_counts]	Table de cache pour l'onglet Tests de configuration distincts dans l'espace de travail du gestionnaire de vulnérabilité.

Traduction automatique

Créer ou modifier des Conformité de la configuration règles d'affectation

Créez des règles pour affecter automatiquement les résultats des tests en fonction des conditions de filtre. Ces règles affectent les résultats des tests au fur et à mesure qu'ils sont importés.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Le système de base est livré avec une règle d'affectation Conformité de la configuration , **Affecter au groupe de support CI**, qui affecte les résultats des tests au même groupe d'affectation que le groupe de support CI. Cette règle est désactivée par défaut.
Vous pouvez effectuer des modifications à l'aide de conditions de filtre. Avec les règles d'affectation, vous définissez une ou plusieurs conditions d'affectation et l'ordre d'exécution.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois qu'un résultat de test correspond à une condition de règle, la recherche d'affectation s'arrête.

Remarque : Les règles nouvelles ou mises à jour sont automatiquement évaluées lors de l'importation suivante ou manuellement à l'aide du bouton **Appliquer les changements** de la liste Règles d'affectation.

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Règles d'affectation**.
2. Ouvrez la règle du **groupe de support Affecter à un CI** ou cliquez sur **Nouveau**.
3. Modifiez la règle **Affecter au groupe de support CI** ou, si elle est **Nouvelle**, remplissez les champs du formulaire comme il convient.

Règle d'affectation de Configuration Compliance

Champ	Description
Nom	Nom de la règle de groupe.
Ordre d'exécution	Ordre dans lequel les règles sont évaluées. Le nombre le plus bas est évalué en premier. Les règles de priorité élevée, les résultats des tests qui nécessitent une gestion spéciale, lorsque le risque est critique, ou un résultat de test qui doit être traité par la conformité réglementaire, doivent être exécutés en premier. Ensuite, exécutez vos règles générales, où aucune manipulation spéciale n'est requise, et vous savez qui doit en être responsable. Enfin, créez une règle par défaut pour affecter les résultats des tests au groupe afin de déterminer à quel groupe d'affectation ils doivent appartenir. Ce groupe pourrait ajouter une autre règle pour couvrir ses décisions. Cette règle par défaut s'exécute en dernier.
Actif	Indique si la règle d'affectation est active.
Condition	
Champs de condition	Conditions qui doivent être remplies. La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.
Nouveau critère	Ajoute d'autres champs de filtre de condition au choix.
Description	Texte décrivant la règle d'affectation.
Affecter à l'aide de	Pour automatiser l'affectation des groupes créés en fonction de cette règle, choisissez l'une des options disponibles. ◦ Groupe d'utilisateurs : sélectionner un groupe d'utilisateurs dans la table de recherche ◦ Champ de groupe d'utilisateurs : sélectionnez un champ de groupe d'utilisateurs dans le menu déroulant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Script : créer ou modifier un script. **Remarque :** La création ou la modification d'un script nécessite ServiceNow une expertise.
Champ du groupe d'utilisateur	Sélectionnez le groupe d'utilisateurs responsable de la correction des tests qui correspondent aux conditions des règles d'affectation.

4. Cliquez sur **Envoyer**.

Conformité de la configuration Règles de cibles de rattrapage

Avec les règles de cibles de rattrapage, vous pouvez définir les délais prévus pour le rattrapage des résultats des tests. Vous pouvez envoyer des notifications aux utilisateurs et aux groupes lorsque les dates cibles approchent et lorsqu'elles sont dépassées.

Rôles requis : administrateur de Configuration Compliance (sn_vulc_admin) ou gestionnaire disposant du rôle sn_vulc.manage_remediation_target_rules.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Règles de cibles de rattrapage

Une tâche planifiée s'exécute *Evaluate and notify remediation targets*quotidiennement et utilise des règles de cibles de rattrapage actives pour évaluer les enregistrements de résultats des tests actifs. Chaque fois que des enregistrements de résultats de test associés à des tâches de rattrapage sont mis à jour ou modifiés, les valeurs modifiées sont évaluées par les règles cibles, et les changements sont déployés et affichés sur les tâches de rattrapage associées.

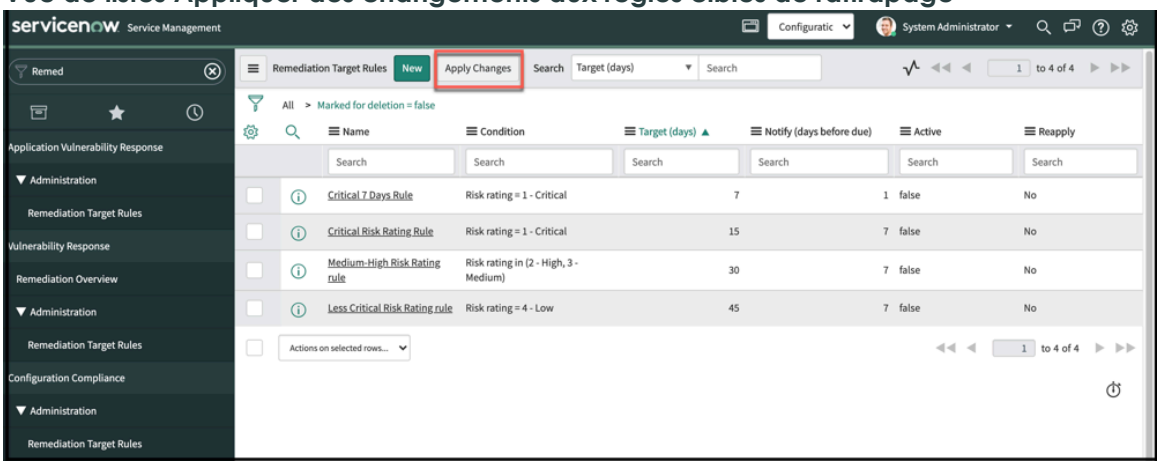
Vous pouvez modifier, désactiver ou supprimer des règles de cible de rattrapage existantes et en créer de nouvelles. Lorsque vous modifiez, désactivez ou créez une règle, vous pouvez cliquer sur **Appliquer les changements** dans la vue de liste Règles de cibles de rattrapage et appliquer manuellement les changements que vous avez introduits avant la tâche planifiée suivante. Avec cette option, vous pouvez réévaluer vos enregistrements de résultats de test sans avoir à attendre. Si vous choisissez de ne pas appliquer vos changements manuellement, la tâche planifiée quotidienne suivante récupère vos changements et les applique.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Règles de cibles de rattrapage** pour afficher les règles de cibles de rattrapage.

Vue de listes Appliquer des changements aux règles cibles de rattrapage



2. Cliquez sur une règle dans la colonne Nom pour ouvrir son enregistrement.
3. Cochez la case **Actif** sur l'enregistrement de règle de cible de rattrapage pour activer (`vrai`) toutes les règles désactivées (`faux`).

Chaque fois que vous modifiez ou ajoutez une règle cible, que vous choisissiez d'appliquer les modifications manuellement ou d'attendre la tâche planifiée suivante, vos modifications sont utilisées pour évaluer tous les résultats des tests actifs, ainsi que toutes les autres règles cibles affectées par vos modifications. Lorsque vous choisissez d'appliquer manuellement les changements, cette évaluation peut prendre un certain temps si vous avez un volume important de résultats de tests actifs, car toutes les règles impactées par vos changements sont utilisées pour une évaluation.

Par exemple, la valeur par défaut pour les jours de rattrapage ciblés est 30. Si vous créez une règle qui dispose également de 30 jours pour le rattrapage ciblé, cette règle et toutes les règles cibles dont les dates cibles sont 30 jours ou plus sont chacune appliquées à vos résultats des tests.

Règles cibles désactivées et supprimées

Lorsqu'une règle est `active, vrai` s'affiche dans la colonne Active de la vue de liste Règles de cibles de rattrapage. Lorsqu'une règle est désactivée (`faux`), elle n'est plus appliquée aux nouveaux résultats des tests. Toutefois, la tâche planifiée continue de suivre tous les résultats des tests existants auxquels la règle a été appliquée. Si la ou les règles désactivées sont réactivées par la suite, tout résultat de test avec un champ **Date cible de rattrapage** vide est évalué par rapport aux règles réactivées. Cela inclut les résultats des tests créés alors que les règles ont été désactivées.

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

Pour désactiver une règle, dans l'enregistrement de règle de cible de rattrapage, désactivez la case à cocher active et cliquez sur **Mettre à jour**. `Faux` s'affiche dans la colonne Active de la vue de liste Règles de cibles de rattrapage.

Pour supprimer une règle, cliquez sur **Supprimer** dans le formulaire ou, dans la vue de liste, sélectionnez la ou les règles et cliquez sur **Supprimer** dans la liste **Actions sur les lignes** . La

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

règle n'est plus affichée dans la liste et la règle suivante dans l'ordre d'opération remplace la règle supprimée.

Si vous désactivez ou supprimez une règle et choisissez d'appliquer vos changements avant la tâche planifiée suivante, la référence de règle est effacée du champ, mais la date de rattrapage et les données d'état sont conservées. Si vous n'appliquez pas vos changements manuellement, la référence à la règle est effacée du champ avec la tâche planifiée suivante.

À propos des règles cibles et de la tâche planifiée Évaluer et notifier les cibles de rattrapage

La *Evaluate and notify remediation targets* tâche planifiée s'exécute une fois à 4:30:00 quotidiennement. Il sélectionne toutes les règles de cibles de rattrapage actives et évalue tous les résultats des tests actifs en commençant par les résultats des tests dont la date cible de rattrapage est la plus précoce. Il évalue tous les résultats des tests qui répondent aux critères suivants :

- Ne sont pas dans un état **Fermé** .
- N'a pas de date cible de rattrapage.
- Les dates cibles de rattrapage sont postérieures aux dates indiquées dans les règles de cibles de rattrapage.
- Ils sont créés une fois l'importation d'un scanner terminée. La tâche planifiée récupère et évalue tous les nouveaux résultats des tests créés à la suite d'une importation.

Une fois qu'une règle cible est définie, les dates cibles de rattrapage sont calculées par la *Evaluate and notify remediation targets* tâche planifiée. La tâche planifiée ajoute une date cible de rattrapage, s'il n'en existe pas, ou, si cette règle contient une date antérieure à celle de l'enregistrement, elle met à jour la date cible existante.

Tous les enregistrements expirés et les dates de rappel qui correspondent aux règles cibles sont récupérés par la tâche et des notifications sont envoyées. Pour les règles désactivées, la tâche efface les champs de rattrapage des enregistrements de résultats des tests et arrête d'envoyer des notifications.

Affichage des dates cibles et de l'état sur les vues de liste et de formulaire

Conformité de la configuration Les gestionnaires peuvent voir la date cible de rattrapage à partir du formulaire des résultats des tests et des vues de listes. Les règles de cible de rattrapage sont également exécutées après l'importation d'un scanner et réexécutées si un résultat de test est rouvert.

La tâche planifiée met à jour la **cible de rattrapage** et l'état de **rattrapage** dans la vue de liste des résultats des tests, ainsi que les champs **Règle de cible de rattrapage**, Cible de **rattrapage** et État de **rattrapage** sur le formulaire des résultats des tests.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

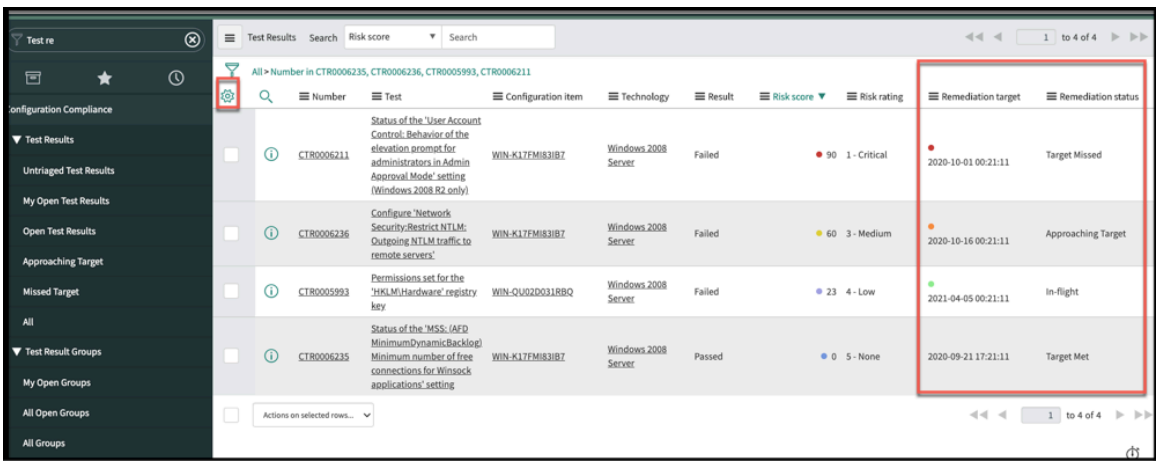
Remarque : Par défaut, les colonnes **Cible de rattrapage** et **État** de rattrapage ne sont pas affichées dans la vue de liste Résultats des tests. Pour afficher ces colonnes, vous devez également les ajouter à la vue de liste. De même, ajoutez la **règle de cible de rattrapage**, la **cible de rattrapage** et l'état de **rattrapage** au formulaire des résultats du test.

Utilisez les zones de liste double dans les menus Paramètres et Action supplémentaire, respectivement, comme illustré dans les images suivantes pour afficher ces colonnes et champs. Pour le menu Action supplémentaire sur l'enregistrement des résultats du test, cliquez sur l'icône de menu, puis sur **Configurer** et **Mise en page du formulaire** pour afficher la zone de sélection et déplacer les champs de **Disponible** à **Sélectionné**.

La date cible de rattrapage est codée dans la vue de liste Résultats des tests sous forme de points colorés :

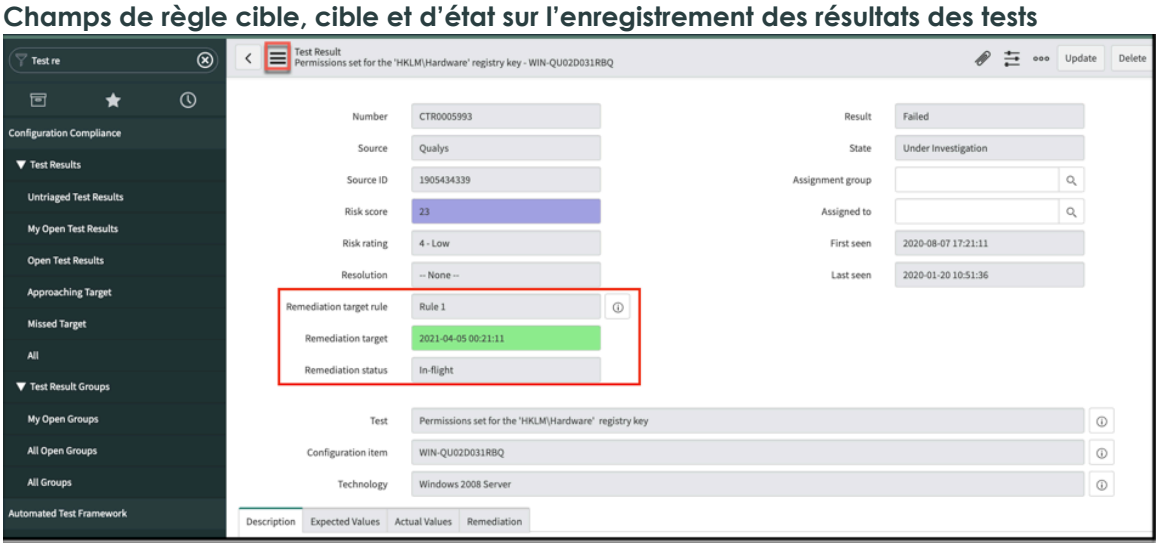
- Les résultats des tests qui n'ont pas atteint leur date de notification sont affichés en vert.
- Les résultats des tests approchant de la date cible de rattrapage sont affichés en orange.
- Les résultats des tests au-delà de la date cible de rattrapage sont indiqués en rouge.

Colonnes de l'état et de la cible de rattrapage de la vue de liste Résultats des tests



- `Cible manquée` : la date cible est dépassée
- `En cours` : le résultat du test est en cours

Champs de règle cible, cible et d'état sur l'enregistrement des résultats des tests



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les enregistrements de résultats des tests sont également affichés visuellement sur le Conformité de la configuration tableau de bord. Accédez à la **Tout** > **Configuration Compliance** > **Vue d'ensemble** et vérifiez l'état du tableau de bord. La vue d'ensemble inclut les widgets existants et l'état du rattrapage. Les couleurs des graphiques correspondent aux couleurs affichées dans la vue de liste Résultats des tests et dans l'enregistrement Résultat des tests.

Scénario de règle de cible de rattrapage

Lorsque plusieurs règles de cible de rattrapage sont appliquées au même résultat de test, la règle la plus restrictive est appliquée.

Par exemple, si un résultat de test identifié pour la première fois le 03/01/2018 remplit les conditions de deux règles de cible de rattrapage :

- Règle 1 de la cible de rattrapage : définie le 03/07/2018 ; l'objectif de rattrapage est de 15 jours depuis la première observation ; La date cible de rattrapage calculée est le 16/03/2018 10:00:00.
- Règle 2 de la cible de rattrapage : définie le 03/10/2018 ; l'objectif de rattrapage est de 10 jours depuis la première apparition ; La date cible de rattrapage calculée est le 03/11/2018 10:00:00.

Remarque :

Les cibles de rattrapage sont calculées à partir de la date du **dernier observé** additionnée au nombre de jours (mesurés par incréments de 24 heures).

À partir de la version 14.5, les cibles de rattrapage sont calculées à partir **de la cible à partir de (date).** La valeur par défaut reste **Dernier observé**. À partir de la version 14.12, la valeur par défaut est **Dernière passe**.

Dans ce scénario, la règle de cible de rattrapage 2 s'applique au résultat du test, car elle comporte la date la plus restrictive : 10 jours depuis l'identification initiale du résultat du test contre 15 jours.

Créer ou modifier des règles cibles et réappliquer les changements

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Règles de cibles de rattrapage** pour afficher, modifier et créer de nouvelles règles de cibles de rattrapage.
2. Dans la colonne Nom, cliquez sur une règle pour ouvrir une règle cible et modifier l'enregistrement, ou cliquez sur **Nouveau** pour créer une règle cible.
3. Remplissez le formulaire pour définir le délai de rattrapage prévu, spécifier les résultats des tests auxquels cette règle s'applique avec des conditions et déterminer quand envoyer des rappels aux utilisateurs ou aux groupes, ou aux deux.

Champ	Description
Nom	Nom de votre règle.
Actif	Activez ou désactivez la règle. La règle est automatiquement activée (vrai) par défaut et est appliquée à vos résultats des tests si vous choisissez d'appliquer les changements manuellement ou après la tâche planifiée suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Cible (jours)	Définissez la date d'échéance ciblée pour le rattrapage en nombre de jours. La valeur par défaut pour les jours de rattrapage ciblés est 30. Par exemple, si vous créez une nouvelle règle qui a également 30 pour une valeur cible, votre nouvelle règle et toutes les autres règles existantes qui ont également 30 jours ou plus comme dates cibles seront appliquées à vos résultats de test.
V14.5 : (date) à partir de la cible	Date à partir de laquelle les dates cibles sont calculées. Vous pouvez spécifier uniquement les champs de date ou de type date et heure. À partir de la version 14.12, la valeur par défaut est *Dernière passe*. Sélectionnez l'une des options suivantes : ◦ Dernier observé ◦ Premier observé ◦ Créé ◦ Dernière transmission Si la dernière passe est vide, la date de création est prise en compte pour le calcul de la cible de rattrapage. Pour personnaliser les valeurs de ce champ, reportez-vous à KB1642413 .
Notifier (jours avant l'échéance)	Définissez un nombre de jours avant la date limite pour rappeler aux utilisateurs et aux groupes.
Description	Brève description de la règle.
Condition	Utilisez le générateur de conditions pour spécifier les résultats des tests auxquels cette règle s'applique. Par exemple, définissez une date cible de rattrapage de 30 jours pour tous les résultats des tests dont le score de risque est supérieur à 70. Envoyer des rappels aux utilisateurs ou aux groupes, ou aux deux, sept jours avant la date de rattrapage. La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire. Avant la version 12.0, la sensibilité à la casse était prise en charge pour le texte de recherche que vous saisissez dans le générateur de conditions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utilisateur et groupes d'utilisateurs ou les deux	Sélectionnez des utilisateurs ou des groupes, ou les deux, pour envoyer des notifications sur les dates cibles proches et dépassées que vous avez définies.

4. Cliquez sur **Envoyer**. Pour enregistrer les règles modifiées, vous pouvez également cliquer sur **Mettre à jour**.

   La vue de liste s'affiche avec votre règle mise à jour ou nouvelle. Les règles de la liste sont classées et exécutées en commençant par celle dont la date cible de rattrapage est la plus basse. Si vous désactivez ou supprimez une règle, la règle suivante dans la séquence d'ordre remplace la règle inactive ou supprimée.

5. Pour appliquer vos nouveaux changements maintenant, cliquez sur **Appliquer les changements**.

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

Conformité de la configuration Groupes de calculateurs

Conformité de la configuration Les calculateurs sont utilisés pour mettre à jour les valeurs d'enregistrement lorsque des conditions prédéfinies sont remplies. Les calculateurs sont regroupés en fonction des critères utilisés pour déterminer comment les enregistrements sont mis à jour.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Conformité de la configuration Groupes de calculateurs

Depuis l'enregistrement du calculateur de risque par défaut, les règles de calcul peuvent être appliquées à tous les résultats des tests affectés et à toutes les collections sur demande. Les gestionnaires de vulnérabilité peuvent utiliser cette fonctionnalité pour ajuster la configuration de leur calculateur de risque. Ils peuvent expérimenter plusieurs schémas de priorisation au début de leur déploiement et appliquer ces changements à la demande pour voir comment ils impactent les résultats d'importation.

Le groupe de calculateurs de score de risque a été renommé Calculateurs de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les calculateurs de déploiement des scores de risque sont inclus avec Conformité de la configuration. Il existe deux types de calculateurs de cumul individuels :

Déploiement du risque de test de configuration

Calculateurs qui déploient les scores de risque de tous les résultats du test avec le même test de configuration afin de fournir un score de risque global du test de configuration. La valeur cumulée s'affiche dans les champs Score de risque.

Déploiement du score de risque de la tâche de rattrapage

Ces calculateurs cumulent les scores de risque pour tous les résultats des tests dans une tâche de rattrapage afin de fournir un score de risque global pour cette tâche de rattrapage. La valeur cumulée s'affiche dans les champs Score de risque.

Le groupe de calculateurs de score de risque et le groupe de calculateurs de déploiement de score de risque sont activés par défaut.

Pour plus d'informations, passez en revue les termes clés suivants pour Conformité de la configuration les calculateurs :

Résultat de test

Un résultat de test est le résultat d'un test de configuration sur un élément de configuration (CI) et la technologie associée. Les résultats des tests dans les états Échec, Erreur et Inconnu identifient le matériel, les logiciels et les actifs qui ne sont pas conformes à vos politiques.

Tâche de rattrapage

Les résultats des tests sont regroupés au moment de l'importation des données en fonction des règles de tâche de rattrapage prédéfinies. Ces tâches de rattrapage sont similaires aux groupes de vulnérabilité dans Réponse aux vulnérabilités. Les tâches de rattrapage organisent les résultats des tests en groupes pour une analyse en bloc et représentent un ensemble d'éléments à corriger.

Score de risque dans un résultat de test

Valeur calculée par les calculateurs de score de risque en fonction du contexte professionnel d'un actif et de la sévérité du test associé. Il s'agit de la moyenne de la criticité opérationnelle de l'actif affecté, telle que définie dans la CMDB, et de la sévérité du test, telle que communiquée par le scanner.

Plusieurs services peuvent être associés à chaque actif. La criticité opérationnelle d'un actif est déterminée par le service ayant la criticité la plus élevée.

La valeur calculée est affichée dans les champs Score de risque des résultats des tests. Les scores affichent des valeurs comprises entre 0 et 100. Les champs sont également codés par couleur pour vous fournir la gravité en un coup d'œil.

Score de risque dans la tâche de rattrapage

Ce score est affiché sur l'enregistrement de tâche de rattrapage et correspond à la valeur cumulée des scores de risque pour tous les résultats des tests actifs dans une tâche de rattrapage. Ce score change au fur et à mesure que les résultats des tests sont corrigés dans la tâche de rattrapage.

Score du risque dans le test de configuration

Ce score est affiché dans les tests de configuration et correspond à la valeur cumulée des scores de risque pour tous les résultats des tests actifs avec ce test

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de configuration. Ce score change au fur et à mesure que les résultats des tests associés à ce test de configuration sont corrigés.

Cote de risque

Degré de risque que représente un résultat de test échoué pour votre système. Il est basé sur une gamme de scores de risque sur une échelle numérique de 1 à 5 qui classe les risques de Critique (1) à Aucun (5). Le score est basé sur une plage de scores de risque et est affiché dans les champs de cote de risque.

Plages de cote de risque

Cote de risque	Score du risque
1 - Critique	90 à 100
2- Élevé	70 à 89
3- Moyen	40 à 69
4- Faible	1 à 39
5- Aucun	0

Calculateurs de déploiement des scores de risque

Il existe deux types de calculateurs de cumul :

- Déploiement du risque du test de configuration : ces calculateurs cumulent les scores de risque pour tous les résultats du test avec le même test de configuration afin de fournir un score de risque global pour le test de configuration. La valeur cumulée s'affiche dans les champs Score de risque. Vous pouvez modifier les valeurs de script pour la pondération et le score de ces calculateurs.
- Déploiement du score de risque de la tâche de rattrapage : ces calculateurs cumulent les scores de risque pour tous les résultats des tests d'une tâche de rattrapage afin de fournir un score de risque global pour cette tâche de rattrapage. La valeur cumulée s'affiche dans les champs Score de risque. Vous pouvez modifier les valeurs de script pour la pondération et le score de ces calculateurs. Pour obtenir un exemple de calculateur de déploiement de score de risque et la façon dont il calcule les scores, reportez-vous à la section Exemple de calcul de déploiement de risque pour Conformité de la configuration (avant la version 15.0).

Score de risque historique

Score de risque inhérent pour tous les résultats des tests réussis dans une tâche de rattrapage. Ce champ affiche la quantité de risque qui a été rattrapée par un groupe de tests et ne s'affiche qu'une fois qu'un groupe de tests est dans l'état « Fermé » et que le score de risque est de zéro.

Les scores sont calculés chaque fois que le score de risque change ou lorsque les résultats des tests sont ajoutés ou supprimés d'une tâche de rattrapage.

Remarque : Pour fonctionner correctement, ce script nécessite le module d'extension Mappage des services . Mappage des services est disponible sous forme d'abonnement distinct et nécessite une activation par ServiceNow le personnel.

Créer un groupe de Conformité de la configuration calculateurs

Conformité de la configuration Les groupes de calculateurs sont utilisés pour regrouper les calculateurs en fonction de la façon dont vous souhaitez les utiliser.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
Le Conformité de la configuration système de base comprend un groupe de calculateurs : **Score de risque**. Au fur et à mesure que vous créez d'autres calculateurs, vous pouvez les ajouter à ce groupe ou créer d'autres groupes et calculateurs. Au sein de chaque groupe, le premier calculateur qui correspond au résultat du test s'exécute.

Deux groupes de calculateurs sont inclus dans l'application Configuration Compliance :

- Calculateurs de risque
- Calculateurs de déploiement des scores du risque

Les calculateurs de risque calculent le score et la cote de risque d'un résultat de test.

Les calculateurs de déploiement des scores de risque cumulent les scores de risque pour tous les résultats des tests et les tâches de rattrapage avec le même test de configuration afin de fournir un score de risque global.

Vous pouvez également créer de nouveaux calculateurs directement à partir de ces groupes.

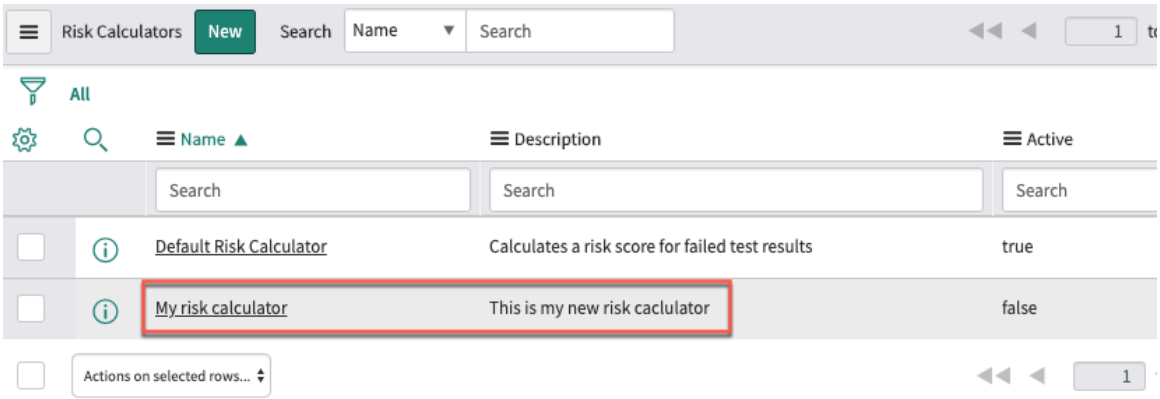
Procédure
1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Groupes de calculateur**.
2. Accédez à la **Tout** > **Configuration Compliance** > **Administration** et sélectionnez **Calculateurs de risque** ou **Calculateurs de déploiement de score de risque**.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom du calculateur.
Description	Description de ce groupe de calculateurs.
Actif	Activez ou désactivez le groupe de calculateurs.

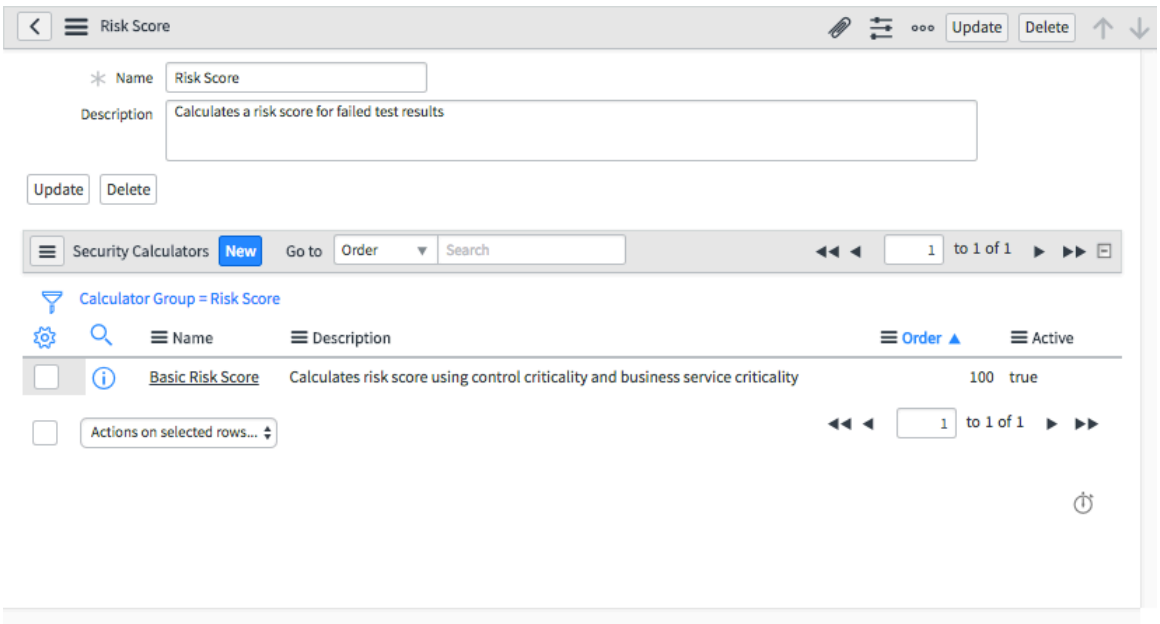
5. Cliquez avec le bouton droit sur **Enregistrer** dans l'en-tête du formulaire ou cliquez sur **Soumettre**.
   Le nouveau groupe de calculateurs s'affiche dans la liste de groupes avec les autres calculateurs. Cliquez sur le nom du nouveau groupe de calculateurs pour ouvrir l'enregistrement. Pour plus d'informations sur la définition des conditions et des valeurs affichées et sur la réapplication des calculatrices, reportez-vous Créer, modifier et réappliquer des calculateurs de risque pour Conformité de la configuration à la section .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La liste connexe **des calculateurs de sécurité** s'affiche.



6. Cliquez sur **Nouveau** pour ajouter des calculateurs et leurs conditions au groupe.

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

Conformité de la configuration Calculatrices et règles de calculatrice

Conformité de la configuration Automatisez le calcul des valeurs initiales pour les champs des résultats des tests. La condition de chaque calculateur est évaluée dans l'ordre, et le premier calculateur correspondant est utilisé.

Conformité de la configuration Calculatrices

Le système de base de conformité de la configuration comprend un calculateur de conformité de la configuration (**calculateur de risque par défaut**) qui définit le **score de risque** de base sur le résultat des tests. Les calculateurs de Configuration Compliance peuvent être conçus pour classer par ordre de priorité et évaluer l'impact des résultats des tests en fonction de n'importe quel critère à l'aide de filtres de condition. Qu'il s'agisse de l'impact sur l'entreprise de la vulnérabilité ou de la classe de l'élément de configuration (CI), vous pouvez créer des calculateurs de conformité de la configuration supplémentaires

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pour définir d'autres champs sur les résultats des tests ou personnaliser les calculateurs de conformité de la configuration existants. Un calculateur peut être écrit pour refléter n'importe quel ensemble de priorités.

Chaque calculateur contient une liste de règles de calcul, avec une condition déterminant quand l'appliquer. Lorsque le calculateur est exécuté, la condition de chaque règle de calcul est évaluée dans l'ordre, et la première règle de calcul correspondante est utilisée.

Tous les calculateurs de conformité de configuration activés définissent les champs sélectionnés chaque fois qu'un résultat de test est créé, lorsqu'un CI associé ou un test de configuration change, ou lorsque le lien connexe **Calculer le score de risque** dans un résultat de test est utilisé. Par exemple, le score de risque est automatiquement mis à jour sur les enregistrements de résultats des tests lorsque la valeur control.criticality est mise à jour sur un résultat de test importé. Une fois qu'une importation de résultats de tests a mis à jour un score de résultat de test, vous pouvez recalculer le score de risque des résultats des tests en sélectionnant le bouton **Réappliquer le calculateur** .

Dans un résultat de test existant, si vous sélectionnez le lien connexe **Calculer le score de risque** et que l'un des calculateurs est activé, le champ Score de risque dans le résultat du test est mis à jour.

Remarque :

- Le lien connexe **Calculer le score de risque** est uniquement visible quand au moins un calculateur de conformité de la configuration est activé.
- À partir de la version 22.0 de , vous pouvez mettre à jour le score de risque d'un résultat de test dans Vulnerability Manager Workspace et IT Remediation Workspace en sélectionnant le bouton Calculer le score de Réponse aux vulnérabilités**risque** dans sa vue d'enregistrement.
- À partir de la version 14.13 de , chaque fois que le score de risque d'un résultat de Conformité de la configurationtest change, les détails suivants sont documentés dans la section Notes du résultat de test :
  - Nom du groupe de calculateurs
  - Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre parenthèses. Pour modifier ou afficher la base de la règle du calculateur, sélectionnez n'importe quelle règle et cochez la case Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. Si le **modèle** est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si **Script** est sélectionné, vous pouvez ajouter ou mettre à jour le script existant.
  - Valeurs de champ avec leur pondération et leur contribution au score de risque
  - Score de risque final

Conformité de la configuration Règles de calcul

Par défaut, un **calculateur de risque par défaut** du système de base est fourni. Si vous souhaitez créer une règle de risque pour ce calculateur, vous devez définir le champ cible du **calculateur de risque par défaut** sur **Score de risque**. Sélectionnez le bouton **Nouvelle règle de risque** pour créer une nouvelle règle de risque. Cela crée une règle de calcul des résultats des tests spécialisée, appelée **règle de risque**, qui à son tour calcule le **score de risque** en fonction de plusieurs valeurs. Par défaut, les valeurs suivantes sont prises en compte pour calculer le score de risque :

- Criticité opérationnelle
- Criticité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez ajuster les valeurs à utiliser dans la **règle de risque par défaut** et le poids à donner à chacune de ces valeurs. Les pondérations sont utilisées pour ajuster l'importance de chaque élément lors de la définition du **score de risque** de base.

À partir de Conformité de la configuration la version 13.0, vous pouvez personnaliser les critères de la règle de risque par défaut. Pour plus d'informations, consultez Définir des champs et des pondérations pour la règle de risque.

Affectation d'un pourcentage de pondération

Vous pouvez également affecter un pourcentage de pondération (0-100) au niveau de la valeur de champ. Par exemple, vous pouvez affecter un pourcentage de pondération à chaque niveau de gravité (de Aucun à Critique). Si la pondération de criticité est de 50 pour la règle de risque et que les valeurs de pondération suivantes sont affectées au niveau de criticité :

Affecter le pourcentage de pondération

Criticité	Score du risque
Critique	100
Élevé	50
Moyen	20
Aucun	0

Si la criticité est critique, la pondération correspondante est de 50. Si la criticité est élevée, la pondération est de 25 et si la criticité est moyenne, la pondération est de 10. Si la criticité est nulle, la pondération correspondante est égale à 0. Pour plus d'informations, consultez l'exemple de calcul du score de risque pour Configuration Compliance.

Chaque règle a un paramètre **d'ordre** . Toutefois, la première à correspondre aux conditions met à jour le champ **Score de risque** dans le résultat du test. Les règles de calculateur non scriptées ont généralement moins d'impact sur les performances que les règles de calculateur scriptées.

Le calculateur du système Conformité de la configuration de base contient des règles de calcul qui attribuent à chaque niveau de criticité (aucun à critique) une valeur (0-100) pour **le score de risque** en fonction de la gravité. Un score de risque de 100 est automatiquement affecté à une gravité inconnue. Ces valeurs peuvent être ajustées, comme le calculateur de risque par défaut, de nouvelles règles de calcul ou de nouvelles règles de risque peuvent être créées.

Poids du score du risque de vulnérabilité

Un score de risque et une évaluation sont attribués à toutes les vulnérabilités en fonction de facteurs tels que la gravité, la criticité, les informations d'exploitation, etc. La règle *`Update Risk Rating from Risk Score`* métier de la table des éléments vulnérables est responsable du calcul de la cote de risque. Chaque fois que le score de risque change, la cote de risque est calculée et renseignée sur les éléments vulnérables. Avant la version 17.1 de l'application Réponse aux vulnérabilités (VR), les évaluations de risque suivantes étaient fournies dans le cadre du script `include VulnerabilityUtils`, qui étaient codés en dur.

Valeur (cote de risque)	Poids (score de risque)
1	90–100

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur (cote de risque)	Poids (score de risque)
2	70–89
3	40–69
4	1–39
5	0

À partir de la version 18.0 de Réponse aux vulnérabilités,

- Les types de cote de risque sont expédiés dans la table de base en tant que cc_risk_rating. Ces types sont transmis dans le cadre de la règle métier sur chaque table où la cote de risque est calculée.
- Le script est modifié afin que vous puissiez interroger les entrées dans les valeurs de la table Poids du score de risque pour le calcul de la cote de risque.
- Ajoutez des entrées supplémentaires pour un type existant ou créez un nouveau type. Lorsque vous créez un nouveau type, assurez-vous d'ajouter les étiquettes pour la nouvelle cote de risque et de modifier les scripts et règles métier connexes. Vous devez également ajouter un nouveau style pour le nouveau score de risque.
- Modifiez le script pour interroger les enregistrements dans la table de base.

Vous pouvez accéder à la table des poids de score de risque en saisissant sn_sec_cmn_risk_score_weight dans le navigateur de filtre.

En outre, le score de risque est automatiquement recalculé dans les scénarios suivants :

- Lorsqu'un élément de configuration (CI) passe d'un mode non accessible sur Internet à un mode accessible sur Internet.
- Lorsque les vulnérabilités et expositions communes (CVE) ou les entrées tierces (TPE) associées sur les éléments de vulnérabilité (VI) sont liées à une vulnérabilité d'exploitation connue CVE (KEV).

Définir des champs et des poids pour la règle de risque

Personnalisez les paramètres et les pondérations de la règle de risque afin de pouvoir générer des scores de risque qui utilisent les données de test et d'actif propres à votre organisation. En sélectionnant les champs inclus dans la règle de risque, vous pouvez définir un cadre de travail de notation des risques efficace.

Avant de commencer

Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Calculateurs de risque**.
2. Cliquez sur **Calculateur de risque par défaut**.
3. Sélectionnez le champ cible en tant que **Score de risque**.
   Le bouton **Nouvelle règle de risque** s'affiche dans la table Règle du calculateur.
4. Cliquez sur le bouton **Nouvelle règle de risque** pour accéder au formulaire **Règle de risque de Configuration Compliance** .
5. Dans la section Critères du calculateur de risque, définissez la pondération de chaque critère en fonction de son importance dans le calcul du score de risque global.
6. Décochez la case **Actif** pour désactiver la règle.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Ajouter des critères** pour ajouter des champs de règle de risque aux critères du calculateur de risque.
8. Renseignez les champs du formulaire.

Formulaire de champ de règle de risque

Champ	Description
Choisir la table de référence	Table que vous utilisez pour définir la pondération du score de risque. Sélectionnez une option parmi les suivantes : ◦ Résultat du test : ajoutez des champs auxquels vous pouvez accéder directement à partir du résultat du test (TR). ◦ Résultat du test : élément de configuration : ajoutez des champs de type « remontée pas à pas » qui font partie des extensions de table de base, comme la table Matériel. Ces champs ne font pas partie de la table de cmdb_ci de base. ◦ Résultat du test : test : ajoutez des champs parcourables par point qui font partie des tables qui étendent la table de base, par exemple, Entrée tierce. Ces champs ne font pas partie de la table de base du test de configuration. ◦ Table de référence des résultats des tests : ajoutez des champs qui font partie des tables connexes (m2m) ou des tables qui font référence au résultat des tests. Ces champs ne sont pas directement accessibles par point à partir du résultat du test. ◦ Table de référence de l'élément de configuration : ajoutez des champs qui font partie des tables connexes (m2m) de cmdb_ci ou des tables qui font référence à cmdb_ci. Ces champs ne sont pas directement accessibles par point à partir du TR. ◦ Table de référence du test : ajoutez des champs qui font partie des tables connexes (m2m) de sn_vulc_test ou des tables qui font référence à sn_vulc_test. Ces champs ne sont pas directement accessibles par point à partir du TR. ◦ Conditions personnalisées : utilisez cette option pour affecter des poids à la règle

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	en évaluant la condition. Par exemple, le filtre accessible sur Internet détermine si un élément de configuration (CI) est externe ou interne.
Champ	Champ utilisé pour le calcul du score de risque pour cette règle.
Poids	Pondération de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
Table	◦ Résultat de test > élément de configuration ◦ Résultat de test > test ◦ Table de référence de résultats des tests ◦ Table de référence de l'élément de configuration ◦ Table de référence de test Ce champ s'affiche uniquement lorsque l'une des options énumérées est sélectionnée dans le champ Choisir une table de référence.
Agrégation	Sélectionnez la valeur minimale ou maximale à prendre en compte pour les calculs lorsque le champ est sélectionné dans les tables connexes (m2m). Ce champ s'affiche uniquement lorsqu'une table de référence est sélectionnée dans le champ Choisir une table de référence.
Définir la pondération de la valeur	Composant permettant d'attribuer des poids à chaque valeur de champ. Pour les champs numériques, définissez les valeurs de champ sous la forme d'une plage (par exemple, de 1 à 5). La valeur doit être un nombre entier compris entre 0 et 100. Ce champ n'apparaît pas si l'option Conditions personnalisées est sélectionnée dans le champ Choisir une table de référence.
Table de condition	Sélectionnez une condition dans la liste. Ce champ s'affiche uniquement lorsque l'option Conditions personnalisées est sélectionnée dans le champ Choisir une table de référence.
Nom de champ	Saisissez un nom pour les critères de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Ce champ s'affiche uniquement lorsque l'option Conditions personnalisées est sélectionnée dans le champ Choisir une table de référence.
Condition	Prévisualisez les éléments de cette table qui correspondent aux conditions définies. Ce champ s'affiche uniquement lorsque l'option Conditions personnalisées est sélectionnée dans le champ Choisir une table de référence.

9. Cliquez sur **Envoyer**.

Que faire ensuite
Dans la page Règle, activez et réappliquez la règle pour réévaluer le score de risque sur le résultat des tests actif.

Modifier les calculateurs de déploiement de risque pour Conformité de la configuration

Modifiez un calculateur de déploiement de risque existant.

Avant de commencer
Rôle requis : Rôle requis : sn_vulc.admin

Procédure
1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** et sélectionnez **Calculateurs de déploiement des scores de risque**.
2. Une fois la liste des calculateurs de déploiement de score de risque affichée, cliquez sur un calculateur pour ouvrir l'enregistrement et modifier le formulaire.

Champ	Description
Nom	Nom du calculateur de déploiement de test de configuration ou de tâche de rattrapage.
Description	Description du calculateur de déploiement de risque.
Table	Table sur laquelle le calculateur de cumul est appliqué.
Inclure le report	Inclut les résultats des tests différés lors du déploiement du score de risque.

3. Définissez les pondérations de l'une des façons suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

◦ Dans la section Poids cumulatifs, affectez des pondérations pour les éléments suivants :

Poids des déploiements

Champ	Description	Pondération par défaut
Score du risque maximal	Score de risque maximal des résultats des tests pris en compte.	85
Score de risque moyen	Agrégat des scores de risque de tous les résultats des tests pris en compte.	0
Nombre de résultats des tests	Nombre de résultats des tests.	15

◦ Cochez la case Vue **avancée** et, dans l'éditeur de **valeurs de script** , modifiez les valeurs du script selon vos besoins.

Remarque : La modification d'un script nécessite une connaissance approfondie de et de Now Platform l'application Conformité de la configuration .

4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Les calculateurs de déploiement sont des travaux planifiés qui s'exécutent toutes les heures pour détecter les changements. Ces travaux planifiés totalisent également les scores de risque pour les tests de configuration et la tâche de rattrapage. Les valeurs cumulées sont affichées dans les champs Score de risque.

Pour obtenir un exemple de la manière dont un calculateur de déploiement de risque détermine les scores, reportez-vous Exemple de calcul de déploiement de risque pour Conformité de la configuration (avant la version 15.0)à .

Créer, modifier et réappliquer des calculateurs de risque pour Conformité de la configuration

Les règles de calcul peuvent être appliquées à tous les résultats des tests affectés et à toutes les collections sur demande. Les gestionnaires de vulnérabilité peuvent utiliser cette fonctionnalité, ajuster la configuration de leur calculateur de risque et appliquer des changements sur demande pour importer les résultats.

Avant de commencer

Rôle requis : sn_vulc.admin

Procédure

1. Pour créer un nouveau calculateur de risque, procédez comme suit.

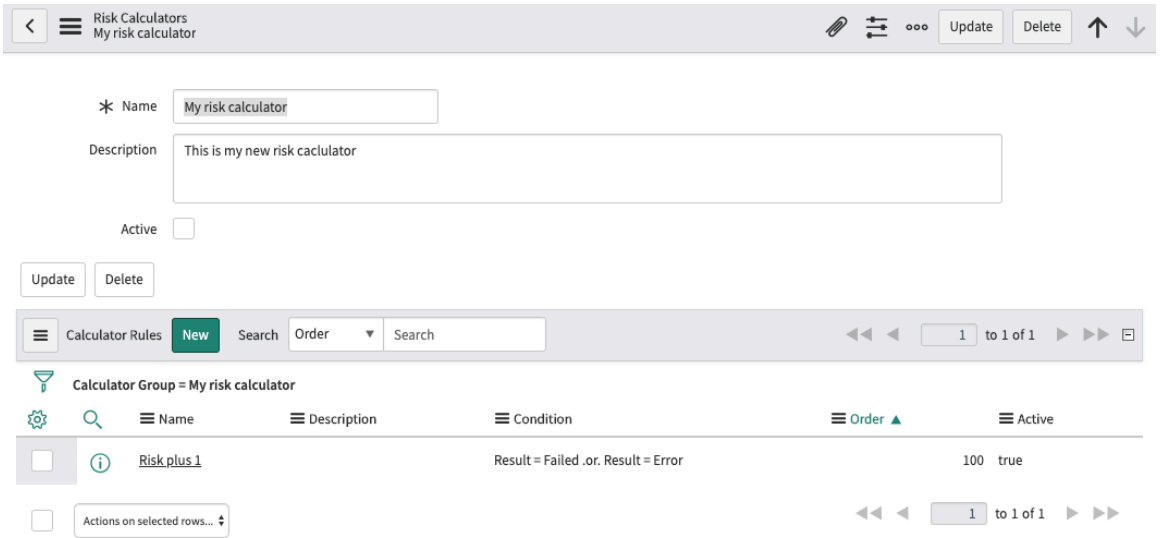
   a. Accédez à la **Tout** > **Configuration Compliance** > **Administration** et sélectionnez **Calculateurs de risque**.

   b. Dans la liste Calculateur de risque, cliquez sur **Nouveau**.

   c. Entrez un nom et une description pour votre nouveau calculateur, puis cliquez sur **Soumettre**.
   Le nouveau calculateur s'affiche dans la liste Calculateur de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Dans la liste, cliquez sur le nouveau calculateur pour créer les conditions dans lesquelles le calculateur s'exécute et spécifiez les champs et les valeurs que vous souhaitez afficher sur les enregistrements de résultats des tests et les tâches de rattrapage.

e. Dans l'enregistrement qui s'affiche, cliquez sur **Nouveau**.

f. Renseignez les champs des onglets comme il convient.

Onglet	Description
Quand cette condition est remplie	Utilisez le générateur de conditions pour créer les conditions dans lesquelles le calculateur s'exécute. Par exemple : `Résultat est Échec ou Résultat est Erreur`.
Définir ces valeurs	Utilisez le modèle pour sélectionner les champs et les valeurs que vous souhaitez afficher.

g. Cliquez sur **Envoyer**.
L'enregistrement s'affiche avec les nouvelles règles de calcul et le groupe auquel il appartient.

2. Pour réappliquer un calculateur existant aux résultats des tests ou pour modifier les règles et les valeurs affichées d'un calculateur de risque existant, procédez comme suit.

a. Dans les listes Calculateurs de risque ou Calculateur de déploiement de risque, sélectionnez le calculateur que vous souhaitez modifier.

b. Pour réappliquer un calculateur de risque aux données de résultats de vos tests existants à partir de l'enregistrement, cliquez sur **Réappliquer le calculateur**.
Tous les résultats des tests qui répondent aux conditions du calculateur sont mis à jour.

Remarque : Selon le nombre de résultats des tests, cette mise à jour peut prendre du temps.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Pour modifier les conditions et les valeurs, cliquez sur le nom du calculateur en bas à gauche dans la colonne Nom.
Pour les calculateurs de risque, l'enregistrement et les onglets **Quand cette condition est remplie** et **Définir ces valeurs** s'affichent.

d. Renseignez le formulaire comme il vous convient.

Onglet	Description de champ
Quand cette condition est remplie	Utilisez le générateur de conditions de filtre pour créer les conditions dans lesquelles vous souhaitez que le calculateur s'exécute.
Définir ces valeurs	Choisissez-en un pour continuer. ▪ Type de valeur : modèle. Choisissez des champs dans la liste et les valeurs correspondantes. ▪ Script : saisissez vos modifications à l'aide de l'éditeur. **Remarque :** La modification d'un script nécessite une connaissance approfondie de et de Now Platform l'application Conformité de la configuration .

3. Facultatif : Pour appliquer les nouvelles règles sur demande à vos données de résultats des tests existantes, procédez comme suit.

a. Une fois la liste des calculateurs de risque affichée, cliquez sur le calculateur que vous souhaitez appliquer.
L'enregistrement s'affiche.

b. Cliquez sur **Réappliquer le calculateur** pour tester et appliquer vos changements sur demande à vos résultats d'importation.

4. Affichez les changements que vous avez apportés aux résultats des tests et continuez à modifier vos calculateurs au besoin.

Exemples pour Conformité de la configuration le calcul du score de risque

À partir de la version 13.0 de , vous pouvez personnaliser les critères de la règle de Conformité de la configurationrisque par défaut. Utilisez les scores de risque fournis par des fournisseurs tiers tels que Qualys et Tenable pour calculer les scores de risque.

Les fournisseurs tiers, tels que Qualys et Tenable, fournissent leurs propres scores. Ces scores sont renseignés dans le champ Criticité de la table sn_vulc_test. Utilisez ce champ pour les calculs de score de risque. Pour utiliser ce score afin de calculer le score de risque, procédez comme suit :

Ajouter la criticité de la source comme critère pour une règle de risque

Utilisez les scores basés sur la criticité fournis par les fournisseurs tiers pour calculer les scores de risque.

Avant de commencer

Rôle requis : sn_vulc.admin

Traduction automatique

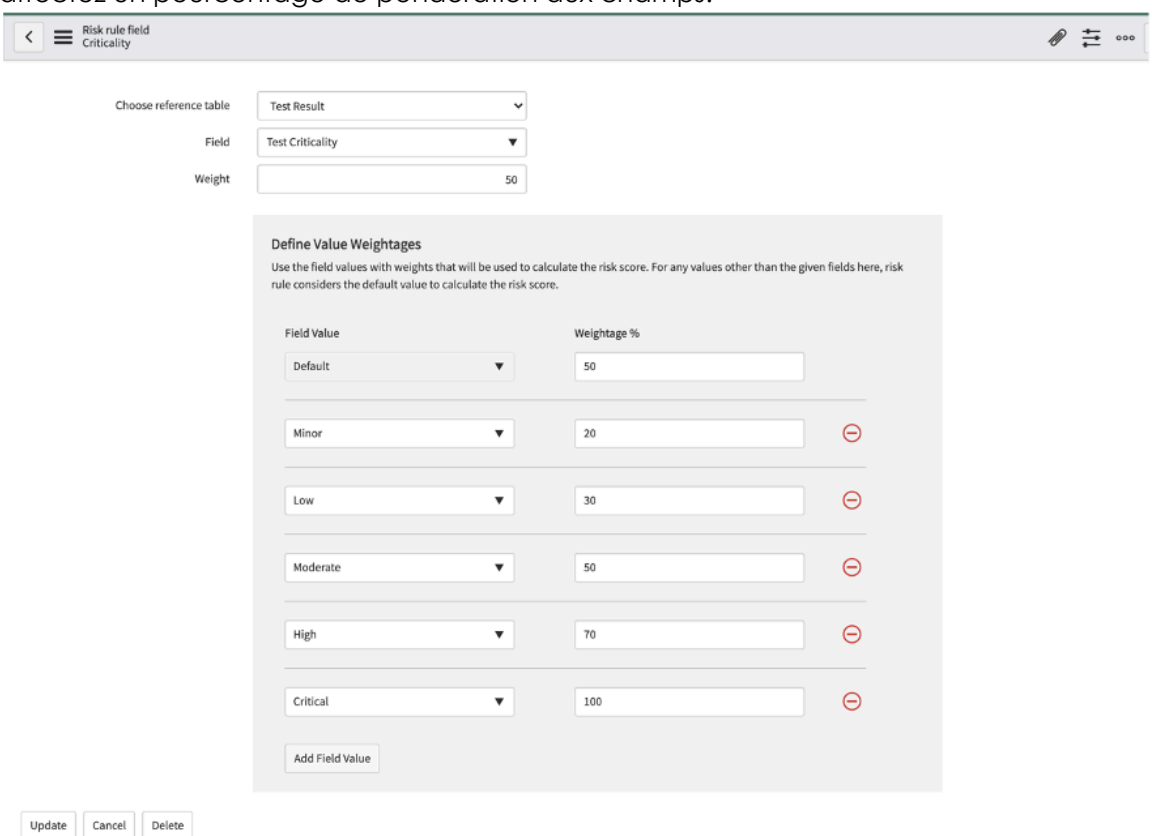
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Les fournisseurs tiers, tels que Qualys et Tenable, fournissent leurs propres scores de risque. Ces scores sont renseignés dans le champ Criticité de la table sn_vulc_test. Utilisez ce champ pour les calculs de score de risque et le calcul du score de risque.

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Calculateurs de risque**.
2. Accédez au formulaire Règle de risque.
3. Décochez la case **Actif** pour désactiver la règle.
4. Cliquez sur **Ajouter des critères**.
5. Dans la liste **Choisir une table de référence** , sélectionnez **Résultat des tests**.
6. Dans la liste **Champ** , sélectionnez **Test.Criticality**.
7. Dans le champ **Poids** , spécifiez l'importance relative de ce champ.
   La valeur doit être un nombre entier compris entre 0 et 100.
8. Dans la section **Définir les pondérations des valeurs** , ajoutez des valeurs de champ et affectez un pourcentage de pondération aux champs.



9. Cliquez sur **Envoyer**.

Ajouter la criticité opérationnelle comme critère pour une règle de risque

Spécifiez une valeur de criticité pour les services aux entreprises et utilisez la criticité opérationnelle pour calculer les scores de risque.

Avant de commencer

Rôle requis : sn_vulc.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

En supposant que votre organisation dispose de nombreux services aux entreprises et qu'un élément de configuration (CI) est utilisé par les services suivants :

Criticité des services d'entreprise

Service d'entreprise	Criticité
Gestion cloud	1 – Très critique
E-commerce	2 – Assez critique
Services à la clientèle	3 – Peu critique
Déplacements et dépenses	4 – Non critique

Le mappage entre le CI et les services est stocké dans la table Services [cmdb_ci_services]. Lorsqu'un CI ne réussit pas un test de configuration, un résultat de test (TR) est créé. Vous pouvez utiliser la valeur de la criticité opérationnelle des services affectés pour calculer le score de risque de ce TR. Suivez la procédure pour utiliser la valeur de criticité de ces services afin de calculer le score de risque.

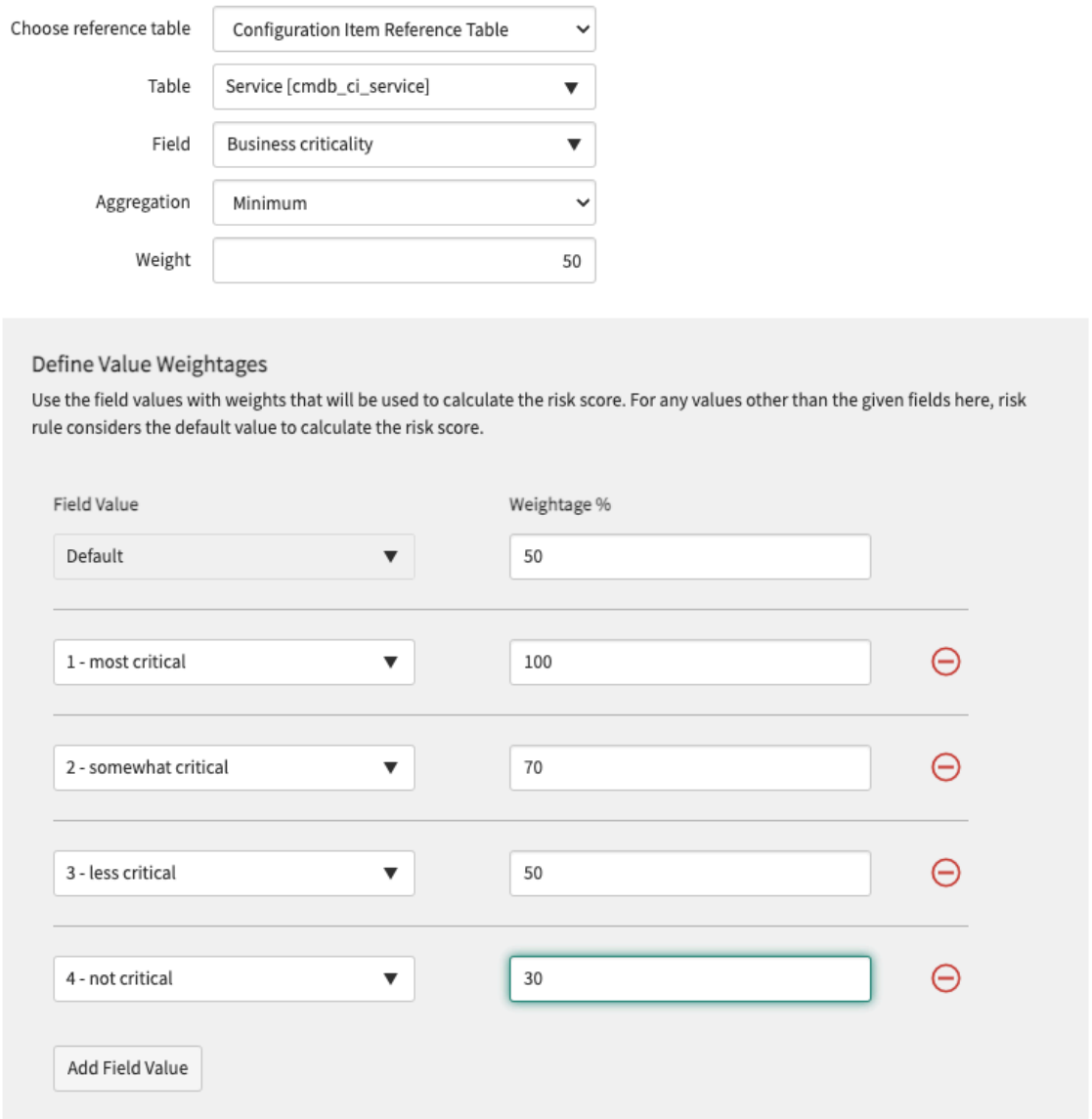
Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Calculateurs de risque**.
2. Accédez au formulaire Règle de risque à partir de la section **Règles du calculateur** .
3. Décochez la case **Actif** pour désactiver la règle.
4. Cliquez sur **Ajouter des critères**.
5. Dans la liste **Choisir une table de référence** , sélectionnez **Table de référence de l'élément de configuration**.
6. Dans la liste **Table**, sélectionnez **Service [cmdb_ci_service].**
7. Dans la liste **Champs**, sélectionnez **Criticité opérationnelle.**
8. Dans le champ **Agrégation** , sélectionnez **Minimum** pour récupérer le service le plus critique pour ce cas d'utilisation (1 : valeur la plus critique) ou **Maximum** pour récupérer le service le moins critique pour ce cas d'utilisation (4 – Valeur non critique).
9. Dans le champ **Poids** , spécifiez l'importance relative de ce champ.
   La valeur doit être un nombre entier compris entre 0 et 100.
10. Dans la section **Définir les pondérations des valeurs** , ajoutez des valeurs de champ et affectez des pondérations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pondération personnalisée de la règle de risque de criticité opérationnelle



Traduction automatique

11. Cliquez sur **Envoyer**.

Ajouter un critère conditionnel au calculateur de risque

Utilisez des conditions personnalisées pour la règle de risque pour le calcul du score de risque.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

En supposant que votre organisation dispose de plusieurs éléments de configuration (CI), dont seuls quelques-uns peuvent être consultés par un utilisateur externe. Les utilisateurs peuvent ajouter des pondérations de score de risque pour ces CI orientés vers l'extérieur.

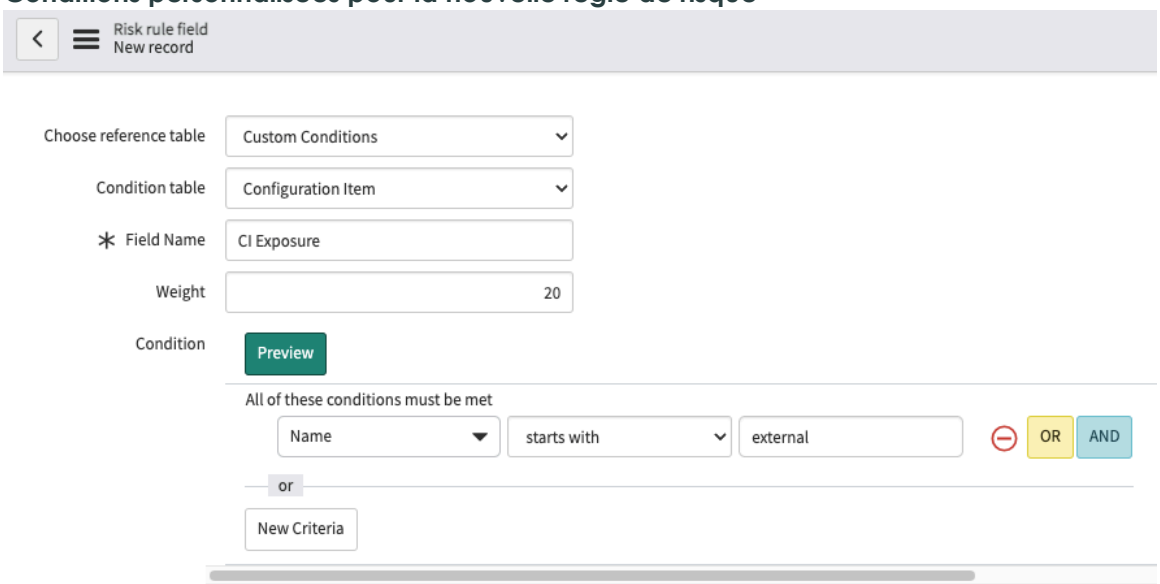
Remarque : Vous pouvez identifier ces CI par leur nom. Les noms commencent par « externe ».

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Calculateurs de risque**.
2. Accédez au formulaire Règle de risque.
3. Décochez la case **Actif** pour désactiver la règle.
4. Cliquez sur **Ajouter des critères**.
5. Dans la liste **Choisir une table de référence** , sélectionnez **Conditions personnalisées**.
6. Dans la liste **Table de conditions** , sélectionnez **Élément de configuration**.
7. Dans le champ **Nom de champ** , entrez l'exposition `CI`.
8. Dans le champ **Poids** , spécifiez l'importance relative de ce champ.
   La valeur doit être un nombre entier compris entre 0 et 100.
9. Dans le champ **Condition** , sélectionnez **Nom > commence**, spécifiez la valeur comme `externe`.

Conditions personnalisées pour la nouvelle règle de risque



10. Cliquez sur **Envoyer**.

Information associée

Groupes de calculateurs de Configuration Compliance

Exemple de calcul du score de risque pour Conformité de la configuration

Déterminez les calculateurs de score de risque pour générer des scores de risque qui utilisent les données de test et d'actif spécifiques à votre organisation.

Exemple de détermination des scores des calculateurs de règles de risque

L'exemple suivant montre comment les scores des calculateurs de règles de risque sont déterminés. Supposons qu'un calculateur de règle de risque soit configuré avec les champs de cette table.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déterminer les scores du calculateur de règle de risque

Champ	Pondération	Répartition du poids
Contrôle.Criticité	50	Par défaut : 0 Mineure : 20 Faible : 30 Modéré : 50 Haute : 70 Critique : 100
Business_Criticality	50	Par défaut : 0 Mineure : 20 Faible : 30 Modéré : 50 Hauteur : 70 Critique : 100

Supposons que les résultats des tests affichés dans cette table sont présents dans le système.

Mappage des résultats des tests

ID	Criticité opérationnelle	Criticité du contrôle
CTR0000001	1 – Très critique	Mineur
CTR0000002	1 – Très critique	Faible
CTR0000003	2 – Assez critique	Mineur
CTR0000004	2 – Assez critique	Modéré
CTR0000005	3 – Peu critique	Faible

Le calcul du score de risque pour le résultat du test est calculé en fonction de la formule :

Score de risque = (W(control.criticality) * FV (control.criticality). + W(business_criticality) * FV(business_criticality)) / 100 où W est le poids et FV est le pourcentage de poids de la valeur de champ.

Le score de risque obtenu pour ces résultats des tests est décrit dans la table suivante :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Score de risque basé sur les résultats des tests

ID	Criticité opérationnelle (50 %)	Criticité du contrôle (50 %)	Score de risque résultant
CTR0000001	1 – Très critique (50 % x100)	Mineure (50 % x 20)	60
CTR0000002	1 – Très critique (50 % x100)	Faible (50 % x 30)	65
CTR0000003	2 – Assez critique (50 % x 70)	Mineure (50 % x 30)	45
CTR0000004	2 – Assez critique (50 % x 70)	Modérée (50 % x 50)	60
CTR0000005	3 – Moins critique (50 % x 50)	Faible (50 % x 30)	40

Si le pourcentage de pondération est modifié pour l'une des valeurs de champ, consultez ce tableau pour les résultats :

Résultats pour le pourcentage de pondération modifié

Champ	Pondération	Répartition du poids
Contrôle.Criticité	50	Par défaut : 0 Mineure : 20 Faible : 30 Modéré : 60 Hauteur : 70 Critique : 100
Business_Criticality	50	Par défaut : 50 1 – Très critique : 100 2 – Assez critique : 70 3 – Peu critique : 20 4 – Non critique : 30

Le score de risque pour les résultats des tests après réapplication du calculateur est affiché dans la table suivante :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Score de risque pour TR lors de la réapplication du calculateur

ID	Criticité opérationnelle (50 %)	Criticité du contrôle (50 %)	Score de risque résultant
CTR0000001	1 – Très critique (50 % x 100)	Mineure (50 % x 20)	60
CTR0000002	1 – Très critique (50 % x 100)	Faible (50 % x 30)	65
CTR0000003	2 – Assez critique (50 % x 70)	Mineure (50 % x 30)	45
CTR0000004	2 – Assez critique (50 % x 70)	Modérée (50 % x 60) *Valeur révisée	65 *Valeur révisée
CTR0000005	3 – Peu critique (50 % x 20) *Valeur révisée	Faible (50 % x 30)	25 *Valeur révisée

Exemple de calcul de déploiement de risque pour Conformité de la configuration (avant la version 15.0)

L'exemple suivant montre comment les scores des calculateurs de déploiement des risques sont déterminés.

Pour le calculateur de déploiement de tâche de rattrapage suivant, la formule de calcul du score de risque de la tâche de rattrapage est la suivante :

(Score de risque maximal/100) * 85 + (facteur * 15).

Le facteur de l'équation précédente est déterminé par le nombre de résultats des tests, comme indiqué dans le tableau suivant.

Nombre de résultats des tests	Facteur
<10	0,2
10-99	0,4
100-1000	0,6
1001-9999	0,8
> 1 000	1

Pour la tâche de rattrapage suivante, TRG0003066, avec trois résultats de test Scores de risque, le score maximal est 90.

Numéro	Score du risque	Tâche de rattrapage	Résultat	Statut
CTR000123	90	TRG0003066	Échoué	Ouvrir
CTR000124	70	TRG0003066	Échoué	Ouvrir

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Numéro	Score du risque	Tâche de rattrapage	Résultat	Statut
CTR000125	40	TRG0003066	Échoué	Ouvrir

Pour la tâche de rattrapage, TRG0003066 :

Le score de risque est de 79, (90/100) * 85 + 0,2 * 15 = Math.floor (76,5 +3) =79.

Le score de risque historique est nul, car la tâche de rattrapage est toujours « ouverte ».

Après l'ingestion des données, les résultats des tests sont « Validés » et la tâche de rattrapage passe à l'état « Fermé », comme illustré dans la table suivante.

Numéro	Score de risque (avant v15.0)	Tâche de rattrapage	Résultat	Statut
CTR000123	0	TRG0003066	Réussi	Fermé
CTR000124	0	TRG0003066	Réussi	Fermé
CTR000125	0	TRG0003066	Réussi	Fermé

L'historique des résultats des tests est affiché dans la table suivante.

Numéro	Score du risque	Dernier résultat	Résultat
CTRH000111	90	CTR000123	Échoué
CTRH000112	70	CTR000124	Échoué
CTRH000113	40	CTR000125	Échoué

Le score de risque est égal à zéro, car il n'existe aucun résultat de test actif dans la tâche de rattrapage.

Pour la tâche de rattrapage, TRG0003066 :

Le score de risque historique est de 79 : (90/100) * 85 + 0,2 * 15 = Math.floor (76,5 +3) =79.

Exemple de calcul de déploiement de risque pour Conformité de la configuration (v15.0 et versions ultérieures)

L'exemple suivant montre comment les scores des calculateurs de déploiement des risques sont déterminés.

Pour le calculateur de déploiement de tâche de rattrapage suivant, la formule de calcul du score de risque de la tâche de rattrapage est la suivante :

(Score de risque maximal* 80/100) + (Score de risque moyen* 5/100) + (Facteur * 15)

Où, les poids sont les suivants :

- Score de risque maximal : 80
- Score de risque moyen : 5
- Facteur : 15

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La pondération par défaut du score de risque moyen est de 0. Pour plus d'informations sur le réglage des pondérations, reportez-vous à la section Modifier les calculateurs de déploiement de risque pour Conformité de la configuration.

Le facteur de l'équation précédente est déterminé par le nombre de résultats des tests, comme indiqué dans le tableau suivant.

Nombre de résultats des tests	Facteur
<10	0,2
10-99	0,4
100-1000	0,6
1001-9999	0,8
>10000	1

Pour la tâche de rattrapage suivante, TRG0003066, avec trois résultats de test Scores de risque, le score de risque maximal est 90 et le score de risque moyen est de 66,67.

Numéro	Score du risque	Tâche de rattrapage	Résultat	Statut
CTR000123	90	TRG0003066	Échoué	Ouvrir
CTR000124	70	TRG0003066	Échoué	Ouvrir
CTR000125	40	TRG0003066	Échoué	Ouvrir

Pour la tâche de rattrapage, TRG0003066 :

Le score de risque est de 81, (90 * 80/100) + (66,67 * 5/100) + (0,2 * 15) = Math.floor (78,3 +3) = 81.

Le score de risque historique est nul, car la tâche de rattrapage est toujours « ouverte ».

Après l'ingestion des données, les résultats des tests sont « Validés » et la tâche de rattrapage passe à l'état « Fermé », comme illustré dans la table suivante. À partir de la version 15.0 de , le score de risque d'un résultat de Conformité de la configurationtest réussi est renseigné pour déterminer le risque atténué.

Numéro	Score du risque	Tâche de rattrapage	Résultat	Statut
CTR000123	90	TRG0003066	Réussi	Fermé
CTR000124	70	TRG0003066	Réussi	Fermé
CTR000125	40	TRG0003066	Réussi	Fermé

L'historique des résultats des tests est affiché dans la table suivante.

Numéro	Score du risque	Dernier résultat	Résultat
CTRH000111	90	CTR000123	Échoué
CTRH000112	70	CTR000124	Échoué

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Numéro	Score du risque	Dernier résultat	Résultat
CTRH000113	40	CTR000125	Échoué

Le score de risque de la tâche de rattrapage est zéro, car il n'existe aucun résultat de test actif dans la tâche de rattrapage.

Pour la tâche de rattrapage, TRG0003066 :

Le score de risque historique est de 81 : (90 * 80/100) + (66,67 * 5/100) + (0,2 * 15) = Math.floor (78,3 +3) = 81.

Créer ou modifier Conformité de la configuration des règles de tâche de rattrapage

Vous pouvez créer des règles pour regrouper automatiquement les résultats des tests en fonction des conditions de filtre. Ces règles regroupent automatiquement les résultats des tests à mesure qu'ils sont importés. Utilisez le filtre pour limiter les résultats des tests regroupés par cette règle, par exemple en sélectionnant tous les résultats des tests avec des exploits.

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
Le système de base est livré avec une règle de tâche de rattrapage, **un groupe d'affectation, un test**, qui regroupe les résultats des tests par groupe d'affectation (préremplis à partir des **règles d'affectation**) et le champ **Test** des résultats des tests. Cette règle peut être modifiée à l'aide de conditions de filtre et de clés de groupe. Les clés de groupe sont des colonnes dans la table des résultats des tests. Sélectionnez jusqu'à six clés pour indiquer les valeurs à utiliser pour regrouper les résultats des tests.

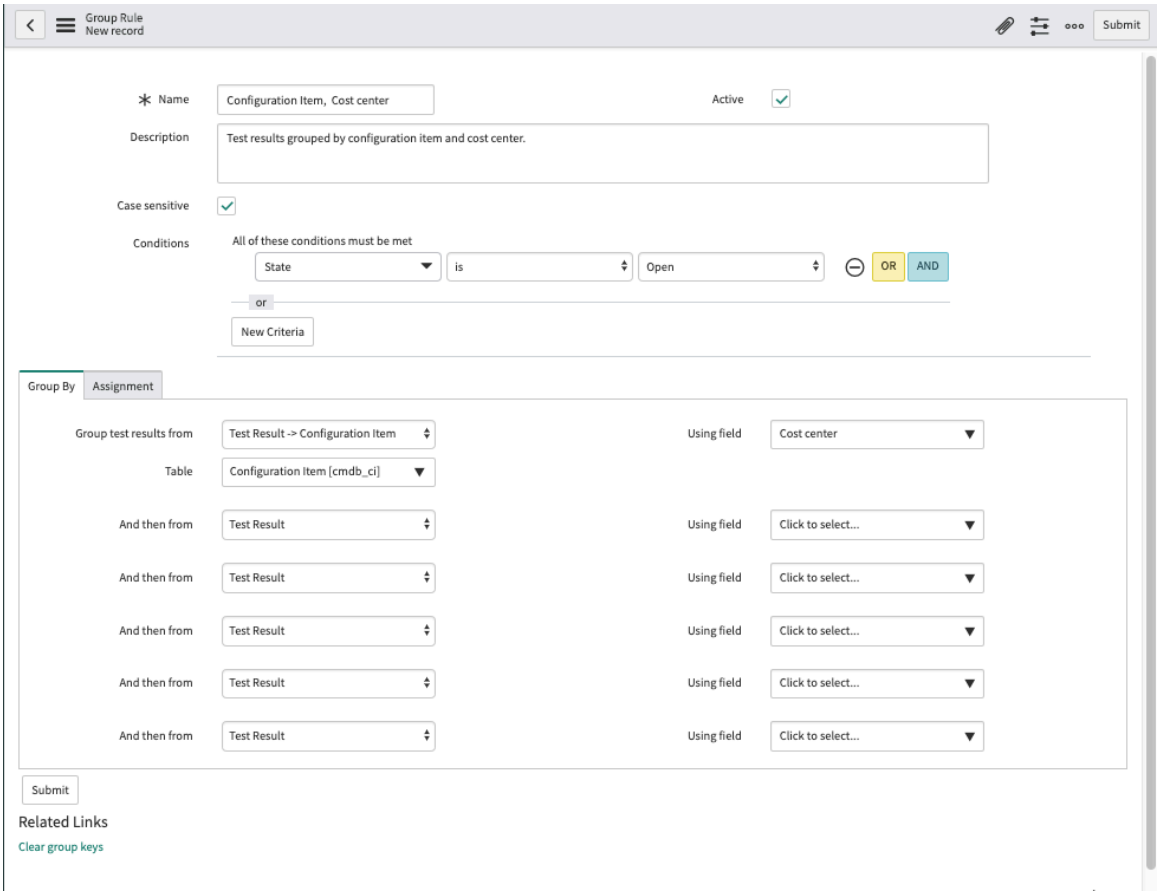
À compter de la version 14.7 de , la règle de tâche de rattrapage de **test du groupe d'affectation**Conformité de la configurationest désactivée pour les nouvelles implémentations.

Remarque : Les règles nouvelles ou mises à jour sont automatiquement évaluées lors de l'importation suivante ou manuellement à l'aide du bouton **Réappliquer** du formulaire Règle de groupe.

Procédure
1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Règles de la tâche de rattrapage**.
2. Ouvrez le **groupe d'affectation,** la règle de test ou cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. S'il s'agit **d'un nouveau**, renseignez les champs du formulaire comme il convient.

Conformité de la configuration Règle de la tâche de rattrapage

Champ	Description
Nom	Nom de la règle de groupe.
Actif	Indique si le groupe est actif.
Description	Texte descriptif de cette règle de tâche de rattrapage.
Sensible à la casse	Détermine si la correspondance de règle est sensible à la casse ou non. **Remarque :** La valeur par défaut n'est pas sensible à la casse.
Conditions	Conditions qui doivent être remplies. Par défaut (case à cocher **sensible à la casse** désactivée), le texte de recherche que vous saisissez dans le générateur de conditions sur les enregistrements et formulaires de règles de groupe n'est pas sensible à la casse. Vous pouvez activer les recherches sensibles à la casse dans les enregistrements de groupe et les formulaires.
Grouper par	
Résultats des tests	Automatiser la création de groupes en fonction de cette règle. Choisissez l'une des options disponibles.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
de groupe de	◦ Résultat de test | Utilisation du champ ◦ Résultat du test >Élément de configuration | Tableau | Utilisation du champ Si un champ **de table** étendue est sélectionné, les résultats des tests qui n'utilisent pas la table étendue correspondante sont regroupés dans une tâche de rattrapage distincte.
Affectation	
Affecter des groupes de résultats des tests par	Automatisez l'affectation des groupes créés en fonction de cette règle. Choisissez l'une des options disponibles. ◦ Clé du groupe Lorsque cette option est sélectionnée, un champ de valeur de clé apparaît, les champs disponibles sont répertoriés dans un menu déroulant. ◦ Groupe d'utilisateurs Lorsque cette option est sélectionnée, un champ de recherche de groupe d'utilisateurs s'affiche.

4. Cliquez sur **Envoyer**.

Remarque : Le lien connexe **Effacer le groupe par clés** supprime les clés du groupe de l'onglet Grouper par du formulaire.

Spécifier la durée d'une exception demandée pour une tâche de rattrapage

Utilisez les propriétés système pour limiter la durée pendant laquelle une exception est demandée pour une tâche de rattrapage. Le rattrapage de la tâche de rattrapage est reporté pour la période spécifiée.

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
La propriété `sn_vulc.exception_max_request_days` est utilisée pour spécifier le nombre maximal de jours pour lesquels une exception pour une tâche de rattrapage peut être demandée. La valeur par défaut est de 365 jours.

Remarque : Vous pouvez utiliser la propriété `sn_vulc.exception_approval_required` pour désactiver le workflow d'approbation d'exception pour la tâche de rattrapage si elle n'est pas requise. Par défaut, cette propriété est activée et sa valeur est `true`.

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Toutes les propriétés**.
2. Sur la page Propriétés système, recherchez `sn_vulc.exception_max_request_days`.
3. Cliquez sur le nom de la propriété pour ouvrir l'enregistrement Propriété système.
4. Pour pouvoir modifier cet enregistrement, assurez-vous que Conformité de la configuration est sélectionné comme l'application actuelle.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Entrez une **valeur** positive et cliquez sur **Mettre à jour**.
   L'enregistrement est mis à jour et enregistré.

Configurer la gestion des exceptions pour Conformité de la configuration

Limitez la durée d'une exception demandée et ajoutez un questionnaire à l'exception à l'aide du Conformité de la configuration module. Par défaut, une exception est demandée à l'aide du ServiceNow® Réponse aux vulnérabilités module. Vous pouvez également demander une exception à l'aide de l'intégration GRC : gestion de la politique et de la conformité .

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
Si Réponse aux vulnérabilités cette option est activée, vous pouvez limiter la durée pendant laquelle une exception peut être demandée. De même, si le GRC : gestion de la politique et de la conformité module est installé, vous pouvez le sélectionner GRC : gestion de la politique et de la conformité sur l'écran de configuration. L'activation de cette option vous permet de demander une exception qui spécifie l'objectif de politique et de contrôle à partir de GRC.

Si vous ajoutez un questionnaire, il est envoyé à la personne qui émet l'exception ou la demande de faux positif. Vous pouvez utiliser le questionnaire par défaut ou en créer un en fonction de vos besoins.

Il est utile que l'approbateur de l'exception comprenne le motif de la demande d'exception.

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire Configuration de la gestion des exceptions, sélectionnez la façon dont vous souhaitez gérer une exception en sélectionnant une option dans la liste Gérer les exceptions à l'aide de.
   - Réponse aux vulnérabilités

     Remarque : À partir de la version 22.0 sur Réponse aux vulnérabilités, vous pouvez également configurer un questionnaire pour les demandes de faux positifs pour l'option Réponse aux vulnérabilités .

   - GRC : gestion de la politique et de la conformité

     Remarque : Vous devez activer le GRC module d'extension à utiliser GRC : gestion de la politique et de la conformité pour demander une exception.

   Remarque : La modification de la configuration n'a pas d'impact sur les données existantes.

3. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Paramètres pour la gestion des exceptions CC

Champ	Description
Durée	Période pour laquelle une exception peut être demandée.
Unité	Unité de temps pour la période spécifiée.
Activer le questionnaire pour demander une exception	Option permettant d'ajouter un questionnaire à la demande d'exception émise.
Questionnaire pour demander une exception	Option permettant d'afficher le questionnaire que vous avez sélectionné pour demander une exception. Le questionnaire d'exceptions est affiché par défaut.
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Questionnaire pour marquer comme faux positif	Option permettant d'afficher le questionnaire que vous avez sélectionné pour le marquer comme faux positif. Le questionnaire pour une demande de faux positif est affiché par défaut.

4. Sélectionnez **Enregistrer**.

Ajouter un approbateur d'exception pour Conformité de la configuration

Ajoutez des utilisateurs aux groupes d'approbateurs afin de pouvoir demander une exception pour une tâche de rattrapage dans Conformité de la configuration.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Une demande d'exception pour une tâche de rattrapage est approuvée à l'aide du workflow d'approbation à deux niveaux par défaut. L'ajout d'utilisateurs au groupe de premier niveau est obligatoire. S'il n'y a pas d'utilisateurs au deuxième niveau, la demande est automatiquement approuvée après l'approbation de premier niveau.

Remarque : S'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée.

Remarque : Jusqu'à Conformité de la configuration la version 13.0, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Toutefois, à partir de la Conformité de la configuration version 13.0, si vous déployez l'application CC pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas le repasser en workflow.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Utilisateurs et groupes** > **Groupes**.
2. Dans la colonne Nom, recherchez **Exception**, puis cliquez sur **Approbateur d'exception - CC de niveau 1**.

   Remarque : À partir de la Conformité de la configuration version 14.7.5, vous pouvez utiliser les propriétés système fournies dans le système de base pour les approbations d'exceptions via le workflow de la table Propriétés système [sys_properties]. Ainsi, lorsqu'une demande d'exception est émise via un workflow, elle est envoyée pour approbation aux ID de groupe définis dans la propriété système. Accédez à la **Tout** > **Propriétés système** et sélectionnez *sn_vulc.exception_approver_L1_CC* ou *sn_vulc.exception_approver_L2_CC* pour modifier la valeur de la propriété.

3. Dans le formulaire CC de niveau 1 de l'approbateur d'exceptions de groupe, accédez à **Membres de groupes** > **Nouveau** (ou **Modifier**).
4. Renseignez les champs du formulaire.

Formulaire d'utilisateur

Champ	Description
ID d'utilisateur	Identificateur unique pour l'utilisateur.
Prénom	Prénom de l'utilisateur.
Nom de famille	Nom de famille de l'utilisateur.
Titre	Fonction de l'utilisateur. Saisissez un titre ou une description de poste, ou sélectionnez-en un dans la liste.
Département	Département de l'utilisateur.
Mot de passe	Mot de passe affecté à l'utilisateur. Ce mot de passe peut être permanent ou temporaire.
Mot de passe à réinitialiser	Option permettant à l'utilisateur de réinitialiser le mot de passe pour garantir la sécurité.
Verrouillé	Option permettant de verrouiller l'utilisateur hors de l'instance et de mettre fin à toutes les sessions actives de l'utilisateur. Le système empêche les utilisateurs disposant du rôle administrateur de se verrouiller eux-mêmes.
Actif	Option pour rendre cet utilisateur actif. Vous seul pouvez voir un utilisateur inactif dans ces zones :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Listes d'utilisateurs ◦ Liste de sélection sur les champs de référence (icône de loupe) ◦ Liste de saisie semi-automatique qui s'affiche lorsque vous entrez du texte dans un champ de référence
Accès au service Web uniquement	Option permettant de désigner cet utilisateur comme utilisateur non interactif.
Utilisateur d'intégration interne	Option permettant de désigner cet utilisateur en tant qu'utilisateur d'intégration interne.
E-mail	Adresse e-mail de l'utilisateur.
Langue	Langue préférée de l'utilisateur.
Intégration du calendrier	Calendrier utilisé pour gérer le calendrier de travail. Par exemple, Outlook.
Fuseau horaire	Fuseau horaire de l'emplacement de cet utilisateur.
Format de date	Format préféré de l'utilisateur pour les dates.
Tél. professionnel	Téléphone professionnel de l'utilisateur.
Tél. mobile	Téléphone portable de l'utilisateur.
Photo	Photo que vous pouvez télécharger en cliquant sur **Cliquer pour ajouter...**.

5. Cliquez sur **Envoyer**.
6. Facultatif : Répétez les étapes 1 à 5 pour créer un approbateur d'exceptions : niveau 2 CC.

   Remarque : Lors de la création d'un approbateur de deuxième niveau, sélectionnez **Approbateur d'exceptions : niveau 2 CC**

7. Facultatif : Si vous sélectionnez **Modifier**, déplacez les utilisateurs de la **collection** vers le panneau **Membres du groupe** , puis cliquez sur **Enregistrer**.
   L'approbateur doit accéder à **Tout** > **Configuration Compliance** > **Mes approbations** et approuver les demandes.

Créer une carte de Conformité de la configuration criticité

Conformité de la configuration Le mappage de criticité fournit une carte de transformation des champs de criticité de source tierce en champs reconnaissables en Conformité de la configuration valeur de gravité.

Avant de commencer

Rôle requis : sn_vulc.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Mappage de criticité**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Mappage de champs

Champ	Description
Source	Nom de la source pour le mappage de criticité.
Valeur de la source	Valeur de criticité de la source.
Valeur cible	Valeur cible. Les choix possibles sont les suivants : Critique Le problème de configuration associé au contrôle perturbe un ou plusieurs CI critiques pour l'entreprise. Élevé Le problème de configuration associé au contrôle constitue une menace, mais n'entraîne pas l'arrêt des ressources réseau critiques. Modéré Le problème de configuration associé au contrôle constitue un risque, mais pas une menace immédiate. Faible Le problème de configuration associé au contrôle est une menace de faible niveau qui peut être ignorée au profit des CI les plus exposés. Mineur Le problème de configuration associé au contrôle représente un risque mineur et peut être ignoré si nécessaire.

4. Cliquez sur **Envoyer**.

Traduction automatique

Créer des notifications par e-mail

Les administrateurs de vulnérabilité peuvent modifier la notification ou en ajouter de nouvelles, en spécifiant quand envoyer la notification, qui la reçoit et quel contenu contient la notification.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez créer des modèles d'e-mail pour différents types de notifications par e-mail. Pour en savoir plus sur la création de modèles d'e-mail, reportez-vous à la section Définir des modèles d'e-mail Réponse aux vulnérabilités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Notifications**.
2. Sélectionnez l'enregistrement de notification de cible de rattrapage ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Pour plus d'informations sur les champs de formulaire, consultez Créer une notification par e-mail .
4. Sélectionnez **Prévisualiser la notification** pour afficher le message.

Résultats

À partir de la version 14.11 de , lorsqu'un destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans ou Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT en fonction de Conformité de la configurationson rôle.

- Les liens s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs ayant le rôle sn_vulc.admin.
- Les liens s'ouvrent dans le Espace de travail de remédiation IT pour les utilisateurs disposant du rôle sn_vulc.remediation_owner.

Si le destinataire n'a aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Configurer des règles d'approbation pour la gestion des exceptions dans Conformité de la configuration

À partir de la Conformité de la configuration version v13.0, utilisez le concepteur de flux pour approuver les demandes d'exception pour la gestion des exceptions et les règles d'exception. Si vous déployez CC pour la première fois, Flow Designer est activé par défaut.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Si vous êtes un utilisateur existant Conformité de la configuration , l'option par défaut est workflow.

Si vous avez déployé Conformité de la configuration la version 13.0 ou ultérieure, la valeur de la propriété *sn_vulc.flow_designer_activation* système est définie sur true. Cela signifie que Flow Designer est activé par défaut.

Si vous utilisez Conformité de la configuration déjà une version antérieure à la version 13.0, la valeur de cette propriété système est définie sur false. Vous pouvez activer le concepteur de flux en changeant la valeur sur vrai.

Remarque : Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer. Pour une comparaison détaillée entre le workflow et Flow Designer, reportez-vous à la section Comparaison du workflow de gestion des exceptions et de Flow Designer dans Conformité de la configuration.

Pour utiliser le concepteur de flux, créez des règles à l'aide du module Règles d'approbation. À l'aide de ce module, vous pouvez configurer des règles d'approbation pour chacun des workflows de gestion des exceptions suivants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Règles d'approbation d'exception pour les groupes de résultats des tests
- Règle d'approbation pour les règles d'exception automatique

Remarque : Vous pouvez également définir des conditions contenant plusieurs niveaux d'approbation au sein d'une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant. Pour plus d'informations sur la configuration des niveaux d'approbation, reportez-vous à la section Créer des niveaux d'approbation pour la gestion des exceptions dans Conformité de la configuration.

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Règles d'approbation** > **Règles d'approbation d'exception pour le groupe de résultats des tests**.
2. Sur la page Règles d'approbation, sélectionnez le groupe pour lequel vous souhaitez définir la règle d'approbation.
3. Renseignez les champs du formulaire.

Formulaire Règle d'approbation

Champ	Description
Nom	Nom de configuration de l'approbation.
Table	Table sur laquelle la règle est appliquée.
Application	La valeur par défaut est Conformité de la configuration.
Type de règle	Spécifie le type de règle. Par exemple, gestion des exceptions ou règle d'exception.
Actif	Activé par défaut, ce qui signifie que la règle d'approbation est utilisée.
Description	Brève description des règles d'approbation.
Expiration de l'approbation (jours) À partir de la v14.11 de Conformité de la configuration	Date jusqu'à laquelle l'approbateur peut approuver la demande.
Notification de l'approbateur (jours) À partir de la v14.11 de Conformité de la configuration	Date après laquelle l'approbateur est invité à prendre des mesures.

4. Sélectionnez **Mettre à jour**.
Dans l'onglet Configurations d'approbation, deux niveaux d'approbateurs sont configurés par défaut. Vous pouvez sélectionner une règle pour définir les conditions en fonction de différents cas d'utilisation au sein d'une règle. Pour en savoir plus, reportez-vous à Créer des configurations pour une règle d'approbation dans Conformité de la configuration.

Remarque : Dans chaque page de configuration, vous pouvez créer plusieurs niveaux d'approbation. Pour en savoir plus, reportez-vous à Créer des niveaux d'approbation pour la gestion des exceptions dans Conformité de la configuration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example:
En fonction des différents cas d'utilisation, vous pouvez définir différents processus d'approbation pour les mêmes résultats des tests trouvés sur différentes tâches de rattrapage.

Créer des configurations pour une règle d'approbation dans Conformité de la configuration

Définissez les conditions pour filtrer les tâches de rattrapage correspondantes pour un niveau d'approbation.

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
Dans le module Configurations d'approbation, vous pouvez configurer plusieurs niveaux d'approbation pour différentes configurations. Définissez des règles basées sur des conditions, chaque règle contenant plusieurs niveaux d'approbation.

Remarque : Utilisez le module Règles d'approbation pour configurer des règles d'approbation pour les workflows de gestion des exceptions. Pour en savoir plus sur la configuration des règles d'approbation, reportez-vous à la section Créer des niveaux d'approbation pour la gestion des exceptions dans Conformité de la configuration.

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Règles d'approbation**.
2. Sélectionnez une règle d'approbation et accédez à l'onglet **Configurations d'approbation** .
3. Sélectionnez une configuration.
4. Renseignez les champs du formulaire.

Formulaire de configuration de l'approbation

Champ	Description
Nom	Nom de configuration de l'approbation.
Règle d'approbation	Contient les détails de table et de type pour la règle d'approbation.
Ordre	Ordre d'exécution des différentes configurations au sein d'une règle. Par exemple, une configuration avec une entrée d'ordre de 100 est exécutée avant une configuration avec une entrée d'ordre de 200.
Actif	Activé par défaut, ce qui signifie que la configuration d'approbation est en cours d'utilisation.
Description	Brève description des niveaux de configuration de l'approbation.

5. Définissez une condition pour les résultats des tests ou les tâches de rattrapage de l'une des façons suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Condition	Identifie les résultats des tests ou les tâches de rattrapage correspondants.
Condition avancée	Script qui définit la condition pour les résultats des tests ou les tâches de rattrapage. **Remarque :** Ce champ s'affiche lorsque vous cochez la case **Avancé** .

6. Sélectionnez **Mettre à jour**.
   Vous pouvez définir des conditions contenant plusieurs niveaux d'approbation au sein d'une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant. Pour plus d'informations sur la configuration des niveaux d'approbation, reportez-vous à la section Créer des niveaux d'approbation pour la gestion des exceptions dans Conformité de la configuration.

Example:
Vous pouvez définir différents chemins d'approbation pour différents types de tâches de rattrapage.

Créer des niveaux d'approbation pour la gestion des exceptions dans Conformité de la configuration

Définissez les niveaux d'utilisateurs et de groupes d'utilisateurs qui vont approuver les demandes d'exception.

Avant de commencer
Rôle requis : sn_vulc.admin

Procédure
1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Règles d'approbation**.
2. Sélectionnez une règle d'approbation et accédez à l'onglet **Configurations d'approbation** .
3. Sélectionnez une configuration.
4. Dans la section **Niveaux d'approbateur** , sélectionnez un niveau d'approbateur.
5. Renseignez les champs du formulaire.

Formulaire du niveau de l'approbateur

Champ	Description
Nom	Nom du niveau d'approbation.
Approbation requise	Sélectionnez le nombre d'approbations requises pour le niveau sélectionné : ◦ Un approbateur requis ◦ Approbation de tous les utilisateurs requise

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Activé par défaut, ce qui signifie que le niveau d'approbation est utilisé.
Ordre	Ordre d'exécution des différentes configurations au sein d'une règle. Par exemple, une configuration avec une entrée d'ordre de 100 s'exécute avant une configuration avec une entrée d'ordre de 200.
Règle d'approbation	Contient les détails de table et de type pour la règle d'approbation. Ce champ est en lecture seule.
Configuration de l'approbation	Contient les configurations d'approbation. Ce champ est en lecture seule.
Affecter à l'aide de	Sélectionnez une option parmi : ◦ Utilisateur et groupe d'utilisateurs ◦ Champ de la table des approbations ◦ Script
Groupes	Groupe de niveau de l'approbateur composé de plusieurs utilisateurs. L'utilisateur doit avoir l'un des rôles suivants pour la gestion des exceptions et les règles d'exception : ◦ sn_vulc.exception_approver ◦ sn_vulc.read ◦ sn_vulc.read_auto_exception_rule
Utilisateurs	Modifier les utilisateurs répertoriés dans les groupes.

6. Pour enregistrer les changements, sélectionnez **Mettre à jour**.

Remarque : Avant la version 13.0, le processus de workflow était fonctionnel s'il n'y avait que des utilisateurs au niveau d'exception 1. Cependant, à partir de la version 13.0, il doit y avoir au moins un utilisateur dans chaque niveau.

Avant la version 13.0, dans le workflow, s'il n'y avait pas d'utilisateur au deuxième niveau, la tâche de rattrapage était différée. Toutefois, à partir de la version 13.0, s'il n'y a pas d'utilisateur au deuxième niveau, la demande d'approbation est automatiquement rejetée.

Example:
Il peut y avoir différents niveaux d'approbation pour les tâches de rattrapage pour les serveurs Linux et Windows.

Comparaison du workflow de gestion des exceptions et de Flow Designer dans Conformité de la configuration

À partir de Conformité de la configuration (CC) v13.0, si vous déployez CC pour la première fois, le concepteur de flux pour l'approbation des demandes d'exception dans la gestion

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

des exceptions est activé par défaut. Si vous disposez déjà d'un utilisateur CC, l'option par défaut est workflow.

Workflow et Flow Designer

Considérations	Workflow	Flow Designer
Version	Avant la version 13.0 de CC.	À partir de la version 13.0 de CC.
Option par défaut	Option par défaut si vous êtes un utilisateur CC existant.	Option par défaut pour les nouveaux utilisateurs CC à partir de la version 13.0.
Définition du processus d'approbation	La gestion des exceptions inclut les demandes et les règles d'exception.	Inclut la définition de différents niveaux et l'ajout de différents approbateurs pour différents cas d'utilisation. Plus facile à mettre en œuvre que le workflow. La gestion des exceptions inclut les demandes et les règles d'exception.
Mise à niveau vers Flow Designer	Vous pouvez effectuer une mise à niveau vers Flow Designer depuis le workflow. Toutefois, les demandes existantes ne peuvent être approuvées qu'à l'aide du workflow.	Flow Designer est activé par défaut.
Propriété système *sn_vulc.flow_designer_activation*	Si vous avez utilisé le workflow pour la gestion des exceptions avant la version 13.0, la propriété système est définie sur false. Pour activer le concepteur de flux, définissez cette propriété sur vrai. **Remarque :** Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer.	Si vous utilisez CC pour la première fois pour la version 13.0 ou ultérieure, la valeur de propriété système est définie sur vrai par défaut.
Module de règles d'approbation	Une fois la propriété système définie sur vrai, la tâche planifiée **Activer les règles d'approbation du module** s'exécute dans les 24 heures. Cette tâche planifiée active le module **Règles d'approbation** . Pour activer ce module instantanément,	Si vous avez déployé CC pour la première fois à partir de CC v13.0, ce module est disponible par défaut.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow et Flow Designer (suite)

Considérations	Workflow	Flow Designer
	exécutez cette tâche manuellement.	
Niveaux d'approbation	Permet de définir uniquement deux niveaux d'approbateurs.	Fournit plusieurs options, telles que la définition d'un nombre illimité de configurations, de niveaux d'approbateurs et l'ajout dynamique d'approbateurs pour chaque règle.

Intégrations de Conformité de la configuration

Les intégrations tierces importent dans l'application les résultats de l'évaluation de configuration, les politiques, les tests, les technologies, les sources de référence et les Conformité de la configuration résultats des tests, ainsi que d'autres données de vulnérabilité.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

L'application Conformité de la configuration prend en charge les intégrations tierces suivantes :

- À partir de la version 14.11, corrigez les failles de sécurité dans les actifs de votre entreprise identifiées par l'application Contrôle de la posture de sécurité en publiant les résultats sous forme de résultats de tests dans l'application Conformité de la configuration . L'application Contrôle de la posture de sécurité et ses applications prises en charge sont disponibles avec des abonnements distincts à partir du ServiceNow® Store. Consultez Contrôle de la posture de sécurité pour plus d'informations.
- Microsoft Defender for Cloud Integration pour Opérations de sécurité
- Intégration des vulnérabilités dans le cloud Palo Alto Prisma
- Qualys intégration avec Conformité de la configuration
- Le Tenable.io produit de l'intégration de vulnérabilité Tenable

Notes supplémentaires pour les intégrations

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 14.8.5 de Conformité de la configuration, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Microsoft Defender for Cloud Integration pour Opérations de sécurité

Il Microsoft Defender for Cloud Integration s'agit d'un système de gestion de la sécurité de l'infrastructure qui améliore la posture de sécurité de vos environnements cloud.

Microsoft Defender for Cloud Integration for Opérations de sécurité s'intègre à l'application Conformité de la configuration pour mapper les tests aux éléments de configuration (CI) afin de créer des résultats de tests. Il découvre en permanence les nouvelles ressources cloud déployées sur les charges de travail et détermine si elles sont configurées conformément aux normes de sécurité telles que le Center for Internet Security (CIS).

À partir de la version 2.2, Microsoft Azure Security Center est renommé en Microsoft Defender for Cloud Integration for Opérations de sécurité.

Versions disponibles

Application	Version
Microsoft Defender for Cloud Integration pour Opérations de sécurité	2.3
Conformité de la configuration	14.3
Security Support Common	13.2
Réponse aux vulnérabilités	16.2

Déploiements multiples de la Microsoft Defender pour le cloud plateforme

Si vous avez plusieurs déploiements de l'application Microsoft Defender pour le cloud Platform, vous pouvez ajouter une intégration pour chaque déploiement. Les ressources identifiées par plusieurs déploiements tiers sont consolidées et rapprochées avec votre Base de données de gestion des configurations (CMDB). Cette consolidation a lieu même lorsque les processus d'analyse se chevauchent entre les différents déploiements.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Microsoft Defender pour le cloud Intégrations

Le Microsoft Defender for Cloud Integration for Opérations de sécurité enrichit les données de conformité sur votre instance en récupérant les données à partir de Microsoft Defender pour le cloud. Une série de travaux planifiés invoque automatiquement les intégrations. Vous pouvez également exécuter ces travaux planifiés manuellement. Les travaux planifiés simplifient le cycle de vie du rattrapage des résultats des tests en synchronisant l'instance avec Microsoft Defender pour le cloud.

Un utilisateur d'exécution en tant que configuré existe pour chaque enregistrement d'intégration, avec la valeur par défaut **VR. Système**. Cette valeur doit rester la même.

Remarque : Si vous ne définissez pas d'utilisateur d'exécution en tant que valide, des pièces jointes de récupération de données en double ou multiples sont créées pour les enregistrements de source de données. Le nombre de pièces jointes augmente chaque fois que l'intégration est exécutée. Cela augmente le temps de traitement, ce qui entraîne des résultats de transformation incohérents.

Microsoft Defender pour le cloud Les tâches d'intégration de plateforme impliquent les rôles suivants.

- sn_vul_asc.configure_integration : capacité de lire, d'écrire et de supprimer des enregistrements.
- sn_vul_asc.read_integration : capacité à lire des enregistrements.

Affichage des Microsoft Defender pour le cloud intégrations

Afficher les intégrations en accédant à **Tout** > **Intégration de Microsoft Defender pour le cloud** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base.

Intégration	Description
Intégration de définition de politique	Récupère les politiques et crée des entrées de politique dans votre instance.
Intégration des métadonnées d'évaluation	Récupère les métadonnées d'évaluation et crée des tests dans votre instance.
Conformité, normes et intégration des contrôles	Récupère les normes et les contrôles, et crée la source d'autorisation et les citations. Il les relie ensuite aux tests créés.
Intégration de l'évaluation	Récupère les évaluations et les traite dans votre instance. La sortie de cette intégration est des résultats de tests.

Créer des CI à l'aide du moteur Identification et Réconciliation

Utilisez le moteur Identification et rapprochement (IRE) pour créer des CI, lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte importé d'un scanner tiers.

Si un CI n'est pas mis en correspondance dans la CMDB, un CI est créé dans la *cmdb_ci_cmp_resource* classe. Par la suite, lorsqu'une détection trouve le même CI, elle enrichit le CI ou en crée un autre.

Remarque : Le rapprochement automatique ne se produit pas pour les ressources cloud.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer et configurer Microsoft Defender for Cloud Integration pour Opérations de sécurité

Installez et configurez le Microsoft Defender for Cloud Integration for Opérations de sécuritéafin de pouvoir utiliser les données importées Microsoft Defender pour le cloud pour classer par ordre de priorité et corriger toute configuration incorrecte de vos actifs.

Avant de commencer

Créer une inscription d'application sur Azure Active Directory. Pour plus d'informations sur l'inscription d'une nouvelle application sur Azure Active Directory, recherchez `Enregistrer une application cliente dans Azure Active Directory` sur le site de documentation de Microsoft . Affectez le rôle **de lecteur de sécurité** pour l'enregistrement de l'application nouvellement créée sur le périmètre approprié avec lequel vous souhaitez vous connecter à ServiceNow. Il peut s'agir d'un niveau de gestion, de groupe ou d'abonnement.

Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Modules d'extension**.
2. Dans la barre de recherche, recherchez `Microsoft Defender for Cloud Integration for Security Operations`.
3. Sélectionnez **Installer**.

   Toutes les dépendances qui seront installées sont affichées.
4. Accédez à la **Tout** > **Intégration de Microsoft Defender pour le cloud** > **Administration** > **Configuration** > **Configuration de Microsoft Defender pour le cloud**.
5. Renseignez les champs du formulaire.

Microsoft Defender pour le cloud Formulaire de configuration

Champ	Description
URL D'API	URL de ressource de l'instance. Exemple : https://management.azure.com (cloud public Azure)
ID de locataire	Identité du locataire de votre organisation.
Instance d'intégration	Instance par défaut. Vous pouvez également créer une instance pour apporter les données à partir de plusieurs locataires ou abonnements Microsoft Defender .
ID client	Identité du client générée après l'enregistrement de l'application Microsoft Defender for Cloud Integration .
Secret client	Secret client généré après l'enregistrement de l'application Microsoft Defender for Cloud Integration .
Importer les conclusions à partir de	Ressources et évaluations qui correspondent aux ID de groupe d'administration et d'abonnement sélectionnés qui doivent être récupérés.
ID des groupes de gestion	Ressources et évaluations correspondant aux ID de groupe de gestion à récupérer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Ce champ s'affiche uniquement lorsque vous sélectionnez **Groupes de gestion spécifiques** dans le champ **Importer les résultats de** .
ID d'abonnements	Numéros d'identification des abonnements pour lesquels les ressources et les évaluations doivent être récupérées. **Remarque :** Ce champ s'affiche uniquement lorsque vous sélectionnez **Abonnements spécifiques** dans le champ **Importer les résultats de** .
État de validation	Indique si les informations d'identification et l'ID d'abonnement fournis sont valides.

6. Configurez ou exécutez les intégrations en sélectionnant **Enregistrer et tester**.

Conformité de la configuration Données importées pour Microsoft Defender for Cloud Integration

Conformité de la configuration importe les politiques, les tests, les sources de référence et les résultats des tests à partir d'intégrations tierces et les stocke dans des modules pour consultation.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Groupes de tests

Un groupe de tests de configuration constitue un groupe de tests. Les groupes de tests sont associés à des documents et des enregistrements de test faisant autorité, et ils peuvent être modifiés pour répondre aux besoins de votre organisation. Un test de configuration peut appartenir à plusieurs groupes de tests.

Si le est installé, les Microsoft Defender for Cloud Integration groupes de tests sont récupérés et renseignés par la tâche planifiée, **Intégration des définitions de stratégies**. Vous pouvez afficher la tâche planifiée en accédant à **Tout** > **Intégration de Microsoft Defender pour le cloud** > **Administration** > **Intégrations** > **Intégration de définitions de politiques**.

Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez d'abord **l'intégration des définitions de politiques** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests

Les tests sont des bibliothèques d'enregistrements de données qui organisent les analyses des ressources informatiques. Les tests de configuration définissent la manière dont les ressources doivent être gouvernées.

Un Conformité de la configuration test est le mécanisme utilisé par les applications d'intégration tierces pour regrouper les actifs par type de résultats des tests.

Si le Microsoft Defender for Cloud Integration est installé, la tâche planifiée, **Intégration des métadonnées d'évaluation**, récupère les tests. Vous pouvez afficher la tâche planifiée en accédant à **Intégration** > **Intégrations principales** > **Intégration des métadonnées d'évaluation**.

Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez **l'intégration des métadonnées d'évaluation** après l'intégration **des définitions de politique**.

À partir de la version 15.0 de , le groupe de Conformité de la configurationtests auquel appartient un test est renseigné dans la colonne **Groupes de tests** de la liste Tests.

Sources de référence

Conformité de la configuration Utilise des sources et des citations de référence lors de la génération d'alertes de vulnérabilité pour les tests. Les sources faisant autorité renvoient généralement à des sections des normes industrielles publiées, telles que **ISO 27001** et **PCI DSS 3.2.1**.

Ces enregistrements sources contiennent des références à des informations sur des problèmes connus de configuration logicielle et matérielle provenant d'experts dans le domaine de la sécurité informatique. Ils définissent les exigences en matière de politiques et de procédures de sécurité.

Si le Microsoft Defender for Cloud Integration est installé, la tâche planifiée, **Normes et contrôles de conformité**, récupère les sources de référence et les contenus des documents de référence. Vous pouvez afficher cette tâche planifiée en accédant à **Tout** > **Intégration de Microsoft Defender pour le cloud** > **Intégrations** > **Conformité, normes et intégration des contrôles**.

Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez **l'intégration des normes de conformité et des contrôles** après l'intégration des **métadonnées d'évaluation**.

Ressources

L'intégration d'évaluation fournit des informations essentielles telles que les balises de ressource et les attributs du cloud. Ces informations sont affichées dans le formulaire Élément détecté. #Il est principalement utilisé pour le filtrage dansConformité de la configuration les règles de tâches d'affectation et de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Balises de ressource : toutes les balises de ressource cloud sont importées en tant que balises hôtes dans le cadre de **l'intégration de l'évaluation**. Les balises cloud de tout type de ressource cloud sont stockées ici, que la ressource soit un hôte ou non.
  - Le stockage des balises n'est pas sensible à la casse. Si une balise Tokyo est créée, une balise **TOKYO** ne peut pas être stockée dans la table de balises Host. **Tokyo** et **TOKYO** sont considérés comme étant la même balise hôte. La balise qui a été importée en premier gagne.
  - L'utilisation de balises hôtes en tant que clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises hôtes sont destinées à être utilisées uniquement dans le générateur de conditions.
- Attributs dans le cloud pour les actifs : voici les attributs du cloud à partir desquels Microsoft Defender pour le cloudles intégrations récupèrent :
  - Compte dans le cloud
  - Région du cloud
  - Type de ressource dans le cloud
  - Fournisseur de services dans le cloud

Résultats des tests

Conformité de la configuration ne calcule pas les résultats des tests, mais les importe dans le cadre d'une intégration tierce. Une fois visibles dans Conformité de la configuration, ils sont corrigés à l'aide de **tâches de rattrapage**.

Si l'intégration Microsoft Defender pour le cloud est installée, la tâche planifiée, **Intégration de l'évaluation**, récupère les résultats des tests. Vous pouvez afficher cette tâche planifiée en accédant à **Tout** > **Intégration de Microsoft Defender pour le cloud** > **Intégrations** > **Intégration de l'évaluation**.

L'importation de l'intégration de l'évaluation est la seule intégration qui utilise le *`Start Time`* paramètre de l'onglet Détails de l'intégration. Toutes les autres Conformité de la configuration importations apportent toutes les données disponibles, indépendamment de *`Start Time`*.

Lorsque l'importation de **l'intégration de l'évaluation** est terminée, un événement est lancé pour déclencher les calculs de fin d'importation.

L'intégration de l'évaluation extrait les évaluations de données uniquement en cas de changement d'état par défaut depuis la dernière exécution réussie de l'intégration. Ainsi, si l'évaluation échoue continuellement au cours des derniers jours, l'intégration ne récupère pas l'évaluation, car il n'y a aucun changement d'état pour l'évaluation. Pour maintenir les résultats des tests à jour avec les évaluations des défenseurs, une nouvelle **intégration d'évaluation complète** est ajoutée, qui extrait les données des sept derniers jours. Il s'exécute chaque semaine et extrait tous les résultats des tests, qui ne sont pas réussis.

Règles de recherche de CI pour identifier les CI à partir des Microsoft Defender pour le cloud intégrations

Lorsque les données sont importées à partir d'une intégration tierce, Conformité de la configuration utilise automatiquement les données de ressource pour rechercher des correspondances dans le , à l'aide des Base de données de gestion des configurations (CMDB)règles de recherche de CI. Ces règles sont utilisées pour identifier les éléments de configuration (CI) et les ajouter à l'enregistrement des résultats des tests pour faciliter le rattrapage. Les règles de recherche de CI du système de base sont disponibles pour l'ID de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ressource, le nom et la catégorie S3. Pour plus d'informations sur les règles de recherche de CI, consultez Règles de verrouillage de CI pour Microsoft Defender for Cloud Integration for Security Operations.

Présentation de Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Prisma Cloud est une solution de sécurité d'infrastructure cloud basée sur des API. Il se connecte à votre environnement cloud et surveille les ressources déployées sur les environnements de cloud public, telles que Amazon Web Services (AWS), Microsoft Azure, et ainsi de suite. Vous bénéficiez d'une visibilité et d'un contrôle complets sur les risques au sein de votre infrastructure de cloud public.

L'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud facilite l'ingestion des politiques et des alertes à partir de Prisma Cloud, respectivement en tant que tests et résultats des tests, dans l'application Conformité de la configuration . Avec la bonne configuration, les résultats des tests peuvent être gérés de manière transparente en affectant des scores de risque appropriés, puis en les regroupant et en les affectant aux utilisateurs et groupes pertinents.

Versions disponibles

La table répertorie les applications qui en dépendent, ainsi que Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud la version de l'application.

Application	Version
Intégration de Prisma Cloud pour Security Operations	2.3
Conformité de la configuration	14.7
Security Support Common	13.5
Réponse aux vulnérabilités	18.0

ServiceNow Intégrations dans le cloud Prisma

L'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud permet d'importer les données Prisma dans votre ServiceNow instance afin d'enrichir votre instance et d'améliorer la gestion. Une série de travaux planifiés invoque automatiquement les intégrations. Vous pouvez également exécuter ces travaux planifiés manuellement. Les travaux planifiés simplifient le cycle de vie de correction des résultats des tests en tenant l'instance à jour en récupérant périodiquement les données à partir du cloud Prisma.

Les tâches d'intégration Prisma Cloud impliquent les rôles suivants.

- sn_vul_prismacloud.configure_integration : capacité de lire, d'écrire et de supprimer des enregistrements.
- sn_vul_prismacloud.read_integration : capacité à lire des enregistrements.

Affichage des intégrations

Vous pouvez afficher les intégrations qui font partie de en Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud accédant à **Intégration dans le cloud Prisma** > **Intégrations**.

Les intégrations suivantes sont disponibles dans le système de base.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exécuter la séquence	Calendrier	Intégration	Description
1	Hebdomadaire	Intégration de la politique Prisma	• Récupère les politiques à partir de Prisma Cloud et crée des entrées de test dans votre instance. • Il ne fournit pas de support incrémentiel. Si vous exécutez l'intégration au cours des 10 derniers jours, le résultat des exécutions d'intégration précédentes s'affiche également.
2	Quotidien	Intégration des alertes Prisma	• Récupère les alertes à partir de Prisma Cloud et crée des entrées de résultats de test dans votre instance. • Fournit un support incrémentiel. L'intégration s'exécute quotidiennement après l'heure de la dernière exécution de l'intégration.

Préparation de l'installation du Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Préparez l'installation en effectuant des Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud tâches de configuration.

Avant de commencer

Pour intégrer Vulnerability Response à Palo Alto Prisma Cloud, un groupe d'autorisations dans Prisma doit vous être affecté qui fournit un accès en lecture seule aux données de politique et d'alerte. Pour plus d'informations sur les groupes d'autorisations, consultez la page Rôles d'administrateur cloud Prisma .

Pour plus d'informations sur les rôles attribués aux différents groupes d'autorisations, consultez la page Autorisations d'administrateur dans le cloud Prisma .

De plus, des clés d'accès doivent être créées pour permettre la lecture des alertes. Pour plus d'informations sur la création de clés d'accès, consultez Créer et gérer des clés d'accès .

Pour installer et configurer le Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud, utilisez la liste de vérification suivante. Avant d'installer l'application, vérifiez que les éléments répertoriés sont terminés.

Liste de vérification de la préparation de l'intégration

Tâche	Description
☐	Vérifiez que vous disposez des ensembles d'informations suivants : • URL de base de l'API • ID de clé d'accès • Clé secrète • Nom d'utilisateur et mot de passe pour accéder à Prisma Cloud.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
	Ces informations d'identification sont utilisées pour se connecter à l'instance Prisma Cloud à partir de l'instance Now Platform® . L'ID de clé d'accès et la clé secrète doivent être générés à partir du portail Prisma Cloud après l'inscription.
☐	Si ce n'est pas déjà fait, installez l'application avant d'installer l'application Réponse aux vulnérabilitésIntégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud . Pour en savoir plus sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 15.2.0 ou Réponse aux vulnérabilités ultérieure.
☐	Si vous n'avez pas déjà l'application sur votre instance, obtenez les autorisations et téléchargez l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud sur votre Now Platform® instance. Consultez .
☐	Assurez-vous d'avoir installé les modules d'extension suivants pour une exécution fluide de l'intégration : • Réponse aux vulnérabilités • Conformité de la configuration • Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud Les modules d'extension suivants sont facultatifs mais peuvent être utiles : • Mise en service et gouvernance du cloud • Schémas de découverte et de mappage des services
☐	Estimez le nombre de résultats des tests que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre de résultats des tests que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance ou si vous avez besoin d'aide, contactez ServiceNow le support technique.
☐	Vérifiez que vous disposez d'un administrateur pour gérer les intégrations et corriger les résultats des tests : L'administrateur installe l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud . Si elle n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous êtes prêt à Installer et configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud.

Installer et configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Installez l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud pour utiliser les données importées à partir de Prisma Cloud. Utilisez ces données pour classer par ordre de priorité et corriger les erreurs de configuration sur vos actifs.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Définition du système** > **Modules d'extension**.
2. Dans la barre de recherche, recherchez `Vulnerability Response Integration with Palo Alto Prisma Cloud`.
3. Cliquez sur **Installer**.

   Toutes les dépendances qui seront installées sont affichées.
4. Accédez à la **Tout** > **Intégration dans le cloud Prisma** > **Administration** > **Configuration** > **Configuration du cloud Prisma**.
5. Renseignez les champs du formulaire.

Champ	Description
Instance d'intégration	Nom de la nouvelle instance d'intégration. Vous pouvez créer une instance ou cliquer sur l'icône de recherche pour sélectionner une instance existante.
URL D'API	URL à intégrer dans le cloud Prisma.
ID de clé d'accès	Clé unique pour authentifier la demande d'accès au cloud Prisma. **Remarque :** Vous devez générer la clé après vous être connecté au portail Prisma Cloud.
Clé secrète	Clé privée permettant d'authentifier la demande d'accès au cloud Prisma. **Remarque :** Vous devez générer la clé secrète après vous être connecté au portail Prisma Cloud.

6. Cliquez sur **Enregistrer et tester**.

Que faire ensuite

Une fois l'installation terminée, accédez à **Intégration dans le cloud Prisma** > **Configuration** pour poursuivre la configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Configurez l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud . Utilisez les données importées de Prisma Cloud pour hiérarchiser et corriger les erreurs de configuration sur vos actifs.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Intégration dans le cloud Prisma** > **Configuration**.
2. Renseignez les champs du formulaire.

Configuration du cloud Prisma

Champ	Description
Instance d'intégration	Nom de la nouvelle instance d'intégration. Vous pouvez créer une instance ou cliquer sur l'icône de recherche pour sélectionner une instance existante.
URL D'API	URL à intégrer dans le cloud Prisma.
ID de clé d'accès	Une clé unique pour authentifier la demande d'accès au cloud Prisma. Vous devez générer la clé après vous être connecté au portail Prisma Cloud.
Clé secrète	Clé privée permettant d'authentifier la demande d'accès au cloud Prisma. Vous devez générer la clé secrète après vous être connecté au portail Prisma Cloud.

3. Cliquez sur **Enregistrer et tester**.

Que faire ensuite

Une fois la configuration terminée, accédez à **Intégration dans le cloud Prisma** > **Intégrations** pour vérifier que l'exécution de l'intégration est réussie.

Vérifier l'état de l'exécution de l'importation Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Utilisez l'état de l'exécution de l'importation Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud pour vérifier la réussite de vos exécutions d'intégration et identifier d'éventuels problèmes.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 14.8.5 de Conformité de la configuration, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à la **Intégration dans le cloud Prisma** > **Intégrations**.
2. Cliquez sur **Intégration des politiques Prisma**.
3. Cliquez sur **Exécuter maintenant**.
   Lorsque cette intégration est exécutée, les tables suivantes sont renseignées dans cet ordre :
   a. sn_vulc_test.list (tests de configuration)
   b. sn_vulc_auth_src (source de référence)
   c. sn_vulc_citation (citations)
4. Sous l'onglet **Éléments** , affichez le nombre de nouveaux tests créés, mis à jour et ignorés en cliquant sur l'exécution de l'intégration de vulnérabilité.

   Remarque : Les politiques sont définies dans Prisma Cloud pour l'instance de cloud sélectionnée. L'instance est analysée en fonction des politiques définies.

5. Cliquez sur **Intégration des alertes Prisma**.
6. Cliquez sur **Exécuter maintenant**.
   Les tables suivantes sont renseignées en fonction de l'intégration :
   - Résultats des tests
   - Éléments détectés : si les éléments de configuration ne sont pas disponibles dans le système, ils sont créés. La classe est toujours Cloud Resource. Sur la page Élément détecté, trois nouveaux champs sont créés : **Type de ressource dans le cloud**, **Fournisseur de services dans le cloud** et **Catégorie d'actif**.

     Sous l'onglet **Éléments** , cliquez sur l'exécution de l'intégration de vulnérabilité pour afficher le nombre de nouveaux résultats de tests importés, mis à jour et ignorés. L'onglet **Éléments de configuration** est également renseigné en fonction du nombre de résultats des tests créés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de données

Les données de Prisma Cloud sont importées dans le Conformité de la configuration module de l'instance ServiceNow .

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Les données de Prisma Cloud sont importées avec un nom Conformité de la configuration différent, comme indiqué dans la table.

Mappage des données dans le cloud Prisma dans Configuration Compliance

Prisma Cloud	Configuration Compliance
Politique	Test
Alerte	Résultat de test
Norme de conformité	Source de référence
Sections	Contenu source d'autorité
Ressource	Élément de détection/Élément de configuration (CI)

Tests

Une stratégie dans Prisma Cloud est importée en tant que test dans .Conformité de la configuration Les politiques sont liées aux documents de référence et aux enregistrements de test, et elles peuvent être modifiées pour répondre aux besoins de votre organisation. Vous pouvez afficher les tests en accédant à **Configuration Compliance** > **Tests**.

Si **Vulnerability Response Integration with Palo Alto Prisma Cloud** est installé, la tâche *`Prisma Policy Integration`* d'intégration récupère les tests. Vous pouvez afficher cette tâche d'intégration en accédant à **Tout** > **Intégrations dans le cloud Prisma** > **Intégration de la politique Prisma**.

Résultats des tests

Une alerte dans Prisma Cloud est importée en tant que résultat de test dans Conformité de la configuration. Les alertes sont corrigées à l'aide de **tâches de rattrapage**. Vous pouvez afficher les résultats des tests en accédant à **Configuration Compliance** > **Résultats des tests**.

Les Conformité de la configuration résultats des tests sont importés dans le cadre d'une intégration tierce. Une fois visibles sur l'application, ils sont corrigés à l'aide Conformité de la configuration de tâches de rattrapage.

Si **Vulnerability Response Integration with Palo Alto Prisma Cloud** est installé, la tâche d'intégration **Prisma Alert Integration** récupère les résultats des tests. Vous pouvez afficher

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

cette tâche d'intégration en accédant à **Tout** > **Intégration dans le cloud Prisma** > **Intégrations** > **Intégration d'alerte Prisma**.

L'intégration d'alerte Prisma est une tâche d'intégration qui s'exécute quotidiennement et extrait les résultats des tests avec changement d'état après l'heure définie dans le champ **Heure de début** de l'onglet **Intégration**.

Remarque : Si vous exécutez manuellement la tâche d'intégration, **Prisma Alert Integration** , exécutez-la après avoir exécuté la tâche d'intégration, **Prisma Policy Integration**.

Lorsque **l'intégration d'alerte Prisma** a terminé l'importation des données, un événement est lancé pour déclencher les calculs de fin d'importation. Si l'alerte échoue continuellement au cours des derniers jours, l'intégration ne récupère pas les alertes, car il n'y a aucun changement d'état pour l'alerte. Ainsi, pour maintenir les données des résultats des tests à jour avec les alertes Prisma, une nouvelle tâche d'intégration, **Prisma Comprehensive alert Integration** , est ajoutée et extrait les alertes mises à jour au cours des sept derniers jours. Il s'exécute chaque semaine et extrait tous les résultats des tests qui ne sont pas réussis.

Sources d'autorité

Conformité de la configuration Utilise des sources et des citations de référence lors de la génération d'alertes de vulnérabilité pour les tests. Les sources faisant autorité renvoient généralement à des sections des normes industrielles publiées, telles que ISO 27001 et PCI DSS 3.2.1.

Ces enregistrements sources contiennent des références à des informations sur des problèmes connus de configuration logicielle et matérielle provenant d'experts dans le domaine de la sécurité informatique. Les références définissent les exigences en matière de politiques et de procédures de sécurité. Accédez à la **Configuration Compliance** > **Sources d'autorité** pour afficher les sources de référence.

Ressources

Si le Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud est installé, la tâche *`Prisma Alerts Integration`* planifiée capture les informations relatives à l'alerte dans le module ou la table Éléments détectés. Vous pouvez afficher cette tâche planifiée en accédant à **Intégration dans le cloud Prisma** > **Intégrations**.

L'intégration des alertes Prisma importe d'autres types d'informations, telles que les balises de ressource et les attributs du cloud, qui sont stockés dans des tables. Ces informations sont affichées dans le formulaire Éléments détectés.

- Balises d'hôte : une ressource peut avoir plusieurs balises. Les balises hôtes sont disponibles sous forme de paires de valeurs clés. Par exemple, le système d'exploitation est Windows 10 et la version Java est 1.8.
- Attributs dans le cloud pour les actifs : les attributs de cloud suivants sont disponibles :
  - Compte dans le cloud : fournit l'ID de compte à partir de l'intégration. Les informations sont renseignées à partir des comptes dans le cloud [sn_sec_cmn_cloud_account. LIST].
  - Région du cloud : indique l'emplacement où la ressource a été hébergée. Les informations sont renseignées à partir des régions du cloud [sn_sec_cmn_region. LIST].
  - Type de ressource dans le cloud : fournit des informations sur le type de ressource, par exemple s'il s'agit d'un ordinateur virtuel ou d'une instance de base de données, entre autres. Les informations sont renseignées à partir du type de ressource dans le cloud [sn_sec_cmn_cloud_resource_type. LIST].

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Fournisseur de services dans le cloud : fournit des informations sur le fournisseur de services dans le cloud, qu'il s'agisse d'Amazon Web Services (AWS), d'Oracle Cloud, entre autres. Les informations proviennent du fournisseur de services dans le cloud [sn_sec_cmn_cloud_service_provider. LIST].
- Groupes de comptes dans le cloud : fournit des informations sur les groupes de comptes. Les informations sont renseignées à partir de la table Groupes de comptes dans le cloud [sn_vul_prismacloud_account_group.list].

Remarque : L'attribut Groupes de comptes dans le cloud n'est disponible que pour Prisma.

Règles de recherche de CI

Les règles de recherche de CI du système de base sont disponibles pour l'ID de ressource, le nom et la catégorie S3. Pour plus d'informations sur les règles de recherche de CI, reportez-vous à Règles de recherche de CI pour Microsoft Defender for Cloud Integration pour Opérations de sécurité et Palo Alto Prisma Cloud.

Prisma Cloud REST Messages

Les messages REST Prisma sont utilisés pour passer des appels à l'interface de programmation d'application (API) Prisma afin d'extraire les données de conformité.

Les messages REST suivants sont fournis avec le système de base.

Intégrations dans le cloud Prisma

Toutes les intégrations Prisma Cloud utilisent le jeton Web JSON (JWT) pour l'authentification et l'autorisation.

Message REST de connexion Prisma

Point de terminaison	Description	Méthode	Corps	Lien vers la documentation de l'API
/connectez-vous	Obtient le jeton JWT pour une utilisation dans toutes les intégrations ultérieures.	*POST*	`{ "username": <<access key id >>, "password": <<secret access key>>}`	https://pan.dev/prisma-cloud/api/cspm/app-login/

Jeton d'actualisation Prisma Message REST

Point de terminaison	Description	Méthode	Corps	Lien vers la documentation de l'API
/auth_token/extend	Renouvelle automatiquement le jeton JWT à son expiration. La durée par défaut de l'expiration du jeton est de 60 minutes.	*GET*	N/A	https://pan.dev/prisma-cloud/api/cspm/extend-session/

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politique Prisma Message REST

Point de terminaison	Description	Méthode	Corps	Lien vers la documentation de l'API
/v2/ politique	Récupère toutes les données de police de Prisma.	*GET*	N/A	https://pan.dev/prisma-cloud/api/cspm/get-policies/

Message REST d'alerte Prisma

Point de terminaison	Description	Méthode	Corps	Lien vers la documentation de l'API
/v2/alerte	Récupère toutes les alertes de Prisma.	*POST*	{ "detailed": "false", "filters": [{ "name": "timeRange.type", "operator": "=", "value": "ALERT_STATUS_UPDATED" }], "sortBy": ["resource.id"], "pageToken": "", "offset": 0, "limit": 2000, "timeRange": { "type": "absolute", "value": { "startTime": <<Import since at integration level>>, "endTime": << Current integration run time>> } } }	https://pan.dev/prisma-cloud/api/cspm/post-alerts/

Pour l'intégration de l'alerte de compréhension Prisma, les filtres de l'auto-test de démarrage (POST) ci-dessus doivent être remplacés comme suit :

```
"filters": [
 {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "open"
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
                },
                {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "dismissed"
                },
                {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "snoozed"
                },
                {
                    "name": "alert.status",
                    "operator": "=",
                    "value": "pending_resolution"
                },
                {
                    "name": "timeRange.type",
                    "operator": "=",
                    "value": "ALERT_UPDATED"
                }

    ],
```

Qualys intégration avec Conformité de la configuration

L'application Qualys Policy Compliance collecte les données et les envoie automatiquement à l'application, qui analyse et corrèle Qualys les informations en continu. Il s'intègre facilement en tant qu'intégration Qualys pour Security Operations pour mapper les résultats de configuration aux CI et aux services d'entreprise afin de déterminer l'impact et la priorité des erreurs de configuration potentielles.

Si vous avez plusieurs déploiements de l'application Qualys Cloud Platform , vous pouvez ajouter une intégration pour chaque déploiement. Les actifs, identifiés par plusieurs déploiements tiers et leurs vulnérabilités, sont consolidés et rapprochés avec votre CMDB. Cette consolidation se produit même lorsque les processus d'analyse se chevauchent entre les différents déploiements. Les données provenant de chaque déploiement sont identifiées et disponibles dans une instance unique de Réponse aux vulnérabilités.

Remarque : Vous ne pouvez pas supprimer l'intégration de vulnérabilité d'origine, mais vous pouvez la désactiver. Les intégrations créées à partir de modèles inactifs sont désactivées par défaut.

Balises d'hôtes

Toutes les balises d'hôte sont importées dans le cadre de l'intégration de la liste d'hôtes Qualys . Les balises d'hôte sont principalement utilisées pour le filtrage dans les Réponse aux vulnérabilités règles d'affectation et de groupe de vulnérabilité. Ils sont affichés dans le formulaire Élément détecté.

Remarque : L'intégration Qualys de la liste d'hôtes doit être exécutée avant la création des règles Réponse aux vulnérabilités de tâche d'affectation ou de rattrapage afin que toutes les balises puissent être présentes dans les règles et avant que les éléments vulnérables ne soient importés et regroupés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le stockage des balises n'est pas sensible à la casse. Si une balise **San Diego** est créée, une balise **SAN DIEGO** ne peut pas être stockée dans la table de balises Host. « San Diego » et « SAN DIEGO » sont considérés comme étant la même balise d'hôte. La balise qui a été importée en premier gagne.
- L'utilisation de balises d'hôte en tant que clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises hôtes sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises hôtes sont contrôlées par la propriété système globale **sn_vul.import_host_tags**. Cette propriété est définie sur vrai par défaut. La désactivation des balises les désactive dans toutes les instances.

Les balises d'hôte (également appelées balises d'actif) sont utilisées pour organiser et suivre les actifs de votre organisation. Vous pouvez affecter des balises à vos ressources hôte. Ensuite, lors du lancement des analyses, vous pouvez sélectionner des balises associées aux hôtes que vous souhaitez analyser. Le module Balises d'hôte vous permet de télécharger des données de balises d'hôte vers Qualys votre instance de manière planifiée.

Intégration Qualys à l'application ServiceNow® Conformité de la configuration

Si le Qualys Vulnerability Integration est déjà installé sur votre système et que vos informations d'identification d'API sont différentes de celles que vous souhaitez utiliser pour Conformité de la configuration, accédez à l'Assistant de configuration (dans Réponse aux vulnérabilités) et affectez-les à chaque intégration **Qualys PC** .

Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Intégrations principales** et modifiez le champ **Informations d'identification de l'API Qualys** sous l'onglet **Détails REST Qualys** .

Configurer les paramètres PCRS

À partir de la version 12.6.3 de Intégration Qualys pour Opérations de sécurité, vous pouvez utiliser Qualys PCRS Policy Host Integration et Qualys PCRS Test Results Integration pour importer les résultats des tests avec de nouveaux ensembles d'API Qualys . Ces intégrations ont besoin d'une URL de passerelle pour extraire des informations à partir de Qualys.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Lorsque vous installez for Intégration Qualys pour Opérations de sécuritéRéponse aux vulnérabilités, vous pouvez configurer les **gateway_url** pour les nouvelles intégrations PCRS dans Conformité de la configuration. Pour plus d'informations sur la recherche de l'URL de passerelle pour votre URL d'API, consultez Identifier votre plateforme Qualys .

L'URL de la passerelle doit être ajoutée dans votre ServiceNow instance.

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Administration** > **Instances d'intégration**.

   Remarque : Assurez-vous que le périmètre dans lequel vous vous trouvez est Qualys for Security Operations.

2. Ouvrez l'instance utilisée par les intégrations PCRS.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans l'onglet Paramètres de l'instance d'intégration, ajoutez l'URL de passerelle pour **gateway_url** configuration.

> **Remarque :** L'intégration des résultats des tests Qualys PCRS dépend de l'intégration de l'hôte de politique Qualys PCRS. Ainsi, si vous antidatez les résultats des tests Qualys PCRS d'intégration, vous devrez peut-être les exécuter à nouveau dans le même ordre.

Composants installés avec Qualys Integration for Security Operations

Les rôles, travaux planifiés et tables suivants sont installés avec Qualys Integration for Security Operations.

> **Remarque :** La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Afficher les listes filtrées pour les composants installés avec une application

Filtrez la table Fichiers d'applications afin que seuls les rôles, les travaux planifiés et les tables installés avec une application s'affichent. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés sur l'instance et dans la table de métadonnées. Procédez comme suit pour afficher les listes filtrées à partir de la table Fichiers d'applications.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application. Par exemple : **Application** > **est** > **Réponse aux vulnérabilités**.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, sélectionnez **ET**, puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
sn_vul_qualys.read	Dispose d'un Qualys Vulnerability Integration accès en lecture aux enregistrements.	
sn_vul_qualys.utilisateur	Utilisateur pour Qualys Vulnerability Integration. Peut lire et écrire des enregistrements	sn_vul_qualys.read
sn_vul_qualys.admin	Administrateur pourQualys Vulnerability Integration. Par exemple, vous pouvez modifier les dates de début d'intégration et effectuer	• sn_vul_qualys.utilisateur • sn_vul.vulnerability_analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	certains paramètres de configuration avancés.	
sn_vul.configure_qualys_integration	Peut configurer l' Qualys Vulnerability Integration	sn_vul_qualys.admin

Travaux planifiés installés

Tâche planifiée	Description
Qualys Politiques PC	Récupère les politiques à partir du Qualysfichier . La sortie est stockée dans la table sn_vulc_policy. L'API utilisée dans cette intégration ne prend pas en charge la pagination, de sorte que toutes les politiques sont téléchargées sur une seule page.
Qualys Détail des politiques PC	Récupère les détails complets de la politique, tels que les technologies et les sections, par exemple.
Qualys Contrôles PC	Récupère les informations sur les contrôles de conformité pour différents ID de contrôle à partir de Qualys.
Qualys Résultats PC	Récupère les enregistrements de posture de conformité à partir de Qualys. Le résultat de cette intégration est Résultats des tests. Par défaut, les détails des paramètres sont transmis pour importer les informations d'hôte, les dates/heures de la dernière analyse, l'ID de contrôle et les informations de preuve.
Qualys Résultats PC complets	Récupère les enregistrements de posture de conformité en fonction de la dernière date d'évaluation Qualys pour les résultats des tests qui ne sont pas réussis. Cette tâche fonctionne une fois par semaine. La sortie de cette intégration est des résultats de tests. Par défaut, les détails des paramètres sont transmis pour importer les informations d'hôte, les dates/heures de la dernière analyse, l'ID de contrôle et les informations de preuve.
Qualys Intégration de l'hôte de la politique PCRS	Récupère les données de Qualys l'hôte et les traite dans votre instance. La sortie de cette intégration est l'ID d'hôtes de politique. Les Qualys données hôtes sont importées dans cette intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
	Remarque : • Cette tâche planifiée n'apparaît que lorsque Conformité de la configuration est installé. • Configurez les paramètres d'instance d'intégration gateway_url et pcrs_page_size avant d'exécuter cette intégration. Ces deux intégrations seront des OOB inactifs. Si vous activez l'une ou l'autre de ces intégrations, les intégrations PC Results seront désactivées. Ces deux intégrations sont ajoutées sur la base des nouvelles API de streaming de Qualys.
Qualys Intégration des résultats des tests PCRS	Récupère les résultats des tests pour chaque ID d'hôte. Cette intégration utilise le paramètre Heure de début dans l'onglet Détails de l'intégration. **Remarque :** • Cette tâche planifiée n'apparaît que lorsque Conformité de la configuration est installé. • Configurez les paramètres d'instance d'intégration gateway_url et pcrs_page_size avant d'exécuter cette intégration. • Si vous choisissez d'exécuter l'intégration manuellement, exécutez Qualys l'intégration des résultats des tests PCRS après Qualys l'intégration des politiques PC, Qualys des détails des politiques PC et Qualys de l'hôte de la politique PCRS.

Remarque : Les Qualys intégrations de l'hôte de politique PCRS et Qualys des résultats des tests PCRS sont inactives par défaut. Ces deux intégrations sont basées sur les nouvelles API de streaming de Qualys. Si vous activez l'une de ces intégrations, l'intégration de Résultats PC sera désactivée et vice versa.

Tables installées

Table	Description
Qualys Importation de résultat PC sn_vul_qualys_pc_result_import	Table étendant la ligne de jeu d'importation. La transformation des cartes de champs est ignorée et la pièce jointe de réponse

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	est traitée directement avec le script onComplete.
ID d'hôte de politique sn_vul_qualys_policy_host_id	Table stockant le mappage entre la politique et l'hôte pour lequel cette politique a été analysée. Cette table est utilisée dans la nouvelle Qualys intégration de PCRS. **Remarque :** Cette table n'apparaît que lorsque Conformité de la configuration est installé.
Qualys Importation de l'hôte de la politique PCRS sn_vul_qualys_pcrs_policy_host_import	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de la réponse est traitée directement avec le script onComplete. **Remarque :** Cette table s'affiche uniquement lorsque Conformité de la configuration est installé.
Qualys Importation de politique PC sn_vul_qualys_pc_policy_import	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de la réponse est traitée directement avec le script onComplete.

Mettre à jour les éléments de configuration avec l'identificateur de partition de réseau pour l'intégration Qualys

Créez des éléments de configuration (CI) uniques pour les actifs de votre environnement qui partagent des adresses IP. Identifiez les actifs distincts dans votre environnement et mettez automatiquement à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous donner plus de détails sur vos vulnérabilités.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Par défaut dans l'application, l'adresse Réponse aux vulnérabilités IP est l'un des moyens d'identifier vos actifs. Dans certains cas, les actifs peuvent partager des adresses IP, mais ils sont stockés en tant que CI unique dans votre CMDB.

Par exemple, comme le montrent les tables suivantes, plusieurs actifs (CI) de votre environnement peuvent partager des adresses IP, mais ont des ID de réseau et de référentiel uniques. Toutefois, par défaut, ces ressources sont généralement identifiées et stockées comme un seul CI `(CI 1)` lors de la recherche d'adresse IP.

Recherche d'adresses IP et création de CI par défaut

Source	Adresse IP	NETWORK_ID	Élément de configuration
Qualys Vulnerability Integration:	123.12.12.141	03712	CI 1

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche d'adresses IP et création de CI par défaut (suite)

Source	Adresse IP	NETWORK_ID	Élément de configuration
Intégrations d'actifs et de vulnérabilités fixes et ouvertes			
	123.12.12.141	03713	CI 1

Source	Adresse IP	REPOSITORY_ID	Élément de configuration
Qualys Vulnerability Integration: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Vous pouvez créer des CI individuels pour les actifs qui ont la même adresse IP afin de pouvoir les identifier en tant qu'actifs distincts. À partir d'une importation de données actualisée, vous pouvez mettre à jour vos CI existants avec une plus grande granularité incluant l'identificateur de partition de réseau [network_partition_identifier] en exécutant la tâche planifiée. *`Update existing discovered items with network partition identifier`*

Cette tâche planifiée est désactivée par défaut. Activez cette fonctionnalité pour les intégrations d'actifs et de vulnérabilités Qualys Vulnerability Integration fixes et ouvertes dans l'assistant de configuration afin d'afficher cet identificateur dans vos enregistrements.

Lorsqu'elle est activée, cette tâche planifiée ajoute l'identificateur de partition de réseau [network_partition_identifier] aux enregistrements de CI existants à partir des données importées. Les CI existants créés par l'IRE sont également mis à jour. La tâche planifiée crée également des CI qui incluent l'identificateur de partition de réseau à partir de la prochaine importation. Vous pouvez également lancer la tâche à la demande pour mettre à jour vos données existantes.

À partir des versions 14.0 et Réponse aux vulnérabilités 12.1 de l'intégration Qualys Vulnerability Integration de vulnérabilité, les modèles de classe CI CMDB (1.0.21.) sont pris en charge. Les modèles de classe ont l'identificateur de partition de réseau [network_partition_identifier] dans les règles d'identification Identification et rapprochement (IRE).

Option	Description
Exécutez les travaux planifiés sur demande.	Mettez à jour vos éléments détectés existants. Les CI de vos données existantes Qualys Vulnerability Integration sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau. Les éléments détectés, les éléments vulnérables et les enregistrements de détection sont tous mis à jour avec les nouveaux CI.

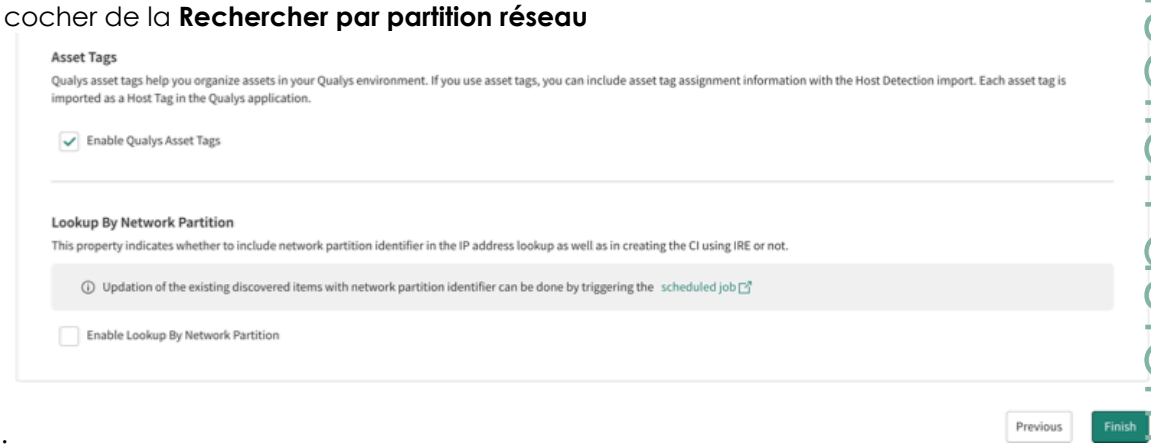
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Attendez les importations de données fraîches des intégrations avec les prochains travaux planifiés.	Créez des CI pour chaque nouvel actif à l'aide de l'identificateur de partition de réseau en commençant par la tâche planifiée suivante. Les enregistrements de CI, d'élément vulnérable et de détection sont tous mis à jour pour inclure la nouvelle granularité. De nouveaux CI sont créés lorsqu'aucune correspondance exacte n'est trouvée.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
2. Choisissez Qualys Vulnerability Integration.
3. **Modifiez** l'intégration requise.
4. Choisir **Configuration de la détection d'hôte**.
5. Choisir **Activer la recherche par partition de réseau** case à cocher de la **Rechercher par partition réseau**



section.

6. Cliquez sur **Terminer**.

Les identificateurs de partition de réseau NETWORK_ID et REPOSITORY _ID inclus dans la recherche d'adresses IP et la création de CI

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Éléments CI : actifs avec identificateur de partition de réseau
Qualys Vulnerability Integration: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Source	Adresse IP	REPOSITORY_ID	CI pour les actifs sans identificateur de partition de réseau	Éléments CI : actifs avec identificateur de partition de réseau
Qualys : Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Les règles de recherche d'identification CI d'adresse IP et d'adresse IP incomplète incluent automatiquement l'attribut d'identificateur de partition de réseau pour une importation de données à partir des intégrations d'actifs et de vulnérabilités fixes et ouvertes pour Qualys Vulnerability Integration.

Après avoir activé la tâche planifiée et enregistré les enregistrements, vous pouvez également mettre à jour vos éléments détectés existants avec des CI qui incluent l'identificateur de partition de réseau en lançant les travaux planifiés sur demande. Les CI de vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection sont automatiquement mis à jour.

Définir des paramètres de filtre supplémentaires pour Qualys les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec la Qualys Vulnerability Integration pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec les intégrations prises en charge Qualys .

Avant de commencer

Cas d'utilisation : en tant que gestionnaire ou analyste des vulnérabilités, vous souhaiterez peut-être filtrer les données de vos requêtes afin de ne pouvoir examiner que certains détails de vulnérabilité. Par exemple, supposons que vous souhaitiez afficher les vulnérabilités importées qui sont filtrées par des adresses IP ou des plages d'adresses IP spécifiques. Vous pouvez également importer uniquement les machines qui se trouvent dans votre champ d'application, par exemple, les seules machines de votre réseau d'entreprise qui ne sont pas des périphériques externes.

Pour vous aider à collecter ces données, vous pouvez ajouter Qualys des paramètres pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

Sans ajouter d'appels d'API ou de codage supplémentaires, cette fonctionnalité vous permet de personnaliser les informations de votre requête HTTP à l'aide Qualys des paramètres de votre Now Platformfichier . Vous modifiez ou ajoutez ces valeurs à votre enregistrement de méthode HTTP sous la méthode REST pour les intégrations prises en charge Qualys du Qualys Vulnerability Integration.

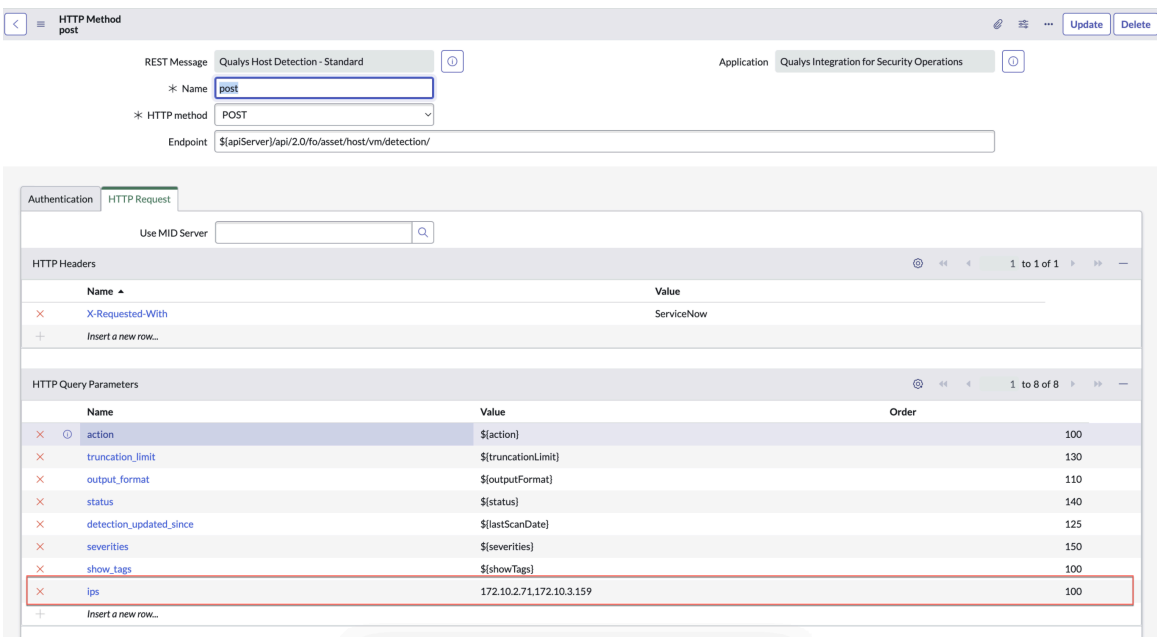
Rôle requis : sn_vul.vulnerability_admin

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Localisez les paramètres pris en charge par le Qualys produit sur le site développeur que vous souhaitez utiliser pour votre filtrage.
   Les paramètres et valeurs que vous entrez à partir Qualys du produit ne sont pris en charge qu'au niveau de l'instance d'intégration dans votre Now Platform. Toutes les Qualys intégrations prennent en charge le filtrage à l'aide de paramètres de requête.
2. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
3. Sur la Qualys page de liste Intégrations, cliquez sur l'enregistrement de l'intégration que vous souhaitez ouvrir.
4. Une fois l'onglet Qualys Détails REST sélectionné, localisez et cliquez sur l'icône d'informations (I) pour la méthode REST, puis sur **Ouvrir l'enregistrement** pour ouvrir l'enregistrement de la méthode HTTP.
5. Sélectionnez l'onglet **de demande HTTP** .
6. Dans les paramètres de requête HTTP du corps de la demande, ajoutez les valeurs que vous avez obtenues du site développeur Qualys .

   Dans l'image suivante, à titre d'exemple, le paramètre qui ingère uniquement certaines adresses `ips={value}` /plages IP a été ajouté. Dans ce cas, la **valeur** correspond à une ou plusieurs adresses IP/plages que vous spécifiez. Plusieurs entrées sont séparées par des virgules, `172.10.2.71, 172.10.3.159`, et une plage est spécifiée par un trait d'union, `10.10.10.1-10.10.10.100`. Consultez le site du Qualys développeur pour plus d'informations.



   Si vous souhaitez entrer plusieurs paramètres, reportez-vous à la documentation pour plus d'informations sur la Qualys séparation de chaque valeur.

   Remarque : Vous devez connaître vos exigences en matière d'API. Vous devrez peut-être ajouter ces propriétés API aux paramètres de requête ou au contenu du corps.

   Voici d'autres paramètres qui pourraient vous être utiles sur le Qualys site développeur :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- *ag_ids* - ID de listes de groupes d'actifs à récupérer. Ce paramètre garantit que seules les machines sous votre périmètre sont importées.
- *qids* - Ce paramètre limite les résultats à certaines vulnérabilités seulement (QID dans la table Third-Party Entry). Cela évite d'inonder votre système d'enregistrements d'informations.

7. Cliquez sur **Mettre à jour**.

Résolution des Qualys problèmes d'intégration de vulnérabilité

Certains problèmes fréquemment rencontrés, ainsi que des solutions de contournement, sont discutés.

Les pièces jointes n'apparaissent pas après l'importation

Si les pièces jointes n'apparaissent pas comme prévu pour les sources de données ou lors d'un incident de sécurité après des importations d'intégration tierce, vérifiez vos restrictions IP.

Les restrictions d'accès IP peuvent empêcher les pièces jointes d'être vues, sauf si vous êtes connecté à partir d'une adresse IP sécurisée. Étant donné qu'une nouvelle pièce jointe est ajoutée à chaque importation, cela peut entraîner des doublons que vous devez supprimer.

Par exemple, lorsque vous exécutez une intégration d'importation d'hôte tiers, si vous ne voyez aucune pièce jointe sur vos sources de données, vérifiez vos restrictions IP et ajoutez des utilisateurs à la liste de sécurité avant l'importation.

Modifier les cartes de transformation

Les cartes de transformation sont fournies avec des configurations de base et sont généralement suffisantes. Vous pouvez modifier les mappages de transformation en fonction des besoins de votre organisation.

Avant de commencer
Rôle requis : sn_vul_qualys.admin + import_admin

Procédure

1. Accédez à la **Tout** > **Ensembles de données à importations système** > **Administration** > **Cartes de transformation** pour afficher les messages REST.
2. Filtrez la liste résultante par application et limitez la liste à l'application **Qualys Vulnerability Integration** .
3. Modifiez les cartes de transformation selon les besoins du client.

   Pour plus d'informations sur les données fournies par l'API Qualys, consultez la documentation de l'API Qualys .

Vérifier la taille de propriété de la pièce jointe XML

Vérifie que la propriété de pièce jointe XML est suffisante pour les fichiers volumineux.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Importer/exporter**.
2. Faites défiler vers le bas jusqu'à **Propriétés d'importation** > **Format XML** en bas de la page.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Si nécessaire, remplacez la valeur par 250 et cliquez sur **Enregistrer**.

Information associée

Propriétés système disponibles

Limites de la récupération de données

Par défaut, il n'existe aucune restriction sur la façon dont les données sont récupérées à partir de Qualys. De nombreux enregistrements peuvent être liés à des vulnérabilités de faible gravité qu'un client n'est pas disposé à corriger à l'aide de son processus Vulnerability Response. La mise à jour des paramètres correspondants du message/de la méthode REST peut modifier ce comportement.

Le message/la méthode REST responsable de cette mise à jour est **Qualys Host Detection – Standard/post**. Pour mettre à jour les valeurs, ajoutez un nouveau paramètre de requête HTTP à la méthode post avec les valeurs suivantes :

- Nom : gravités
- Valeur : 3-5 (ou toute autre gravité appropriée souhaitée)

L'intégration de la base de connaissances Qualys échoue

Résolvez Qualys l'échec de l'intégration de la base de connaissances en réduisant la taille de la pièce jointe de la charge utile Qualys reçue jusqu'à la limite spécifiée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Assurez-vous que la taille de la pièce jointe de la charge utile se trouve dans la limite spécifiée.

a. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration**.

b. Sélectionnez l'onglet **Paramètres de l'instance d'intégration** .

c. Sélectionnez **max_delta_days** et remplacez la valeur par défaut par 3.

2. Si l'intégration échoue toujours, procédez comme suit :

a. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Intégrations principales**.

b. Sélectionnez **la base de connaissances Qualys**.

c. Sélectionnez l'onglet **Détails de l'intégration** .

d. Dans le champ **Heure de début** , sélectionnez la date actuelle pour ignorer l'exécution de l'exécution pour ce jour.

e. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Sélectionnez l'onglet **Paramètres de l'instance d'intégration** .

g. Sélectionnez **kb_backfill_full_import** et remplacez la valeur par défaut par vrai.

Résultats
L'exécution de l'intégration du remplissage de la base de connaissances Qualys met à jour toutes les entrées tierces (TPE) dans le système. Alors que l'intégration de la détection d'hôte Qualys crée une entrée d'espace réservé, l'intégration du remplissage de la base de connaissances Qualys la met à jour.

Qualys Graphique d'état de l'exécution de l'intégration

Le Qualys module État d'exécution de l'intégration est une vue graphique de l'état des exécutions d'intégration Qualys .

Pour afficher l'état des exécutions d'intégration, accédez à **Intégration de vulnérabilité Qualys** > **État de l'exécution de l'intégration**.

À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

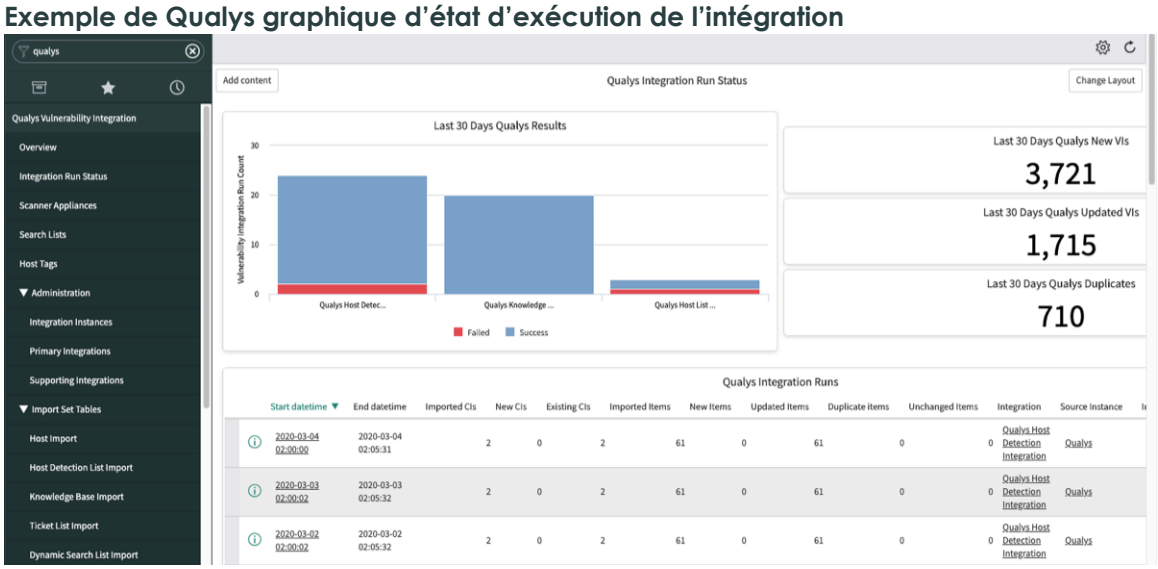
Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Dans le graphique, pointez sur n'importe quelle pièce (barre, secteur, point de données, etc.) pour afficher des données générales spécifiques à cette pièce. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

L'état Qualys de l'exécution de l'intégration affiche l'état de l'exécution de l'intégration de vulnérabilité au cours des 30 derniers jours. Le nombre de VI mis à jour Qualys[qualys] indique le nombre de détections uniques dans le même actif. Le VI est ensuite mis à jour avec la nouvelle détection.

Remarque : Le nombre d'exécutions de l'intégration de vulnérabilité n'est affiché que pour les intégrations qui sont définies sur l'état actif. Accédez à la **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales** et définissez l'état sur actif.

Exemple de Qualys graphique d'état d'exécution de l'intégration



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les valeurs de la colonne Éléments importés représentent le nombre total d'enregistrements créés à partir d'une exécution d'intégration.
- La colonne Nouveaux éléments affiche le nombre d'enregistrements créés à partir d'une exécution d'intégration.
- La colonne Éléments dupliqués n'est plus renseignée. Vous préférez peut-être supprimer cette colonne de l'affichage.
- La colonne Éléments mis à jour affiche le nombre de fois où les enregistrements sont mis à jour au cours d'une exécution d'intégration. Cette valeur n'est pas le nombre d'enregistrements uniques qui sont mis à jour. Si, par exemple, un enregistrement est mis à jour deux fois au cours de l'exécution de l'intégration, il est compté deux fois et affiché sous la forme `de 2` éléments mis à jour.
- La colonne Éléments inchangés affiche les enregistrements trouvés pendant l'exécution de l'intégration qui existent déjà dans la base de données mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

Remarque : L'intégration s'exécute avec zéro résultat pour les quatre valeurs suivantes : **Nouveaux CI**, **CI existants**, **Nouveaux éléments** et **Éléments mis à jour** sont exclus de la liste des **exécutions d'intégration Qualys** .

Qualys Rapports de graphiques d'état de l'exécution de l'intégration

Nom	Description
Résultats des 30 derniers jours Qualys	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Exécuter dans un visuel de barre.
Nouveaux VI au cours des 30 derniers jours Qualys	Nombre de nouveaux enregistrements importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour au cours des 30 derniers jours Qualys	Nombre d'enregistrements mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Doublons des 30 derniers jours Qualys	Nombre d'enregistrements en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Qualys Exécutions des intégrations	L'exécution de l'intégration enregistre dans une liste. **Remarque : V16.1 :** Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection de la *sn_vul_detection* table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, après la fin de l'exécution de l'intégration.
Mesures de performance d'ingestion d'élément vulnérables au cours	Mesures de performances quotidiennes pour les éléments vulnérables comparées au cours des 30 derniers jours.

Traduction automatique

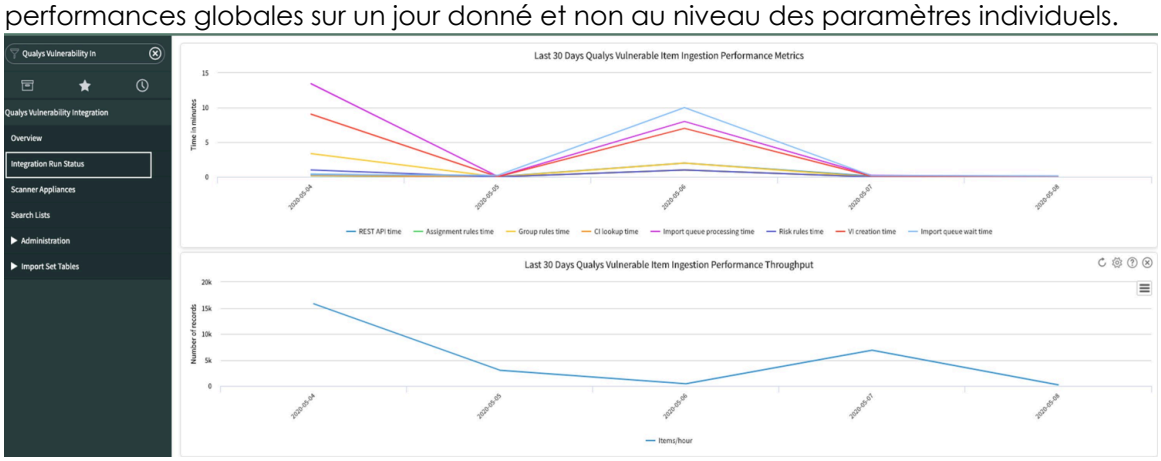
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Qualys Rapports de graphiques d'état de l'exécution de l'intégration (suite)

Nom	Description
des 30 derniers jours Qualys	
Rendement de performance d'ingestion d'élément vulnérable au cours des 30 derniers jours Qualys	Débit quotidien d'ingestion d'éléments vulnérables mesuré pour l'intégration de détection d'hôte Qualys au cours des 30 derniers jours.

Plusieurs facteurs peuvent avoir un impact sur les performances de l'exécution de l'intégration, comme la quantité de données et le temps nécessaire pour traiter ces données. Deux graphiques comparent les mesures de performance :

- Qualys Mesures de performances d'ingestion d'éléments vulnérables : comparez les mesures de performances quotidiennes pour les règles d'affectation, les règles de groupe, les règles de risque, le temps d'attente en file d'attente, le temps de traitement de la file d'attente et d'autres statistiques pour les éléments vulnérables au cours des 30 derniers jours, afin d'identifier la cause de tout écart de performance. La performance est calculée en fonction du temps pris pour chaque activité. Ces paramètres sont calculés et associés au niveau de l'exécution de l'intégration. Chaque paramètre est codé par couleur pour faciliter l'identification.
- Qualys Rendement de performance d'ingestion d'éléments vulnérables : comparez le débit quotidien d'ingestion d'éléments vulnérables pour l'intégration de la détection d'hôte Qualys . Le débit est mesuré en éléments par heure. Ce rapport affiche les performances globales sur un jour donné et non au niveau des paramètres individuels.



Messages REST Qualys

Les messages REST Qualys sont utilisés pour effectuer des appels à l'API Qualys afin d'extraire les données de conformité.

Les messages REST suivants sont fournis avec le système de base.

Politiques de PC Qualys Message REST

Le message REST Politiques PC Qualys récupère les données de politique de Qualys. Les changements apportés à l'enregistrement de méthode de message REST ont un impact sur la demande faite à Qualys pour récupérer les informations de politique.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politiques de PC Qualys Paramètres de message REST

Nom de paramètre	Valeur	Description
action	liste	Indique le type d'opération demandée. Paramètres requis.
Détails	Tout	Indique le niveau de détail affiché pour les politiques récupérées. Il est sûr de modifier selon vos besoins.

Contrôles de PC Qualys Message REST

Le message REST de Qualys PC Controls récupère les informations de contrôle de conformité pour différents ID de contrôle Qualys.

Contrôles de PC Qualys Paramètres de message REST

Nom de paramètre	Valeur	Description
action	liste	Indique le type d'opération demandée. Paramètres requis.
Détails	Tout	Indique le niveau de détail affiché pour les contrôles récupérés. Il est sûr de modifier selon vos besoins.

Détails des politiques de PC Qualys Message REST

Le message REST Détails des politiques PC Qualys récupère tous les détails de la politique, tels que les technologies et les sections.

Détails des politiques de PC Qualys Paramètres de message REST

Paramètre	Valeur	Description
action	liste	Indique le type d'opération demandé. Paramètres requis.
show_user_controls	Booléen	• Définissez la valeur sur 1 pour inclure les contrôles définis par l'utilisateur (CDU) dans la sortie XML. • Lorsqu'ils ne sont pas spécifiés, les CDU ne sont pas inclus. Il s'agit d'un paramètre facultatif. Il est sûr de modifier selon vos besoins.
show_appendix	Booléen	(Facultatif) Définissez la valeur 1 pour afficher la section d'annexe dans la sortie XML. Lorsqu'il n'est pas spécifié.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats PC Qualys Message REST

Le message REST Résultats de PC Qualys récupère les enregistrements de posture de conformité de Qualys.

Résultats de PC Qualys Paramètres de message REST

Champ source	Valeur	Description
action	liste	Indique le type d'opération demandée. Paramètres requis. Les changements ne sont pas recommandés.
show_extended_evidence	Booléen	• Définissez la valeur sur 1 pour afficher les informations de preuve étendues dans la sortie. • Défini sur 0 ou, lorsqu'il n'est pas spécifié, les informations de preuve étendues ne sont pas affichées dans la sortie. **Remarque :** • Vous ne pouvez pas spécifier `show_extended_evidence=1` dans la même requête que `hide_evidence=1`. Il en résulte une erreur. La preuve étendue fait partie des données de preuve et n'est affichée que lorsque les données de preuve sont affichées. • Ce paramètre n'est pas fourni avec le système de base.
cause_of_failure	Booléen	Si vous réussissez « 1 », Qualys renverra la cause de l'échec. Si vous transmettez « 0 », Qualys ne retourne pas ces attributs. **Remarque :** Ce paramètre n'est pas fourni avec le système de base.
policy_id		Affiche les enregistrements d'informations sur la posture de conformité pour une politique spécifiée. Un ID de politique valide est requis.
Détails	Tout	Indique le niveau de détail affiché pour les postures récupérées. Il est sûr de modifier selon vos besoins.
show_remediation_info		(Facultatif) Définissez la valeur 1 pour afficher les informations de rattrapage dans la sortie XML ou CSV. Par défaut, la sortie n'inclut pas les informations de rattrapage. Lorsqu'elles ne sont pas spécifiées, les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats de PC Qualys Paramètres de message REST (suite)

Champ source	Valeur	Description
		informations de rattrapage ne sont pas incluses dans la sortie.

Politique Qualys PCRS Intégration de l'hôte Message REST

L'intégration de l'hôte de la politique Qualys PCRS récupère les données de l'hôte de Qualys et les traite dans votre instance.

Politique Qualys PCRS Intégration de l'hôte Paramètres de message REST

Nom de paramètre	Valeur	Description
policyId	${lastRunDatetime}	ID de politiques pour l'évaluation de la conformité.

Intégration des résultats des tests Qualys PCRS

La table affiche les paramètres de demande qui sont envoyés.

Intégration des résultats des tests Qualys PCRS Paramètres de message REST

Nom de paramètre	Valeur	Description
evidenceRequired (en anglais)	${lastRunDatetime}	• La valeur par défaut est de 0, ce qui indique que les données de preuve ne seront pas récupérées pour la posture de l'hôte. • Définissez la valeur sur 1 pour récupérer les données de preuve. **Remarque :** Changer la valeur à 1 augmente le temps nécessaire pour extraire les données de posture.
compressionrequise		• La valeur par défaut est 1, ce qui indique que la sortie sera compressée. • Définissez la valeur sur 0 si vous ne souhaitez pas que les données soient compressées. **Remarque :** Le fait de ne pas compresser les données augmente le temps nécessaire à l'extraction des données de posture.

Présentation de l'intégration Tenable Vulnerability

L'application Intégration de Réponse aux vulnérabilités à Tenable développée par ServiceNow l'ingénierie pour Tenable Vulnerability Integration utilise des données importées des Tenable.io produits et Tenable.sc pour vous aider à hiérarchiser et à corriger les

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérabilités de vos actifs. L'application est disponible avec un abonnement distinct à partir du ServiceNow® Storefichier .

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

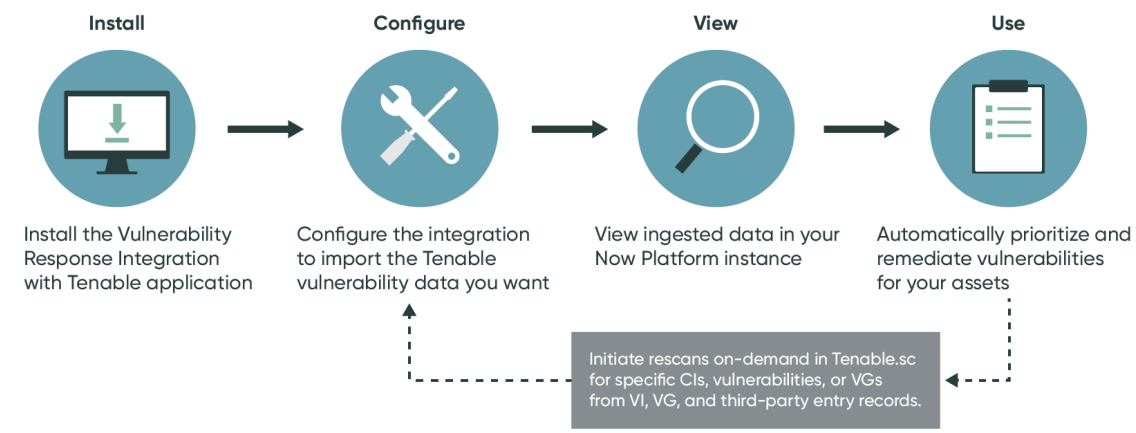
L'intégration de vulnérabilité Tenable utilise deux intégrations Tenable.io Tenable et Tenable.sc, pour importer des données d'analyseurs tiers concernant vos actifs et vos vulnérabilités. L'application Intégration de Réponse aux vulnérabilités à Tenable prend en charge le produit à partir de la Tenable.sc version 5.13.

- Tenable.io est une intégration d'entreprise basée sur le cloud.
- Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le produit et votre Tenable.scNow Platform instance se trouvent dans le même environnement.
- Si le produit et votre Tenable.scNow Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID.

L'application Intégration de Réponse aux vulnérabilités à Tenable est disponible sur le ServiceNow Store avec un abonnement séparé.

Pour obtenir des listes et des descriptions des intégrations dans , consultez Tenable Vulnerability IntegrationTenable.ioIntégrations avec les applications ET Réponse aux vulnérabilitésConformité de la configuration et Tenable.scIntégrations avec l'application Réponse aux vulnérabilités.

Intégration de vulnérabilité tenable



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions disponibles pour Xanadu

Version	Notes de publication
Intégration de Réponse aux vulnérabilités à Tenable v3.5, v3.6	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production

Termes et fonctionnalités clés des intégrations

Éléments vulnérables et vulnérabilités

Un élément vulnérable est créé dans votre instance lorsque :Now Platform

- Une vulnérabilité importée à partir d'un scanner tiers est mise en correspondance avec un actif existant (un élément de configuration dans votre CMDB). Le produit Tenable qualifie ces **correspondances de vulnérabilités**.
- Une vulnérabilité importée à partir d'un scanner tiers ne correspond pas à un actif existant dans votre CMDB. Dans ce cas, un CI sans correspondance est également créé ainsi qu'un élément vulnérable.

  Pour les CI sans correspondance, vous pouvez également utiliser le moteur Identification et réconciliation (IRE) pour créer des CI dans deux nouvelles classes lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte. Dans le cas contraire, des CI sans correspondance sont créés dans les classes de CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement.

Entrées et modules d'extension de vulnérabilité tiers

Les entrées de vulnérabilité tierces sont importées à partir d'analyseurs tiers et répertoriées dans la table Entrées de vulnérabilité tierces de votre Now Platform instance. Les entrées de vulnérabilité tierces de Tenable sont ingérées et mises en Réponse aux vulnérabilités correspondance avec les actifs existants répertoriés dans votre CMDBfichier . Tenable fait référence aux entrées de vulnérabilité tierces en tant que **modules d'extension.**

Élément de configuration (CI)

Les éléments de configuration sont les actifs existants répertoriés dans votre CMDBfichier .

Élément détecté

Les ressources ingérées à partir de l'importation d'actif Tenable sont mises en correspondance avec des éléments de configuration existants dans votre CMDB. Les actifs importés sont mis à jour.

Si aucune correspondance n'est trouvée, un CI est créé dans la classe CI sans correspondance du CMDB. Si le module d'extension Modèles de classe CI CMDB est activé, le moteur Identification et réconciliation (IRE) crée de nouveaux CI à l'aide de nouvelles classes. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et rapprochement. Si le CI d'origine, sans correspondance, est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

reclassé, les enregistrements d'éléments détectés sont mis à jour pour refléter l'état. Les éléments détectés vous donnent une visibilité sur la façon dont les actifs sont identifiés et mappés aux CI dans le CMDB.

Règles de recherche de CI

Lorsque les données sont importées à partir d'une intégration tierce, Vulnerability Response utilise automatiquement les données de l'hôte (actif) pour rechercher des correspondances dans la base de données de gestion des configurations (CMDB). Les règles de recherche de CI sont utilisées pour identifier les CI et les ajouter aux enregistrements de VI lorsque des VI sont créés pour vous aider à y remédier.

Nouvelle analyse et analyse de rattrapage

Vous pouvez lancer une commande de nouvelle analyse ciblée sur un élément de configuration, une tâche de rattrapage ou une entrée de tiers spécifique directement à partir des enregistrements d'élément vulnérable, de tâche de rattrapage et d'entrée de vulnérabilité tiers dans votre Now Platform instance. Tenable fait référence à cette nouvelle analyse en tant **qu'analyse de rattrapage**.

Fermer automatiquement les VI plus anciens

Le module Fermer automatiquement les éléments vulnérables périmés de votre Now Platform, vous pouvez nettoyer les éléments vulnérables (VI) anciens et périmés qui n'ont pas été trouvés récemment par vos intégrations tierces. Le déplacement de ces VI vers **Fermé** vous aide à réduire le nombre d'éléments vulnérables actifs et de tâches de rattrapage, ainsi qu'à rapprocher les actifs dans votre CMDB. Vous pouvez utiliser toutes les intégrations avec le Intégration de Réponse aux vulnérabilités à Tenable pour fermer automatiquement les VI périmés.

Instance

Ce terme fait référence à une occurrence distincte de votre Now Platform® application.

Intégration

Une intégration est une référence spécifique à un produit d'une intégration, comme l'intégration des actifs ou l'intégration Tenable.io du module d'extension Tenable.sc . Il s'agit des intégrations distinctes qui appartiennent à des produits Tenable spécifiques dans l'intégration de vulnérabilité Tenable de votre instance.

Instance d'intégration

Ce terme désigne les intégrations Tenable distinctes répertoriées par leur Tenable.io et Tenable.sc leurs produits.

Déploiement

Lorsqu'une intégration prend en charge plusieurs sources, une existence d'intégration unique et distincte est appelée déploiement de votre intégration. Le terme est utilisé pour désigner la ou les intégrations et les produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de diverses intégrations des produits et Tenable.ioTenable.sc dans votre environnement.

Les Tenable.io intégrations et Tenable.sc incluent également les fonctionnalités clés suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les résultats de l'évaluation de configuration, c'est-à-dire les résultats des tests, ainsi que les politiques, les tests de configuration (contrôles) et les citations avec des sources de référence peuvent être importés dans l'application Conformité de la configuration avec le Tenable.io produit. Consultez Tenable.ioIntégrations avec les applications ET Réponse aux vulnérabilitésConformité de la configuration et Explorer Conformité de la configuration pour en savoir plus sur le fonctionnement de cette intégration avec l'application Conformité de la configuration .
- À partir de la version 2.1 du , créez des éléments de Tenable Vulnerability Integrationconfiguration (CI) uniques qui incluent différents identificateurs de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. Identifiez les actifs distincts dans votre environnement et mettez à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous donner plus de détails sur vos vulnérabilités.
- Vous pouvez planifier le moment où vous souhaitez que les tâches s'exécutent pour toutes les Tenable.io intégrations and Tenable.sc . Vous pouvez également exécuter manuellement des travaux planifiés sur demande.
- Pour les importations d'actifs avec Tenable.io, vous pouvez activer les balises d'actif pour organiser et suivre les actifs répertoriés dans CMDB votre Tenable.io environnement.
- Les Tenable.io intégrations et Tenable.sc vous permettent de configurer des règles de recherche de CI pour définir la manière dont les données d'actifs de sources tierces sont utilisées pour identifier les éléments de configuration (CI) dans votre Now Platform CMDB.
- Les Tenable.io intégrations et Tenable.sc vous permettent de définir des filtres d'importation sur l'importation des vulnérabilités afin d'importer uniquement les vulnérabilités de Tenable que vous souhaitez. Pour Tenable.io, vous avez la possibilité d'importer des vulnérabilités **corrigées** de Tenable avec l'importation des vulnérabilités.
- Pour Tenable.sc, vous pouvez lancer de nouvelles analyses sur demande directement à partir d'enregistrements d'éléments vulnérables, de tâches de rattrapage et d'entrées tierces dans votre Now Platform instance. Si des VI sont passés à **l'état Fermé/Fixe** , mais ne sont pas encore mis à jour dans votre instance, vous pouvez vérifier que les vulnérabilités sur des éléments de configuration spécifiques ont été corrigées. Consultez Lancer une nouvelle analyse pour l'intégration Tenable.sc.

Les sections suivantes répertorient plus d'informations sur les intégrations Tenable.

Rôles Now Platform requis

Les tâches d'intégration nécessitent les rôles suivants dans votre Now Platform instance.

administrateur

L'administrateur système utilise l'Assistant de configuration pour installer l'application Intégration de Réponse aux vulnérabilités à Tenable . Si elle n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'Assistant de configuration.

sn_vul.vulnerability_admin

Une fois cette affectation effectuée, l'administrateur de vulnérabilité termine la configuration des intégrations Tenable dans l'assistant de configuration. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. L'administrateur de vulnérabilité configure toutes les applications et toutes les règles de réalité virtuelle pour les intégrations tierces installées.

sn_vul_tenable.configure_integration

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce rôle contient le rôle granulaire sn_vul_tenable.read_integration et les utilisateurs dotés de ce rôle peuvent configurer l'application Intégration de Réponse aux vulnérabilités à Tenable .

sn_vul_tenable.read_integration

Les utilisateurs disposant de ces rôles peuvent afficher (lire) mais pas modifier les enregistrements de l'application Intégration de Réponse aux vulnérabilités à Tenable .

Groupe Vulnerability Response

Par défaut, le groupe Vulnerability Response est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Vulnerability Response héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner.

Éléments vulnérables

Les éléments vulnérables sont regroupés en tâches de rattrapage en fonction des règles de tâche de rattrapage et affectés pour le rattrapage en fonction de vos règles d'affectation. Pour plus d'informations, consultez Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage et Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Règles de recherche d'éléments de configuration (CI)

Les règles de recherche de CI identifient les CI et déterminent quand les ajouter à un élément vulnérable. Pour plus d'informations sur le fonctionnement des règles de recherche de CI, reportez-vous à Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Remarque : Les règles, une fois supprimées, ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Les règles de recherche suivantes Tenable.io sont fournies avec le système de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- Nom d'hôte
- DNS
- IP

Les règles de recherche suivantes Tenable.sc sont fournies avec le système de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Remarque : Plusieurs valeurs pour ip_address, mac_address, FQDNS et network_interfaces sont utilisées pour un actif. Toutes les valeurs sont prises en compte dans les règles de recherche de CI pour la correspondance. Toutes les valeurs sont utilisées pour créer plusieurs cartes réseau à l'aide d'IRE.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur la configuration de la catégorisation des ressources cloud inégalées dans votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

Nouvelles propriétés pour ignorer les adresses IP

Dans Tenable.io, deux propriétés sont disponibles si vous souhaitez ignorer plusieurs adresses IP ou plusieurs adresses Mac dans le cadre de vos règles de recherche de CI :

ignoreIPAddress

Une liste d'adresses IP à ignorer pour la recherche de CI et la création de CI.

ignoreMacAddress

Une liste d'adresses MAC à ignorer pour la recherche de CI ou la création de CI.

Éléments détectés

Ce module répertorie les éléments de configuration détectés lors de l'importation à partir des intégrations d'éléments vulnérables Tenable et d'actifs Tenable.

Remarque : Le filtre par défaut de cette liste est défini sur `Sans correspondance`. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour plus d'informations sur le module Éléments détectés, reportez-vous à la section Éléments détectés.

Balises d'actifs

Les balises d'actif (également appelées balises d'hôte) sont utilisées pour organiser et suivre les actifs de votre organisation. Vous pouvez affecter des balises à vos ressources. Ensuite, lors du lancement des analyses, vous pouvez sélectionner des balises associées aux ressources que vous souhaitez analyser. Le module Balises d'actif vous permet de télécharger les données des balises d'actif Tenable.io depuis votre instance de manière planifiée. Les données d'actif Tenable.io qui incluent des balises d'actif sont extraites et transformées à l'aide des cartes de transformation d'intégration Tenable.io Asset Transform .

Toutes les balises d'actif sont importées dans le cadre de l'intégration d'actif Tenable.io . Les balises d'actifs sont généralement utilisées pour le filtrage dans Réponse aux vulnérabilités les règles d'affectation et les règles de tâche de rattrapage. Les balises sont affichées dans le formulaire Élément détecté.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Exécutez l'intégration Tenable.io des actifs avant de créer Réponse aux vulnérabilités des règles d'affectation ou des règles de tâche de rattrapage dans l'application afin que toutes les balises soient disponibles pour ces règles avant que Réponse aux vulnérabilités les éléments vulnérables ne soient importés et regroupés. Notez également les points suivants concernant les balises :

- Le stockage des balises n'est pas sensible à la casse. Par exemple, si vous créez une balise pour décrire les actifs de votre emplacement San Diego, et que vous créez la balise `San Diego` , vous ne pouvez pas également créer une balise `SAN DIEGO` et la stocker dans la table Balise d'actif. `San Diego` et `SAN DIEGO` sont considérés comme étant la même balise d'actif par le système. La balise importée en premier est celle qui est stockée et reconnue à l'avenir.
- L'utilisation de balises d'actifs en tant que clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises d'actif sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises d'actifs sont contrôlées par la propriété système globale sn_vul.import_asset_tags. Cette propriété est définie sur `vrai` par défaut. La désactivation des balises les désactive dans toutes les Now Platform® instances.

Filtres de récupération de données

Les paramètres de récupération de données vous aident à déterminer spécifiquement le type et le périmètre des données que vous souhaitez importer de l'application Tenable vers votre Now Platform® instance. Pour obtenir la liste des paramètres les plus couramment utilisés, reportez-vous à la section Paramètres de récupération de données pour Tenable Vulnerability Integration.

Évaluation de priorité de vulnérabilité (VPR)

L'évaluation de priorité de vulnérabilité (VPR) est un attribut du produit Tenable qui est importé et utilisé avec un nouveau calculateur de risque par défaut dans Réponse aux vulnérabilités. La règle de risque Tenable est installée avec l'application dans le Intégration de Réponse aux vulnérabilités à Tenable cadre du calculateur de risque par défaut dans les calculateurs de vulnérabilité à partir de Réponse aux vulnérabilités.

Cette règle de risque est désactivée par défaut.

En activant la règle du calculateur de risque Tenable, les valeurs VPR importées sont utilisées pour calculer le score de risque pour les éléments vulnérables. Distribution de pondération par défaut pour ce calculateur de risque : VPR = 70 %, Actif = 15 % et Criticité opérationnelle = 15 %. L'activation de cette règle du calculateur de risque Tenable peut avoir un impact sur vos performances d'ingestion de données. Pour en savoir plus sur Réponse aux vulnérabilités les calculateurs et la règle du calculateur de risque Tenable, reportez-vous à la section Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.

Installation et configuration

Après avoir téléchargé le Intégration de Réponse aux vulnérabilités à Tenable à partir du , l'installation ServiceNow® Storeet la configuration sont prises en charge par l'assistant de configuration dans Réponse aux vulnérabilités. Consultez Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration pour plus d'informations.

Tenable.ioIntégrations avec les applications ET Réponse aux vulnérabilitésConformité de la configuration

Les Tenable.io intégrations dans l'application Intégration de Réponse aux vulnérabilités à Tenable sont disponibles dans les Réponse aux vulnérabilités applications et Conformité de la configuration .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste des Tenable.io intégrations

Multisource est pris en charge pour toutes les Tenable.io intégrations .Tenable.sc Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'Assistant de configuration dans Réponse aux vulnérabilités. Vous pouvez également installer et configurer l'application à partir de l'Assistant Intégration de Réponse aux vulnérabilités à Tenable de configuration.

Tenable.io est une intégration d'entreprise basée sur le cloud. Consultez le tableau suivant pour connaître les noms et les descriptions des intégrations prises en charge pour le Tenable.io produit.

L'intégration Tenable.io des résultats de conformité et l'intégration du remplissage des Tenable.io résultats de conformité sont inactives par défaut.

Pour les activer :

1. Accédez à la **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.
2. Dans la liste Intégrations Tenable, cliquez sur un nom d'intégration pour ouvrir l'enregistrement et cochez la case **Actif** pour l'activer. Vous préférerez peut-être conserver les paramètres de calendrier dans leurs valeurs par défaut pour que ces intégrations démarrent.

Intégrations de Tenable.io

Intégration	Description
Tenable.io Intégration des actifs	• Récupère toutes les données d'actif, y compris les balises d'actif, du Tenable.io produit et les traite dans votre instance. • À partir de la version 3.0, si l'intégration des résultats de conformité est activée, vous pouvez importer des données d'évaluation Tenable.io de configuration sécurisée ainsi que des données d'actif importées. Ces données peuvent vous aider à identifier et à répondre aux vulnérabilités liées à la configuration sur vos actifs. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API Asset. • La sortie de cette intégration est les éléments détectés. • Les données sont importées par blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours. • À partir de la version 2.2, *Last Scan Time* les actifs présentant des vulnérabilités sont importés et mis à jour uniquement.
Tenable.io Intégration des résultats de conformité	• À partir de la version 3.0, les données d'évaluation de la configuration sécurisée importées à partir de l'intégration des résultats de conformité, ainsi que les données

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	importées à partir de l'intégration des actifs, peuvent vous aider à identifier les vulnérabilités liées à la configuration sur vos actifs et à y répondre. • Si cette option est activée, elle récupère les données d'évaluation de la configuration sécurisée de haut niveau et les traite dans votre Now Platform instance. Les données importées comprennent les résultats des tests, ainsi que les politiques, les tests de configuration (contrôles) et les citations avec des sources de référence. • Les données d'évaluation pour les actifs manquants ou les actifs sans ID d'actif ne sont pas importées. • Si un résultat de test est importé et que son actif correspondant ne peut pas être mis en correspondance dans votre instance, le résultat du test est ignoré et l'ID de l'actif manquant est stocké dans un enregistrement temporaire dans la table [sn_vul_tenable_missing_asset]. • La valeur totale des actifs **ignorés (manquants**) est répertoriée dans le champ CI ignorés de l'onglet **Configuration** de l'enregistrement d'exécution de l'intégration pour cette intégration.
Tenable.io Intégration du remplissage des résultats de conformité	• Lorsqu'elle est activée, cette intégration s'exécute automatiquement une fois l'intégration des actifs terminée avec succès dans le cadre d'une exécution d'intégration chaînée. Cette intégration associe les données d'évaluation de la configuration aux actifs manquants répertoriés dans la table [sn_vul_tenable_missing_asset]. • Importe jusqu'à 200 ID d'actifs pour tous les actifs manquants détectés ou présents dans l'instance une fois l'importation de l'intégration des actifs terminée avec succès. • Supprime les enregistrements temporaires de la table [sn_vul_tenable_missing_asset] lorsque les actifs peuvent être mis en correspondance avec les données d'évaluation de configuration correspondantes.
Tenable.io Intégration des informations d'identification de numérisation	• Cette intégration récupère les informations d'identification de numérisation configurées dans Tenable.io. • Coordonne les appels de message REST à l'API d'informations d'identification. • Le résultat de cette intégration est les informations d'identification d'analyse renseignées dans la table [sn_vul_tenable_scan_credential].

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	• Les informations d'identification importées sont utilisées pour accéder au scanner lorsque des demandes d'analyse sont lancées à partir du Now Platform. • Cette intégration est planifiée pour s'exécuter chaque semaine.
Tenable.io Intégration de modèle	Un enregistrement de modèle est envoyé lors de la Tenable.io nouvelle analyse. Cette intégration récupère les informations d'identification disponibles Tenable.io à utiliser pour les nouvelles analyses. Les informations d'identification sont spécifiques à l'instance et un enregistrement de modèle unique est importé et stocké temporairement en toute sécurité sur la table [sn_vul_tenable_io_template].
Tenable.io Intégration du module d'extension	• Récupère les données du module d'extension à partir du Tenable.io produit. Les données récupérées sont basées sur la date à laquelle les modules d'extension ont été mis à jour pour la dernière fois par une exécution d'intégration Tenable.io . • Cette importation garantit que les Tenable.io identificateurs (dix ID) sont à jour. • Coordonne les appels de message REST à l'API du module d'extension. • La sortie de cette intégration est constituée de vulnérabilités tierces.
Tenable.io Intégration des vulnérabilités corrigées	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.io produit et les traite dans votre instance. Les éléments vulnérables sont créés pour les enregistrements de détection qui sont dans les états **Ouvert** et **Rouvert** , car ces enregistrements nécessitent une correction. Les éléments vulnérables existants sont mis à jour par Vulnerability Response si les détections sont **corrigées**, mais les éléments vulnérables ne sont pas créés pour les détections **corrigées** par défaut, car Tenable considère les vulnérabilités **corrigéescomme atténuées**. • Lorsque le marqueur **Créer des temps de vulnérabilité pour les détections de vulnérabilité fixes** est activé dans l'Assistant de configuration, de nouveaux éléments vulnérables sont créés à l'état **Fixe** afin que vous ayez une visibilité sur les détections qui les ont créés. Étant donné que les VI sont créés pour les détections **fixes** qui n'existent pas déjà dans votre instance, cela peut avoir un impact négatif sur vos performances d'importation. Vous préférez peut-être laisser cette fonctionnalité désactivée afin que les détections **corrigées** ne fassent

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	que mettre à jour l'état des éléments vulnérables existants. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API de vulnérabilités. • La sortie de cette intégration est les éléments vulnérables (VI) **fermés/fixes** . Il crée également des actifs et des entrées tierces s'ils n'existent pas. • Les données sont importées par blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours. Cette exécution d'intégration est planifiée. Il s'agit d'une intégration enchaînée, ce qui signifie qu'une fois qu'une exécution est terminée avec succès, l'intégration des vulnérabilités ouvertes décrite ci-dessous est déclenchée. À partir de la version 3.3 de Tenable, vous pouvez afficher les informations suivantes pour les exécutions d'intégration de vulnérabilité : • **Blocs totaux :** Nombre total de blocs générés par Tenable • **Blocs disponibles :** Nombre de blocs disponibles au téléchargement pour ServiceNow
Tenable.io Intégration des vulnérabilités ouvertes	• Cette intégration est déclenchée une fois l'intégration Tenable.io des vulnérabilités corrigée terminée. • Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.io produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API de vulnérabilités. • La sortie de cette intégration est des éléments vulnérables (VI) **nouveaux/rouverts** . Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas. Tenable considère les vulnérabilités **actives comme cumulatives** (actuelle). • Les données sont importées par blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	À partir de la version 3.3 de Tenable, vous pouvez afficher les informations suivantes pour les exécutions d'intégration de vulnérabilité : • **Blocs totaux :** Nombre total de blocs générés par Tenable • **Blocs disponibles :** Nombre de blocs disponibles au téléchargement pour ServiceNow

Tenable.scIntégrations avec l'application Réponse aux vulnérabilités

Les Tenable.sc intégrations dans l'application Intégration de Réponse aux vulnérabilités à Tenable .

À partir de la Réponse aux vulnérabilités version 20.0, si un actif est analysé par un agent, la colonne L'agent existe affiche la valeur (vrai) dans la liste Éléments détectés qui indique qu'il s'agit d'une analyse authentique.

Liste des Tenable.sc intégrations

Multisource est pris en charge pour toutes les Tenable.io intégrations .Tenable.sc Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'Assistant de configuration dans Réponse aux vulnérabilités. Vous pouvez également installer et configurer l'application à partir de l'Assistant Intégration de Réponse aux vulnérabilités à Tenable de configuration.

- Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le produit et votre Tenable.scNow Platform instance se trouvent dans le même environnement.
- Si le produit et votre Tenable.scNow Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID.

Intégrations de Tenable.sc

Intégration	Description
Tenable.sc Intégration des actifs	Pour éviter de créer des éléments détectés en double avec des données d'actif importées, l'intégration des actifs du Tenable.sc produit est composée de deux intégrations. Intégration Tenable.sc des actifs ouverts Cette intégration importe les données de vulnérabilité de vos actifs que Tenable considère **comme cumulatifs** (actuels) ou **ouverts**. Les éléments vulnérables (VI) créés dans votre instance avec ces données d'actif importées sont considérés comme ouverts, c'est-à-dire à l'état **Ouvert** . Ces éléments vulnérables nécessitent une enquête et peuvent nécessiter une correction. L'intégration Tenable.sc des actifs immobilisés Cette intégration importe les données de vulnérabilité de vos actifs que Tenable

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	considère comme **atténuées** (n'étant plus vulnérables) ou **corrigées**. Les éléments vulnérables de ces actifs passent de l'état **Ouvert** à l'état **Fermé/Fixe** dans votre instance, car les résultats des analyses montrent qu'ils ne sont plus vulnérables. • Récupère toutes les données d'actif du Tenable.sc produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API Assets. • La sortie de cette intégration est les éléments détectés. • Le filtre de requête Tenable que vous sélectionnez dans l'assistant de configuration s'applique également à l'intégration Tenable.sc des actifs. Seuls les actifs présentant les vulnérabilités qui correspondent aux conditions du filtre de requête sont importés.
Tenable.sc Intégration du module d'extension	• Récupère les données du module d'extension à partir du Tenable.sc produit. Les données récupérées sont basées sur la date à laquelle les modules d'extension ont été mis à jour pour la dernière fois par une exécution d'intégration Tenable.sc . • Cette importation garantit que les Tenable.sc identificateurs (dix ID) sont à jour et que seules les vulnérabilités actives sont importées. • Coordonne les appels de message REST à l'API des modules d'extension. • La sortie de cette intégration est constituée de vulnérabilités tierces.
Tenable.sc Intégration des vulnérabilités corrigées	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.sc produit et les traite dans votre instance. Les éléments vulnérables sont créés pour les enregistrements de détection qui sont dans les états **Ouvert** et **Rouvert** , car ces enregistrements nécessitent une correction. Les éléments vulnérables existants sont mis à jour par Vulnerability Response si les détections sont **corrigées**, mais les éléments vulnérables ne sont pas créés pour les détections **corrigées** par défaut, car Tenable considère les vulnérabilités **corrigéescomme atténuées**. • Lorsque le marqueur **Créer des temps vulnérables pour les détections de vulnérabilité fixes** est activé dans l'Assistant de configuration, il crée de nouveaux VI à l'état

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	Fixe afin que vous ayez une visibilité sur les détections qui les ont créés. Étant donné que les VI sont créés pour les détections **fixes** qui n'existent pas déjà dans votre instance, cela peut avoir un impact négatif sur vos performances d'importation. Vous préférez peut-être laisser cette fonctionnalité désactivée afin que les détections **corrigées** ne fassent que mettre à jour l'état des éléments vulnérables existants. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API de vulnérabilités. • La sortie de cette intégration est les éléments vulnérables (VI) **fermés/fixes** . Il crée également des actifs et des entrées tierces s'ils n'existent pas. Cette exécution d'intégration est une exécution planifiée. Il s'agit d'une intégration chaînée, ce qui signifie qu'une fois qu'une exécution est terminée avec succès, l'intégration Tenable.sc des vulnérabilités ouvertes décrite ci-dessous est déclenchée. **Remarque :** Par défaut, les ID de famille 0 et 39 sont exclus de cette intégration.
Tenable.sc Intégration des vulnérabilités ouvertes	• Cette intégration est déclenchée une fois l'intégration Tenable.sc des vulnérabilités corrigée terminée. • Récupère les données de vulnérabilité en fonction des filtres de requête sélectionnés dans le Tenable.sc produit et les traite dans votre instance. • Crée des éléments vulnérables correspondants pour les vulnérabilités actives. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de message REST à l'API de vulnérabilités. • Le résultat de cette intégration est **Mettre à jour/Créer de nouveaux** éléments vulnérables (VI) s'ils n'existent pas déjà. Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas. **Remarque :** Par défaut, les ID de famille 0 et 39 sont exclus de cette intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
Tenable.sc Intégration des informations d'identification de numérisation	• Cette intégration récupère les informations d'identification de numérisation configurées dans Tenable.sc. • Coordonne les appels de message REST à l'API d'informations d'identification. • Le résultat de cette intégration est les informations d'identification d'analyse renseignées dans la table [sn_vul_tenable_scan_credential]. • Les informations d'identification importées sont utilisées pour accéder au scanner lorsque des demandes d'analyse sont lancées à partir du Now Platform. • Cette intégration est planifiée pour s'exécuter chaque semaine.
Tenable.sc Intégration des vulnérabilités de remplissage	• Cette intégration de remplissage importe toutes les vulnérabilités ouvertes et corrigées qui auraient pu être manquées lors d'une importation. • Cette intégration importe les vulnérabilités ouvertes et corrigées des sept derniers jours pour mettre à jour vos détections et éléments vulnérables. • Cette intégration peut avoir un impact sur vos performances. • Cette intégration est désactivée par défaut. • Pour mettre à jour vos données de vulnérabilité et éviter d'éventuels problèmes de performances, vous préférez peut-être planifier l'exécution des intégrations des vulnérabilités corrigées Tenable.sc et des vulnérabilités ouvertes lorsqu'aucune autre analyse n'est en cours d'exécution. • Le résultat de cette intégration est : ◦ Éléments vulnérables (VI) **fermés/fixes**. Il crée également des actifs et des entrées tierces s'ils n'existent pas. ◦ **pour mettre à jour/créer de nouveaux** éléments vulnérables (VI) s'ils n'existent pas déjà. Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas.

Authentification utilisateur et Tenable.sc

L'authentification utilisateur est prise en charge par votre instance et la Now Platform® version 5.13 du Tenable.sc produit. L'authentification de l'utilisateur est requise si vous utilisez la version 5.12 ou antérieure du Tenable.sc produit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous sélectionnez l'authentification utilisateur pour les intégrations, les jetons peuvent expirer et être remplacés lors de l'exécution de l'intégration Tenable.sc . Dans la colonne Notes de l'enregistrement d'exécution de l'intégration de vulnérabilité (VIN), le message suivant s'affiche pour un processus à l'expiration d'un jeton, `Erreur : échec de la validation du jeton`. Aucune action n'est requise si ce message s'affiche. Les jetons expirés sont automatiquement actualisés en arrière-plan et le message n'indique pas une pause ou une erreur dans le processus d'intégration.

Préparation de l'intégration Tenable Vulnerability

Préparez l'intégration Tenable ServiceNow® Vulnerability en effectuant les tâches de configuration suivantes.

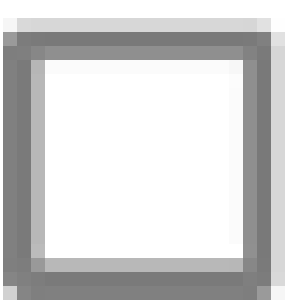
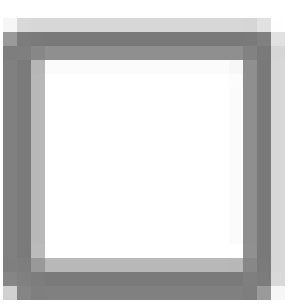
Avant de commencer

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Pour une installation et une configuration fluides de l'application Intégration de Réponse aux vulnérabilités à Tenable , il est préférable d'imprimer la liste de vérification suivante et de vérifier que les éléments répertoriés sont terminés avant d'installer l'application et d'importer les données de vulnérabilité dans votre Now Platform® instance.

Remarque : Si vous avez importé des données avec l'intégration créée par Tenable et que vous souhaitez commencer à utiliser Vulnerability ServiceNow® Response Integration avec Tenable, consultez le

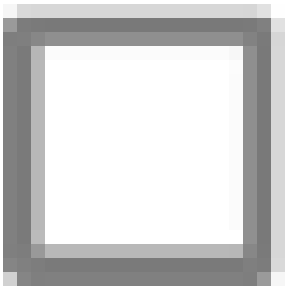
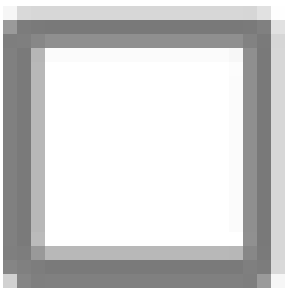
Pour obtenir des informations actuelles sur le nettoyage et la migration des données de l'intégration créée par Tenable vers l'intégration créée par ServiceNow, consultez l'article Directives pour migrer de l'intégration Tenable Vulnerability Response vers l'intégration ServiceNow Vulnerability Response avec Tenable [KB0960667].

Rôle requis : admin pour télécharger et installer l'application.

Tâche	Description
	(Facultatif) Si elle n'est pas déjà installée et activée, il peut être préférable d'installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour en savoir plus sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 12.1 ou Réponse aux vulnérabilités ultérieure.
	Si vous ne l'avez pas déjà sur votre instance, obtenez les autorisations et téléchargez l'application Intégration de Réponse aux vulnérabilités à Tenable sur votre Now Platform® instance. L'application Intégration de Réponse aux vulnérabilités à Tenable prend en charge le produit à partir de la Tenable.sc version 5.13. Consultez .

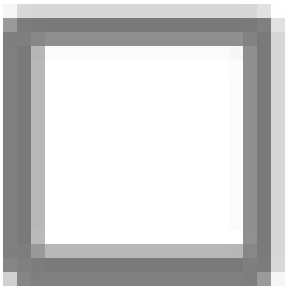
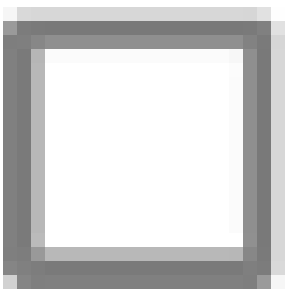
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

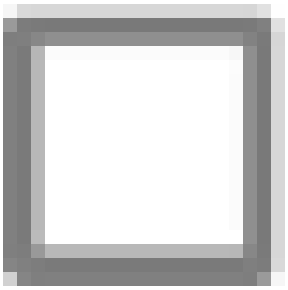
Tâche	Description
	Estimez le nombre d'éléments vulnérables que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, ou si vous avez besoin d'aide, contactez ServiceNow® le support technique.
	Vérifiez que vous disposez de groupes ou d'utilisateurs pour gérer les intégrations et corriger les éléments vulnérables. administrateur L'administrateur système utilise l'Assistant de configuration pour installer l'application Intégration de Réponse aux vulnérabilités à Tenable . Si elle n'est pas affectée, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'Assistant de configuration. sn_vul.vulnerability_admin Une fois cette affectation effectuée, l'administrateur des vulnérabilités termine la configuration des intégrations Tenable. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Configure toutes les applications et les règles de VR et configure les intégrations tierces. sn_vul_tenable.configure_integration Peut configurer l'intégration de vulnérabilité Tenable. Ce rôle contient le rôle granulaire sn_vul_tenable.read_integration. sn_vul_tenable.read_integration Peut afficher (lire) les enregistrements de l'intégration de vulnérabilité Tenable. Groupe Vulnerability Response Par défaut, le groupe Vulnerability Response est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Vulnerability Response héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner. L'administrateur système effectue l'affectation initiale des rôles aux utilisateurs et aux groupes dans l'Assistant de configuration pour l'intégration. Par défaut, le groupe Vulnerability Response est disponible. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance avant d'utiliser l'Assistant de configuration. Reportez-vous à la section Créer un groupe d'utilisateurs .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Des rôles granulaires et de profil sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.
	Pour améliorer les performances de votre première importation, vous pouvez désactiver certaines fonctionnalités, règles ou tâches dans votre instance. • Désactivez les calculateurs de vulnérabilité si vous ne les utilisez pas. Ces calculateurs, ainsi que ceux que vous avez définis, s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est créé ou mis à jour. Reportez-vous à la section Désactiver les calculateurs de vulnérabilité. • Lors de l'importation initiale des enregistrements, certaines règles métier liées aux notifications peuvent entraîner la génération de nombreuses notifications, ce qui a un impact sur les performances. Avant votre importation initiale, vous préférerez peut-être désactiver les règles métier liées aux notifications, comme décrit dans .Importer les modifications pour l'intégration de vulnérabilité Tenable
	Vérifiez que vous avez activé toutes les fonctionnalités, règles, modules d'extension de dépendance ou tâches dans votre instance requises pour l'intégration. • Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le produit et votre Intégration de Réponse aux vulnérabilités à TenableNow Platform instance se trouvent dans le même environnement. Si le produit et votre Tenable.scNow Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID. Pour plus d'informations sur les MID Servers dans votre instance, consultez Serveur MID . • Vérifiez que le module d'extension Centre d'intégration est installé et activé. Ce module d'extension permet aux composants du système de base d'appeler des systèmes externes à l'aide d'API d'intégration et active les étapes de protocole telles que REST. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tout** et localisez le module d'extension. S'il n'est pas installé dans votre instance, installez-le et activez-le.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Obtenez les informations d'identification Tenable. Vérifiez que vous disposez de tous les noms de compte, mots de passe et autres informations de service requis par vos produits Tenable afin d'y avoir accès. Tenable.io nécessite l'accès Administrateur avec un attribut d'autorisation supérieur ou égal à 64. Tenable.sc nécessite l'accès Analyste ou Gestionnaire de sécurité. **Remarque :** À partir de la version 3.8 de Intégration de Réponse aux vulnérabilités à Tenable, l'accès Tenable.io ne nécessite plus de privilèges d'administrateur. Un utilisateur de base avec un attribut d'autorisation égal à 16 peut également accéder au produit.

Vous êtes prêt à Installer l'application à l'aide de l'Assistant Intégration de Réponse aux vulnérabilités à Tenable de configuration.

Installer l'application à l'aide de l'Assistant Intégration de Réponse aux vulnérabilités à Tenable de configuration

Avant d'exécuter Tenable ServiceNow® Vulnerability Integration, vous devez télécharger l'application Intégration de Réponse aux vulnérabilités à Tenable à partir de et ServiceNow Store l'installer et la configurer à l'aide de l'assistant de configuration de l'application Réponse aux vulnérabilités .

Avant de commencer

Avant d'installer l'application Tenable, vérifiez que vous avez rempli tous les éléments de la liste de vérification dans Préparation de l'intégration Tenable Vulnerability.

Remarque : Ce processus s'applique uniquement aux applications téléchargées sur les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à la section .

Rôles requis : admin pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application Tenable dans l'Assistant de configuration. Administrateur de vulnérabilité (sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) pour configurer l'application dans l'Assistant de configuration après son installation.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation de l'application d'intégration**.

   Après quelques instants, les applications disponibles pour installation sur votre instance s'affichent.

2. Localisez la vignette **Tenable (Tenable Platform)** et cliquez sur **Installer**.

   Cette action installe l'application Intégration de Réponse aux vulnérabilités à Tenable que vous avez téléchargée à ServiceNow Storepartir du .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Suivez les instructions fournies dans l'assistant de configuration pour poursuivre l'installation.
4. Pour en savoir plus sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'Assistant de configuration.

Que faire ensuite

Une fois l'installation terminée dans l'Assistant de configuration, accédez à **Configuration d'intégration>Intégrations de scanners dans l'Assistant** de configuration pour poursuivre la configuration. Si vous souhaitez plus d'informations pour compléter les invites fournies dans l'Assistant de configuration, reportez-vous à la section Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration.

Paramètres de récupération de données pour Tenable Vulnerability Integration

Les paramètres de récupération de données suivants vous aident à déterminer spécifiquement le type et le périmètre des données que vous souhaitez importer de Tenable ServiceNow® Vulnerability Integration vers votre Now Platform® instance.

Les paramètres décrits dans les sections suivantes vous aident à contrôler les données que vous souhaitez importer. En outre, vous pouvez définir les valeurs de ces filtres dans les instances d'intégration. Pour afficher les instances d'intégration, accédez à **Intégration de vulnérabilité tenable** > **Instances d'intégration** et cliquez sur votre intégration, Tenable.io ou Tenable.scsur .

Sur la page Instance d'intégration qui s'affiche, cliquez sur Paramètres de l'instance d'intégration pour afficher une liste des paramètres ou sur les onglets Intégrations de vulnérabilité pour un calendrier, Détails REST, Détails de l'intégration, Sources de données et Informations sur l'exécution de l'intégration.

Paramètres et filtres courants de gravité et de récupération pour Tenable.io et Tenable.sc dans votre Now Platform instance

Les paramètres suivants sont disponibles pour les Tenable.io intégrations et Tenable.sc dans votre Now Platform instance. Ces paramètres de configuration, ainsi que d'autres, sont affichés sur la page Instance d'intégration de votre Now Platform instance. Vous préférerez peut-être laisser ces paramètres dans leurs valeurs par défaut pour les premières exécutions d'intégration.

Tenable.io

insert_fixed

Si vous activez le marqueur **insert_fixed** dans l'assistant de configuration pour l'intégration d'importation des vulnérabilités, de nouveaux VI sont créés pour les détections à l'état **Fixe** qui n'existent pas déjà dans votre instance.

severity_critical

Ce filtre est activé par défaut (vrai) pour recevoir les vulnérabilités de gravité critique des intégrations de vulnérabilités ouvertes et Tenable.io des Tenable.io vulnérabilités corrigées.

severity_high

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de gravité élevée à partir des intégrations des vulnérabilités ouvertes et Tenable.io des Tenable.io vulnérabilités corrigées.

severity_medium

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce filtre est désactivé par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité moyenne à partir des intégrations de vulnérabilités ouvertes et Tenable.io de Tenable.io vulnérabilités corrigées.

severity_info

Ce filtre est désactivé par défaut (faux). Activez ce filtre pour recevoir les vulnérabilités de gravité au niveau des informations des intégrations de vulnérabilités ouvertes et Tenable.io des Tenable.io vulnérabilités corrigées.

severity_low

Ce filtre est désactivé par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité de faible niveau à partir des intégrations de vulnérabilités ouvertes et Tenable.io de Tenable.io vulnérabilités corrigées.

taille

Ce paramètre définit le nombre d'enregistrements de module d'extension à inclure dans l'ensemble de résultats à partir de l'intégration des modules d'extension Tenable.io . Doit être au format int32. La valeur par défaut est 1 000. La taille maximale est de 10 000 personnes.

num_assets

Le nombre maximal de vulnérabilités par bloc exporté à partir des intégrations Tenable.io des vulnérabilités corrigées et Tenable.io des vulnérabilités ouvertes. La valeur par défaut est 50.

chunk_size

Spécifie le nombre d'actifs par bloc exporté par l'intégration Tenable.io des actifs. La valeur par défaut est 1 000.

Tenable.sc

async_request

Ce paramètre est désactivé par défaut (faux). Activez ou désactivez ce paramètre pour effectuer des appels d'API asynchrones ou synchrones avec Tenable.sc , respectivement. Pour les appels synchrones, s'il y a un délai d'attente à 30 secondes, contactez l'assistance du produit Tenable pour régler le boîtier. Ce paramètre, une fois activé, est applicable pour toutes les intégrations de Tenable.sc. Pour les clients existants utilisant des appels asynchrones, un script correctif est disponible, qui ajoute un nouveau paramètre async_request aux instances d'intégration existantes Tenable.sc . Pour afficher les scripts correctifs, accédez à **Définition du système** > **Scripts correctifs**.

insert_fixed

Si vous activez le marqueur **insert_fixed** dans l'assistant de configuration pour l'intégration d'importation des vulnérabilités, de nouveaux VI sont créés pour les détections à l'état **Fixe** qui n'existent pas déjà dans votre instance.

décalage

Spécifie le nombre d'actifs, de modules d'extension et de vulnérabilités importés en une seule exécution d'intégration.

Filtres de requête

Les filtres de requête sont configurés à partir de la console Tenable. Ces filtres de requête ont des ID qui peuvent être sélectionnés à partir de l'Assistant de configuration ou de la page Instances d'intégration de votre Now Platform instance. Ces filtres sont appliqués lors de la récupération des données à partir des Tenable.sc intégrations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Messages REST pour l'intégration Tenable Vulnerability

Les ServiceNow® messages REST de l'intégration de vulnérabilité de Tenable sont utilisés pour effectuer des appels à l'API de Tenable.

Tenable.io Message REST Actifs

Le Tenable.io message REST Actifs récupère les informations sur les actifs pour l'intégration Tenable.io des actifs. Les modifications apportées à l'enregistrement de méthode de message REST ont un impact sur les demandes effectuées pour Tenable.io récupérer les informations sur les actifs. La tâche d'exportation des actifs est soumise avec les filtres suivants :

- « is_deleted » : faux
- « is_licensed » : vrai

Tenable.io Modules d'extension Message REST

Le Tenable.io message REST Modules d'extension récupère les informations du module d'extension pour l'intégration du module d'extension Tenable.io . Les changements apportés à l'enregistrement de méthode de message REST impactent les demandes effectuées pour récupérer des informations sur les modules d'extension Tenable.io .

Tenable.io Vulnérabilités Message REST

Le Tenable.io message REST Vulnérabilités récupère les informations sur la vulnérabilité pour les vulnérabilités ouvertes et fermées à partir de l'intégration Tenable.io de vulnérabilité. Les changements apportés à l'enregistrement de méthode de message REST ont un impact sur les demandes effectuées pour Tenable.io récupérer des informations sur les vulnérabilités.

Requêtes Tenable.sc Message REST

Le message REST Requêtes Tenable.sc récupère les informations du filtre de requête pour l'intégration des actifs Tenable.sc et des vulnérabilités Tenable.sc où le filtre de requête est configuré.

Tenable.sc Modules d'extension Message REST

Le Tenable.sc message REST du module d'extension récupère les informations du module d'extension pour l'intégration des modules d'extension Tenable.sc . Les modifications apportées au message REST Obtenir l'enregistrement de méthode des modules d'extension ont un impact sur les demandes effectuées pour récupérer les informations sur les modules d'extension Tenable.sc .

Nom de paramètre	Valeur	Description
type	Actif	Indique la source à partir de laquelle Tenable extrait les données. Utilisé par code. Les changements ne sont pas recommandés.
champs	id, description, cvssVector,cvssV3Vector, cvssV3TemporalVector, synopsis, cvssVector, baseScore,temporalScore,	Indique la liste des champs importés de Tenable.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
	cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, family, riskFactor, cpe, seeAlso, solution, exploitAvailable, exploitFrameworks, type, copyright, version, sourceFile, dependencies, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	

Tenable.sc Vulnérabilités Message REST

Le Tenable.sc message REST de vulnérabilités récupère les informations de vulnérabilité à partir de l'intégration Tenable.sc . Les modifications apportées au message REST Extraire les vulnérabilités ou la méthode Extraire les vulnérabilités corrigées ou, à partir des versions 14.0 Réponse aux vulnérabilités et v2.2 de Tenable Vulnerability Integration, l'extraction de l'enregistrement des vulnérabilités de remplissage ont un impact sur les demandes faites Tenable.sc pour récupérer les informations sur les vulnérabilités.

Tenable.sc Informations d'identification de numérisation Message REST

Tenable.sc Message REST de la politique

Le Tenable.sc message REST POST de politique ajoute une politique pour les modules d'extension demandés. La politique générée sera utilisée dans Tenable.sc les demandes d'analyse.

Tenable.sc Analyser le message REST

Le message POST REST de l'analyse Tenable.sc ajoute une analyse qui dépend de l'accès et de l'autorisation définis dans le corps de la demande du message REST. Il utilise la politique, l'ID de module d'extension et la ou les adresses IP dans le corps de la demande d'analyse.

Tenable.sc Résultat de l'analyse Message REST

Le Tenable.sc message REST Résultat de l'analyse GET fournit les détails de l'analyse générée à l'aide du message REST d'analyse. Il utilise scanResultId dans la réponse des messages REST de l'analyse et récupère les détails de l'analyse pour l'analyse déclenchée.

Tenable.sc Informations d'identification de numérisation

Le Tenable.sc message REST des informations d'identification d'analyse récupère les informations d'identification à partir de Tenable.sc. Les changements apportés à l'enregistrement de méthode « Importation » du message REST ont un impact sur les demandes effectuées Tenable.sc pour récupérer les informations d'identification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
champs	id,nom,description,type	Indique la liste des champs importés à partir de Tenable.sc
filtre	utilisable	Indique que l'intégration extrait uniquement les informations d'identification utilisables de Tenable.sc Il n'est pas recommandé de modifier l'un ou l'autre des paramètres.

Transformation des données pour l'intégration Tenable Vulnerability

Une fois que vous avez identifié les données à importer, celles-ci sont récupérées à partir du produit Tenable et traitées via un ensemble de sources de données et de transformations dans votre instance.

Lors de l'installation, les cartes de gravité normalisées sont installées dans le module Mappage de gravité normalisée. Ces cartes transforment les niveaux de gravité Tenable importés en niveaux de gravité standard pour le traitement dans votre instance. Pour plus d'informations sur la création de cartes de gravité, consultez Créer une carte de gravité Vulnerability Response dans la Réponse aux vulnérabilités documentation.

Importation d'actif Tenable.io

Les données d'actif importées sont d'abord chargées dans la table d'importation d'actifs Tenable.io [sn_vul_tenable_io_asset_import].

La carte de transformation d'intégration des actifs Tenable.io est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données provenant de l'importation d'actifs Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. `Recherchez Tenable.io transformation d'actif`.

Les tables suivantes répertorient les champs de carte de transformation par intégration.

Champs de carte de transformation d'actif Tenable.io

Champ source	Champ cible	Description
u_id	source_id	Tenable fournit un ID unique pour les actifs et les mappe à l'enregistrement d'élément détecté et est utilisé pour la recherche de CI.
u_ipv4s	ip_address	Mappe la première valeur IP au champ ip_address sur l'enregistrement de l'élément détecté.
u_mac_addresses	mac_address	Mappe la première valeur mac_address au

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation d'actif Tenable.io (suite)

Champ source	Champ cible	Description
		champ d'adresse MAC sur l'enregistrement de l'élément détecté.
u_fqdns	fqdn	Mappe la première valeur de nom de domaine complet au champ de nom de domaine complet sur l'enregistrement d'élément détecté.
u_netbios_names	Netbios	Mappe la première valeur netbios au champ netbios sur l'enregistrement de l'élément détecté.
u_operating_systems	système d'exploitation	Mappe la première valeur de système d'exploitation au champ système d'exploitation sur l'enregistrement de l'élément détecté.
(Avant les versions 14.0 Réponse aux vulnérabilités et 2.2 de Tenable Vulnerability Integration)u_last_scan_time	last_scan_date	Mappé au champ last_scan_date sur l'enregistrement de l'élément détecté.
u_last_authenticated_scan_date	last_auth_scan_date	Mappe au champ last_auth_scan_date sur l'enregistrement de l'élément détecté.
[script]	name	Mappe le nom d'hôte à l'aide de la logique du script.
u_tags		Les balises sont enregistrées dans sn_sec_cmn_host_tag. Le mappage des balises aux ressources est enregistré dans sn_sec_cmn_m2m_src_ci_tag.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Délai et objectif du script de la carte de transformation des actifs Tenable.io

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque le script est exécuté	Objectif
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs dans l'hôte et vérifier si l'hôte existe déjà. En fonction des résultats, modifie les valeurs d'un import_set. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Intégration des modules d'extension Tenable.io

La carte de transformation des modules d'extension Tenable.io est utilisée pour transformer les modules d'extension importés à partir de Tenable.io.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données reçues des modules d'extension Tenable sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la transformation du module d'extension Tenable.io.

La charge utile des modules d'extension tenable.io contient tous les champs de la colonne u_attributes de la table sn_vul_tenable_io_plugin_import. Le champ d'attributs est analysé et mappé aux enregistrements de table d'entrée tiers, tels que répertoriés dans la table suivante.

Champ source	Champ cible	Description
id	id	Mappe l'ID à partir de la source et lui ajoute le préfixe TEN-. Par exemple, si l'ID reçu est 12345, l'ID de la table cible est TEN-12345.
Description	résumé	Mappe la description du module d'extension à la colonne Résumé.
[script]	source	La source du TPE importé est Tenable.io.
[script]	source_instance	Référence au déploiement Tenable qui importe cet enregistrement.
famille	catégorie	Mappe la famille de module d'extension à la colonne de catégorie
plugin_modification_date	last_modified	Mappe la plugin_modification_date au champ de la dernière modification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
plugin_publication_date	date_published	Mappe le plugin_publication_date à la date de publication.
has_patch	remediation_type	Mappe le type de rattrapage à partir de has_patch valeur.
synopsis	menace	Mappe les informations sur la menace concernant cette vulnérabilité.
cvss_base__score	score	Mappe le score de base CVSS à la colonne de score dans la table d'entrée tierce.
solution	solution	Mappe la solution fournie par le scanner à la colonne de solution dans la table d'entrée tierce.
exploit_available	exploit	Mappe les exploit_available fournies par le scanner à la colonne Exploit dans la table d'entrée tierce
vpr.score	source_risk_score	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 – 7 – Moyen • 0-4 - Faible
vpr.drivers.age_of_vuln	age_of_vuln	Mappe l'âge de la vulnérabilité du scanner à la colonne age_of_vuln dans la table d'entrée tierce.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
vpr.drivers.product_coverage	product_coverage	Mappe la couverture du produit depuis le scanner jusqu'au product_coverage dans la table d'entrée tierce.
vpr.drivers.threat_sources_last28	threat_sources	Mappe les sources de menace au cours des 28

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		derniers jours, du scanner au threat_sources dans la table tierce.
vpr.drivers.threat_intensity_last28	threat_intensity	Mappe l'intensité de la menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_intensity dans la table d'entrée tierce.
vpr.drivers.threat_recency	threat_recency	Mappe les informations de récence de la menace du scanner à threat_recency dans la table d'entrée tierce.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mappe le score d'impact cvss3 à v3_impact_subscore colonne dans la table d'entrée tierce.
cvss_temporal_score	cvss_temporal_score	Mappe le score temporel pour CVSS v2.
cvss_v3_temporal_score	v3_temporal_score	Mappe le score temporel pour CVSS v3.
risk_factor	source_severity	Mappé à la gravité de la source dans la table d'entrée tierce.
name	name	Mappe le nom du module d'extension au nom dans la table d'entrée tierce.
stig_severity	stig_severity	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
plugin_type	check_type	Mappe le type de module d'extension au check_type dans la table d'entrée tierce.
unsupported_by_vendor	unsupported_by_vendor	Mappe le champ de unsupported_by_vendor à la colonne unsupported_by_vendor.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction de exploit_available et v3_attack_vector de colonnes.

En plus des champs directs, d'autres informations sont ajoutées sous forme de listes connexes aux entrées de tiers.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
cve	Insère les données liées aux CVE dans la table de référence (sn_vul_nvd_entry). Si la même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvée, elle associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
offre	La liste des traqs de bogues est ajoutée en tant que référence.
see_also	La liste des URL est ajoutée en tant que référence.
xrefs	La liste de X-REF est ajoutée en tant que référence.
[script]	Liste des exploits pour ce module d'extension et insère le mappage pour le cadre de travail de l'exploit applicable et le module d'extension à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs de l'entrée tierce et vérifier si l'entrée tierce existe déjà. En fonction des résultats, modifie les valeurs d'une entrée de tiers. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

L'include de script TenableIOPluginsImportProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de Tenable.io intégration des modules d'extension et la transforme en Now Platform entrées de vulnérabilité tierces. Toute modification apportée à cet include de script peut altérer la transformation des données de Tenable.io modules d'extension dans la table d'entrée tierce.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation des vulnérabilités Tenable.io

Les Tenable.io cartes de transformation des éléments vulnérables sont utilisées pour transformer les informations sur les vulnérabilités ouvertes et corrigées importées depuis Tenable.io.

Remarque : Les changements apportés à cette carte de transformation modifient la façon dont les données provenant de l'importation des vulnérabilités Tenable sont traitées.

La même carte de transformation est utilisée pour l'intégration des vulnérabilités fixes Tenable.io et l'intégration des vulnérabilités ouvertes Tenable.io. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la `carte de transformation de l'élément vulnérable Tenable.io`.

Champ source	Champ cible	Description
u_asset.uuid	id	Uuid est mappé au champ d'ID de l'enregistrement de cmdb_ci.
u_asset.ipv4	ip_address	Le champ ipv4 est mappé au champ d'adresse ip de l'enregistrement cmdb_ci.
u_asset .last_authenticated_results	last_auth_scan_date	La date de la dernière analyse authentifiée est mappée à la date de la dernière analyse d'authentification de l'enregistrement cmdb_ci.
u_asset.mac_addess	mac_address	L'adresse Mac est mappée au champ d'adresse MAC de l'hôte de l'enregistrement cmdb_ci.
u_asset.netbios_name	Netbios	Netbios est mappé au champ netbios de cmdb_ci enregistrement.
u._plugin.cvss3_base_score	v3_base_score	Le score de base CVSS v3 est mappé au score de base v3 de l'enregistrement d'entrée tierce.
u._plugin.cvss3_temporal_score	v3_temporal_score	Le score temporel CVSS v3 est mappé au score temporel v3 dans l'enregistrement d'entrée tierce.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u._plugin.cvss_base_score	score	Le score de base CVSS est mappé au champ de score de l'enregistrement d'entrée tierce.
u._plugin.cvss_temporal_score	temporal_score	Le score temporel est mappé au score temporel dans l'enregistrement d'entrée tierce.
u_plugin.description	résumé	La description est mappée au champ Résumé dans l'enregistrement d'entrée tierce.
u_plugin.famille	catégorie	Mappe la famille de module d'extension à la colonne de catégorie de l'enregistrement d'entrée tierce.
u_plugin.modification_date	last_modified	La dernière date modifiée est mappée à la date de la dernière modification du module d'extension dans l'enregistrement d'entrée tierce.
u_plugin.date_publication_	date_published	La date de publication est mappée au champ Date de publication de l'enregistrement d'entrée tierce.
u_plugin.risque_facteur	source_severity	Le facteur de risque est mappé au champ source_severity de l'enregistrement d'entrée tierce.
u_plugin.solution	solution	La solution est mappée au champ de solution de l'enregistrement d'entrée tierce.
u_plugin.synopsis	menace	Le synopsis est mappé au champ de menace de l'enregistrement d'entrée de tiers.
u_severity_id	Priorité	La priorité est mappée à l'ID de gravité de la

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		charge utile. La valeur par défaut est de 5.
u_plugin.exploit_disponible	exploit	Mappe les exploit_available fournies par le scanner à la colonne Exploit dans la table d'entrée tierce.
vpr.score	source_risk_score	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 – 7 – Moyen • 0-4 - Faible
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	Mappe l'âge de vulnérabilité depuis le scanner jusqu'aux age_of_vuln dans la table d'entrée tierce.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mappe la couverture du produit depuis le scanner jusqu'au product_coverage dans la table d'entrée tierce.
u_plugin.vpr.drivers.threat_sources_last28	threat_sources	Mappe les sources de menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_sources dans la table d'entrée tierce.
u_plugin.vpr.drivers.threat_intensity_last28	threat_intensity	Mappe l'intensité de la menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_intensity dans la table d'entrée tierce.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_plugin.vpr.drivers.threat_recency	threat_recency	Mappe les informations de récence de la menace du scanner aux threat_recency dans la table d'entrée tierce.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mappe le score d'impact CVSS3 v3 à v3_impact_subscore colonne dans la table d'entrée tierce.
u_plugin.type	check_type	Mappe le type de module d'extension au check_type dans la table d'entrée tierce.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Mappe le champ unsupported_by_vendor du module d'extension à la colonne unsupported_by_vendor.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction de exploit_available et v3_attack_vector de colonnes.
u_plugin.family_id	Family_id	Mappe l'ID de famille de modules d'extension à family_id colonne de la table d'entrée tierce.
port	port	Le port est mappé au champ port de l'enregistrement d'élément vulnérable.
protocol	protocol	Le protocole est mappé au champ Protocole de l'enregistrement d'élément vulnérable.
u_first_found	first_found	Le premier trouvé est mappé au champ du premier trouvé de l'enregistrement d'élément vulnérable.
u_last_found	last_found	Dernier trouvé est mappé au champ Dernier trouvé de l'enregistrement d'élément vulnérable.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_state	État	L'état est mappé au champ État dans l'enregistrement de l'élément vulnérable
[script]	source	La source de l'intégration est renseignée. Les éléments vulnérables créés à partir de cette intégration ont Tenable.io comme source.
[script]	integration_instance	Le integration_instance est le nom de l'instance à partir de laquelle l'élément vulnérable est importé.
u_plugin.name	name	Mappe le nom du module d'extension au nom dans la table d'entrée tierce.
u_plugin.stig_severity	stig_severity	Mappe la gravité stig du module d'extension à la colonne gravité stig dans la table d'entrée tierce

En plus des champs directs, d'autres informations sont ajoutées sous forme de listes connexes aux entrées de tiers.

Champ source	Description
cve	Insère les données liées aux CVE dans la table de référence (sn_vul_nvd_entry). Si la même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvée, elle associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
offre	La liste des traqs de bogues est ajoutée en tant que référence.
see_also	La liste des URL est ajoutée en tant que référence.
xrefs	La liste de X-REF est ajoutée en tant que référence.
[script]	Liste des exploits pour ce module d'extension et insère le mappage de l'infrastructure de l'exploit applicable et du module d'extension à sn_vul_m2m_framework_vul.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation déclenche TenableIOVulnerabilitiesProcessor qui importe les données des Tenable.io à l'aide du jeu d'importation et charge chaque enregistrement dans la table CI CMDB, la table des éléments vulnérables et la table de vulnérabilité tierce. Pour un usage interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction permettant de vérifier si l'entrée et les détections tierces existent déjà. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour mettre à jour le nombre de CI, de VI et de détections tels qu'importés à partir de Tenable.io. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Importation d'actif Tenable.sc

Les données d'actif importées à partir de Tenable.sc sont d'abord chargées dans la table d'importation d'actifs Tenable.sc (sn_vul_tenable_sc_asset_import). La carte de transformation de l'intégration des actifs Tenable.sc est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données provenant de l'importation d'actifs Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la `transformation de l'actif Tenable.sc`.

Champ source	Champ cible	Description
u_uuid	id	L'uuid n'étant pas renseigné à partir de l'API Tenable, l'attribut « u_uniqueness » est donc utilisé pour créer un champ uuid unique pour les actifs et le mapper à l'enregistrement cmdb_ci.
u_ip	ip_address	Mappe le champ IP de l'API au champ ip_address d'un enregistrement cmdb_ci.
u_macaddress	mac_address	Mappe le champ macaddress de l'API au

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		champ d'adresse sur l'enregistrement cmdb_ci.
u_dnsname	fqdn	Mappe le champ dnsname de l'API au champ fqdn de l'enregistrement cmdb_ci.
u_netbiosname	Netbios	Mappe le champ netbios de l'API au champ netbios de l'enregistrement cmdb_ci.
u_oscpe	système d'exploitation	Les informations sur le système d'exploitation sont extraites de l'attribut oscpe dans la charge utile et les mappent au champ système d'exploitation de l'enregistrement cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mappe le champ lastauthrun de l'API au champ last_auth_scan_date sur l'enregistrement de l'élément détecté.
u_lastauthrun et u_lastunauthrun	last_scan_date	Le lastauthrun est extrait de l'api Tenable ou du lastunauthrun. En fonction de la valeur qui apparaît dans la charge utile, le champ last_scan_date de l'enregistrement de l'élément détecté est renseigné.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs dans l'hôte et vérifier si l'hôte existe déjà. En fonction des résultats, modifie les valeurs d'un import_set. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.sc Importation des modules d'extension

Les données des modules d'extension importées à partir de Tenable.sc sont d'abord chargées dans la table d'importation des modules d'extension Tenable.sc (sn_vul_tenable_sc_plugin_import). La carte de transformation du module d'extension Tenable.sc est utilisée pour transformer les informations des modules d'extension qui ont été importées. Les changements apportés à cette transformation modifient la façon dont les données provenant de l'importation du module d'extension Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez `Tenable.sc carte de transformation de module d'extension`.

Champ source	Champ cible	Description
u_id	id	Mappe l'ID à partir de la source et ajoute le préfixe TEN-. Par exemple, si l'ID reçu est 12345, l'ID de la table cible est TEN-12345.
u_description	résumé	Mappe la description du module d'extension à la colonne Résumé.
[script]	source	Le TPE importé à partir de cette intégration a Tenable.sc comme source.
[script]	source_instance	Référence au déploiement Tenable qui importe cet enregistrement.
u_family	catégorie	Mappe le champ Nom dans l'objet de famille du module d'extension à la colonne Catégorie.
u_plugin_modification_date	last_modified	Mappe la plugin_modification_date au champ de la dernière modification.
u_plugin_publication_date	date_published	Mappe le plugin_publication_date à la date de publication.
u_has_patch	Remediation_type	Mappe le type de rattrapage à partir de has_patch valeur.
u_synopsis	menace	Mappe les informations sur la menace concernant cette vulnérabilité.
u_cvss_base_score	score	Mappe le score de base CVSS à la colonne de score dans la table d'entrée tierce.
u_solution	solution	Mappe la solution fournie par le scanner à la colonne

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		de solution dans la table d'entrée tierce.
u_cvss_temporal_score	cvss_temporal_score	Mappe le score temporel pour CVSS v2.
u_cvss_v3_temporal_score	v3_temporal_score	Mappe le score temporel pour CVSS v3.
u_risk_factor	Gravité de la source	Mappé à la gravité de la source dans la table d'entrée tierce.
u_cvss_v3_base_score	v3_base_score	Mappe le score de base CVSS dans la table d'entrée tierce.
u_exploit_available	exploit	Mappe l'exploitDisponible fourni par le scanner à la colonne Exploit dans la table d'entrée tierce.
u_vpr_score	source_risk_score	Mappe le score VPR du scanner au score du risque source dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 – 7 – Moyen • 0-4 - Faible
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mappe l'âge de la vulnérabilité depuis le scanner jusqu'aux age_of_vuln dans la table d'entrée tierce.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_vpr_context[id=product_coverage]	product_coverage	Mappe la couverture du produit depuis le scanner jusqu'au product_coverage dans la table d'entrée tierce.
u_vpr_context[id="threat_sources_last_28"]	threat_sources	Mappe les sources de menace au cours des 28 derniers jours, du scanner à l'threat_sources dans la table tierce.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_vpr_context[id="threat_intensity_last_28"]	threat_intensity	Mappe l'intensité de la menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_intensity dans la table d'entrée tierce.
u_vpr_context[id="threat_recency"]	threat_recency	Mappe les informations de récence de la menace du scanner aux threat_recency de la table d'entrée tierce.
u_vpr_context[id=cvssV3_impact_score]	v3_impact_subscore	Mappe le score d'impact CVSS v3 du scanner au v3_impact_subscore dans la table d'entrée tierce.
u_name	name	Mappe le nom du module d'extension à la colonne nom dans la table d'entrée tierce.
u_stig_severity	stig_severity	Mappe le champ stig_severity du module d'extension à stig_severity dans la table d'entrée tierce.
u_check_type	check_type	Mappe le type de chèque au check_type dans la table d'entrée tierce.
u_family.id	family_id	Mappe les family_id de module d'extension aux family_id dans la table d'entrée tierce.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction de exploit_available et v3_attack_vector de colonnes.

En plus des champs directs, d'autres informations sont ajoutées sous forme de listes connexes aux entrées de tiers.

Champ source	Description
u_cpe	La liste des CPE est ajoutée à titre de référence.
u_see_also	La liste des URL est ajoutée en tant que référence.
u_exploit_frameworks	Liste des exploits pour ce module d'extension et insère le mappage pour le cadre de travail de l'exploit

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
	applicable et le module d'extension à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs dans l'entrée tierce et vérifier si l'entrée tierce existe déjà. En fonction des résultats, modifie les valeurs d'une entrée de tiers. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation permet de définir les valeurs des modules d'extension créés et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

L'include de script TenableSCPluginsImportProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de l'intégration des modules d'extension Tenable.sc et la transforme en entrées de vulnérabilité tierces ServiceNow. Toute modification apportée à cet include de script peut altérer la transformation des données de Tenable.sc modules d'extension dans la table d'entrée tierce.

Tenable.sc Importation des vulnérabilités

La carte de transformation des vulnérabilités ouvertes Tenable.sc est utilisée pour transformer les données importées de l'intégration des vulnérabilités ouvertes Tenable.sc, et la carte de transformation des vulnérabilités Tenable.sc et corrigées est utilisée pour transformer les données importées de l'intégration des vulnérabilités corrigées Tenable.sc.

Remarque : Les changements apportés à ces cartes de transformation modifient la façon dont les données provenant de l'importation des vulnérabilités Tenable corrigées/ouvertes sont traitées.

Pour accéder aux cartes de transformation des vulnérabilités ouvertes et corrigées Tenable.sc, naviguez vers **Intégration de vulnérabilité tenable** > **Administration** > **Instances d'intégration** > **Tenable.sc Intégration des vulnérabilités corrigées/ouvertes** > **Sources de données** > **Tenable.sc vulnérabilités ouvertes/corrigées** > **Transformations**.

Champ source	Champ cible	Description
u_pluginID	ID	Utilisé comme identificateur pour le module d'extension.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		Ce champ est mappé à l'ID du module d'extension dans l'enregistrement d'entrée tierce.
u_riskfactor	source_severity	Ce champ est mappé à source_severity dans l'enregistrement d'entrée tierce.
u_severity	Priorité	Le champ de priorité est mappé avec la gravité. La valeur par défaut est de 5.
u_hasbeenmitigated	État	Hasbeenmitigated est mappé au champ d'état de l'enregistrement de vulnérabilité. Pour l'intégration des vulnérabilités corrigées, tous les VI sont à l'état « Fermé ».
u_ip	ip_address	L'adresse IP est mappée au champ IP de l'hôte de cmdb_ci table.
u_port	port	Le port est mappé au champ port de l'enregistrement d'élément vulnérable.
u_protocol	protocol	Le protocole est mappé au champ de port de l'enregistrement de l'élément vulnérable.
u_firstSeen	first_found	La première valeur vue est mappée au premier champ trouvé de l'enregistrement VI.
u_lastSeen	last_found	La dernière valeur observée est mappée au dernier champ trouvé de l'enregistrement VI.
u_exploitAvailable	exploit	ExploitAvailable est mappé au champ Exploit dans l'enregistrement d'entrée tierce.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_synopsis	menace	Le synopsis est mappé au champ Menace dans l'enregistrement d'entrée tierce.
u_description	résumé	La description est mappée au champ Résumé dans l'enregistrement d'entrée tierce.
u_solution	solution	La solution est mappée au champ de solution dans l'enregistrement d'entrée tierce.
u_basescore	score	Le score de base est mappé au champ de score dans l'enregistrement de l'entrée tierce.
u_temporalScore	temporal_score	Le score temporel est mappé au score temporel dans l'enregistrement d'entrée tierce.
u_cvssv3basescore	v3_base_score	Cvssv3basescore est mappé au score de base v3 dans l'enregistrement d'entrée tierce.
u_cvsstemporalscore	v3_temporal_score	Le score temporel Cvssv3 est mappé au score temporel v3 dans l'enregistrement d'entrée tierce.
u_pluginpubdate	date_published	La date de publication du module d'extension est mappée à la date de publication du module d'extension dans l'enregistrement d'entrée tierce.
u_pluginmoddate	last_modified	La dernière date modifiée est mappée à la date de la dernière modification du module d'extension dans l'enregistrement d'entrée tierce.
u_dnsname	fqdn	DnsName est mappé au champ FQDN

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		de l'enregistrement cmdb_ci.
u_macaddress	mac_address	MacAddress est mappé au champ mac_address de l'enregistrement cmdb_ci.
u_netbiosName	Netbios	NetbiosName est mappé au champ NETBIOS de l'enregistrement cmdb_ci.
u_ip	ip	L'adresse IP est mappée au champ IP de cmdb_ci enregistrement.
hostUniqueness	uuid	L'unicité de l'hôte n'est mappée à aucun champ, mais est utilisée pour déterminer l'uuid de l'hôte.
u_family	catégorie	Mappe le champ de nom dans l'objet de famille du module d'extension à la colonne de catégorie de l'enregistrement d'entrée tiers.
u_plugintext	proof	Le texte du module d'extension est mappé à la preuve dans l'enregistrement TPE.
[script]	source	La source de l'intégration est renseignée. Les éléments vulnérables créés à partir de cette intégration ont Tenable.sc comme source.
[script}	integration_instance	Le integration_instance est le nom de l'instance à partir de laquelle l'élément vulnérable est importé.
u_vpr_score	source_risk_score	Mappe le score VPR du scanner au score du risque source dans la table d'entrée tierce.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 – 7 – Moyen • 0-4 - Faible
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mappe l'âge de la vulnérabilité depuis le scanner jusqu'aux age_of_vuln dans la table d'entrée tierce.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_vpr_context[id=product_coverage]	product_coverage	Mappe la couverture du produit depuis le scanner jusqu'au product_coverage dans la table d'entrée tierce.
u_vpr_context[id="threat_sources_last_28]	threat_sources	Mappe les sources de menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_sources dans la table tierce.
u_vpr_context[id="threat_intensity_last_28]	threat_intensity	Mappe l'intensité de la menace au cours des 28 derniers jours depuis le scanner jusqu'à threat_intensity dans la table d'entrée tierce.
u_vpr_context[id="threat_recency"]	threat_recency	Mappe les informations de récence de la menace du scanner aux threat_recency de la table d'entrée tierce.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mappe le score d'impact CVSS v3 du scanner au v3_impact_subscore

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		dans la table d'entrée tierce.
u_pluginname	name	Mappe le nom du module d'extension à la colonne nom dans la table d'entrée tierce.
u_stigseverity	stig_severity	Mappe le champ stig_severity du module d'extension à stig_severity dans la table d'entrée tierce.
u_checktype	check_type	Mappe le type de vérification à check_type dans la table d'entrée tierce.
u_family.id	family_id	Mappe les family.id de module d'extension aux family_id dans la table d'entrée tierce.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table third_party_entry est renseignée en fonction de exploit_available et v3_attack_vector de colonnes.

Champ source	Description
u_cve	Insère les données liées aux CVE dans la table de référence (sn_vul_nvd_entry). Si la même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvée, elle associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
u_bid	La liste des traqs de bogues est ajoutée en tant que référence.
u_cpe	La liste des CPE est ajoutée à titre de référence.
u_seealso	La liste des URL est ajoutée en tant que référence.
u_xrefs	La liste des X-REF est ajoutée à titre de référence.
u_exploitframeworks	Liste des exploits pour ce module d'extension et insère le mappage de l'infrastructure de l'exploit

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
	applicable et du module d'extension à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie le moment d'exécution de chaque script et son but.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a démarré la transformation)	Cette transformation est utilisée pour initialiser les valeurs du import_set du processus d'intégration. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onBefore (avant qu'un jeu d'importation n'ait terminé sa transformation).	Fonction utilisée pour mettre à jour les valeurs de la vulnérabilité et vérifier si la vulnérabilité existe déjà. En fonction des résultats, modifie les valeurs d'une table d'éléments vulnérables. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux VI créés et des VI qui ont été mis à jour et ignorés. Réservée à une utilisation interne. La modification ou la suppression n'est pas recommandée.

Définir des paramètres de filtre supplémentaires pour Tenable.io les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec la Tenable Vulnerability Integration pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec le Tenable.io produit.

Avant de commencer

Cas d'utilisation : en tant que gestionnaire ou analyste des vulnérabilités, vous souhaiterez peut-être filtrer les données de vos requêtes afin de ne pouvoir examiner que certains détails de vulnérabilité. Par exemple, supposons que vous souhaitiez afficher les vulnérabilités importées qui sont filtrées par *cidr_range*, *num_assets*, *indexed_at*et *plugin_family*. Supposons que vous souhaitiez exécuter une Tenable.io intégration de sorte qu'une exécution importe uniquement les vulnérabilités critiques toutes les quatre heures et qu'une autre s'exécute toutes les 24 heures pour récupérer toutes les autres vulnérabilités non critiques.

Pour vous aider à collecter ces données, vous pouvez ajouter des paramètres pris en charge par Tenable pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

Sans ajouter d'appels d'API ou de codage supplémentaires, cette fonctionnalité vous permet de personnaliser les informations de votre requête HTTP avec les paramètres Tenable dans votre Now Platformfichier . Les intégrations suivantes Tenable.io prennent en charge le filtrage en fournissant du contenu JSON dans le corps de la demande :

- Intégration des actifs
- Intégration de vulnérabilité fixe
- Intégration des vulnérabilités ouvertes

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous devez savoir comment utiliser JSON des chaînes pour cette fonctionnalité.

Rôle requis : sn_vul.vulnerability_admin

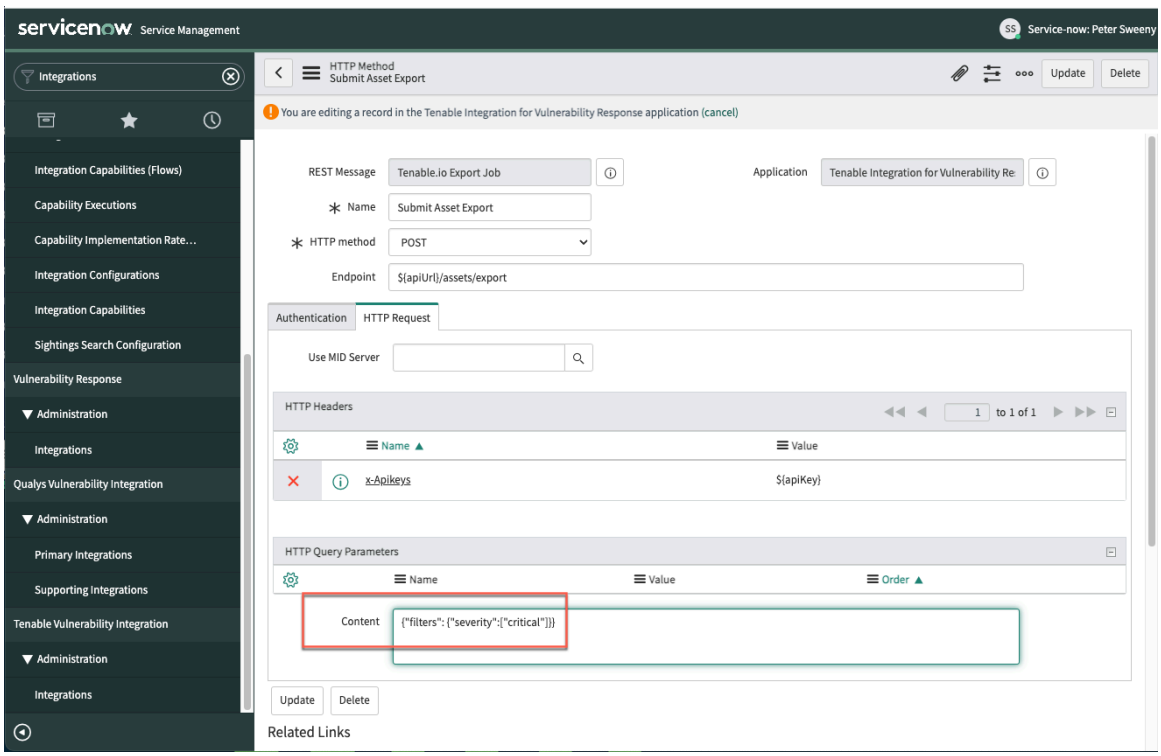
Procédure

1. Localisez les paramètres pris en charge par le Tenable.io produit sur le site développeur que vous souhaitez utiliser pour votre filtrage.

   Les paramètres et les valeurs que vous entrez à partir du produit ne sont pris en charge qu'au niveau de l'instance d'intégration Tenable.io .

2. Accédez à la **Tout** > **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.
3. Sur la page de liste Intégrations Tenable, cliquez sur l'enregistrement de l'intégration Tenable.io que vous souhaitez ouvrir.
4. Une fois l'onglet Méthodes REST Tenable sélectionné, cliquez sur l'icône d'informations (I) pour la méthode REST, puis sur **Ouvrir l'enregistrement**.
5. Sélectionnez l'onglet **de demande HTTP** .
6. Pour modifier l'enregistrement, en haut de la page, cliquez sur le lien, Pour modifier l'enregistrement, cliquez **ici**.
7. Dans l'enregistrement Méthode REST, dans le champ Contenu, saisissez le contenu JSON que vous souhaitez intégrer au corps de la demande.

   Dans l'image suivante, à titre d'exemple, le paramètre de gravité pour les vulnérabilités `{"filters": {"severity": ["critical"]}}` importées a été personnalisé pour l'intégration Tenable.io des actifs. Cette valeur importe uniquement les vulnérabilités critiques (score CVSS de 10,0).



   Si vous souhaitez entrer plusieurs paramètres, reportez-vous à la documentation pour plus d'informations sur la Tenable.io séparation de chaque valeur.

8. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Reporting sur l'intégration de vulnérabilité tenable

Affichez les rapports sur les vulnérabilités et les éléments vulnérables sur les Réponse aux vulnérabilités tableaux de bord.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à suivre la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en visualisant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Reportez-vous à la rubrique Réponse aux vulnérabilités Espaces de travailet Exploration de l'Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Versions précédentes de Réponse aux vulnérabilités

Le tableau de bord de vue d'ensemble de Vulnerability Response (Gestion des vulnérabilités) fournit une vue d'ensemble des vulnérabilités et des éléments vulnérables, ce qui aide l'administrateur de vulnérabilité à identifier rapidement les zones de préoccupation. Le tableau de bord de rattrapage de Vulnerability Response (Vulnerability Remediation) permet à un spécialiste de la remédiation de se concentrer sur les tâches de remédiation et les éléments vulnérables qu'il possède.

Consultez Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités pour plus d'informations.

Rôle requis : propriétaire du rattrapage.

Des rôles granulaires et de profil sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.

Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pour afficher le tableau de bord, accédez à **Réponse aux vulnérabilités** > **Aperçu du rattrapage**.

Graphique d'état de l'exécution de l'intégration pour Tenable Vulnerability Integration

Le module État de l'exécution de l'intégration Tenable vous fournit une vue graphique de l'état des exécutions d'intégration Tenable.

Dans le diagramme, pointez sur n'importe quelle partie du graphique pour afficher un résumé des données spécifiques à cette partie. Si vous cliquez sur une partie du graphique à barres, une liste s'ouvre pour fournir des informations plus détaillées.

Rôle requis : administrateur de vulnérabilité.

Des rôles granulaires et de profil sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

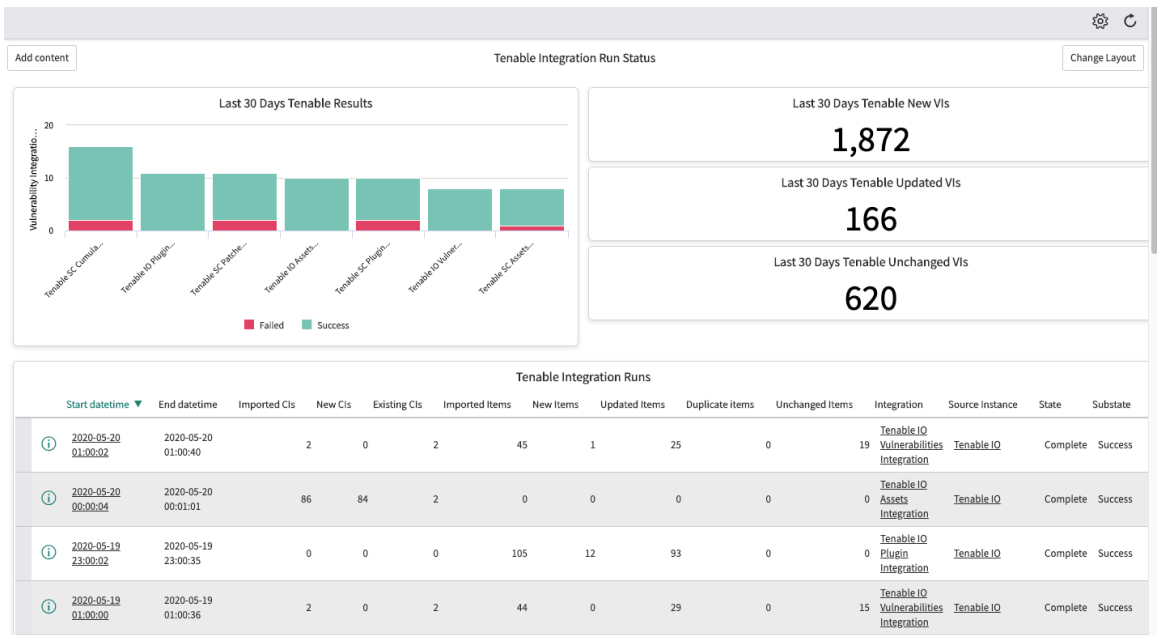
Pour en savoir plus sur la gestion des rôles granulaires, reportez-vous à Gérer les profils et les rôles granulaires pour Réponse aux vulnérabilités.

Pour afficher les données, accédez à **Tout** > **Intégration de vulnérabilité tenable** > **État de l'exécution de l'intégration**.

À partir de la version 19.0 de , ce tableau de bord est disponible dans l'interface utilisateur Nouvelle Réponse aux vulnérabilitésexpérience.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

État d'exécution



Rapports sur les graphiques d'état de l'exécution de l'intégration Tenable

Nom	Description
Résultats Tenable au cours des 30 derniers jours	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Chaque exécution est affichée sous forme de barre dans le graphique.
Nouveaux VI Tenable au cours des 30 derniers jours	Nombre de nouveaux éléments vulnérables importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour Tenable au cours des 30 derniers jours	Nombre d'éléments vulnérables mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI inchangés Tenable au cours des 30 derniers jours	Nombre d'éléments vulnérables en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Exécutions de l'intégration Tenable	L'exécution de l'intégration enregistre dans une liste.

Traduction automatique

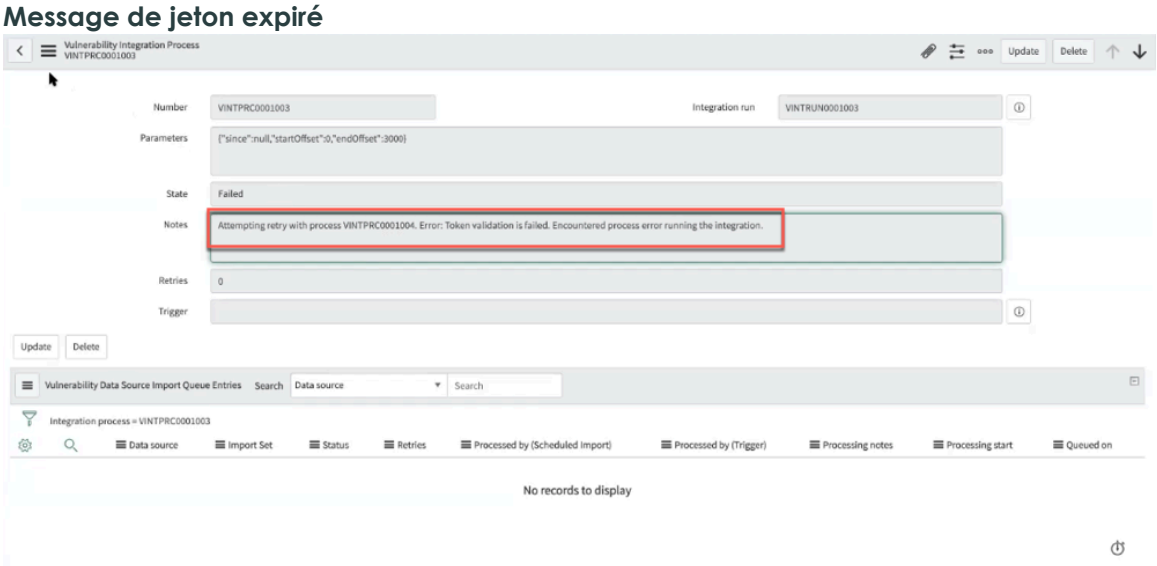
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
	Remarque : V16.1 : Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection de la *sn_vul_detection* table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, après la fin de l'exécution de l'intégration.

Expiration de la validation du jeton

Si l'exécution d'une intégration de Tenable.sc échoue pour une raison quelconque, le jeton d'authentification pour Tenable.sc expire automatiquement et un message s'affiche sur l'enregistrement du processus d'intégration de vulnérabilité.

Message de jeton expiré



Un nouveau jeton est automatiquement généré pour le prochain processus d'intégration. Tous les processus d'intégration, qu'ils aient échoué ou réussi, sont affichés dans l'onglet Processus d'intégration de vulnérabilité de l'enregistrement Processus d'intégration de vulnérabilité.

Lancer une nouvelle analyse pour l'intégration Tenable.sc

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans la plateforme Tenable. Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Tenable.sc produit à partir de votre Now Platform® instance.

Avant de commencer

Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Remarque : Tenable.sc Ne prend pas en charge le lancement d'une nouvelle analyse sur les ordinateurs basés sur un agent.

Vérifiez que votre scanner est activé avant de commencer. Accédez à la **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche
Pour lancer une nouvelle analyse à partir des espaces de travail, reportez-vous à la section Analyser Tenable.io à nouveau et Tenable.sc les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail.

Suivez les étapes ci-dessous pour lancer une nouvelle analyse dans l'environnement classique.

Pour aider à réduire les frais généraux et le volume impliqués par les analyses complètes planifiées, les responsables des rattrapages, les spécialistes informatiques, les analystes de vulnérabilité ou les gestionnaires de vulnérabilités peuvent lancer de nouvelles analyses ciblées sur demande pour des vulnérabilités spécifiques sur des actifs (éléments de configuration) dans leurs environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de remédiation (RT), d'entrée tierce (TPE) ou d'éléments détectés à partir de votre Now Platform instance.

Les nouvelles analyses permettent à vos propriétaires de rattrapage et à vos analystes de vulnérabilité de vérifier que vos activités de rattrapage, vos correctifs et vos autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

À titre d'exemple, l'ensemble de votre environnement est analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été effectuée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines la prochaine analyse planifiée pour vérifier qu'elle a été corrigée. Pour vérifier que votre correctif corrige avec succès une vulnérabilité critique détectée lors d'une analyse précédente, vous pouvez lancer une nouvelle analyse ciblée à partir de votre Now Platform recherche Tenable.sc d'éléments vulnérables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous demandez une nouvelle analyse à partir de votre Now Platform® instance, la sélection des informations d'identification Intégration de Réponse aux vulnérabilités à Tenable est facultative. L'intégration ServiceNow® Tenable.sc des informations d'identification de numérisation importe et met à jour les informations d'identification du scanner à partir Tenable.sc du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable.

Notez que ces données importées n'incluent pas les mots de passe Tenable ni d'autres informations sensibles sur le compte Tenable. L'intégration ServiceNow® Tenable.sc des informations d'identification de numérisation est activée (`active`) automatiquement à partir de l'assistant de configuration de votre instance lorsque vous configurez les Tenable.sc intégrations de vulnérabilités (Tenable.sc intégrations de vulnérabilités ouvertes et fixes).

Notez les informations suivantes au sujet des informations d'identification que vous importez afin que vos utilisateurs puissent les afficher selon leurs besoins à partir de votre Now Platform instance :

- Les informations d'identification créées avec le Tenable.sc rôle d'utilisateur administrateur sont disponibles pour les utilisateurs de toutes vos organisations.
- Les informations d'identification créées avec le rôle d'utilisateur de l'organisation Tenable.sc ne sont disponibles que pour les utilisateurs de cette organisation. Ces informations d'identification ne sont pas importées dans le référentiel Now Platform pour les utilisateurs extérieurs à l'organisation du créateur, sauf si elles sont partagées avec le compte de l'utilisateur utilisé pour se connecter à l'instance.

Consultez le site web de la Tenable.sc documentation pour plus d'informations.

Consultez Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration pour plus d'informations sur la configuration de l'application Tenable.sc . Pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation, naviguez vers **Tout** > **Intégration de vulnérabilité tenable** > **Intégrations** > **Intégration des informations d'identification Tenable.sc Scan**.

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Vous ne pouvez lancer de nouvelles analyses que pour les VI dont Tenable.sc la source est la source. Verify Tenable.sc s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le Créateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue Liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône **Personnaliser la liste** (icône Engrenage) et utilisez la zone de sélection pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** pour la tâche de rattrapage ou les enregistrements d'entrées de tiers, respectivement, que vous souhaitez utiliser pour la nouvelle analyse.

   En fonction de votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

   - Sur un enregistrement de VI unique, le VI doit provenir du Tenable.sc produit et se trouver dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent provenir du produit Tenable.sc et être dans un état autre que **Fermé**.
   - Sur un enregistrement RT, la tâche de rattrapage peut être dans n'importe quel état autre que **Fermé** et tous les VI associés doivent provenir du Tenable.sc produit.
   - Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du produit dans un Tenable.sc état autre que **Fermé**.

4. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**. Vous êtes invité à choisir les informations d'identification du scanner pour y accéder. Il s'agit des informations d'identification importées par l'intégration des informations d'identification Tenable.sc de numérisation.
5. Dans la boîte de dialogue, sélectionnez les filtres et les types d'informations d'identification souhaités.
6. Cliquez sur **Demander l'analyse**.

   Un message s'affiche pour indiquer que votre analyse est en cours de traitement. L'état de toutes les nouvelles analyses peut être consulté à tout moment sous les listes relatives à l'analyse sur les enregistrements VI, RT, TPE que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le champ État de l'enregistrement d'analyse parent est marqué comme terminé lorsque toutes les analyses enfants sont terminées avec succès. L'enfant analyse les données d'importation. L'enregistrement d'analyse parent est un conteneur pour les analyses enfants.

Votre Now Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine correctement ou jusqu'à l'expiration de la période de suivi définie, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de votre Now Platform® nouvelle analyse a cessé, et non à la date à laquelle la nouvelle analyse elle-même s'est arrêtée. Tous les VI qui sont passés ou passeront à **l'état Fermé/Fixe** sont importés avec la prochaine importation planifiée de l'intégration des vulnérabilités Tenable.sc Fixe.

Lancer une nouvelle analyse pour l'intégration Tenable.io

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans la plateforme Tenable. Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Tenable.io produit à partir de votre Now Platform® instance.

Avant de commencer

Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Vérifiez que votre scanner est activé avant de commencer. Accédez à la **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.

Pourquoi et quand exécuter cette tâche

- Consultez et Analyser à nouveau les enregistrements et les tâches de rattrapage dans Vulnerability Manager Workspace pour Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT lancer une nouvelle analyse dans les espaces de travail Vulnerability Response.
- Suivez les étapes ci-dessous pour lancer une nouvelle analyse dans l'environnement classique.

Remarque : Tenable.io Ne prend pas en charge le lancement d'une nouvelle analyse sur les ordinateurs basés sur un agent.

Pour aider à réduire les frais généraux et le volume impliqués par les analyses complètes planifiées, en tant que propriétaire du rattrapage, spécialiste informatique, analyste de vulnérabilité ou gestionnaire de vulnérabilité, vous pouvez lancer de nouvelles analyses ciblées sur demande. Vous pouvez rechercher des vulnérabilités spécifiques sur les actifs (éléments de configuration) de vos environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de rattrapage (VUL), d'entrée tierce (TPE) ou d'éléments détectés (SDI) à partir de votre Now Platform instance. Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, vos correctifs et vos autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous demandez une nouvelle analyse à partir de votre Now Platform® instance, la sélection des informations d'identification Intégration de Réponse aux vulnérabilités à Tenable est facultative. L'intégration ServiceNow® Tenable.io des informations d'identification de numérisation importe et met à jour les informations d'identification du scanner à partir Tenable.io du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable.

Notez que ces données importées n'incluent pas les mots de passe Tenable ni d'autres informations sensibles sur le compte Tenable.

Les informations suivantes décrivent les informations d'identification que vous importez afin que vos utilisateurs puissent les afficher selon leurs besoins à partir de votre Now Platform instance :

- Les informations d'identification créées avec le Tenable.io rôle d'utilisateur administrateur sont disponibles pour les utilisateurs de toutes vos organisations.
- Les informations d'identification créées avec le rôle d'utilisateur de l'organisation Tenable.io ne sont disponibles que pour les utilisateurs de cette organisation. Ces informations d'identification ne sont pas importées dans le référentiel Now Platform pour les utilisateurs extérieurs à l'organisation du créateur, sauf si elles sont partagées avec le compte de l'utilisateur utilisé pour se connecter à l'instance.

  Consultez le site web de la Tenable.io documentation pour plus d'informations.

- L'intégration Tenable.io du modèle et l'intégration des informations d'identification Tenable.io de numérisation doivent être activées avant de lancer de nouvelles analyses. Pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation, naviguez vers **Intégration de vulnérabilité tenable** > **Intégrations** > **Intégration des informations d'identification Tenable.io Scan**.

  Par défaut, les intégrations d'informations d'identification de modèle et d'analyse sont désactivées. Lorsque vous saisissez vos informations d'identification pour Tenable.io, toutes les Tenable.io intégrations sont automatiquement activées. Pour activer ou désactiver manuellement ces intégrations :

  1. Accédez à la **Tout** > **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.
  2. Dans la liste qui s'affiche, localisez les enregistrements d'intégration Tenable.io souhaités.
  3. Ouvrez chaque enregistrement et cochez la case **Actif** pour activer l'intégration.
  4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.
  5. Revenez à l'assistant de configuration pour poursuivre la configuration avec Tenable Vulnerability IntegrationRéponse aux vulnérabilités.

Pour plus d'informations sur la configuration des Tenable.io produits and, reportez-vous Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration à la section .Tenable.sc

Supposons que l'ensemble de votre environnement soit analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été effectuée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines la prochaine analyse planifiée pour vérifier qu'elle a été corrigée. Pour vérifier que votre correctif corrige avec succès une vulnérabilité critique détectée lors d'une analyse précédente, vous pouvez

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

lancer une nouvelle analyse ciblée à partir de votre Now Platform recherche Tenable.io d'éléments vulnérables.

Vous pouvez afficher les résultats mis à jour sur les enregistrements à partir desquels vous avez initié les analyses après la prochaine importation planifiée de l'intégration des vulnérabilités corrigées.

Lors de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans des pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou rester bloqué, ce qui entraîne une erreur de délai d'attente d'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter ce malentendu, à partir de la version 18.2.4 de Réponse aux vulnérabilités, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il est également antérieur à une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit l'heure après laquelle l'entrée de file d'attente d'importation doit être expirée.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Si vous utilisez le Tenable.io scanner, vous ne pouvez lancer de nouvelles analyses que pour les VI dont Tenable.io la source est la source. Verify Tenable.io s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le Créateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue Liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône **Personnaliser la liste** (icône Engrenage) et utilisez la zone de sélection pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** pour les enregistrements que vous souhaitez utiliser pour la nouvelle analyse.

   En fonction de votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

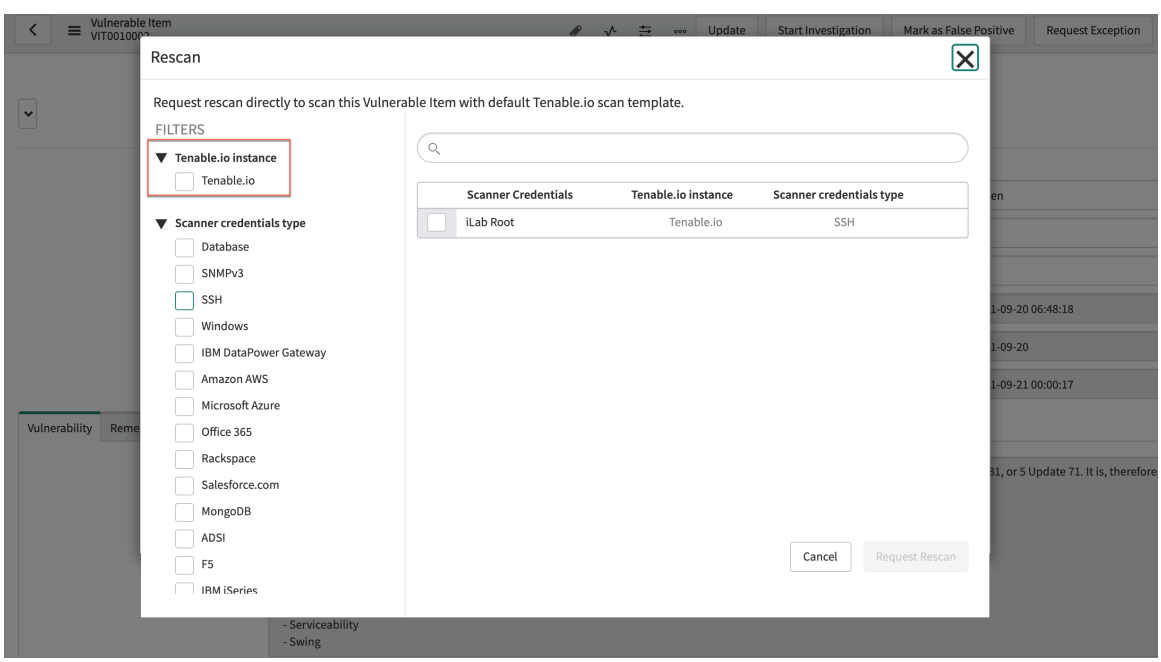
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sur un seul enregistrement de VI, le VI doit être dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent provenir du Tenable.io produit et se trouver dans un état autre que **Fermé**.
- Pour les enregistrements de tâches de **rattrapage** , seules les tâches de rattrapage d'un état autre que Fermé sont prises en charge. Tous les VI associés doivent être dans un état autre que **Fermé** et être utilisés Tenable.io comme source.
- Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du produit dans un Tenable.io état autre que **Fermé**.
- Sur les enregistrements d'éléments détectés, l'enregistrement doit avoir au moins un enregistrement de VI associé du produit dans un Tenable.io état autre que **Fermé**.
- Dans la liste Éléments vulnérables, vous pouvez sélectionner les éléments vulnérables individuels que vous souhaitez analyser à nouveau. Utilisez le menu Actions sur les lignes sélectionnées en bas à gauche de l'écran pour lancer la nouvelle analyse. Vous êtes invité à saisir vos informations d'identification.

4. Dans l'angle supérieur droit d'un enregistrement, cliquez sur **Analyser à nouveau**. Vous êtes invité à choisir l'instance ou les instances pour la nouvelle analyse et les informations d'identification du scanner que vous souhaitez utiliser pour accéder au scanner. Les informations d'identification affichées sont celles importées par l'intégration des informations d'identification de numérisation Tenable.io .
5. Dans la boîte de dialogue, sélectionnez l'instance et/ou les instances et les types d'informations d'identification que vous souhaitez utiliser.

   L'image suivante montre une instance d'intégration `Tenable.io` . Si vous avez plusieurs Tenable.io instances, elles sont toutes affichées sous la section `Tenable.io` du formulaire.



Champ	Description
Instance Tenable.io	Choisissez une Tenable.io instance d'intégration à partir de laquelle vous souhaitez lancer la nouvelle analyse. Toutes vos instances d'intégration s'affichent Tenable.io . Si un VI existe dans plusieurs instances d'intégration, vous pouvez

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	utiliser ce filtre pour limiter ou développer les instances que vous souhaitez analyser. **Remarque :** Si vous choisissez d'analyser à nouveau les VI à partir d'un enregistrement de tâche de rattrapage pour une seule instance d'intégration, seuls les VI actifs associés à cette tâche de rattrapage, pour cette instance, à l'aide des informations d'identification que vous sélectionnez sont analysés.
Filtre de type d'informations d'identification du scanner	Utilisez ce filtre pour afficher les informations d'identification par type.
Volet avec les informations d'identification du scanner, Tenable.io l'instance, le type d'informations d'identification du scanner	Il s'agit des informations d'identification du scanner disponibles importées à partir des Tenable.io produits. Choisissez une ou plusieurs informations d'identification à utiliser pour l'analyse.

6. Cliquez sur **Demander une nouvelle analyse**.

Un message s'affiche indiquant que votre analyse est en cours de traitement et qu'un enregistrement d'analyse parent a été créé. L'état de toutes les analyses enfants peut être consulté à tout moment sous les listes connexes Analyse des enregistrements VI, Tâche de rattrapage, TPE et SDI que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

Le champ État de l'enregistrement d'analyse parent est marqué comme terminé lorsque toutes les analyses enfants sont terminées avec succès. L'enfant analyse les données d'importation. Chaque analyse prend en charge une combinaison unique d'instance d'intégration, de TPE, d'adresse IP et d'ID réseau. Vous pouvez voir plusieurs analyses enfants sur un enregistrement d'analyse parent. Par exemple, le nombre maximum d'adresses IP qu'une analyse enfant peut prendre en charge est de 1 000. S'il existe 1 002 adresses IP pour un élément vulnérable, deux analyses enfants sont créées et répertoriées sur la liste connexe Analyses pour prendre en charge la demande. L'enregistrement d'analyse parent est un conteneur pour les analyses enfants et son état reflète l'état des analyses enfants.

Votre Now Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine correctement ou jusqu'à l'expiration de la période de suivi définie, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de votre Now Platform® nouvelle analyse a cessé, et non à la date à laquelle la nouvelle analyse elle-même s'est arrêtée. Tous les VI qui sont passés ou passeront à **l'état Fermé/Fixe** sont importés avec la prochaine importation planifiée de l'intégration Tenable.io des vulnérabilités corrigées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour les analyses présentant des erreurs, vous pouvez vérifier les analyses enfants sur l'enregistrement d'analyse parent. Affichez l'erreur dans la charge utile de réponse de l'analyse enfant.

Vous pouvez afficher les résultats mis à jour sur les enregistrements à partir desquels vous avez initié les analyses après la prochaine importation planifiée de l'intégration des vulnérabilités corrigées.

Mettre à jour les éléments de configuration avec l'identificateur de partition de réseau pour le Tenable Vulnerability Integration

Créez des éléments de configuration (CI) uniques pour les actifs de votre environnement qui partagent des adresses IP. Identifiez les actifs distincts dans votre environnement et mettez automatiquement à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous donner plus de détails sur vos vulnérabilités.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Par défaut dans l'application, l'adresse Réponse aux vulnérabilités IP est l'un des moyens d'identifier vos actifs. Dans certains cas, les actifs peuvent partager des adresses IP, mais ils sont stockés en tant que CI unique dans votre CMDB.

Par exemple, comme le montrent les tables suivantes, plusieurs actifs (CI) de votre environnement peuvent partager des adresses IP, mais ont des ID de réseau et de référentiel uniques. Toutefois, par défaut, ces ressources sont généralement identifiées et stockées comme un seul CI `(CI 1)` lors de la recherche d'adresse IP.

Recherche d'adresses IP et création de CI par défaut

Source	Adresse IP	Network_id	Élément de configuration
Tenable.io: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	Adresse IP	Repository_id	Élément de configuration
Tenable.sc: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Vous pouvez créer des CI individuels pour les actifs qui ont la même adresse IP afin de pouvoir les identifier en tant qu'actifs distincts. À partir d'une importation de données actualisée, vous pouvez mettre à jour vos CI existants avec une plus grande granularité incluant l'identificateur de partition de réseau [network_partition_identifier] en exécutant la tâche planifiée. *`Update existing discovered items with network partition identifier`*

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette tâche planifiée est désactivée par défaut. Activez cette fonctionnalité pour les intégrations Actifs et Vulnérabilités fixes et ouvertes pour les Tenable.io et Tenable.sc les produits dans l'assistant de configuration afin d'afficher cet identificateur dans vos enregistrements.

Lorsqu'elle est activée, cette tâche planifiée ajoute l'identificateur de partition de réseau [network_partition_identifier] aux enregistrements de CI existants à partir des données importées. Les CI existants créés par l'IRE sont également mis à jour. La tâche planifiée crée également des CI qui incluent l'identificateur de partition de réseau à partir de la prochaine importation. Vous pouvez également lancer la tâche à la demande pour mettre à jour vos données existantes.

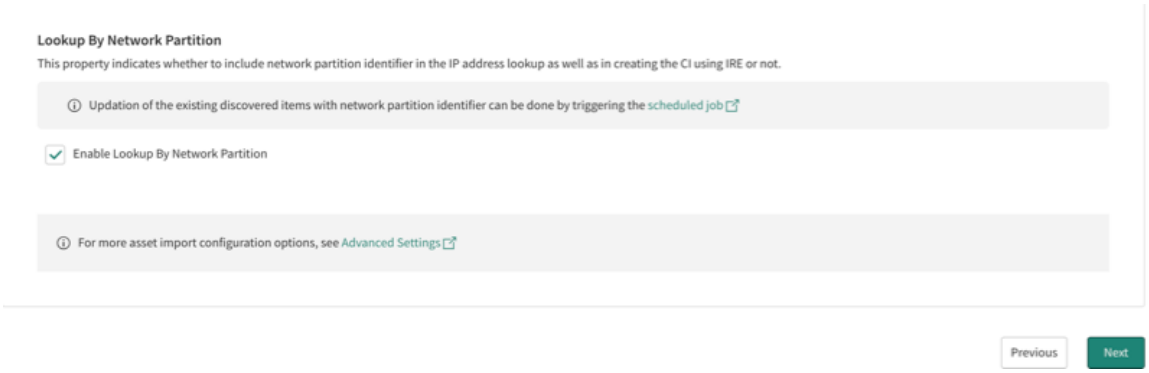
Lorsque vous effectuez une mise à niveau à partir de la version 14.0 et de Réponse aux vulnérabilités la version 2.2 de Tenable Vulnerability Integration, les modèles de classe CI CMDB (1.0.21.) sont pris en charge. Les modèles de classe ont l'identificateur de partition de réseau [network_partition_identifier] dans les règles d'identification Identification et rapprochement (IRE).

Option	Description
Exécutez les travaux planifiés sur demande.	Mettez à jour vos éléments détectés existants. Les CI de vos données Tenable existantes sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau. Les éléments détectés, les éléments vulnérables et les enregistrements de détection sont tous mis à jour avec les nouveaux CI.
Attendez les importations de données fraîches des intégrations avec les prochains travaux planifiés.	Créez des CI pour chaque nouvel actif à l'aide de l'identificateur de partition de réseau en commençant par la tâche planifiée suivante. Les enregistrements de CI, d'élément vulnérable et de détection sont tous mis à jour pour inclure la nouvelle granularité. De nouveaux CI sont créés lorsqu'aucune correspondance exacte n'est trouvée.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
2. Sélectionnez Tenable.io Intégrations ou Tenable.sc Intégrations.
3. **Modifiez** l'intégration requise.
4. Sélectionner **Configuration de l'importation d'actifs**.
5. Sélectionner **Activer la recherche par partition de réseau** case à cocher de la **Activer la recherche par partition de réseau** section.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Suivant**.

Les identificateurs de partition de réseau NETWORK_ID et les _ID REPOSITORY sont inclus et mettent à jour les CI existants ou créent des CI avec la tâche planifiée suivante.

Attribut d'identificateur de partition de réseau inclus dans la recherche d'adresses IP et la création de CI

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Éléments CI : actifs avec identificateur de partition de réseau
Tenable.io: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Source	Adresse IP	REPOSITORY_ID	CI pour les actifs sans identificateur de partition de réseau	Éléments CI : actifs avec identificateur de partition de réseau
Tenable.sc: Intégrations d'actifs et de vulnérabilités fixes et ouvertes	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Avec la tâche planifiée suivante, les règles de recherche d'identification CI Adresse IP et Adresse IP incomplète incluent automatiquement l'attribut d'identificateur de partition de réseau pour une importation de données à partir des intégrations Actifs et Vulnérabilités fixes et ouvertes pour les Tenable.io produits et Tenable.sc .

Après avoir activé la propriété système et enregistré les enregistrements, vous pouvez également mettre à jour vos éléments détectés existants avec des CI qui incluent l'identificateur de partition de réseau en lançant les travaux planifiés sur demande.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer les modifications pour l'intégration de vulnérabilité Tenable

Configurez les modifications facultatives et rationalisez certaines des données spécifiquement pour l'intégration d'importation des vulnérabilités Tenable dans l'intégration des vulnérabilités ServiceNow® Tenable.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Cet ensemble de tâches nécessite du codage et des connaissances avancées sur le Now Platformfichier .

Suivez ces étapes pour créer des importations séparées par domaine pour les intégrations de vulnérabilités Tenable. L'exemple suivant concerne l'intégration des vulnérabilités ouvertes Tenable.io, mais ce contenu est applicable aux autres intégrations Tenable.

Procédure

1. Créez un domaine.
2. Pour chaque domaine que vous créez, créez un utilisateur et affectez-le à ce domaine.

   Considérez cet utilisateur comme un espace réservé run_as pour le domaine dans Tenable.io.

3. Intégration des vulnérabilités ouvertes.
   L'utilisateur est l'équivalent de la VR. Utilisateur système dans le domaine global et doit disposer des rôles suivants : sn_vul.tenable_configure_integration, import_admin et sn_vul.vulnerability_write. Cet utilisateur doit accéder aux sources de données, aux cartes de transformation et aux données de vulnérabilité.

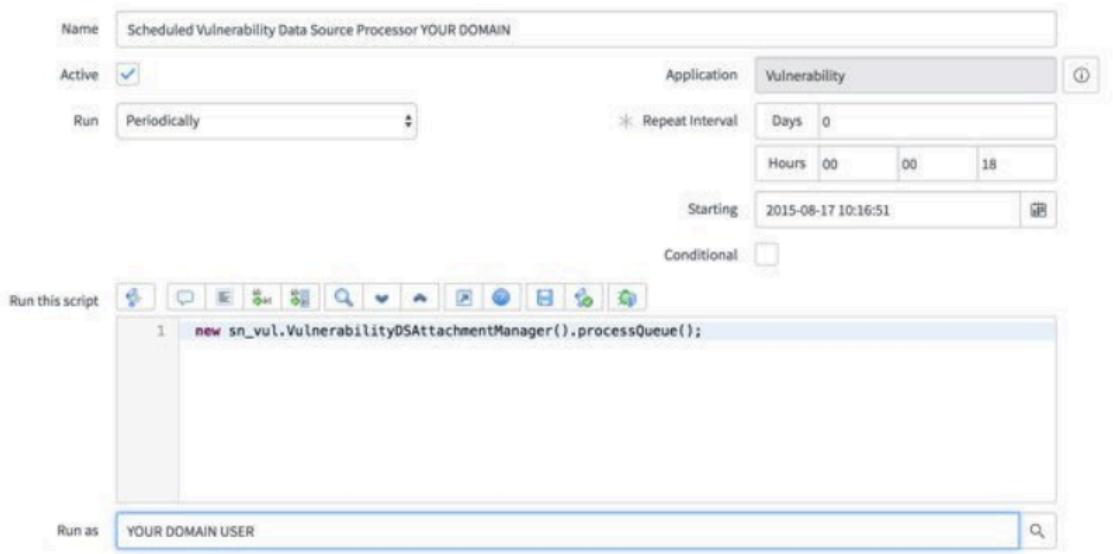
   Remarque : Considérez cet utilisateur comme spécifique à ce rôle. L'utilisateur ne doit pas avoir d'autre but

4. Dans chaque domaine, créez une tâche planifiée en copiant le processeur de source de données de vulnérabilité planifiée qui se trouve sous **Définition du système** > **Travaux planifiés**.
5. Ajoutez le domaine au nom pour identifier la tâche planifiée.
6. Remplacez l'utilisateur run_as par l'utilisateur que vous avez créé à l'étape précédente.

   Remarque : Modifiez l'action d'interface utilisateur suivante afin que l'intégration s'exécute dans le domaine de l'utilisateur run_as.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Modifiez l'action d'interface utilisateur Exécuter maintenant dans l'intégration des vulnérabilités ouvertes Tenable.io pour ajouter ce bloc de code en haut du fichier.
//sys_id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){current.run_as = gs.getUserID();}

Remarque : Modifiez les includes de script suivants afin que l'intégration s'exécute dans le domaine de l'utilisateur run_as.

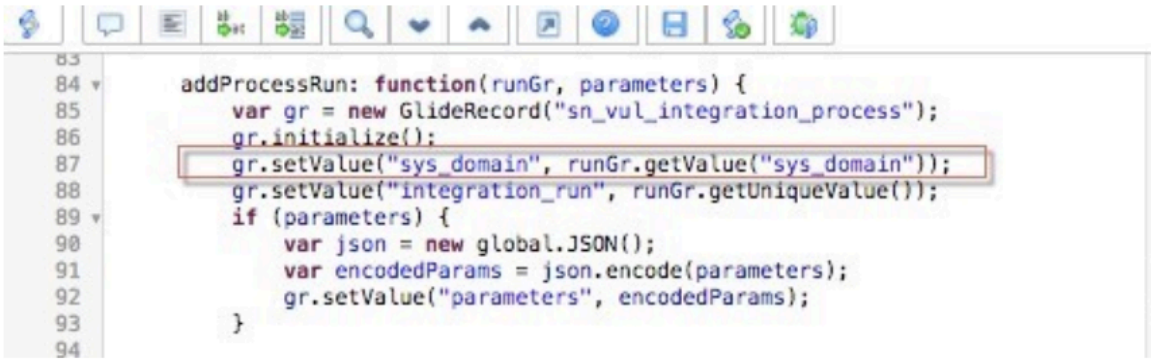
8. Modifiez la méthode d'include de script VulnerabilityIntegrationUtils addIntegrationRun pour ajouter le code en surbrillance.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Modifiez la méthode d'include de script VulnerabilityIntegrationUtils addProcessRun pour ajouter le code en surbrillance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Modifier la méthode d'include de script DataSourceVulnReportRefreshProcessor _processFromDataSourceGroups pour modifier ce code d'origine : Code _processFromDataSourcesGroups d'origine en Code _processFromDataSourcesGroups modifié.
11. Modifiez la méthode d'include de script VulnerabilityDSAttachmentManager, queueItem pour ajouter les blocs de code en surbrillance suivants, queueItem, _getNext _processQueueEntry fonction.

    Vous êtes prêt pour les importations de détections d'hôtes séparées par domaine.

    Désactiver les calculateurs avant l'importation

    Suivez ces étapes pour désactiver le calculateur par défaut s'il n'est pas utilisé. Si vous n'utilisez pas de calculateurs de vulnérabilité, il est préférable de désactiver les calculateurs par défaut en plus de tous les autres que vous avez définis. Les calculateurs de vulnérabilité s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est consulté et peuvent avoir un impact sur les performances de l'instance.

    Rôle requis : sn_vul.vulnerability_admin.

12. Accédez à la **Tout** > **Vulnérabilité** > **Administration** > **Calculateurs de vulnérabilités**.
13. Ouvrez le groupe Impact de vulnérabilité.
14. Ouvrez le calculateur de score et d'impact basé sur le service.
15. Désélectionnez le champ Actif pour désactiver le calculateur.
16. Cliquez sur Mettre à jour.

    Vous avez désactivé le calculateur par défaut.

    Désactiver les règles métier basées sur la notification avant l'importation initiale

    Suivez ces étapes pour désactiver la désactivation des règles métier liées aux notifications avant l'importation initiale de l'enregistrement. Lors de l'importation initiale des enregistrements, certaines règles métier liées aux notifications peuvent générer de nombreuses notifications, ce qui a un impact sur les performances. Ces règles métier doivent être modifiées pour les désactiver lors de l'importation.

    Le rôle requis est sn_vul.vulnerability_admin.

17. Accédez à la **Tout** > **Définition du système** > **Règles métier**.
18. Recherchez les notifications de CI affectés.
19. Ouvrez la règle métier et insérez la condition suivante : *`current.sys_class_name != "sn_vul_vulnerable_item"`*.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

20. Cliquez sur **Mettre à jour**.
21. Répétez cette procédure pour les règles métier suivantes :
    - Notifications des centres de coûts affectés
    - Notifications des groupes affectés
    - Notifications d'emplacements affectés

    Remarque : Une fois l'importation d'enregistrement initiale terminée, vous pouvez réactiver ces règles métier. Cependant, envisagez de les laisser handicapés. Elles peuvent générer un grand nombre de notifications et avoir un impact sur les performances de votre instance.

    Modifier une date de début initiale

    Procédez comme suit pour modifier une date de début initiale. Lors de l'installation à l'aide de l'Assistant de configuration, vous définissez une date de début initiale pour les intégrations Tenable. Vous pouvez réinitialiser cette date de début dans l'Assistant de configuration ou à partir de l'intégration principale, comme indiqué dans les étapes suivantes.

22. Accédez à la **Tout** > **Intégration de vulnérabilité tenable** > **Administration** > **Intégrations**.
23. Cliquez sur n'importe quelle intégration.
24. Cliquez sur Détails de l'intégration.
25. Définissez le champ Heure de début sur une valeur passée, de sorte que toutes les vulnérabilités analysées et détectées depuis cette heure soient détectées.

    Si vous avez configuré Tenable à l'aide de l'assistant de configuration, le champ Heure de début est pré-rempli, initialement jusqu'à trois mois avant la date d'aujourd'hui, puis jusqu'à la date d'aujourd'hui. Remarque : Envisagez de définir la valeur à un maximum d'un mois dans le passé. Cela permet d'éviter qu'une grande quantité de données ne dépasse les limites de débit de l'API de Tenable et de déclencher des délais d'exécution.

26. Cliquez sur **Envoyer** ou **Mettre à jour**.
27. Facultatif : Cliquez sur **Exécuter maintenant** pour l'exécuter immédiatement.

Conformité de la configurationCorrection

Conformité de la configuration Le rattrapage est avant tout un processus manuel complété par des travaux planifiés (intégrations), des tâches de rattrapage, des workflows et des demandes de changement.

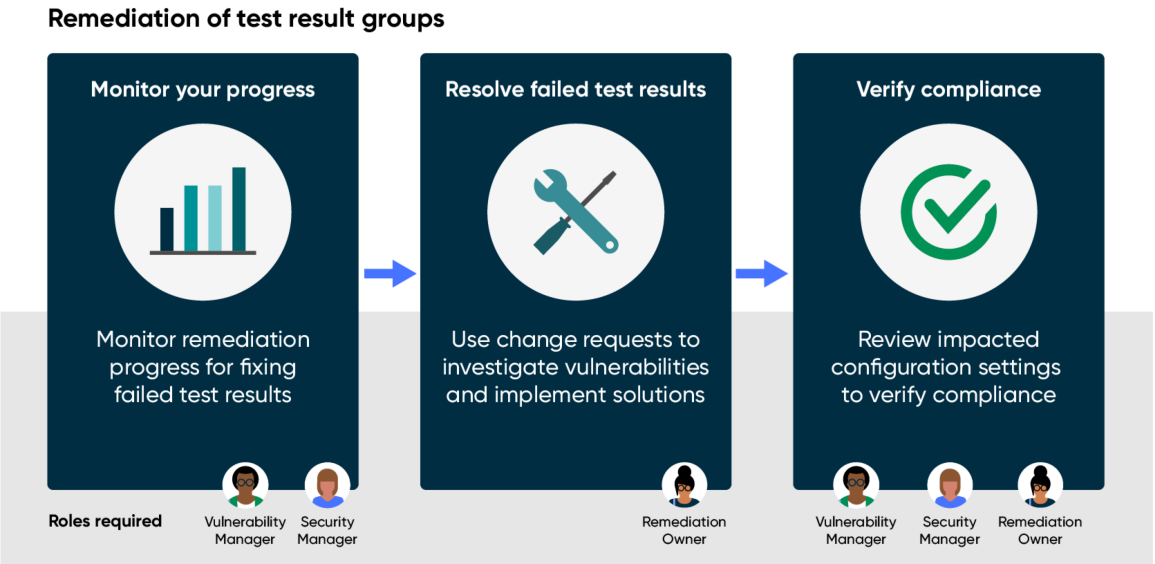
Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Des modules d'extension SCA tiers distincts acquièrent et transforment des données au format Conformité de la configuration. Avant de pouvoir Conformité de la configuration corriger des éléments de configuration, vous devez installer une intégration de scanner tiers et effectuer au moins une analyse réseau.

Utilisez les demandes de changement pour corriger les échecs de test individuels à partir des tâches de rattrapage.

Les états des tâches de rattrapage passent automatiquement à mesure que les demandes de changement associées traversent leur cycle de vie avec Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage. Les utilisateurs disposant du rôle ITIL peuvent créer et gérer des demandes de changement directement à partir des tâches de rattrapage.

Créer manuellement une tâche de Conformité de la configuration rattrapage

Vous pouvez créer manuellement une tâche de rattrapage à partir du module **Tâches de rattrapage** et effectuer un rattrapage.

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
L'utilisation des règles de tâche de rattrapage remplit automatiquement l'onglet **Résultats des tests** . La création manuelle est utile pour un groupe qui n'a pas besoin d'une règle ou d'être répété.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

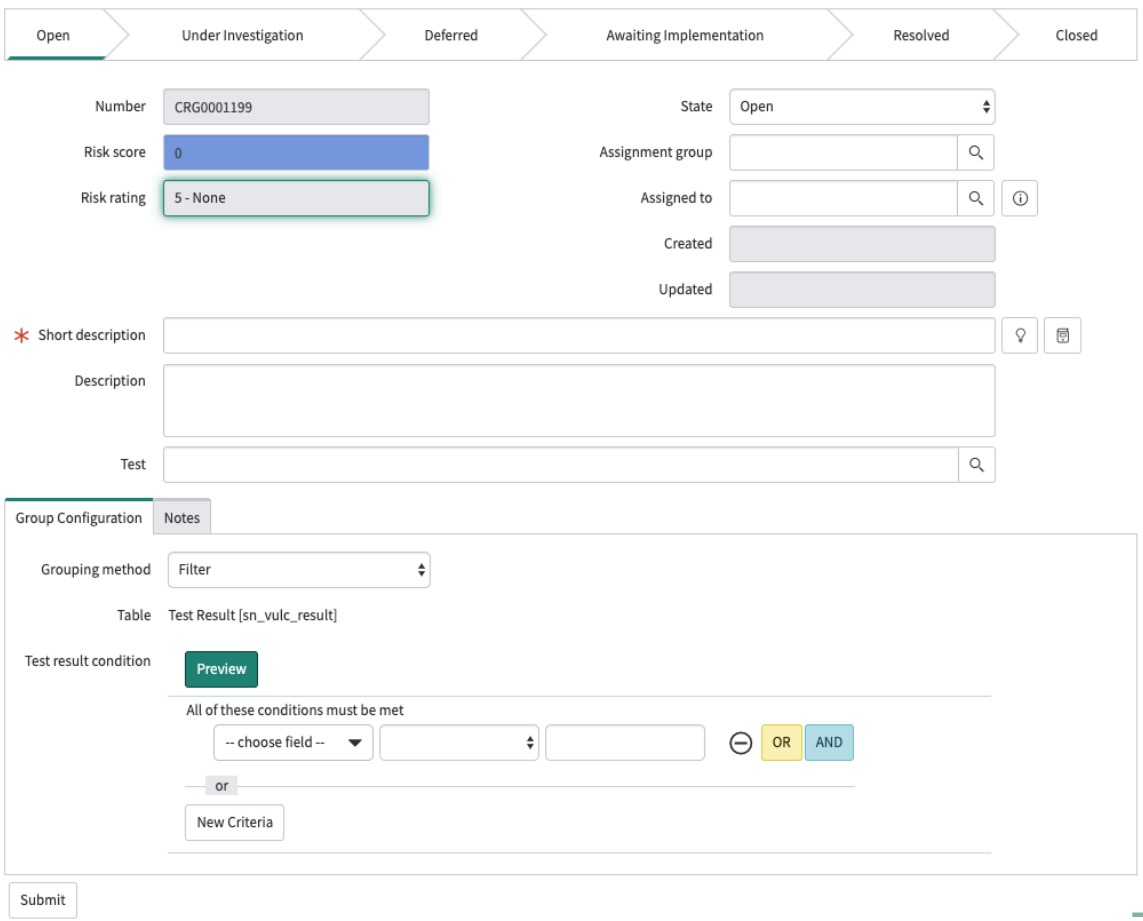
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Tâches de remédiation**.
2. Dans le panneau de navigation, cliquez sur **Mes tâches ouvertes** ou **Toutes les tâches ouvertes** pour afficher la liste.
3. Cliquez sur **Nouveau**.

Formulaire de tâche de rattrapage



4. Renseignez les champs du formulaire de tâche de rattrapage comme il convient.

Formulaire de tâche de rattrapage

Champ	Description
Numéro	ID affecté automatiquement dans le système.
Score du risque	Renseigné automatiquement par le calculateur de score de risque. Il s'agit d'un score de risque de déploiement. Ce score de risque est pondéré : 85 % du score du score de risque maximal pour tous les résultats des tests ne sont pas « Fermés » (Ouvert, En cours d'examen, En attente d'implémentation, Différé, Résolu) et 15 % du score provient du nombre de résultats des tests qui ne sont pas « Fermés ».
Cote de risque	Renseigné automatiquement par le calculateur de score de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

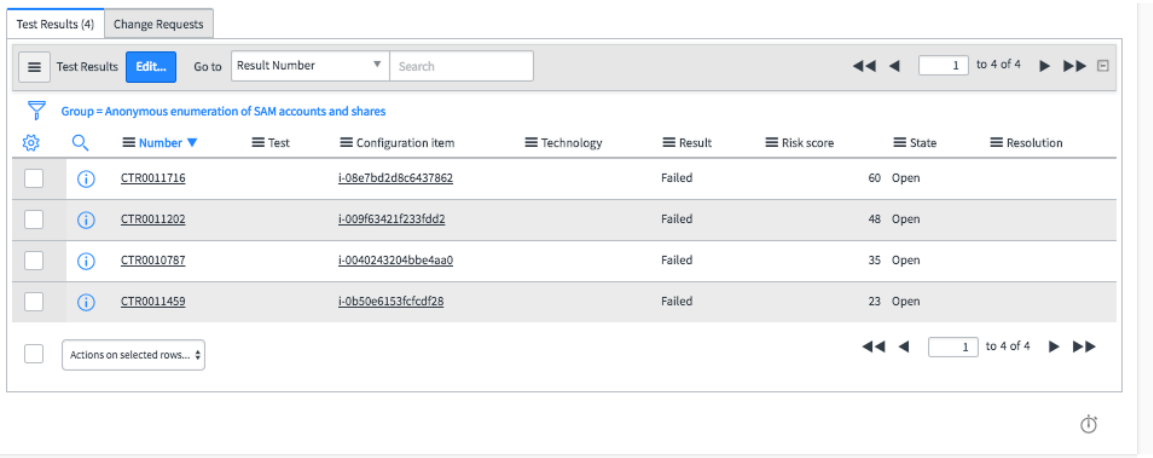
Champ	Description
	Basé sur une plage de scores de risque sur une échelle numérique de 1 à 5 qui évalue le risque global en fonction d'une plage de scores de risque allant de 1 - Critique à 5 - Aucun. Ce champ remplace le champ Priorité dans les versions précédentes.
État	**Initialement ouvert** correspond à l'état de rattrapage du groupe. Pour plus d'informations, consultez Conformité de la configuration États.
Groupe d'affectation	Affectez la tâche de rattrapage à un groupe de rattrapage.
Affecté à	Affectez du personnel pour corriger la tâche de rattrapage.
Créé	Date à laquelle vous avez créé ce groupe.
Mis à jour	Date à laquelle vous avez mis à jour ce groupe.
Description brève	Nom de la tâche de rattrapage.
Description	Description de cette tâche de rattrapage.
Test	Sélectionnez un test de configuration pour cette tâche de rattrapage.
Onglets associés	
Configuration du groupe	Méthodes de regroupement à utiliser : ◦ Manuel (par défaut) : ◦ Règle de filtre ou de groupe : Table : présélectionnée comme Résultat du test [sn_vulc_result] Condition de résultat du test : choisissez les filtres à utiliser. **Remarque :** Le lien Condition de correspondance des enregistrements au-dessus des conditions de filtre affiche les enregistrements de résultats des tests que vous avez choisis dans une nouvelle fenêtre. Cliquez sur **Aperçu** pour afficher le nombre de résultats renvoyés par vos critères de filtre avant d'enregistrer le nouveau groupe. La liste connexe Résultats des tests doit être créée manuellement en cliquant sur le bouton **Modifier** dans l'onglet **connexe Résultats des tests** .
Notes	Notes de travail relatives à cette tâche de rattrapage.

5. Cliquez avec le bouton droit dans l'en-tête pour **enregistrer** ou cliquez sur **Soumettre** pour enregistrer et revenir à la liste des tâches de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affiche les listes connexes **Résultats des tests** et **Demande de changement** .



Créer manuellement une Conformité de la configuration tâche de rattrapage à partir de la liste Résultats des tests

Vous pouvez créer manuellement une tâche de rattrapage à partir de la liste **des résultats des tests** et effectuer un rattrapage à partir de la tâche de rattrapage résultante.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Cette méthode nécessite de sélectionner les résultats des tests à inclure et de créer le groupe à partir du menu **Actions sur les lignes sélectionnées...** Cette méthode est idéale pour les résultats qui ne sont pas facilement filtrés ou pour les situations dans lesquelles vous souhaitez spécifier des résultats de test pour le rattrapage.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

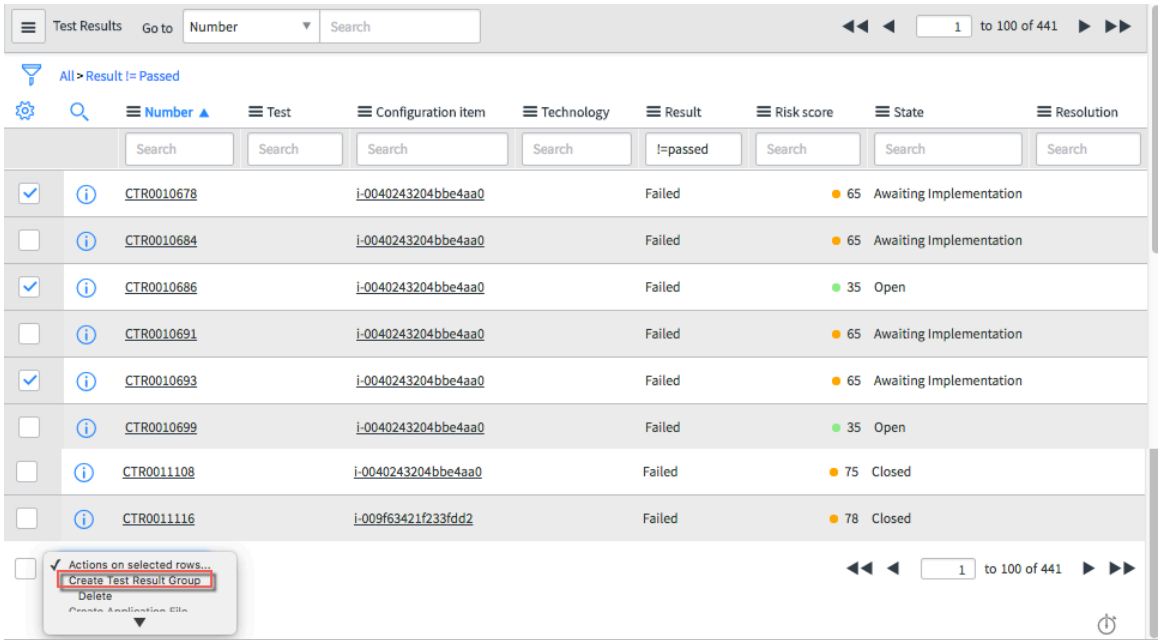
Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

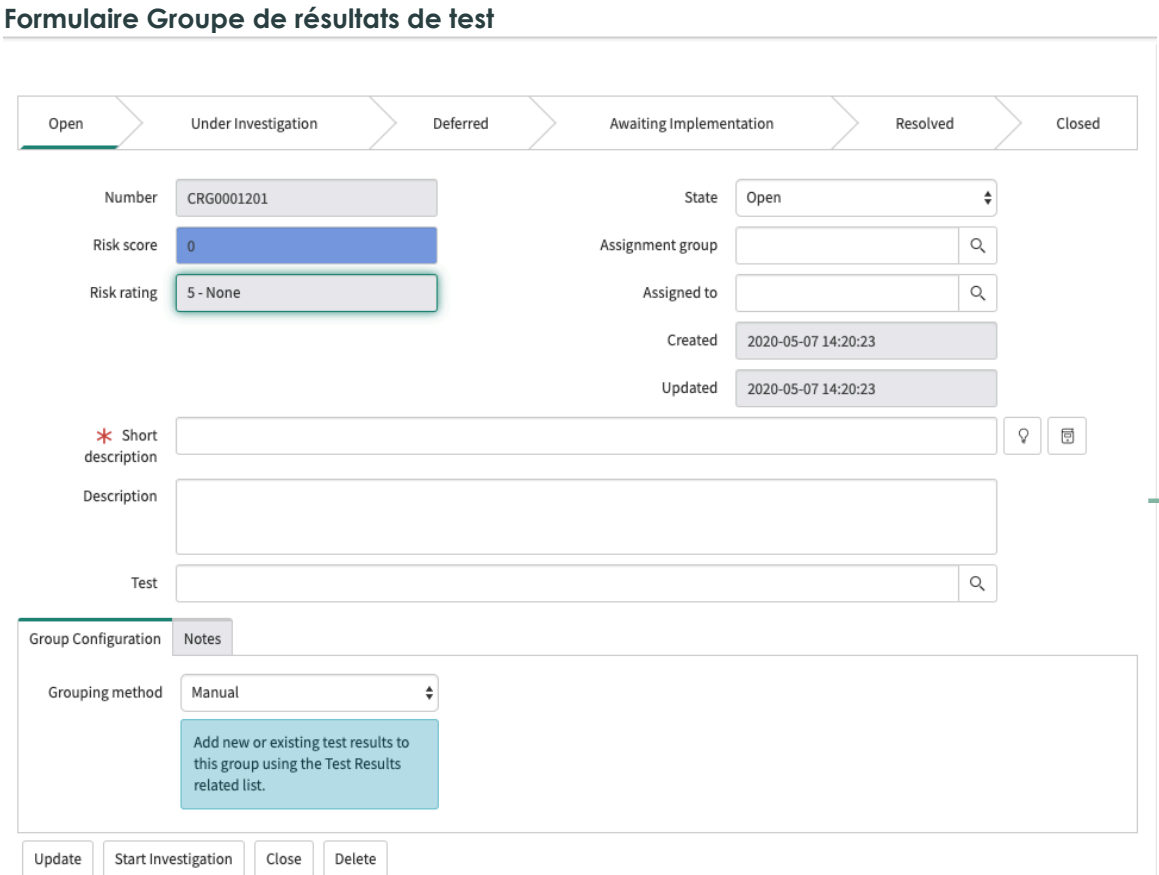
1. Accédez à la **Tout** > **Configuration Compliance** > **Résultats des tests**.
2. Dans le panneau de navigation, sélectionnez un module Résultat de test pour ouvrir une liste.
3. Sélectionnez les résultats des tests à inclure dans le groupe en cochant la case à côté de chacun.
4. Ouvrez le menu **Actions sur les lignes sélectionnées...** en bas de la liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



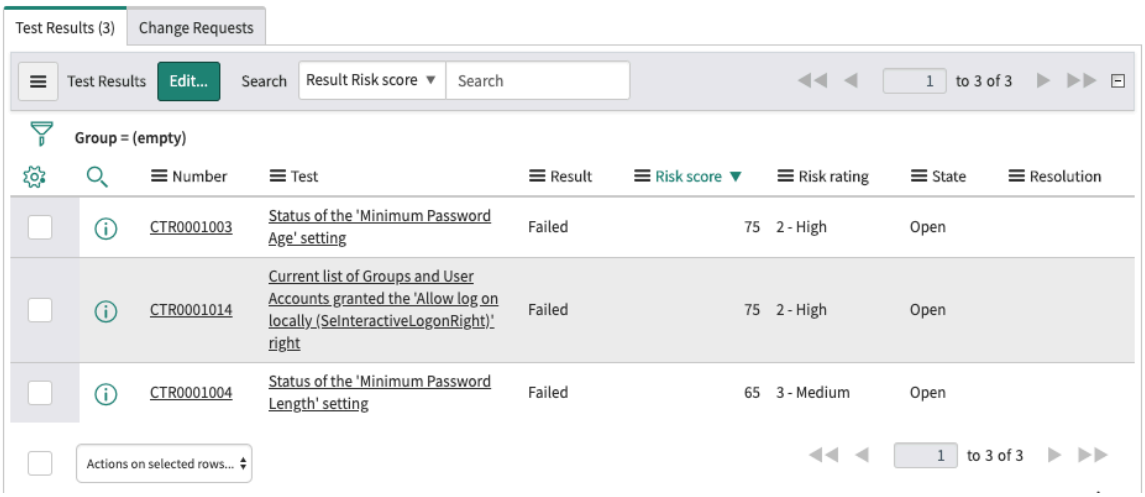
5. Choisissez **Créer une tâche de rattrapage**.
   La tâche de rattrapage est créée et s'ouvre.



Les résultats des tests que vous avez sélectionnés pour le groupe sont affichés dans la liste connexe Résultats des tests avec toutes les demandes de changement associées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Renseignez les champs du formulaire comme il convient.

Champ	Description
Numéro	ID affecté automatiquement dans le système.
Score	Renseigné automatiquement par le calculateur de déploiement de score de risque. Il s'agit d'un score de risque de déploiement. Ce score de risque est pondéré : 85 % du score du score de risque maximal pour tous les résultats des tests ne sont pas « Fermés » (Ouvert, En cours d'examen, En attente d'implémentation, Différé, Résolu) et 15 % du score provient du nombre de résultats des tests qui ne sont pas « Fermés ».
Évaluation	Renseigné automatiquement par le calculateur de déploiement de score de risque. Basé sur une plage de scores de risque sur une échelle numérique de 1 à 5 qui évalue le risque global en fonction d'une plage de scores de risque allant de 1 - Critique à 5 - Aucun. Ce champ remplace le champ Priorité dans les versions précédentes.
Score de risque historique	Renseigné automatiquement par le calculateur de déploiement de score de risque. Score de risque inhérent pour tous les résultats des tests réussis dans une tâche de rattrapage. Ce champ affiche la quantité de risque qui a été rattrapée par un groupe de tests et ne s'affiche qu'une fois qu'un groupe de tests est dans l'état « Fermé » et que le score de risque est de zéro.
État	**Initialement ouvert** correspond à l'état de rattrapage du groupe. Pour plus d'informations, consultez Conformité de la configuration États.
Groupe d'affectation	Affectez la tâche de rattrapage à un groupe de rattrapage.
Affecté à	Affectez du personnel pour corriger le groupe.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Créé	Date à laquelle vous avez créé ce groupe.
Mis à jour	Date à laquelle vous avez mis à jour ce groupe.
Description brève	Nom de la tâche de rattrapage.
Description	Texte descriptif de cette tâche de rattrapage.
	Sélectionnez un test de configuration pour cette tâche de rattrapage.
Onglets associés	
Configuration du groupe	Méthodes de regroupement à utiliser : ◦ Manuel (par défaut) ◦ Filtre Table : présélectionnée comme Résultat de test Condition de résultat du test : choisissez les filtres à utiliser. **Remarque :** Le lien Condition de correspondance des enregistrements au-dessus des conditions de filtre affiche les enregistrements de résultats des tests que vous avez choisis dans une nouvelle fenêtre. Cliquez sur **Aperçu** pour afficher le nombre de résultats renvoyés par vos critères de filtre avant d'enregistrer le nouveau groupe.
Notes	Notes de travail relatives à cette tâche de rattrapage.
Listes connexes	
Résultats des tests	Résultats des tests inclus dans ce groupe.
Demandes de changement	Demandes de changement associées à ce groupe.

7. Cliquez avec le bouton droit sur l'en-tête pour **enregistrer** ou cliquez sur **Soumettre** pour enregistrer et revenir à la liste des tâches de rattrapage.

Créer une demande de changement dans Conformité de la configuration

Vous pouvez créer une demande de changement à partir d'une tâche de rattrapage dans l'application Conformité de la configuration .

Avant de commencer
Rôle requis : utilisateur ayant le rôle itil

Pourquoi et quand exécuter cette tâche
En tant que spécialiste informatique ou du rattrapage, créez une demande de changement (CHG) directement à partir d'une tâche de rattrapage pour tous les résultats des tests du groupe. Créez une demande de changement avec des informations pré-remplies pour accélérer votre enquête sur les vulnérabilités qui nécessitent une intervention manuelle.

Vous pouvez créer, approuver, implémenter, examiner et fermer des demandes de changement directement à partir des tâches de rattrapage qui vous sont affectées. Vous

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pouvez créer trois types de demandes de changement avec des informations pré-remplies à partir d'une tâche de rattrapage :

Standard

Un changement pré-autorisé à risque faible, relativement commun et qui suit une procédure ou une instruction de travail spécifique.

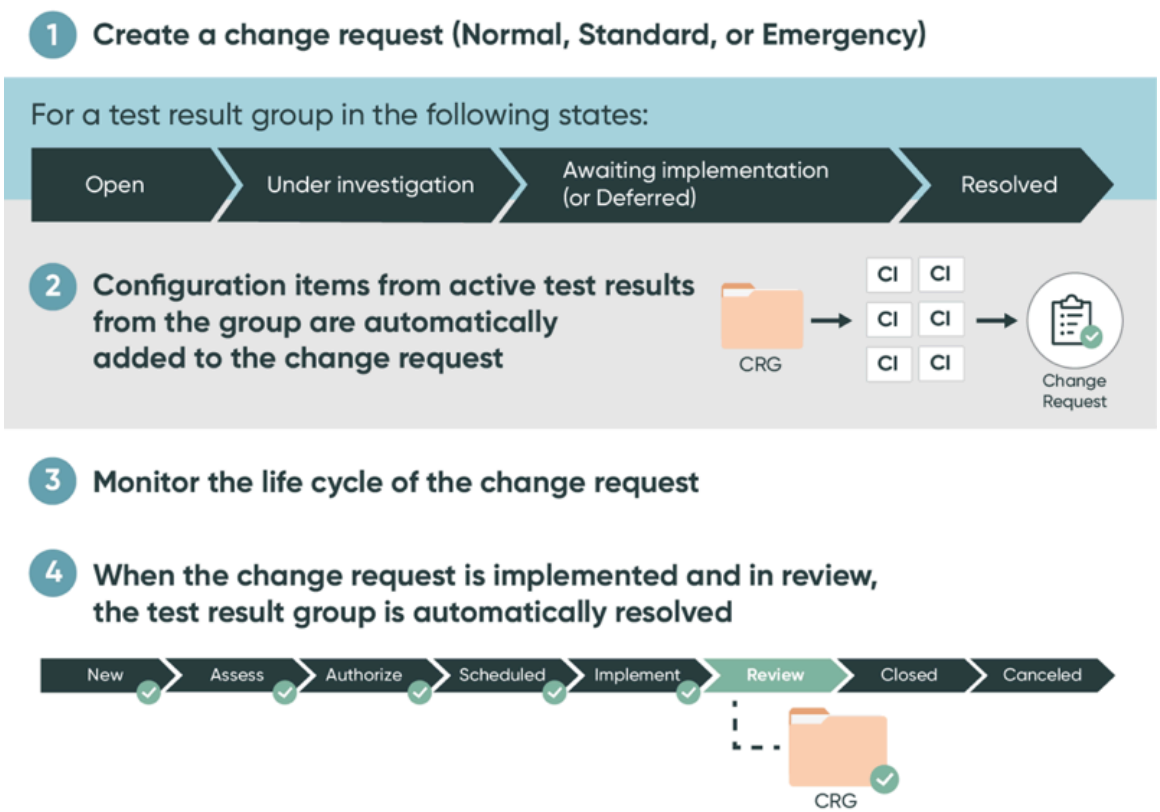
Normal

Les demandes de changement normal suivent un processus prescriptif qui requiert deux niveaux d'approbation avant leur implémentation, revue et fermeture.

Urgence

Un changement pour résoudre un incident majeur.

L'image suivante illustre le flux de base pour la création d'une demande de changement à partir d'une tâche de rattrapage. Les étapes détaillées de ce flux suivent l'image.



À partir de la version 19.0 de Réponse aux vulnérabilités, vous pouvez créer des demandes de changement pour les tâches de remédiation à partir de l'espace de travail de remédiation informatique. Pour plus d'informations, consultez Créer une demande de changement dans Espace de travail de remédiation IT.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Tâches de remédiation** > **Mes groupes ouverts**.
   La liste des tâches de rattrapage affectées à vos groupes s'affiche.
2. Dans la colonne Nombre, cliquez sur la tâche de rattrapage pour laquelle vous souhaitez créer une demande de changement.
   Vous pouvez créer des demandes de changement à partir des tâches de rattrapage dont l'état n'est pas **Fermé** ou **En cours de révision**.

   L'enregistrement de la tâche de rattrapage s'affiche.
3. En haut à droite de l'enregistrement, cliquez sur **Créer un changement**.
   Le formulaire de demande de changement s'affiche.
4. Renseignez les champs.
   a. Dans la liste du champ **S'applique à, choisissez-en** un pour continuer.

Option	Description
Tous les résultats des tests actifs dans ce groupe	Si cette option est sélectionnée, tous les résultats des tests actifs de cette tâche de rattrapage avec un état autre que **Fermé** sont ajoutés automatiquement à la demande de changement après que vous avez cliqué sur **Créer un changement**.
Tous les résultats des tests actifs dans ce groupe correspondant à un ensemble de conditions	Si cette option est sélectionnée, le générateur de conditions s'affiche. Entrez des critères de filtre pour identifier les résultats des tests que vous souhaitez pour la nouvelle demande de changement. Un exemple de filtre que vous pourriez créer localiserait uniquement les résultats des tests du groupe qui correspondent à un état et à un score de risque spécifiques : L'état est **Ouvert** et le score de risque est supérieur à **50**.

5. Pour la case à cocher **Ajouter des CI au CR, choisissez-en** une pour continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Case à cocher sélectionnée	Cette valeur est sélectionnée par défaut. Si la case est cochée, tous les éléments de configuration (CI) appartenant aux résultats des tests actifs de cette tâche de rattrapage sont ajoutés à cette demande de changement. Le résultat du test passe à **l'état En attente d'implémentation**.
Case décochée	Décochez la case si vous ne souhaitez pas que les CI des résultats des tests actifs de cette tâche de rattrapage soient ajoutés à la nouvelle demande de changement. La tâche de rattrapage reste dans son état actuel.

6. Dans la liste du champ **Type de changement** , choisissez-en un pour continuer.

Option	Description
Urgence	Un changement pour résoudre un incident majeur.
Normal	Type de changement utilisé pour implémenter tout changement apporté à un service qui n'est ni standard ni urgent.
Standard	Demande de changement préautorisée et à faible risque fréquemment implémentée. Les demandes de changement standard approuvées peuvent être prédéfinies dans un catalogue de modèles pour améliorer l'accès et le processus de demande d'un changement standard. Si cette option est sélectionnée, deux champs s'affichent. Sélectionnez une option dans chaque liste pour remplir les champs suivants : ◦ **Catégorie de changement** : sélectionnez une catégorie pour le changement dans votre catalogue existant, par exemple, `Matériel`, `Changements standard de serveur`, `Logiciel`. ◦ **Modèle de changement** : sélectionnez un modèle disponible pour les demandes de changement avec des tâches de prise en charge prédéfinies dans votre catalogue. Pour plus d'informations sur les catégories, les modèles et les types de changement de demande de changement ITSM, consultez Types de changement .

La fonctionnalité lit automatiquement les types de demandes de changement que vous configurez dans votre catalogue dans ITSM Change Management. Par exemple, si vous

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

changez le nom de vos demandes de changement standard dans ITSM de `Standard` à `Préapprouvé`, votre nouveau nom s'affiche automatiquement dans la liste Type de changement du formulaire Créer une demande de changement.

7. Les champs de la section Aperçu de la demande de changement du formulaire sont pré-remplis avec les informations issues de la tâche de rattrapage.
   Si nécessaire, modifiez ces champs.
8. Cliquez sur **Créer un changement**.
   La demande de changement s'affiche. Dans la liste connexe CI affectés, les CI des résultats des tests qui correspondent à vos critères sont affichés. Si la demande de changement nécessite une approbation, le bouton **Demander l'approbation** s'affiche.

   Une fois la demande de changement créée, le groupe de résultats des tests passe à l'état **En attente d'implémentation** . Une fois la demande de changement de cette tâche de rattrapage résolue, s'il n'y a pas d'autres demandes de changement ouvertes associées à cette tâche de rattrapage, la tâche de rattrapage passe également à l'état **Résolu** .

   Consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage pour plus d'informations.

   Remarque : Vous pouvez toujours déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre sur leurs enregistrements respectifs lorsque la synchronisation d'état est activée, mais lorsque le système enregistre qu'une demande de changement a changé d'état, ou que vous ajoutez une demande de changement ou que vous la supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la tâche de rattrapage des états `Fermé ou Différé`.

Associer une tâche de rattrapage à une demande de changement existante

Associez une tâche de rattrapage dans Conformité de la configuration l'application à une demande de changement existante.

Avant de commencer

Rôle requis : un utilisateur ayant le rôle itil

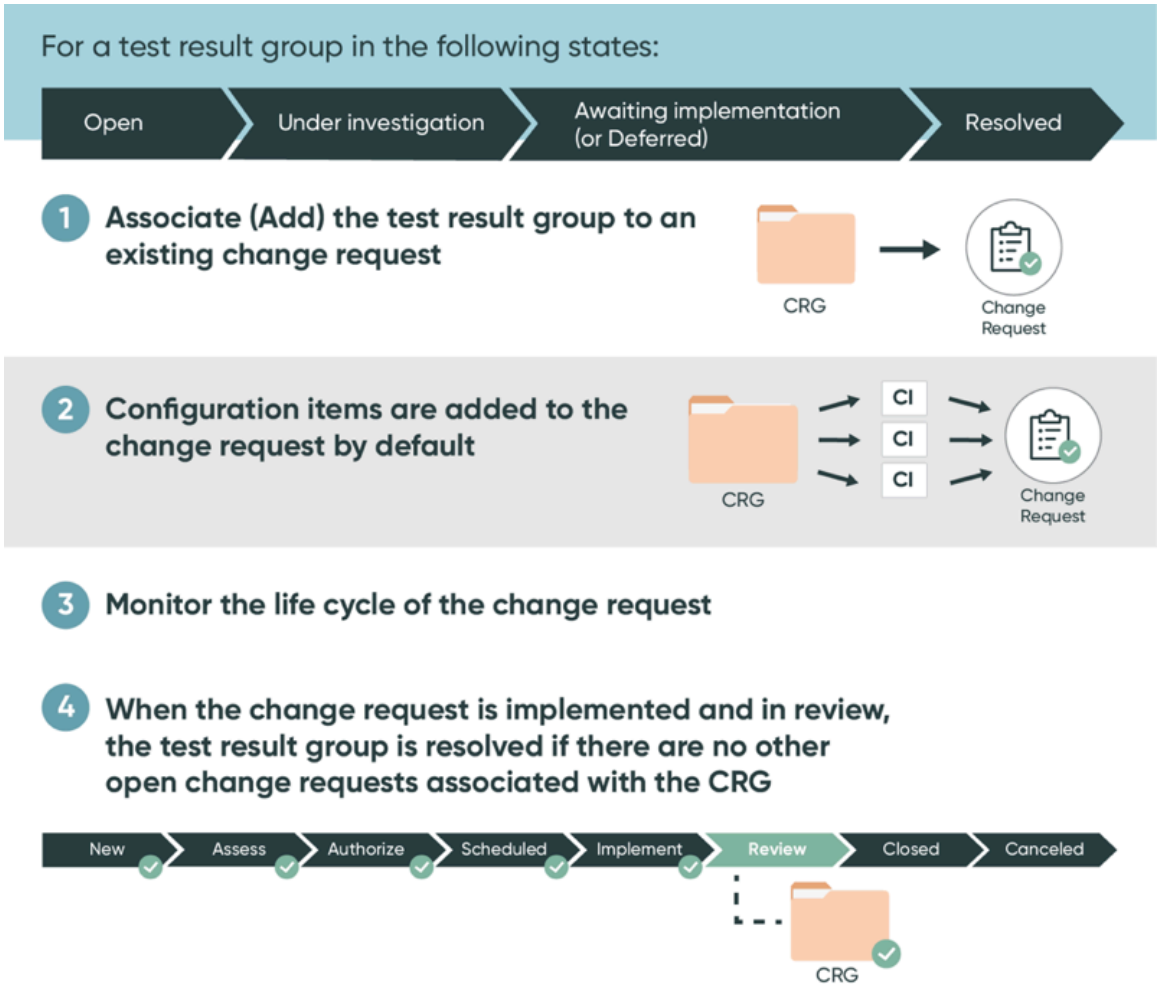
Pourquoi et quand exécuter cette tâche

En tant que spécialiste de l'informatique ou du rattrapage, évitez de créer des demandes de changement (CHG) en double pendant que vous travaillez à la résolution de vos tâches de rattrapage en associant une tâche de rattrapage (RT) à une demande de changement déjà disponible dans votre instance.

Vous pouvez associer des tâches de rattrapage qui vous sont affectées ou qui sont affectées à votre groupe d'affectation à des demandes de changement existantes directement à partir des enregistrements de tâches de rattrapage. L'image suivante illustre le flux de base pour associer une demande de changement existante à une tâche de rattrapage. Les étapes détaillées de ce flux suivent l'image.

Remarque : Vous pouvez associer une demande de changement existante à une tâche de rattrapage dans n'importe quel état autre que **Annulé** (**Ouvert**, **En cours d'examen**, **En attente d'implémentation**, **Fermé** et **Différé**). Les demandes de changement, y compris celles fermées au cours des 90 derniers jours, peuvent être associées à partir du formulaire. Lorsque vous associez une demande de changement à une tâche de rattrapage existante, seuls les résultats des tests actifs et leurs éléments de configuration sont ajoutés à la demande de changement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Tâches de remédiation** > **Mes tâches ouvertes**.
   La liste des tâches de rattrapage affectées à vos groupes s'affiche.
2. Dans la colonne Nombre, cliquez sur la tâche de rattrapage pour laquelle vous souhaitez créer une demande de changement.

   L'enregistrement de la tâche de rattrapage s'affiche.
3. En haut à droite de l'enregistrement, cliquez sur **Créer un changement**.
   Le formulaire de demande de changement s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Faites défiler l'écran jusqu'à la liste connexe Demandes de changement et sélectionnez-la.
   Toutes les demandes de changement associées à la tâche de rattrapage sont affichées avec le bouton **Ajouter** .
5. Cliquez sur **Ajouter**.
   La boîte de dialogue Ajouter une demande de modification existante au groupe de résultats de test s'affiche.
6. Cliquez sur l'icône de recherche et sélectionnez un élément dans la liste.
   Vous pouvez filtrer la liste qui s'affiche pour affiner votre recherche.
7. Cliquez sur **Envoyer**.
   Le TRG est affiché avec un message indiquant que la demande de changement a été associée avec succès à la tâche de rattrapage. La nouvelle demande de changement s'affiche sous la liste connexe des demandes de changement. Les CI de la tâche de rattrapage sont, par défaut, ajoutés à la demande de changement et affichés dans la liste connexe CI affectés. Vous pouvez également ajouter des CI à la demande de changement à partir de cette liste connexe. Un message indique le nombre de résultats des tests qui ont été transférés vers le nouveau groupe, et le nouveau TRG s'affiche.

   Remarque : Pour moins de 200 résultats de test, l'opération de division est effectuée de manière synchrone et les résultats des tests sont affichés dans le nouveau groupe.

   Au-delà de 200 résultats des tests, l'opération de division est effectuée de manière asynchrone en arrière-plan, et il peut s'écouler quelques secondes avant que les résultats des tests n'apparaissent dans le nouveau groupe. Le message suivant s'affiche également : `n résultats des tests seront transférés de TRGxxxxxxx vers le nouveau groupe de résultats de test GRCxxxxx sous peu.`

Vous pouvez associer n'importe quelle demande de changement à la tâche de rattrapage, avec les exceptions suivantes :

- Demandes de changement à l'état **Annulé** .
- Demandes de changement à l'état **Fermé** datant de plus de 90 jours.
- Demandes de changement déjà associées au TRG. Le système ne vous permettra pas d'associer une demande de changement qui est déjà associée au TRG.

Une fois la demande de changement de cette tâche de rattrapage résolue, s'il n'y a pas d'autres demandes de changement ouvertes associées à cette tâche de rattrapage, la tâche de rattrapage passe également à l'état**Résolu** .

Remarque : Vous pouvez toujours déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre sur leurs enregistrements respectifs lorsque la synchronisation d'état est activée, mais lorsque le système enregistre qu'une demande de changement a changé d'état, ou que vous ajoutez une demande de changement ou que vous la supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la tâche de rattrapage des états `Fermé ou Différé`.

Pour plus d'informations, consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Diviser une tâche de rattrapage

À partir d'une tâche de rattrapage existante dans l'application Conformité de la configuration , identifiez un sous-ensemble de résultats des tests que vous souhaitez déplacer vers une nouvelle tâche de rattrapage.

Avant de commencer

Rôle requis : un utilisateur ayant le rôle itil

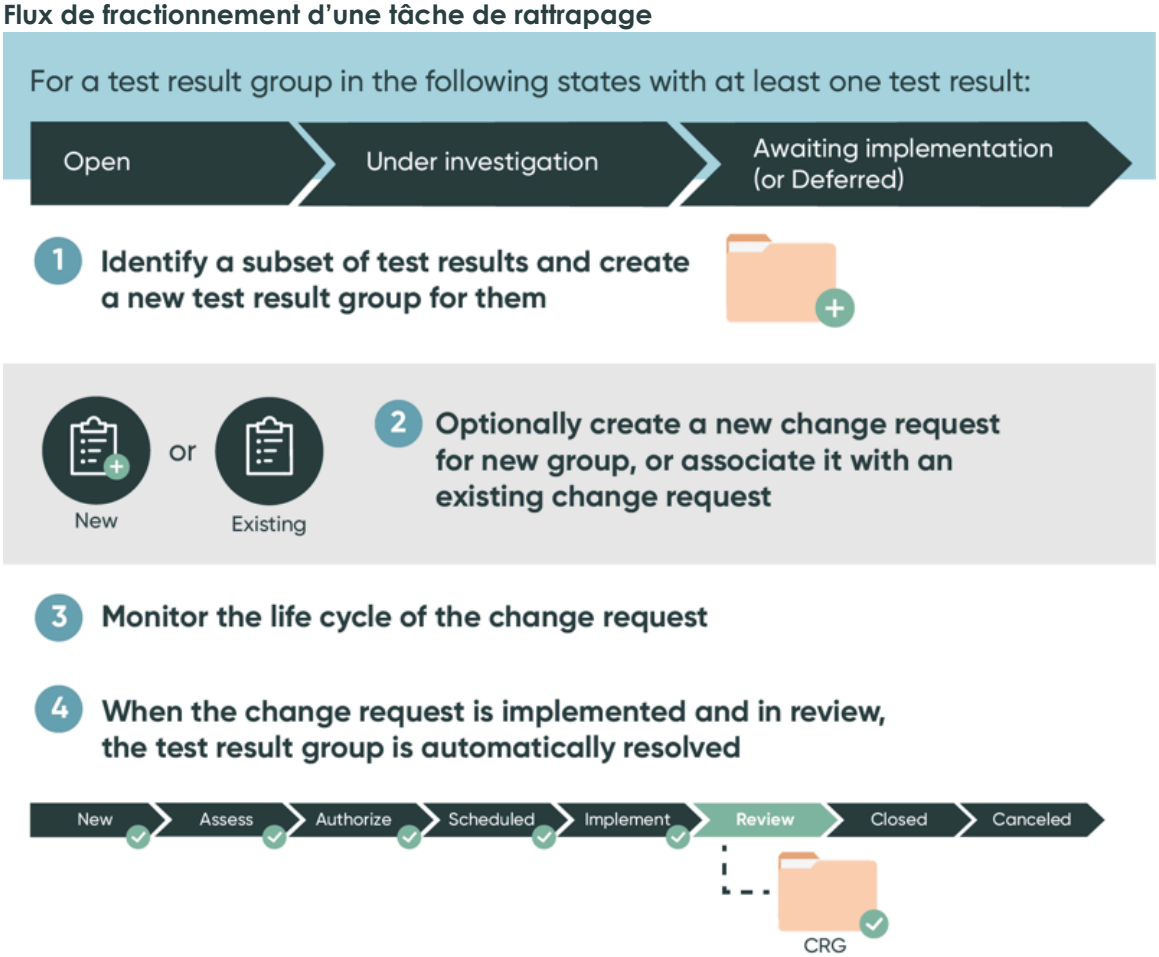
Pourquoi et quand exécuter cette tâche

En tant que spécialiste de l'informatique ou du rattrapage, vous pouvez diviser les tâches de rattrapage existantes dans les états **Ouvert**, **En cours d'examen** ou **En attente d'implémentation** avec plusieurs résultats de test. En créant une nouvelle tâche de rattrapage avec des résultats des tests qui correspondent à des critères spécifiques, vous pouvez utiliser un groupe spécifique de résultats des tests sans affecter la tâche de rattrapage d'origine.

Lorsque vous spécifiez les conditions des résultats des tests que vous souhaitez déplacer vers une nouvelle tâche de rattrapage avec le créateur de conditions, seuls les résultats des tests actifs qui correspondent à vos critères sont déplacés vers la nouvelle tâche. Vous n'avez pas besoin de créer des demandes de changement lorsque vous fractionnez une tâche de rattrapage. Vous pouvez diviser une tâche de rattrapage en même temps que vous créez une demande de changement, ou vous pouvez diviser une tâche de rattrapage sans créer de demande de changement.

L'image suivante illustre le flux de base pour fractionner une tâche de rattrapage. Les étapes détaillées de ce flux suivent l'image.

Flux de fractionnement d'une tâche de rattrapage



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les cas d'utilisation de fractionnement des résultats des tests des tâches de remédiation existantes en nouvelles tâches peuvent inclure les exemples suivants :

- Lorsque vous souhaitez créer une demande de changement ou des demandes de changement pour un groupe divisé.
- Lorsque vous réaffectez une tâche fractionnée à un autre utilisateur de votre groupe d'affectation.
- Lorsque vous demandez un report ou une exception pour une tâche fractionnée parce que vous savez que certains résultats des tests sur des éléments de configuration (CI) spécifiques ne peuvent pas être corrigés dans un délai donné.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Tests** > **Tâches de remédiation** > **Mes tâches ouvertes**.
   La liste des tâches de rattrapage affectées à vos groupes s'affiche.
2. Dans la colonne Nombre, cliquez sur la tâche de rattrapage que vous souhaitez fractionner.

   L'enregistrement de la tâche de rattrapage s'affiche.
3. Pour créer un sous-ensemble de résultats des tests pour une nouvelle tâche qui correspond à des critères spécifiques, procédez comme suit.

   En haut à droite de l'enregistrement, cliquez sur **Fractionner le groupe**.

   Vous préférerez peut-être cette méthode de création d'un nouveau groupe si vous travaillez à partir d'un grand groupe avec plusieurs résultats de tests.

   Le formulaire Diviser la tâche de rattrapage s'affiche.
4. Une fois le générateur de conditions affiché, spécifiez les conditions des résultats des tests que vous souhaitez déplacer vers une nouvelle tâche de rattrapage.

   Par exemple, vous pouvez préférer filtrer uniquement les résultats des tests qui correspondent aux conditions suivantes :

   - À l'état **Ouvert** .
   - Scores de risque supérieurs à 75.
   - Le résultat est **Échec**.

   Si les résultats des tests correspondent à votre filtre une fois que vous avez entré les conditions, un message s'affiche avec le nombre de résultats des tests correspondants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si un message s'affiche indiquant qu'aucun résultat de test ne correspond à votre filtre ou que tous vos résultats de test correspondent à vos critères, ajustez les conditions de sorte qu'au moins un résultat de test corresponde à vos critères de filtre.

5. Cliquez sur **Prévisualiser les éléments** pour afficher les résultats des tests correspondants. Une nouvelle fenêtre, Tâches de remédiation, affiche les éléments.
6. Pour prévisualiser les détails des résultats des tests qui correspondent à vos critères de filtre, procédez comme suit avant de cliquer sur **Diviser le groupe** pour créer le nouveau groupe. Ces détails incluent le groupe d'affectation et la personne à qui le résultat du test est affecté. L'affichage de ces informations dans l'aperçu peut aider à s'assurer que la nouvelle tâche est correctement affectée.

   a. Une fois la liste des rattrapages affichée dans l'aperçu, cliquez sur un élément dans la colonne Résultats.
   L'enregistrement des résultats du test s'affiche.

   b. Vérifiez que les champs **Groupe d'affectation** et **Affecté à** sont corrects.

   c. Cliquez sur **Mettre à jour**.

7. Lorsque vous êtes prêt à créer le nouveau groupe, cliquez sur **Diviser le groupe**.
   Un message indique le nombre de résultats des tests qui sont transférés vers le nouveau groupe et la nouvelle tâche de rattrapage s'affiche. Pour vous aider à identifier la nouvelle tâche, vous pouvez modifier le texte dans le champ **Brève description** et modifier à nouveau les champs Groupe d'affectation ou Affecté à, si nécessaire.

   Remarque : Pour moins de 200 résultats de test, l'opération de division est effectuée de manière synchrone et les résultats des tests sont affichés dans la nouvelle tâche.

   Au-delà de 200 résultats de test, l'opération de division est effectuée de manière asynchrone en arrière-plan, et il peut s'écouler quelques secondes avant que les résultats du test n'apparaissent dans la nouvelle tâche. Le message suivant s'affiche également : `n résultats des tests seront transférés de TRGxxxxxxx vers le nouveau groupe de résultats de test GRCxxxxx sous peu.`

8. Vous pouvez également créer une nouvelle tâche de rattrapage en sélectionnant les résultats des tests directement à partir de la liste connexe Résultats des tests sur une tâche de rattrapage.

   Vous préférerez peut-être cette méthode si vous n'avez que quelques résultats de test dans un groupe, ou si vous savez exactement quels tests vous souhaitez déplacer vers une nouvelle tâche.

   a. Une fois l'enregistrement de la tâche de rattrapage affiché, faites défiler jusqu'à la liste connexe Résultats des tests.

   b. Dans la colonne située tout à gauche, cochez les cases en regard des résultats des tests pour lesquels vous souhaitez créer une tâche de rattrapage.

   c. Dans la liste Actions sur les lignes sélectionnées en bas à gauche de l'enregistrement, cliquez sur **Fractionner le groupe**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Dans le formulaire Tâche de rattrapage de division qui s'affiche, pour vous aider à identifier le nouveau groupe, vous préférez peut-être modifier le texte du champ **Brève description** .

e. Cliquez sur **Diviser le groupe**.
Un message indique le nombre de résultats des tests qui ont été transférés vers la nouvelle tâche, et la nouvelle tâche de rattrapage s'affiche.

Une fois la demande de changement de cette tâche de rattrapage résolue, s'il n'y a pas d'autres demandes de changement ouvertes associées à cette tâche de rattrapage, la tâche de rattrapage passe également à l'état **Résolu** .

Remarque : Vous pouvez toujours déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre sur leurs enregistrements respectifs lorsque la synchronisation d'état est activée, mais lorsque le système enregistre qu'une demande de changement a changé d'état, ou que vous ajoutez une demande de changement ou que vous la supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la tâche de rattrapage des états `Fermé ou Différé`.

Pour plus d'informations, consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.

Que faire ensuite

Vous pouvez créer ou associer des demandes de changement pour vos nouvelles tâches de rattrapage. Pour plus d'informations, consultez Associer une tâche de rattrapage à une demande de changement existante et Créer une demande de changement dans Conformité de la configuration.

Supprimer les affectations des tâches de rattrapage pour vous ou vos groupes

Réaffectez les enregistrements de résultats des tests dans l'application Conformité de la configuration si les enregistrements vous ont été attribués de manière incorrecte ou si votre groupe les a été affectés de manière incorrecte.

Avant de commencer

Rôle requis : sn_vulc.remediation_owner

Pourquoi et quand exécuter cette tâche

À partir de la version 14.3 de l'application Conformité de la configuration , si vous déterminez que les tâches de rattrapage (RT) et les résultats des tests qui leur sont associés ne sont pas dans votre champ d'application pour le rattrapage, ou si vous pensez que les enregistrements vous ont été affectés de manière incorrecte ou à vos groupes, vous pouvez vous retirer, vous ou vos groupes, des champs Affecté à et Groupe d'affectation des enregistrements TRG.

Le bouton **Annuler l'affectation** s'affiche sur les enregistrements de tâche de rattrapage dont l'état n'est pas Fermé ou Résolu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à un enregistrement de tâche de rattrapage qui vous est affecté et dont l'état n'est pas Fermé ou Résolu.
2. Pour effacer les champs **Affecté à** et **Groupe d'affectation** , en haut de l'enregistrement, sélectionnez **Annuler l'affectation**.
3. Dans la boîte de dialogue **Annuler l'affectation** , fournissez des notes de travail et sélectionnez **Soumettre**.
   - Les notes de travail que vous avez fournies sont affichées dans la section Notes.
   - Dans l'onglet **Approbation de changement d'état** , l'enregistrement d'approbation de changement d'état (CA#) affiche l'état En cours de révision, ce qui vous aide à suivre le workflow d'approbation.
   - Dans l'onglet **Approbations demandées** , votre demande de suppression de vous-même ou de votre groupe d'affectation s'affiche sous la forme de l'état Demandé.

Résultats

La demande est approuvée à l'aide d'un workflow d'approbation à un niveau par défaut. Pour plus d'informations, consultez Approuver une demande de désaffectation dans Configuration Compliance.

- Si votre demande est approuvée, l'enregistrement d'approbation de changement d'état et l'enregistrement d'approbation demandé passent à **l'état Approuvé**. Vous et vos groupes êtes supprimés des champs Affecté à et **Groupe d'affectation**. `Non affecté` s'affiche dans le champ **Type d'affectation** et la tâche de rattrapage s'affiche dans la liste du module Non affecté de l'application Conformité de la configuration .

  Les notifications indiquant que les enregistrements ne sont pas affectés sont envoyées automatiquement aux gestionnaires de vulnérabilités ou aux analystes du groupe de notification Annuler l'affectation. Pour plus d'informations sur les notifications et les propriétés de cette fonctionnalité, consultez Suppression des affectations des groupes de résultats des tests de Configuration Compliance.

- Si votre demande est rejetée, l'enregistrement de l'approbation de changement d'état et l'enregistrement de l'approbation demandée basculent à l'état Rejeté.

Remarque : En tant qu'administrateur de vulnérabilité, vous pouvez définir la *sn_vulc.unassign_test_result_group.approval_required* propriété système sur **false** pour désactiver le processus d'approbation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Accédez au module Non affecté pour l'application Conformité de la configuration , surveillez tous les enregistrements non affectés pour les éléments qui pourraient entrer dans votre champ d'application, puis réaffectez-les à vous-même.

Approuver une demande de désaffectation dans Conformité de la configuration

Approuvez les demandes de suppression des tâches de rattrapage d'un groupe d'affectation ou d'un utilisateur individuel dans l'application Conformité de la configuration .

Avant de commencer
Rôle requis : sn_vulc.unassign_approver

Pourquoi et quand exécuter cette tâche
Une configuration d'approbation est fournie par défaut. Pour les approbations sans affectation, un approbateur est requis dans le groupe d'approbation Approbateur – niveau 1. Par défaut, le groupe d'approbation de `désaffectation (Désaffecter l'approbateur CC : niveau 1)` est créé et les utilisateurs qui font partie de ce groupe peuvent approuver la demande. Par défaut, ce groupe contient le rôle d'approbateur de désaffectation, sn_vulc.unassign_approver. Vous pouvez modifier ou créer un groupe et mettre à jour la configuration de l'approbation en accédant à **Tout** > **Configuration Compliance** > **Mes approbations** > **Règles d'approbation** > **Demande de changement de champ de groupe de résultats de test** > **Désaffecter le groupe de résultats des tests**.

Procédure
1. Accédez à la **Tout** > **Configuration Compliance** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande en ajoutant les commentaires appropriés.

Fermeture automatique des résultats des tests

Vous pouvez fermer automatiquement les résultats des tests (TR) associés aux éléments de configuration (CI) mis hors service.

Pour configurer l'option de fermeture automatique, accédez à la propriété système **sn_vulc.auto_close_test_results_linked_to_retired_CIs** et définissez-la sur vrai. Pour fermer automatiquement les TR associés aux CI mis hors service, reportez-vous à la section Fermer automatiquement les résultats des tests associés aux CI mis hors service.

Pour plus d'informations sur l'utilisation d'éléments de configuration mis hors service, reportez-vous à la section Utiliser des éléments de configuration mis hors service dans Configuration Compliance.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser des éléments de configuration mis hors service dans Configuration Compliance

Les éléments de configuration (CI) mis hors service passent à l'état Mis hors service, Archivé ou Supprimé dans le Base de données de gestion des configurations (CMDB). Conformité de la configuration contient des résultats des tests (TR) qui sont constitués de CI. Lorsque l'état d'un CI est mis à jour sur Mis hors service, les TR associés sont fermés avec le sous-état « CI désactivé ».

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Si la CMDB définit l'état de l'étape du cycle de vie d'un CI sur Mis hors service, vous pouvez choisir de fermer automatiquement les TR associés. Pour plus d'informations sur la fermeture automatique des TR associés, reportez-vous à la section Fermer automatiquement les résultats des tests associés aux CI mis hors service.

Le CI mis hors service est éventuellement archivé ou définitivement supprimé du CMDBfichier .

Impact de la mise hors service des CI :

- **Impact sur les éléments détectés :** Lorsque le CI est mis hors service, le DI associé est marqué comme « CI désactivé ».
- **Impact sur les résultats des tests :** Lorsque l'état d'un DI est mis à jour sur « CI désactivé », le TR associé est fermé et la section Notes est automatiquement mise à jour.

Remarque : L'état d'un élément de données est automatiquement mis à jour sur « CI désactivé » chaque fois que l'état du cycle de vie d'un CI est mis à jour. D'autre part, l'état d'un TR est mis à jour sur Fermé uniquement lorsque la propriété **sn_vulc.auto_close_test_results_linked_to_retired_CIs** est définie sur vrai. Pour plus d'informations sur la fermeture automatique des TR associés, reportez-vous à la section Fermer automatiquement les résultats des tests associés aux CI mis hors service.

La tâche *Close Test Results for decommissioned CIs* planifiée est exécutée quotidiennement pour les DI mis à jour. Si l'option de configuration de fermeture automatique est activée pour les CI mis hors service, elle identifie le DI contenant un CI désactivé et ferme le TR associé avec le sous-état « CI désactivé ». Si tous les TR d'une tâche de rattrapage sont fermés et que leur sous-état est CI désactivé, la tâche de rattrapage est également fermée avec le sous-état « Annulé ».

Remarque : Si un CI revient à l'état d'origine depuis l'état « Hors service », l'entrée « Éléments détectés » est également mise à jour. Les TR sont automatiquement ouverts lorsque les données sont à nouveau ingérées à partir du scanner.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fermer automatiquement les résultats des tests associés aux CI mis hors service

Si l'état Base de données de gestion des configurations (CMDB) de l'étape du cycle de vie d'un élément de configuration (CI) passe à Mis hors service, vous pouvez choisir de fermer automatiquement les résultats des tests (TR) associés.

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
Pour fermer automatiquement les résultats des tests associés, vous devez activer la propriété système **sn_vulc.auto_close_test_results_linked_to_retired_CIs** pour fermer automatiquement les résultats des tests associés aux CI mis hors service. Si cette option est activée, les résultats des tests nouveaux et existants signalés pour le même CI sont automatiquement créés ou mis à jour dans l'état « Fermé ». Ceux-ci sont basés sur l'ID d'actif dans la charge utile du scanner et l'état de saisie des éléments détectés. Pour en savoir plus sur l'impact des CI mis hors service, reportez-vous à Utiliser des éléments de configuration mis hors service dans Configuration Compliance.

Remarque : L'état d'un élément de données est défini sur « CI désactivé » chaque fois que l'état du cycle de vie d'un CI est mis à jour. D'autre part, l'état d'un TR est mis à jour sur Fermé uniquement lorsque la propriété système **sn_vulc.auto_close_test_results_linked_to_retired_CIs** est activée.

Procédure
1. Accédez à la **Propriétés système** > **Toutes les propriétés** et filtrer par *sn_vulc.auto_close_test_results_linked_to_retired_CIs* dans la colonne Nom.
2. Sélectionnez la propriété.
3. Pour fermer automatiquement les résultats des tests associés aux CI mis hors service, définissez la valeur de la propriété sur vrai.

Fermeture automatique des résultats des tests périmés dans Conformité de la configuration

Vous pouvez activer la fonctionnalité Fermer automatiquement les résultats des tests périmés pour fermer automatiquement les résultats des tests plus anciens qui n'ont pas été trouvés récemment par vos intégrations tierces. Le déplacement de ces résultats des tests vers **Fermé-Périmé** réduit le nombre de résultats des tests actifs et de tâches de rattrapage dans votre instance et vous aide à rapprocher les actifs dans votre Base de données de gestion des configurations (CMDB)fichier .

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Vue d'ensemble

Le module Fermer automatiquement les résultats des tests périmés vous aide à fermer automatiquement les résultats des tests anciens et périmés qui n'ont pas été trouvés

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

récemment par vos intégrations tierces. Les résultats des tests sont déplacés vers **Fermé-Périmé** en fonction des conditions que vous définissez dans le générateur de conditions.

Termes clés

Résultat de test

Les résultats des tests sont des résultats importés à partir de bibliothèques de tests de configuration mappés sur des cadres de travail, des politiques et des sources de référence qui définissent la manière dont une classe d'actifs technologiques doit être gouvernée. L'application Conformité de la configuration ne calcule pas les résultats des tests, mais les importe avec des intégrations tierces.

Date de la dernière analyse de l'actif

Fait référence à la valeur de la colonne Dernière date de l'analyse Configuration Compliance de la table Élément détecté associée au résultat des tests. Cette date fait référence à la date et à l'heure les plus récentes auxquelles un actif a été analysé pour la dernière fois par un scanner tiers.

Date du dernier échec

Fait référence à la date de la colonne Dernier observé de la table Résultats des tests lorsque la valeur du champ **Résultat** est [échec].

Résultats des tests périmés

Désigne les résultats des tests dans votre instance qui sont anciens et n'ont pas été trouvés, mis à jour ou détectés par les analyses d'intégration tierce pendant une période significative.

Derniers résultats des tests trouvés

Cette option de recherche utilise une date et une heure fournies par l'analyseur tiers. Ce terme fait référence à la date la plus récente, ou la plus récente (en jours) à laquelle les résultats des tests ont été retrouvés par le scanner. Ce paramètre peut être configuré.

Cas d'utilisation

Parfois, les actifs (éléments de configuration) peuvent être mis hors service dans votre environnement ou purgés par des scanners tiers. Lorsque cela se produit, les résultats des tests de configuration associés aux actifs ne sont pas mis à jour dans l'application Conformité de la configuration par les détections importées et ils deviennent inactifs (périmés).

Pour réduire le nombre de résultats des tests (TR) et de tâches de rattrapage (RT) actifs dans votre instance, activez la fonctionnalité Fermer automatiquement les résultats des tests périmés. Cette fonctionnalité ferme automatiquement les résultats des tests anciens qui ont un état inchangé ou qui n'ont pas été importés récemment par vos intégrations.

À titre d'exemple, supposons qu'un élément de configuration particulier (CI) possède plusieurs ID d'actif et que l'un de ces ID n'a pas été importé lors des détections d'un scanner tiers au cours des 90 derniers jours. Si vous configurez le générateur de conditions dans le module Fermer automatiquement les résultats des tests périmés pour fermer les résultats des tests qui n'ont pas été trouvés ou mis à jour au cours des 90 derniers jours ou plus, cette fonctionnalité ferme automatiquement tous les résultats des tests qui correspondent à ce filtrage.

Remarque : Cette fonctionnalité ferme uniquement les détections des résultats des tests en fonction des conditions de filtre que vous définissez dans le créateur de conditions et qui sont détectées par vos intégrations de scanner tiers.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le champ Résolution

Pour différencier les détections fermées par des analyseurs tiers tels que les Qualys produits and Tenable.io et la fonctionnalité Fermer automatiquement les résultats des tests périmés dans votre instance, une nouvelle valeur pour le champ **Résolution** , [Fermé-Périmé], a été ajoutée. **Fermé-Périmé** indique qu'un TR a été fermé par la fonction de fermeture automatique. **Fermé** ou **Fixe-Fermé** indique qu'un TR a été fermé par un scanner.

Déploiement des états TR aux TRG avec la fonctionnalité de fermeture automatique

La progression de l'état et la priorité pour les résultats des tests sont les suivantes : **Ouvrir** > **Fermé** > **Fixe-Fermé** > **Fermé : périmé**.

1. Si des TRG sont **ouverts** dans un TRG, l'état TRG n'est pas modifié.
2. Si au moins un TR est **Fermé - Fixe** et que les autres sont **Fermé - Périmé**, l'état TRG passe à **Fermé - Fixe**.
3. Si tous les TRG d'un TRG sont **Fermé - Périmé**, l'état du TRG passe à **Fermé - Annulé**.

Intégrations prises en charge

Pour en savoir plus sur les intégrations tierces prenant en charge cette fonctionnalité, reportez-vous aux rubriques Présentation de Qualys Vulnerability Integration et Tenable.ioIntégrations avec les applications ET Réponse aux vulnérabilitésConformité de la configuration.

Utiliser la fermeture automatique des résultats des tests périmés dans Conformité de la configuration

Activez l'option Fermer automatiquement les résultats des tests périmés pour fermer automatiquement les résultats des tests plus anciens en fonction des conditions de filtre que vous définissez.

Avant de commencer

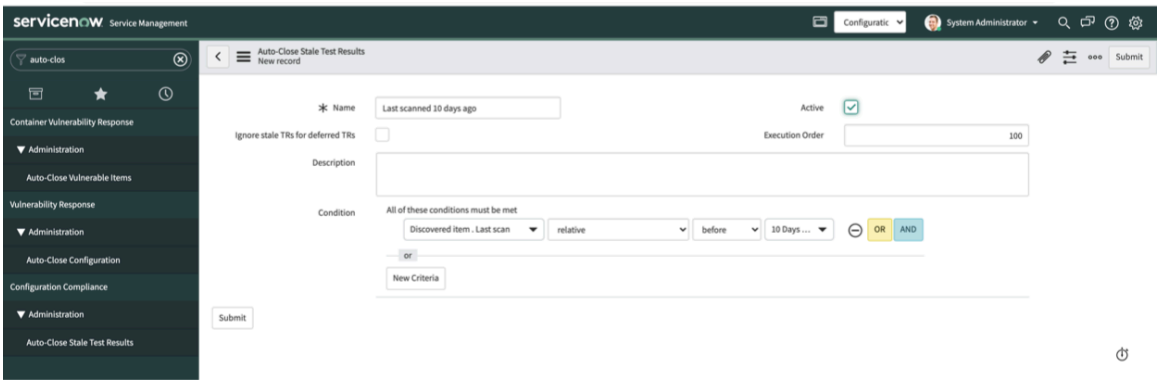
Pour plus d'informations sur cette fonctionnalité, les termes clés et toute configuration qui peut être requise pour vos intégrations tierces qui importent des données de résultats des tests, reportez-vous à la section Fermeture automatique des résultats des tests périmés dans Conformité de la configuration.

Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Administration** > **Fermer automatiquement les résultats des tests périmés**.
2. Renseignez les champs du formulaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Champ	Valeur
Nom	Nom de cet enregistrement de configuration.
Actif	Si cette option est sélectionnée, cet enregistrement est actif et il fermera automatiquement tous les résultats des tests qui correspondent à ses critères de filtrage.
Ignorer les résultats des tests périmés pour les résultats des tests différés	Si cette option est sélectionnée, tous les TR mappés aux états **En cours de révision** ou **Différé** sont ignorés et ne sont pas fermés. Si vous décochez cette option, tous les TR qui correspondent à vos critères seront fermés.
Ordre d'exécution	100 est la valeur par défaut. Cette valeur détermine l'ordre d'exécution par ordre croissant pour chaque enregistrement de configuration utilisé pour localiser et marquer les résultats des tests périmés.
Description	Description de cet enregistrement. Ce texte peut vous aider à le retrouver facilement si vous créez un plus grand nombre d'enregistrements.
Condition	Conditions de filtrage utilisées pour trouver les TR que vous souhaitez fermer. Le filtre par défaut est **Élément détecté** > **Dernière analyse** > .

3. Cliquez sur **Envoyer**.

   La tâche planifiée, *`Auto-Close Stale Test Results`*, s'exécute quotidiennement. Cette tâche identifie les TR en fonction des conditions que vous avez fournies et fait la transition de celles qui correspondent à **Fermé-Périmé**.

   Une fois que les résultats des tests sont marqués comme **fermés-périmés**, si le scanner les trouve à nouveau, les résultats des tests sont rouverts et les états passent à**Ouvert**.

   Si un TR est marqué comme **Fermé-Périmé** et que le scanner détecte qu'il a été corrigé, il passe à**Fermé-Corrigé**. Les états se déploient également sur les tâches de rattrapage, comme décrit dans la liste suivante :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Si des résultats des tests dans une tâche de rattrapage sont **ouverts**, l'état de la tâche de rattrapage n'est pas modifié.

b. Si au moins un TR est **Fermé - Fixe** et que les autres sont **Fermés - Périmés**, l'état de la tâche de rattrapage passe à **Fermé - Fixe**.

c. Si tous les TR d'une tâche de rattrapage sont **Fermé - Périmé**, l'état du TRG passe à **Fermé - Annulé**.

Fermer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage peut être fermé immédiatement sans autre analyse, vous pouvez utiliser la fonctionnalité **Fermer** .

Avant de commencer

Rôle requis :

- sn_vulc.admin
- sn_vulc.remediation_owner

> **Remarque :** Le rôle sn_vulc.remediation_owner vous permet de réaffecter ou de fermer les tâches de rattrapage qui vous sont affectées ou qui sont affectées à vos groupes d'affectation.

Pourquoi et quand exécuter cette tâche

À partir de la version 15.0 de , le bouton **Fermer** a été supprimé pour une tâche de Conformité de la configurationrattrapage.

Lorsque vous résolvez une tâche de rattrapage, les notes de résolution se reflètent dans les notes de travail de tous ses résultats de test.

Procédure

1. Ouvrez l'enregistrement de la tâche de rattrapage.

2. Cliquez sur le bouton **Fermer** .

3. Décrivez la raison de la fermeture du problème dans la fenêtre contextuelle.

4. Sélectionnez **Fermer**.

Information associée

Conformité de la configuration États

Demande et approbation d'une exception pour une tâche de rattrapage

Vous pouvez demander à différer le rattrapage d'une tâche de rattrapage pour une période spécifiée. Les utilisateurs qui font partie du groupe d'approbateurs peuvent approuver les demandes d'exception.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Pour demander ou approuver des demandes d'exception, consultez :

- Demander une exception pour une tâche de rattrapage dans Conformité de la configuration
- Approuver une demande d'exception dans Conformité de la configuration

Remarque :

Des notifications par e-mail sont envoyées à chaque étape de la gestion des exceptions, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'une exception est demandée, le demandeur reçoit un e-mail confirmant que la demande est émise. L'approbateur reçoit également un e-mail l'informant qu'une exception a été demandée.

À partir de la version 14.11 de Conformité de la configuration, vous pouvez configurer les délais d'approbation des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est déclenchée, le résultat du test passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, le résultat du test revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez la rubrique Configurer les règles d'approbation pour la gestion des exceptions.

Demander une exception pour une tâche de rattrapage dans Conformité de la configuration

Demandez une exception pour différer le rattrapage d'une tâche de rattrapage pendant une période spécifiée s'il n'est pas possible d'y remédier immédiatement.

Avant de commencer

Rôle requis : sn_vulc.remediation_owner

Pourquoi et quand exécuter cette tâche

Important : Vous pouvez demander une exception pour :

- Tâches de rattrapage dans et Espace de travail du gestionnaire de vulnérabilitésEspace de travail de remédiation IT. Pour plus d'informations, consultez Demander une exception dans le Espace de travail de remédiation IT.
- Plusieurs résultats de test simultanément à partir du Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Demander une exception en bloc dans Vulnerability Manager Workspace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Tâches de remédiation** > **Toutes les tâches**.
2. Sélectionnez la tâche de rattrapage pour laquelle vous souhaitez demander une exception.
   La tâche sélectionnée doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Sur le formulaire Tâche de rattrapage, cliquez sur **Demande d'exception**.

   Remarque : Selon que Réponse aux vulnérabilités ou GRC : gestion de la politique et de la conformité est sélectionné ou non dans le **Configuration Compliance** > **Gestion des exceptions** , le formulaire Demande d'exception change. Reportez-vous à la rubrique Configurer la gestion des exceptions pour Conformité de la configuration.

4. Si Réponse aux vulnérabilités cette option est sélectionnée dans l'écran Gestion des exceptions, procédez comme suit :

   a. Renseignez les champs du formulaire.

Formulaire Demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée sélectionnée dans le **Tout** > **Configuration Compliance** > **Administration** > **Gestion des exceptions** écran. Lorsque la demande d'exception expire, le groupe revient à son état Ouvert.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : À partir de la version 14.7 de (CC), si une tâche de Conformité de la configuration rattrapage différée est rouverte par un analyseur avant l'expiration de la fenêtre d'exception, l'état de la tâche de rattrapage passe de Ouvert à Différé. Cette fonctionnalité est désactivée par défaut. Pour activer cette fonctionnalité, définissez la valeur de la propriété *sn_vulc.auto_defer_test_result_in_active_exc* système sur vrai. En outre, la date de fin différée persiste même après la réouverture de la tâche de rattrapage après la date d'expiration.
Motif	Raison de l'exception. Les choix sont les suivants : ▪ Risque accepté ▪ En attente de fenêtre de maintenance ▪ Correctif non disponible ▪ Contrôle d'atténuation en place ▪ Autre Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à la section Définir les mappages des motifs de politique.
Information supplémentaire	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ doit être mis à jour par le propriétaire du rattrapage.

b. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**.

Résultats
L'état de la tâche de rattrapage passe à En cours de révision. Utilisez l'onglet **Approbation de changement d'état** pour suivre l'état de la demande d'exception.

Demander une extension pour une règle d'exception dans Conformité de la configuration

Demandez une prolongation pour une règle d'exception différée avant qu'elle n'atteigne sa date de report jusqu'à échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer
Rôle requis : sn_vul.exception_approver

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension à partir Réponse aux vulnérabilités des espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Règles d'exception**.
2. Sélectionnez une règle d'exception approuvée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle la règle d'exception doit être prolongée.
Motif	Entrez le motif du report de la règle d'exception. Les choix sont les suivants : ◦ Risque accepté ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les champs Reporté jusqu'à, Motif et Informations supplémentaires sont mis à jour sur la règle d'exception et les tâches de rattrapage associées. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure de l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Si une règle d'exception différée est à nouveau étendue, le nombre de reports prolongés augmente dans le back-end.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander une exception pour les tâches de rattrapage à l'aide de GRC : gestion de la politique et de la conformité

Demandez des exceptions de politique à l'aide de l'option GRC de gestion des exceptions de politique de l'application à partir de .Gestion de la politique et de la conformitéConformité de la configuration

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions de politique, vous devez télécharger l'application GRC : gestion de la politique et de la conformité à partir du ServiceNow Store.

Rôle requis : sn_vulc.remediation_owner

Vous pouvez également demander des exceptions dans l'interface utilisateur classique.

Pourquoi et quand exécuter cette tâche

À partir de la version 19.0 de , vous pouvez demander des exceptions de politique pour les tâches de Réponse aux vulnérabilitésremédiation (RT) dans IT Remediation Workspace. Pour plus d'informations, consultez Demander une exception à l'aide GRC : gestion de la politique et de la conformité de Espace de travail de remédiation IT.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Application Vulnerability Response** > **Éléments vulnérables de l'application** (ou **Tâches de rattrapage**)>**Tous**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.
   L'élément ou le groupe sélectionné doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Sur le formulaire sélectionné, cliquez sur **Demande d'exception**.
3. Si GRC : gestion de la politique et de la conformité cette option est sélectionnée dans l'écran Gestion des exceptions, procédez comme suit.

   a. Renseignez les champs du formulaire.

Formulaire Demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	aucune politique n'est sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date du jour. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et à laquelle l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert. **Remarque :** Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale (jours) de l'exception** que vous avez définie pour la politique dans Politique et conformité. Pour plus d'informations, reportez-vous à la section Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ doit être renseigné par le propriétaire du rattrapage.

b. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**. L'état de la tâche de rattrapage passe à En cours de révision et une exception de politique est créée. Utilisez l'onglet **Approbation de changement d'état** pour suivre l'état de la demande d'exception.

c. Affichez l'exception de politique en cliquant sur la liste connexe Exceptions de politique.

d. Cliquez sur le numéro d'exception de politique.

e. Dans le champ **Approbateur** , sélectionnez le nom de l'approbateur.

f. Cliquez sur l'onglet Source et sélectionnez un objectif de contrôle dans le champ **Objectif de contrôle** .

g. Cliquez sur l'onglet Évaluation des risques et sélectionnez l'évaluation des risques dans le champ **Évaluation des risques** .

h. Enregistrez le formulaire.

i. Cliquez sur l'onglet **Contrôles concernés** .

j. Ajoutez les contrôles en cliquant sur **Ajouter**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

k. Enregistrez le formulaire.

> **Remarque :** Vous pouvez soumettre un examen de conformité en cliquant sur **Demander un examen de conformité**.

Le formulaire d'approbation est envoyé à l'approbateur.

L'approbateur peut approuver la demande en cliquant sur **Approuver** ou demander une approbation supplémentaire en cliquant sur **Demander une approbation supplémentaire**.

L'état de l'enregistrement devient Différé. Le motif indiqué est celui que vous avez sélectionné lors de l'émission de la demande d'exception. L'onglet **Report** fournit des notes supplémentaires sur l'enregistrement.

> **Remarque :** Si la demande est rejetée, l'enregistrement passe à son état précédent.

4. Cliquez sur **Envoyer**.
Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez la configuration facultative de Gestion de la politique et de la conformité .

Approuver une demande d'exception dans Conformité de la configuration

Approuvez les demandes d'exception pour les tâches de rattrapage qui ne peuvent pas être corrigées immédiatement. Vous devez évaluer les risques de ces demandes, puis approuver leur report jusqu'à ce qu'elles puissent être corrigées.

Avant de commencer
Rôle requis : sn_vulc.exception_approver

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Mes approbations**.

2. Sélectionnez une demande dans votre file d'attente.

3. Approuvez ou rejetez la demande avec les commentaires appropriés.

> **Remarque :** Dans le cas d'un workflow d'approbation à deux niveaux, après l'approbation de premier niveau, la demande est soumise au deuxième niveau pour une approbation supplémentaire. S'il n'y a pas d'utilisateurs au deuxième niveau, la demande est automatiquement approuvée après l'approbation de premier niveau.
>
> Une fois la demande approuvée, la tâche de rattrapage passe à un état Différé. En cas de rejet, la tâche de rattrapage revient à son état antérieur.

Définir les mappages des motifs de politique

Vous pouvez définir les choix de motifs afin qu'ils soient disponibles pour n'importe quel utilisateur qui demande une exception.

Avant de commencer
Rôles requis : sn_vul.compliance.manager et sn_vulc.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Politique et Conformité** > **Exceptions de politique** > **Registre d'intégration**.

   Remarque : Vous pouvez sélectionner un motif parmi les choix de motifs disponibles dans la table Choix du motif ou ajouter un nouveau motif.

2. Cliquez sur le registre d'intégration de Container Vulnerability Response - CVIT.
3. Pour ajouter un choix de motif existant, procédez comme suit :
   a. Dans la liste Choix du motif, cliquez sur **Nouveau**.
   b. Cliquez sur l'icône en forme de loupe pour sélectionner un motif.
4. Pour ajouter de nouveaux choix de motifs à la table Choix du motif, procédez comme suit :
   a. Dans la liste Choix du motif, cliquez sur **Nouveau**.
   b. Cliquez sur l'icône de la loupe.
   c. Cliquez sur **Nouveau**.
   d. Renseignez les champs du formulaire.

Formulaire de liste de choix de motifs

Champ	Description
Étiquette	Étiquette unique pour ce choix.
Valeur	Valeur unique pour ce choix. Cette valeur est mappée dans la table Mappages de motifs d'exception de politique pour les applications respectives. Pour accéder à cette table, saisissez sn_sec_cmn_policy_reason_mapping. LIST dans le navigateur de filtre.
Ordre	Ordre pour ce choix. Les motifs sont classés en fonction de ce nombre.
Par défaut	Option pour indiquer que ce choix de motif sera disponible chaque fois qu'une exception de politique sur demande est demandée. Si le registre d'intégration ne contient pas de choix spécifiques à l'application, tous les choix de motif pour lesquels le champ **Par défaut** est sélectionné sont disponibles.
Actif	Option permettant d'afficher le choix dans la liste des choix de motifs.

5. Cliquez sur **Envoyer**.

Solutions d'analyse et de génération de rapports pour Conformité de la configuration

Les rapports suivants sont fournis à des fins de surveillance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichez les politiques, les CI, les tests et les résultats des tests dans les rapports Vue d'ensemble Conformité de la configuration .

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Conformité de la configuration Rapports

La Conformité de la configuration page d'accueil fournit une vue d'ensemble des politiques, des CI, des tests et des résultats des tests, ce qui permet au personnel de sécurité d'identifier rapidement les zones de préoccupation. Conformité de la configuration Des graphiques de signification peuvent être ajoutés, au besoin. Vous pouvez également renvoyer Conformité de la configuration des informations relatives à à l'aide de la fonction de recherche globale.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

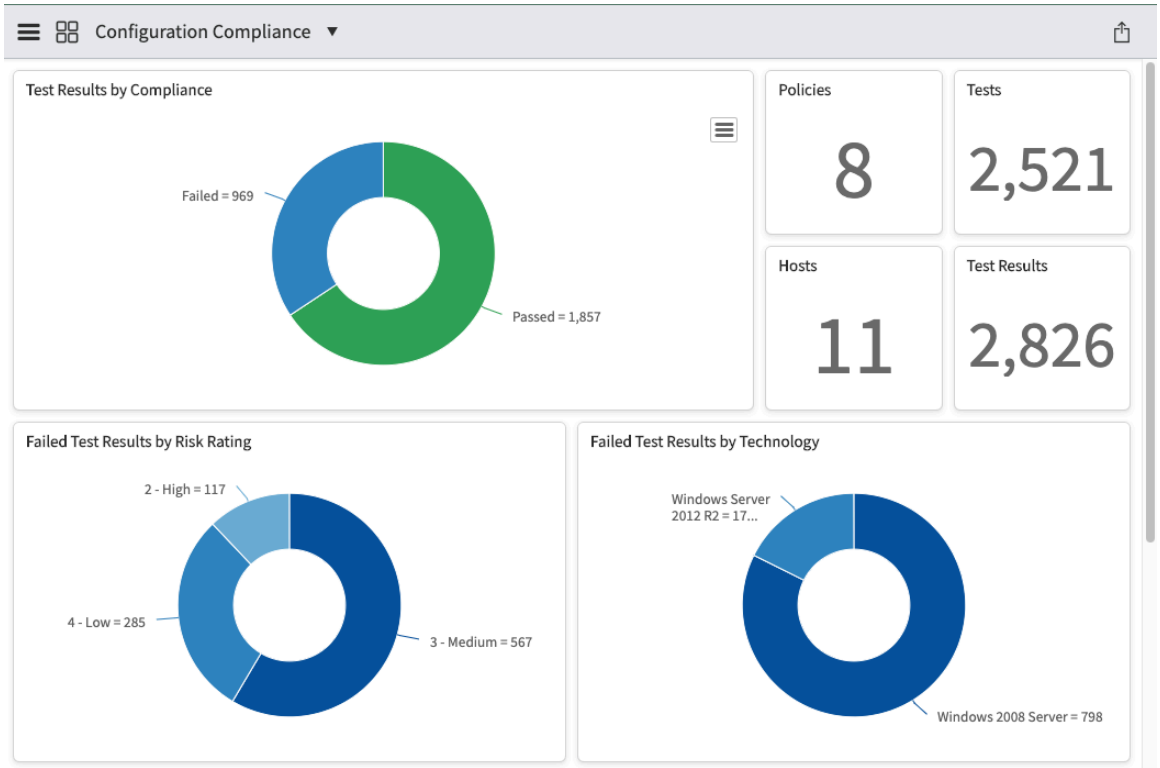
Dans chaque graphique, vous pouvez pointer sur n'importe quelle partie d'un graphique (barre, secteurs, point de données) pour afficher des données générales spécifiques à cette partie du graphique. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

Remarque : Toute personne disposant du rôle sn_vulc.read peut afficher le tableau de bord. Toute personne disposant du rôle sn_vulc.write ou sn_vulc.admin peut créer et modifier un tableau de bord. Seul sn_vulc.admin peut supprimer un tableau de bord.

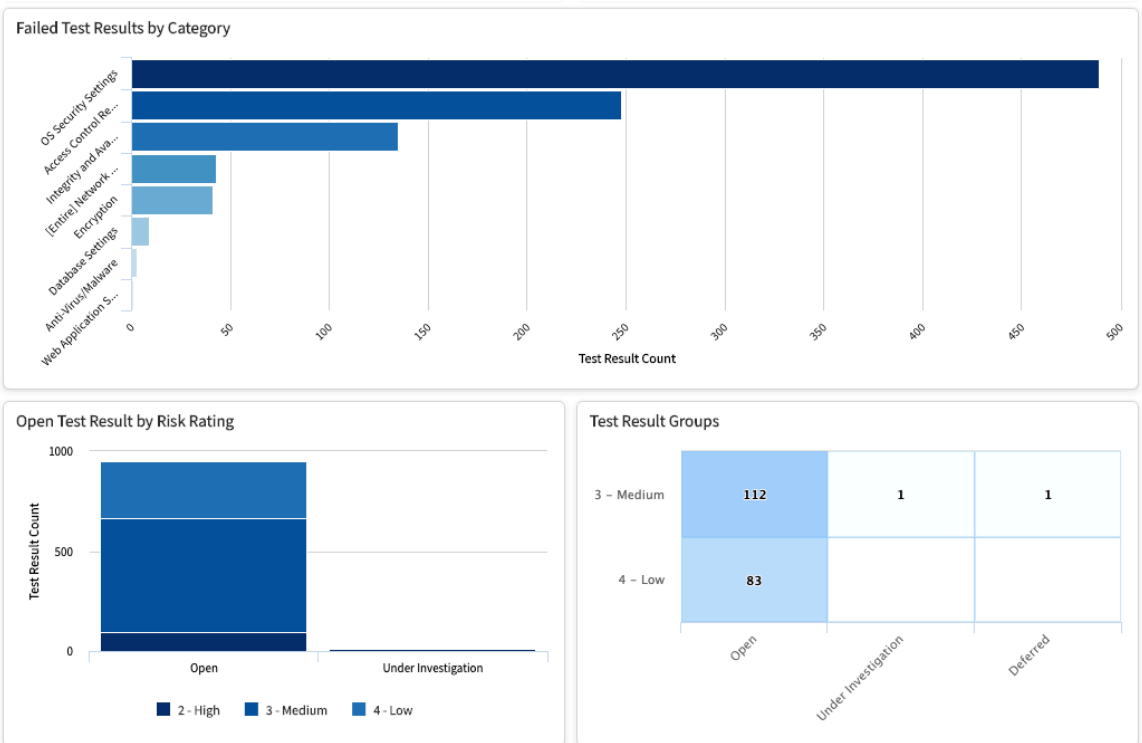
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports Vue d'ensemble de la vulnérabilité



Rapport de Configuration Compliance



Rapports Vue d'ensemble de la vulnérabilité

Nom	Visuel	Description
Résultats des tests par conformité	Couronne	Affiche le nombre de tests ouverts qui ont réussi ou échoué.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports Vue d'ensemble de la vulnérabilité (suite)

Nom	Visuel	Description
Politiques	Numéro	Nombre de politiques avec des résultats des tests ayant échoué.
Tests	Numéro	Nombre de tests avec des résultats de test ayant échoué.
Hôtes	Numéro	Nombre d'hôtes avec des résultats des tests ayant échoué.
Résultats des tests	Numéro	Affiche le nombre de résultats des tests.
Résultats des tests ayant échoué par cote de risque	Couronne	Affiche le nombre de tests ayant échoué par cote de risque.
Résultats des tests échoués par technologie	Couronne	Affiche les modèles avec des tests ayant échoué.
Résultats des tests échoués par catégorie	Histogramme	Affiche les catégories avec le plus grand nombre d'échecs aux tests.
Ouvrir les résultats des tests par cote de risque	Histogramme	Affiche le nombre de résultats des tests ouverts par cote de risque.
Tâches de remédiation	Graphique	Affiche les tâches de remédiation par état et par cote de risque.

Conformité de la configuration tableau de bord

Celui-ci Solution Analyse des performances et Reporting contient du contenu préemballé Analyse des performances et Reporting du contenu à utiliser avec d'autres Now Platform produits. Cela Solution Analyse des performances et Reporting fournit une visibilité sur les configurations non conformes au niveau de l'hôte et du plan de contrôle du cloud.

Cette solution Platform Analytics contient du contenu pré-package d'analyse des performances et de génération de rapports à utiliser avec d'autres produits Now Platform. Cette solution Platform Analytics offre une visibilité sur les configurations non conformes au niveau de l'hôte et du plan de contrôle du cloud.

Le tableau de bord Analyse des performances pour Configuration Compliance contient plusieurs widgets qui présentent des données pour différentes dimensions. Il fournit une vue complète des tendances de conformité, des problèmes de configuration, des tendances de rattrapage et de la gestion des exceptions.

Remarque : Le Analyse des performances module d'extension for Conformité de la configuration doit être installé pour afficher le Conformité de la configuration tableau de bord [PA] dans le cadre de Next Experience travail. S'il n'est pas installé, vous pouvez afficher le tableau de bord existant, qui est créé à l'aide du cadre de travail de génération de rapports.

Activer Analyse des performances pour Conformité de la configuration

Activez l'application de pack ServiceNow Store de contenu pour le Solution Analyse des performances et Reporting.

Avant de commencer

Activez la version complète de l'abonnement de Analyse des performances sur l'instance où vous activez cette Solution Analyse des performances et Reporting. Vous pouvez activer

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Analyse des performances sur une instance de non-production sans acheter d'abonnement. Pour plus d'informations, consultez Activer votre abonnement Analyse des performances .

Vous avez besoin d'un compte et d'une autorisation pour demander des Now Support demandes pour les instances considérées. Le Now Support compte et l'instance doivent faire partie de la même société. Pour plus d'informations, voir Installer un produit ServiceNow dans le ServiceNow Store.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Utilisez Analyse des performances le Conformité de la configuration tableau de bord pour générer des rapports sur les tâches de rattrapage, l'état de conformité, les actions de rattrapage et les demandes d'exception.

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications** > **ServiceNow Store**.
2. Recherchez Analyse des performances et vérifiez Conformité de la configuration que vous disposez des autorisations valides.
3. `Recherchez Analyse des performances pour Configuration Compliance`.
4. Installez l'application.

   Lorsque vous installez cette application, vous l'activez Conformité de la configuration également.

Affichage du Analyse des performances tableau de bord for Conformité de la configuration

Vous pouvez gérer vos problèmes de configuration les plus importants et les résoudre rapidement en affichant les rapports sur le Conformité de la configuration Analyse des performances tableau de bord (PA).

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Rôles Now Platform requis

Les rôles suivants sont requis pour le Conformité de la configuration Analyse des performances tableau de bord :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- admin : un administrateur peut installer et activer le Analyse des performances for Conformité de la configuration et apporter des modifications aux propriétés système.
- pa_admin : Un administrateur Performance Analytics peut créer et examiner les tâches en arrière-plan, les indicateurs, les répartitions, les widgets et les tableaux de bord. Cet administrateur peut également configurer et démarrer la collecte de données.
- sn_vulc.read : un utilisateur disposant du rôle read peut examiner les données du tableau de bord.

Accéder au Conformité de la configuration tableau de bord

Pour ouvrir le tableau de bord, accédez à **Tout** > **Configuration Compliance** > **Vue d'ensemble**.

À partir de la version 14.9 de , ce tableau de bord peut également être consulté dans la nouvelle interface utilisateur d'expérience Conformité de la configuration. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez les tableaux de bord dans Vulnerability Manager Workspace et les tableaux de bord dans IT Remediation Workspace.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une certaine perte fonctionnelle.

Conformité de la configuration [PA] Onglets de tableau de bord

Onglet Vue d'ensemble

L'onglet **Vue d'ensemble** fournit cinq filtres. Il s'agit de la catégorie d'actifs, du type de ressource dans le cloud, du fournisseur de services dans le cloud, du compte dans le cloud et de la région dans le cloud, que vous pouvez appliquer pour visualiser les rapports correspondant aux filtres appliqués. Si vous sélectionnez une catégorie et appliquez les modifications, tous les widgets prenant en charge la catégorie sont actualisés. Chaque widget affiche le filtre appliqué en bas et le nombre de filtres appliqués sur l'icône de filtre du widget. Cliquez sur le rapport dans un widget pour afficher les informations supplémentaires dans l'onglet **Détails des KPI** . Dans l'onglet **Détails des KPI** , vous pouvez :

- Affichez les enregistrements.
- Comparez les enregistrements.
- Changez le type de graphique.
- Sélectionnez la plage de dates.
- Affichez les tendances basées sur la durée.
- Appliquez les filtres supplémentaires, y compris les filtres qui ne sont pas disponibles dans l'onglet **Vue d'ensemble** . La balise Host en est un exemple.

L'exemple suivant montre comment appliquer les filtres dans l'onglet **Vue d'ensemble** et effectuer les actions dans l'onglet **Détails des KPI** .

Onglet Vue d'ensemble dans le tableau de bord Configuration Compliance

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Conformité

L'onglet **Conformité** affiche le pourcentage de conformité pour les différentes sources faisant autorité, telles que la loi HIPAA (Health Insurance Portability and Accountability Act) et la DISA (Data Interchange Standards Association). Vous pouvez affiner cette liste en utilisant les filtres d'en-tête de colonne et en sélectionnant une catégorie.

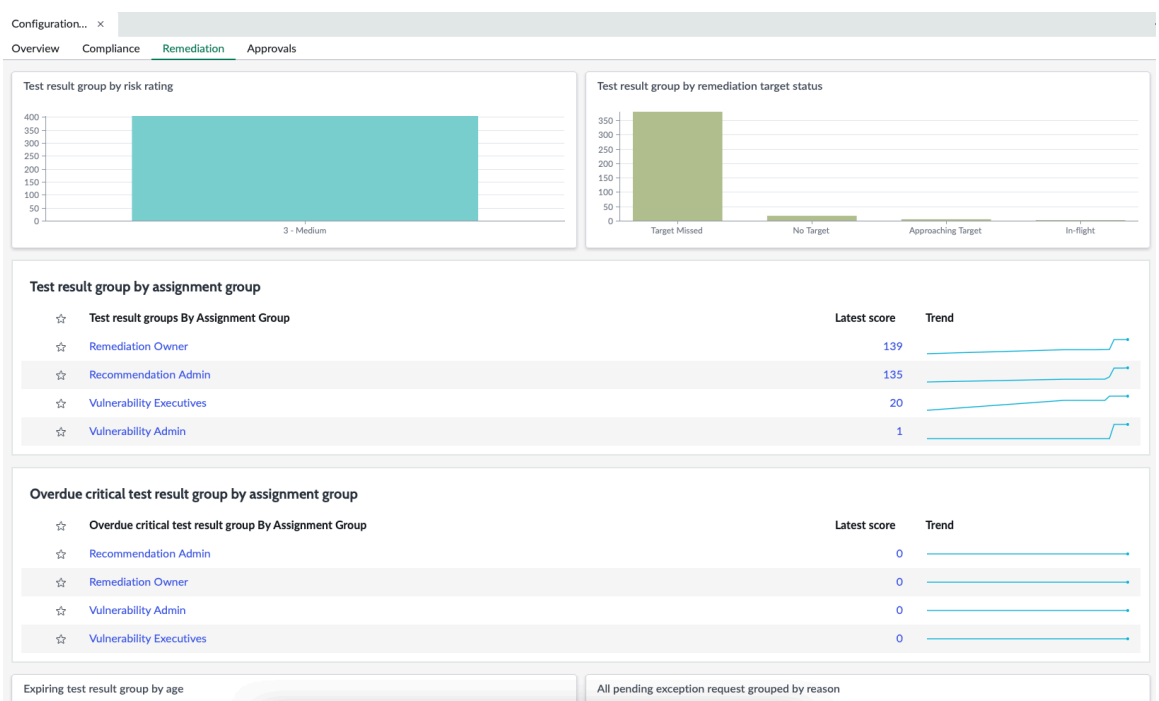
L'exemple suivant montre comment filtrer les données dans l'onglet **Conformité** .

Onglet Conformité du tableau de bord Configuration Compliance

Onglet Rattrapage

L'onglet **Rattrapage** affiche des informations sur la progression du rattrapage. Vous pouvez utiliser cet onglet pour voir dans l'hygiène de correction de la mauvaise configuration.

L'exemple suivant montre l'onglet **Correction** .



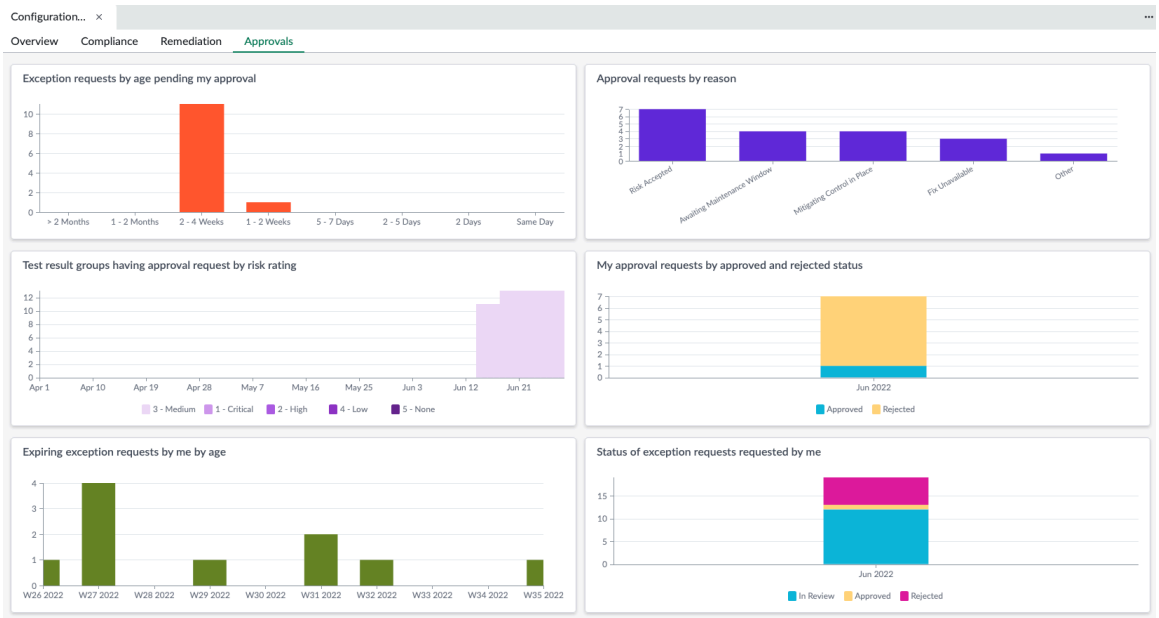
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Approbations

Les rapports de l'onglet **Approbations** affichent des informations sur les demandes d'exception et leur état d'approbation.

L'exemple suivant montre l'onglet **Approbations** .



Répartitions

Les répartitions utilisées par les indicateurs sont les suivantes :

- Raison de l'ajournement
- Âge
- Groupe d'affectation
- État du rattrapage
- Résultat
- Cote de risque
- Catégorie d'actif
- Balise d'hôte
- Test de configuration
- Fournisseur de services dans le cloud
- Région du cloud
- Compte dans le cloud
- Type de ressource dans le cloud

Filtres

Dans l'onglet **Vue d'ensemble** , vous pouvez appliquer les filtres suivants aux widgets pour visualiser les données filtrées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Catégorie d'actif	Choix	Type d'actif. Les quatre options sont les suivantes : • Dans le cloud • Conteneur • Infra • OT
Type de ressource dans le cloud	Choix	Type de ressource. Un ordinateur virtuel en est un exemple. Les données du filtre sont renseignées lorsque vous exécutez l'intégration.
Fournisseur de services dans le cloud	Choix	Fournisseur de service pour le cloud. Les trois options sont les suivantes : • Amazon Web Services (AWS • Microsoft Azure • Google Cloud Platform (GCP)
Compte dans le cloud	Choix	ID de compte créé lorsqu'un compte est créé dans un service dans le cloud. Par exemple, AWS. Les données d'ID de compte sont renseignées dans le filtre lorsque vous exécutez l'intégration.
Région du cloud	Choix	Emplacement où la ressource est hébergée.

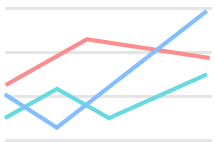
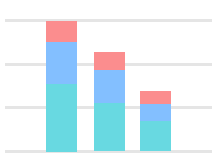
Remarque : Vous pouvez sélectionner plusieurs options parmi les filtres et sélectionner **Appliquer**. Chaque widget affiche les filtres appliqués et ceux qui ne le sont pas. En fonction des données disponibles, le rapport est généré. Le widget indique également le nombre de filtres pris en charge.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations des données

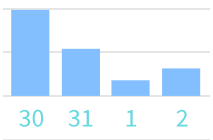
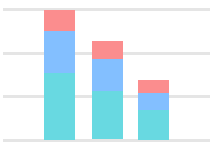
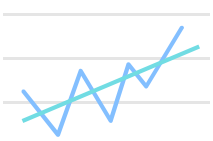
Visualisations de l'onglet Vue d'ensemble

Nom du rapport	Type	Table source	Description
Tendance de conformité	Graphique en courbes 	Résultats des tests	Informations sur la tendance de conformité : • Ressources : nombre total de ressources disponibles dans le système. • Échec : nombre de ressources avec au moins un résultat de test ayant échoué. • Réussite : nombre de ressources avec tous les résultats des tests dans l'état Réussi.
Tâche de rattrapage	Score unique 	Résultats des tests	Nombre de tâches de rattrapage présentes dans le système et à l'état actif.
Tâches de remédiation critiques proches de l'échéance	Score unique 	Résultats des tests	Nombre de tâches de rattrapage dont la cote de risque est « critique » et dont l'état de rattrapage est « proche de la cible ».
Résultats des tests par cote de risque	Histogramme 	Résultats des tests	Résultats des tests à l'état Échec, qui sont regroupés en fonction de la cote de risque.
Résultats des tests par âge	Histogramme	Résultats des tests	Résultats des tests à l'état Échec, qui

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

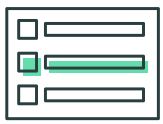
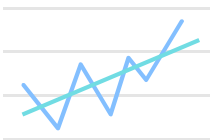
Visualisations de l'onglet Vue d'ensemble (suite)

Nom du rapport	Type	Table source	Description
			sont regroupés en fonction de la date de création des résultats des tests.
Résultats des tests fermés par respect de la cible de rattrapage	Histogramme 	Résultats des tests	Résultats du test à l'état Réussi, ce qui indique que ce test est fermé.
Résultats des tests critiques en retard par groupe d'affectation	Liste et score 	Résultats des tests	Nombre de résultats des tests pour lesquels la cote de risque est « critique » et l'état du rattrapage est « cible manquée ». Le rapport indique que les résultats des tests sont à l'état Ouvert. Si les résultats du test dépassent la date cible de rattrapage, cela est considéré comme en retard.
Résultats des tests en retard - Services	Liste, score et tendance  	Vue de base de données des tableaux de bord PA pour Services	Nombre de résultats des tests pour les services pour lesquels l'état de rattrapage est « Cible manquée ». Ce rapport affiche également le nom des services ou des départements ayant obtenu les meilleurs résultats aux tests.
Résultats des tests en retard : propriétaires de services	Liste, score et tendance	Vue de base de données des tableaux de bord PA pour Services	Nombre de résultats des tests pour les propriétaires de services dont l'état

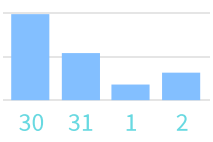
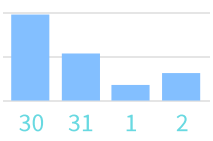
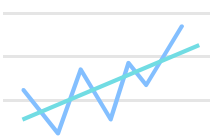
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations de l'onglet Vue d'ensemble (suite)

Nom du rapport	Type	Table source	Description
	 		de rattrapage est « Cible manquée ». Ce rapport affiche également le nom des services ou des départements ayant obtenu les meilleurs résultats aux tests.

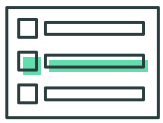
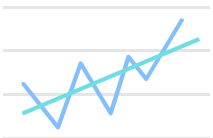
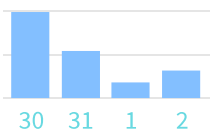
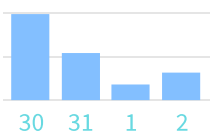
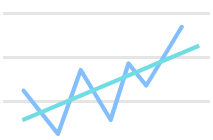
Visualisations de l'onglet Rattrapage

Titre	Type	Table source	Description
Tâches de remédiation par cote de risque	Histogramme 	Tâche de rattrapage	Répartition des évaluations de risque de tous les groupes de résultats des tests qui sont dans l'état actif.
Tâches de remédiation par état de la cible de remédiation	Histogramme 	Tâche de rattrapage	Répartition des cibles de rattrapage de tous les groupes de résultats des tests qui ont manqué la cible, n'ont pas de cible et s'approchent de la cible.
Tâche de remédiation par groupe d'affectation	Liste, score et tendance  	Tâche de rattrapage	Répartition des tâches de rattrapage basées sur un groupe d'affectation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

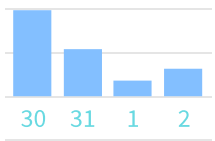
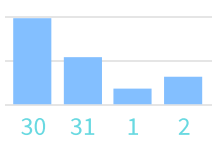
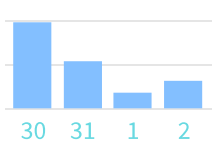
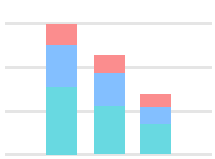
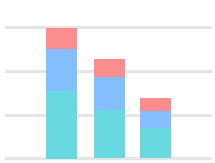
Visualisations de l'onglet Rattrapage (suite)

Titre	Type	Table source	Description
Tâche de remédiation critique en retard par groupe d'affectation	Liste, score et tendance  	Tâche de rattrapage	Répartition des tâches de rattrapage basées sur un groupe d'affectation. Ces tâches de rattrapage ont une cote de risque comme « critique » et leur cible de rattrapage n'a pas été atteinte.
Tâches de remédiation arrivées à expiration par âge	Histogramme 	Tâche de rattrapage	Tâches de rattrapage qui vont expirer au bout d'une certaine durée. Un maximum de 10 compartiments de durée peut être créé.
Toutes les demandes d'exception en attente regroupées par motif	Histogramme 	Approbation de changement de l'état	Demandes d'approbation de changement d'état regroupées par motif de l'exception.
Exceptions critiques sur les résultats des tests par groupe d'affectation	Liste, score et tendance  	Résultats des tests	Résultats des tests qui sont dans un état Différé et Critique et qui sont regroupés en fonction du groupe d'affectation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

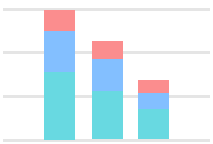
Visualisations de l'onglet Approbations

Rapports	Type	Table source	Description
Demandes d'exception par âge en attente de mon approbation	Histogramme 	Approbation	Demandes d'exception que vous avez créées et qui sont en attente d'approbation. Les demandes sont regroupées en fonction de la durée de la demande.
Demandes d'approbation par motif	Histogramme 	Approbation de changement de l'état	Demandes d'approbation de changement d'état pour créer une exception et inclure le motif de l'exception.
Tâches de remédiation avec une demande d'approbation par cote de risque	Histogramme 	Tâche de rattrapage	Tâches de rattrapage qui ont une demande d'approbation basée sur la criticité.
Mes demandes d'approbation par état approuvé et rejeté	Histogramme 	Approbation de changement de l'état	Demandes d'exception regroupées selon les états approuvé et rejeté.
Mes demandes d'exception arrivant à échéance par âge	Histogramme 	Approbation de changement de l'état	Demandes d'exception qui vont arriver à expiration dans les semaines à venir. Les demandes d'exception sont regroupées par semaines. Chaque fois qu'une demande d'exception est créée, une date est sélectionnée pour la validité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations de l'onglet Approbations (suite)

Rapports	Type	Table source	Description
			de la demande d'exception. Le calcul de l'âge de la demande est basé sur cette date.
État des demandes d'exception demandées par moi	Histogramme 	Approbation de changement de l'état	Demandes d'exception que vous avez créées et qui sont regroupées en fonction des états suivants : • En cours de révision • Approuvé • Rejeté

Conformité de la configuration Informations de référence

Plusieurs types de composants sont installés avec l'activation de l'application, notamment les tables, les travaux planifiés et les Conformité de la configuration rôles d'utilisateur.

Les rubriques suivantes vous fournissent des informations de référence et de dépannage, ainsi que des données de champ sur les formulaires et enregistrements disponibles dans Conformité de la configuration.

- Composants installés avec Conformité de la configuration
- Champs Résultats des tests
- Résolution des Conformité de la configuration problèmes d'importation
- Modifier la date de début des résultats de l'application PC Qualys

Afficher les Conformité de la configuration groupes de tests

Une fois que vous avez importé les résultats d'une analyse tierce dans votre instance, vous pouvez voir la conformité de vos tests au niveau du groupe de tests. Utilisez cette vue avant un audit de ce groupe de tests et de tous les enregistrements de tests associés.

Avant de commencer

Rôle requis : sn_vulc.read et sn_vulc.remediation_owner pour afficher

Pourquoi et quand exécuter cette tâche

Les politiques sont des enregistrements importés et non modifiables à l'intérieur .Conformité de la configuration

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Groupes de tests**.
   La liste des résultats des tests s'affiche. À partir de la version 15.0 de , la colonne **% de conformité** des Conformité de la configurationrésultats des tests affiche le pourcentage de résultats des tests conformes aux tests d'un groupe de tests.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

% de conformité des résultats des tests = (Nombre de résultats des tests fermés dans un groupe de tests/Nombre total de résultats des tests associés à un groupe de tests) * 100

2. Cliquez sur la **Description brève** du groupe de tests que vous souhaitez afficher.

Conformité de la configuration Champs du formulaire Groupe de tests

Champ	Description
Source	Nom du système de l'analyseur tiers, ou nom saisi dans le module d'extension ServiceNow de l'API utilisée pour communiquer avec Conformité de la configuration.
Technologies	Liste des technologies associées au groupe de tests dans l'application de scanner tierce.
ID source	Identificateur affecté à ce groupe de tests par le scanner tiers.
Source créée	La date et l'heure auxquelles le groupe de tests a été défini dans l'application de scanner tiers.
Source mise à jour	Date et heure auxquelles le groupe de tests a été modifié pour la dernière fois dans l'application de scanner de stratégie tierce.
Description brève	Description ou titre du résumé affecté au groupe de tests dans l'application de scanner tiers.
Description	Description détaillée du groupe de tests tel que défini dans l'application de scanner tiers.
Tests	Liste des tests qui référencent ce groupe de tests. Importée à partir de l'analyseur tiers. Si nécessaire, vous pouvez accéder à la liste pour obtenir des informations détaillées sur un test spécifique.
État du rattrapage (version 12.0)	
Exclut les éléments différés	Ces valeurs n'incluent pas les CI provenant de résultats des tests différés. ◦ **CI restants** : nombre d'éléments de configuration (CI) avec des résultats des tests actifs (tout état autre que **Fermé**) pour cette politique. ◦ **% des CI rattrapés** : pourcentage de CI conformes pour ce groupe de tests. Ce

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	nombre exclut les CI avec des résultats des tests différés. ◦ **CI totaux** : nombre total de CI impactés par ce groupe de tests. Ce nombre exclut les résultats des tests différés.
Inclut les éléments différés	Les valeurs représentent les CI de tous les résultats des tests actifs (tout état autre que **Fermé**). ◦ **CI restants** : nombre de CI uniques associés à un ou plusieurs résultats des tests non fermés auxquels ce groupe de tests a été appliqué. ◦ **% de CI rattrapés** : pourcentage de CI conformes pour ce groupe de tests. ◦ **CI totaux** : nombre total de CI impactés par ce groupe de tests.

À partir de la version 12.0, pour mettre à jour ces valeurs sur demande, sous l'onglet État du rattrapage, cliquez sur le lien connexe **Mettre à jour l'état** . Un message s'affiche indiquant que les données sont en cours d'actualisation. Cliquez sur le lien **Afficher l'état** pour afficher la progression de la mise à jour. Après quelques instants, toutes les données qui ont changé ou été mises à jour depuis la dernière tâche planifiée sont actualisées dans l'enregistrement. Les valeurs de champ mises à jour sont actualisées.

3. Facultatif : Désactivez l'importation des résultats des tests pour un groupe de tests en cliquant sur le bouton **Désactiver l'importation** .

   (Optional) La valeur de la colonne **L'importation est-elle désactivée** devient *vrai*. Les résultats des tests pour le groupe de tests ne sont pas importés à partir de l'ingestion à venir.

   Remarque : Le bouton **Désactiver l'importation** n'est disponible que pour les résultats des tests obtenus à partir Qualys du scanner.

   À partir de la v23.0 de Réponse aux vulnérabilités:

   - Vous pouvez activer ou désactiver l'importation des résultats des tests pour un groupe de Qualys tests dans le Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Activer ou désactiver l'importation de résultats des tests pour un groupe de Qualys tests.
   - Le bouton **Marquer comme déconseillé** est renommé en **Désactiver l'importation**.
   - La colonne **Est déconseillée** est renommée en **Est importation désactivée**.

Afficher Conformité de la configuration les sources de référence

Utilisez ce module pour afficher des informations récapitulatives sur chaque source de référence et pour rechercher les publications sources qui ont été utilisées pour créer la notice.

Avant de commencer

Rôle requis :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vulc.admin à mettre à jour
- sn_vulc.remediation_owner à afficher

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Données associées** > **Sources d'autorité**.
2. Cliquez sur la **Description brève** de la source de référence que vous souhaitez afficher.

Conformité de la configuration Champs de formulaire Sources de référence

Champ	Description
Numéro	Numéro d'ID affecté à la source de référence par votre instance pendant le processus d'importation.
Source	Nom du système de l'application de scanner tierce ou nom saisi dans le module d'extension de scanner pour l'API qui communique avec Conformité de la configuration.
ID source	Identificateur affecté à la source de référence par le scanner tiers.
Description brève	Nom donné à cette source de référence dans l'analyseur tiers.
Éditeur	Nom de l'organisation ou de la publication qui était la source d'information d'origine pour cette source faisant autorité.
Contenu des documents de référence	Liste des informations citées sur les résultats des tests. Importée à partir de l'analyseur tiers. Vous pouvez accéder à cette liste pour obtenir des informations détaillées sur un test spécifique, si nécessaire.

3. Facultatif : Ajouter un **éditeur**.
4. Cliquez sur **Mettre à jour**.
5. Vous pouvez supprimer cet enregistrement en cliquant sur **Supprimer**.
   Supprime l'enregistrement de votre instance. S'il est toujours utilisé dans votre intégration tierce, il est renvoyé lors de l'importation suivante

Afficher Conformité de la configuration les technologies

Utilisez ce module pour afficher des informations récapitulatives sur chaque source et citation faisant autorité (également connu sous le nom de cadre de travail dans Qualys). Vous pouvez rechercher les publications sources qui ont été utilisées pour créer l'enregistrement.

Avant de commencer

Rôle requis :

- sn_vulc.admin à mettre à jour
- sn_vulc.remediation_owner à afficher

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Données associées** > **Technologies**.
2. Cliquez sur la **Description brève** de la source de référence que vous souhaitez afficher.

Conformité de la configuration Champs de formulaire Sources de référence

Champ	Description
Numéro	Numéro d'ID affecté à la source de référence par votre instance pendant le processus d'importation.
Source	Nom du système de l'analyseur tiers ou nom saisi dans le module d'extension de scanner tiers pour l'API qui communique avec Conformité de la configuration.
ID source	Identificateur affecté à la source de référence par le scanner tiers.

3. Vous pouvez supprimer cet enregistrement en cliquant sur **Supprimer**.
   Supprime l'enregistrement de votre instance. S'il est toujours utilisé dans votre intégration tierce, il est renvoyé lors de l'importation suivante

Afficher les Conformité de la configuration tests

Utilisez ce module pour rechercher des informations détaillées sur ces tests. Sont incluses les citations de sources expertes qui ont été utilisées lors de leur création, les politiques de configuration tierce dans lesquelles elles sont utilisées et les résultats obtenus à partir de l'analyse.

Avant de commencer

Rôle requis :

- sn_vulc.admin à mettre à jour
- sn_vulc.remediation_owner à afficher

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Contrôles**.
2. Accédez à la **Tout** > **Configuration Compliance** > **Tests**
3. Dans la liste, ouvrez le contrôle (test de conformité) que vous souhaitez afficher.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de la version 12.0, pour mettre à jour ces valeurs sur demande, sous l'onglet État du rattrapage, cliquez sur le lien connexe Mettre **à jour l'état** . Un message s'affiche indiquant que les données sont en cours d'actualisation. Cliquez sur le lien **Afficher l'état** pour afficher la progression de la mise à jour. Après quelques instants, toutes les données qui ont changé ou été mises à jour depuis la dernière tâche planifiée sont actualisées dans l'enregistrement. Les valeurs de champ telles que le**score de risque**, la **cote de risque**, la **date cible de rattrapage**,**l'état** et les champs de l'onglet État de rattrapage sont actualisées.

Conformité de la configuration Champs de formulaire de test

Champ	Description
Numéro	Numéro affecté au contrôle pendant le processus d'importation.
Résultat	État de l'analyse. Réussite ou échec. Si ce test appartient à plusieurs tâches de rattrapage, son état est déterminé suivant un ordre de priorité.
Source	Nom du système de l'application d'intégration tierce ou nom saisi dans le module d'extension de l'API utilisée pour communiquer avec Conformité de la configuration.
Criticité	Gravité du ou des problèmes de configuration associés au contrôle tels que définis dans l'intégration tierce. Le niveau de criticité est ajusté pour correspondre à la granularité des indicateurs de vulnérabilité similaires disponibles dans Réponse aux vulnérabilités. Les niveaux possibles sont les suivants : Critique Le problème de configuration associé au contrôle perturbe un ou plusieurs CI critiques pour l'entreprise. Élevé Le problème de configuration associé au contrôle constitue une menace, mais n'entraîne pas l'arrêt des ressources réseau critiques. Modéré Le problème de configuration associé au contrôle constitue un risque, mais pas une menace immédiate. Faible Le problème de configuration associé au contrôle est une

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	menace de faible niveau qui peut être ignorée au profit des CI les plus exposés. Mineur Le problème de configuration associé au contrôle représente un risque mineur et peut être ignoré si nécessaire.
ID source	Identificateur affecté au contrôle par l'intégration tierce.
Catégorie	Catégorie de classification majeure donnée à ce type de contrôle par le fournisseur tiers.
Score du risque	Il s'agit d'un score de risque de déploiement. Ce score de risque est pondéré : 85 % du score du score de risque maximal pour tous les résultats des tests ne sont pas « Fermés » (Ouvert, En cours d'examen, En attente d'implémentation, Différé, Résolu) et 15 % du score provient du nombre de résultats des tests qui ne sont pas « Fermés ». Valeur calculée par les calculateurs de score de risque qui est basée sur les valeurs de criticité opérationnelle et de criticité de test des résultats des tests.
Sous-catégorie	Sous-catégorie affectée à cette classe de test par le fournisseur tiers.
Cote de risque	Basé sur une plage de scores de risque sur une échelle numérique de 1 à 5 qui évalue le risque global en fonction d'une plage de scores de risque allant de 1 - Critique à 5 - Aucun. Ce champ remplace le champ Priorité dans les versions précédentes.
Technologies	Liste des technologies couvertes par ce test.
Source créée	Date à laquelle le test a été défini pour la première fois dans l'intégration tierce.
Source mise à jour	Date de la dernière mise à jour du test dans l'intégration tierce.
Description brève	Résumé, description ou titre saisi ou affecté au test dans l'intégration tierce.
État du rattrapage (v 12.0)	
Exclut les éléments différés	Ces valeurs n'incluent pas les résultats des tests différés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ **Résultats des tests ouverts** : nombre (nombre) de résultats des tests actifs (tout état autre que **Fermé**) pour ce test de configuration. ◦ **% des résultats des tests corrigés** : pourcentage de résultats des tests rattrapés pour cette tâche de rattrapage. ◦ **Résultats des tests totaux** : nombre total de résultats des tests pour cette tâche de rattrapage.
Inclut les éléments différés	Ces valeurs incluent les résultats des tests différés. ◦ **Résultats des tests ouverts** : nombre de résultats des tests actifs (tout état autre que Fermé) pour cette tâche de **rattrapage**. ◦ **% des résultats des tests corrigés** : pourcentage de résultats des tests rattrapés pour cette tâche de rattrapage. ◦ **Résultats des tests totaux** : nombre total de résultats des tests pour cette tâche de rattrapage.
Description	Longue description du test. Pour Qualys Vulnerability Integration, ce champ correspond par défaut au contenu de la Qualys Cloud Platform page de couverture.
Rattrapage	Étapes : instructions décrivant comment corriger la non-conformité.
Onglets associés	
Contenu des documents de référence	Liste des citations saisies pour chaque source faisant autorité associée au test.
Groupes de tests	Liste des groupes de Conformité de la configuration tests qui utilisent ce test.
Résultats des tests	Liste des CI affectés par le ou les problèmes de configuration associés à ce test. Si nécessaire, vous pouvez accéder aux tests individuels, ServiceNow aux éléments de configuration ou à la liste des technologies concernées.
Déclarations de politique GRC	Si le module d'extension GRC Gestion de la politique et de la conformité est installé, cet onglet contient la stratégie connexe

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	GRC . Vous pouvez modifier cette liste pour ajouter ou supprimer des déclarations de politique.

Afficher les Conformité de la configuration résultats des tests

Affichez Conformité de la configuration les résultats des tests à des fins d'audit et de correction. Les résultats des tests sont automatiquement créés lors des importations d'intégration de vulnérabilité tierce.

Important : Vous pouvez afficher les résultats des tests créés lors des importations d'intégration de vulnérabilité tierce dans l'espace de travail du gestionnaire de vulnérabilité. Pour plus d'informations, consultez Vue d'ensemble des listes.

Avant de commencer

Rôle requis :

- sn_vulc.read pour afficher
- sn_vulc.remediation_owner pour afficher et mettre à jour
- sn_vulc.delete à supprimer

Pourquoi et quand exécuter cette tâche

Conformité de la configuration ne crée ni ne met à jour les résultats des tests, mais les importe dans le cadre d'une intégration tierce. Une fois qu'ils sont visibles dans , ils sont corrigés à Conformité de la configurationl'aide de **groupes de résultats des tests**.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Résultats des tests**.
   À partir de la version 15.0 de , les colonnes suivantes apparaissent dans la liste Résultats des Conformité de la configurationtests.

Liste des résultats des tests

Colonne	Description
Actif	Indique si un résultat de test est actif. Un résultat de test est marqué : ◦ Vrai : si l'état n'est pas fermé. ◦ Faux : si l'état est Fermé.
Âges à la fermeture	Période pendant laquelle un résultat de test est à l'état Fermé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Description
	Ce champ est vide pour un résultat de test actif. Format : Jours HH :MM : SS
Âge	Période pendant laquelle un résultat de test est actif depuis sa dernière ouverture. Ce champ est vide pour les résultats des tests fermés. Format : Jours HH :MM : SS
Fermé	Horodatage de la fermeture d'un résultat de test. Format : AAAA-MM-JJ HH :MM : SS
Dernières ouvertures	Horodatage auquel un résultat de test est ouvert, c'est-à-dire lorsque la valeur du champ **Actif** bascule sur *vrai*.

2. Ouvrez le contrôle que vous souhaitez afficher.

Conformité de la configuration Champs du formulaire Résultat de test

Champ	Description
Numéro	Numéro affecté au test au cours du processus d'importation.
Source	Nom du système de l'application SCA tierce ou nom saisi dans le module d'extension de l'application pour l'API utilisée pour communiquer avec Conformité de la configuration.
ID source	Identificateur affecté au contrôle par l'application SCA.
Résultat	Réussi, Échec, Erreur ou Inconnu. Importé de Qualys.
Score du risque	Résultat du calculateur pour ce test. Avant la version 15.0 de , le score de risque d'un résultat de Conformité de la configurationtest réussi est défini sur « 0 ». À partir de la version 15.0 de Conformité de la configuration, le score de risque du résultat des tests réussis n'est pas modifié en « 0 » afin que vous puissiez estimer le risque atténué. Le score de risque du résultat du test réussi n'est pas inclus dans le calcul du score de risque d'une tâche de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Cote de risque	Basé sur une plage de scores de risque sur une échelle numérique de 1 à 5 qui évalue le risque global en fonction d'une plage de scores de risque allant de 1 - Critique à 5 - Aucun. Ce champ remplace le champ Priorité dans les versions précédentes.
État	Calculé à partir des tâches de rattrapage auxquelles appartient le résultat du test. Si le résultat du test appartient à plusieurs groupes, un ordre de priorité est appliqué pour déterminer l'état .
Résolution	Calculé à partir des tâches de rattrapage auxquelles appartient le résultat du test. Si le résultat du test appartient à plusieurs groupes, un ordre de priorité est appliqué pour déterminer la résolution.
Premier observé	Date de la première importation dans Conformité de la configuration. À partir de la version 13.1.1, le champ **Premier observé** affiche la date fournie par le scanner. Sinon, il affiche la date de la première importation dans Conformité de la configuration.
Dernier observé	Date de la dernière importation dans Conformité de la configuration. À partir de la version 13.1.1, le champ **Dernier observé** affiche la date fournie par le scanner. Dans le cas contraire, la date de la dernière importation dans Conformité de la configuration.
Dernière transmission	Dernière date à laquelle le résultat du test est réussi.
Test	Nom du test.
Élément de configuration	Nom du CI joint au test.
Technologie	Version du logiciel en cours d'exécution sur le CI.
Description	Description du test
Valeurs attendues	Valeurs attendues configurées dans Qualys et importées par Conformité de la configuration. Cette valeur est une expression booléenne qui, lorsqu'elle est évaluée à vrai, rend le résultat du test **réussi.** L'expression peut être une combinaison d'opérateurs d'expression logique, ensemestre ou régulière.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Valeurs réelles	Valeurs retournées par le test. Ces valeurs sont insérées dans l'expression booléenne des valeurs attendues pour déterminer si le résultat doit réussir ou échouer. Ils sont importés de Qualys À partir de la version 14.9 de Conformité de la configuration, les valeurs Extended Evidence (Preuve étendue) et Cause of Failure (Cause de défaillance) sont ajoutées dans la colonne Valeurs réelles.
Rattrapage	Instructions de rattrapage.
Onglets associés	
Tâches de remédiation	Tâches de rattrapage associées à ce résultat de test.
Historique des résultats des tests	Liste connexe des résultats des tests qui affiche l'historique des résultats de réussite/échec pour le même CI/technologie/test.

Afficher une tâche de rattrapage

Vous pouvez afficher ou créer une tâche de rattrapage et effectuer un rattrapage.

Important : Vous pouvez afficher les tâches de rattrapage dans l'espace de travail du gestionnaire de vulnérabilité. Pour plus d'informations, consultez Vue d'ensemble des listes.

Avant de commencer

Rôle requis :

- sn_vulc.admin pour mettre à jour ou créer
- sn_vulc.remediation_owner à afficher

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Configuration Compliance** > **Tâches de remédiation**.
2. Dans la liste, cliquez sur l'enregistrement que vous souhaitez afficher.
3. Vous pouvez également cliquer sur **Nouveau** pour créer une nouvelle tâche de rattrapage et renseigner les champs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs du formulaire Tâche de rattrapage de Configuration Compliance

Champ	Description
Numéro	Numéro généré automatiquement pour cet enregistrement.
État	État de progression du groupe. ◦ Ouvrir ◦ En cours d'examen ◦ En attente d'implémentation ◦ Différé ◦ Résolu ◦ Fermé
Score du risque	Ce score est la valeur cumulée des scores de risque pour tous les résultats des tests actifs dans une tâche de rattrapage. Ce score change au fur et à mesure que les résultats des tests sont corrigés dans le groupe de résultats des tests.
Groupe d'affectation	Groupe sélectionné pour travailler sur cette tâche de rattrapage.
Cote de risque	Degré de risque que représente un résultat de test échoué pour votre système. Il est basé sur une gamme de scores de risque sur une échelle numérique de 1 à 5 qui classe les risques de Critique (1) à Aucun (5).
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cet ensemble de tâches.
Cible de rattrapage	Date à laquelle les résultats des tests doivent être corrigés, dès lors qu'ils ont été identifiés pour la première fois.
Créé	Date et heure de création de cette tâche de rattrapage.
État du rattrapage	État du rattrapage pour le groupe. Il est déterminé par le résultat du test dont la date d'échéance est la plus proche. Pour les groupes ouverts, les états incluent En vol, Cible en approche et Cible manquée. Pour les groupes fermés, les états incluent Aucune cible, Cible atteinte et Cible manquée. Pour les dates cibles de rattrapage calculées, si la tâche de rattrapage est fermée, l'état de rattrapage global de tous les résultats des tests fermés est affiché

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	dans la tâche de rattrapage. Ceux-ci déterminent si le groupe a respecté sa date ou non. L'état de rattrapage d'une tâche de rattrapage fermée est **Aucun objectif** si aucun de ses résultats fermés n'avait de date cible de rattrapage. Il s'agit **d'une cible manquée** si l'un de ses résultats fermés a manqué sa date cible. **L'objectif est atteint** si au moins un résultat fermé a atteint son objectif et qu'aucun des autres ne l'a manqué.
Mis à jour	Date et heure de la dernière modification de cet enregistrement.
Description brève	Brève description de ce groupe de résultats de test.
Description	Description longue du groupe de résultats des tests incluant la liste des logiciels associés à ce groupe de résultats des tests.
Test	Test de configuration associé à ce groupe de résultats de test.
État du rattrapage (version 12.0)	
Exclut les éléments différés	Ces valeurs n'incluent pas les résultats des tests différés. ◦ **Résultats des tests ouverts** : nombre de résultats des tests actifs (tout état autre que Fermé) pour cette tâche de **rattrapage**. ◦ **% des résultats des tests corrigés** : pourcentage de résultats des tests corrigés (fermés) pour ce groupe de résultats des tests. ◦ **Résultats des tests totaux** : nombre total de résultats des tests pour cette tâche de rattrapage.
Inclut les éléments différés	Les valeurs représentent tous les résultats des tests actifs (tout état autre que **Fermé**). ◦ **Résultats des tests ouverts** : nombre de résultats des tests actifs (tout état autre que **Fermé**) pour ce groupe de résultats des tests. ◦ **% de résultats des tests corrigés** : pourcentage de résultats des tests

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	rattrapés (fermés) pour cette tâche de rattrapage. ◦ **Résultats des tests totaux** : nombre total de résultats des tests pour cette tâche de rattrapage.
Configuration du groupe	Type de filtrage utilisé pour sélectionner les résultats des tests pour la tâche de rattrapage.
Méthode de regroupement	Nom de la méthode utilisée.
Règle de groupe	Nom de la règle de groupe utilisée.
Notes	Notes système associées à l'enregistrement.
Liens connexes	**Version 12.0 : mettre à jour le lien d'état**. Mettre à jour les valeurs de l'enregistrement des résultats des tests sur demande. Affichez toutes les données qui ont changé ou été mises à jour depuis la dernière tâche planifiée.
Résultats des tests	Résultats du test dans cette tâche de rattrapage.
Demandes de changement (v 12.0)	Liste des demandes de changement associées à ce groupe de résultats de test.
Approbations de changement de l'état (v 12.0)	État et états des approbations de demande de changement associées à cette tâche de rattrapage.

Transitions d'état des résultats des tests et des tâches de rattrapage dans l'application Conformité de la configuration

Les états des enregistrements de tests de configuration et des tâches de rattrapage (RT) qui leur sont associées sont impactés si les enregistrements de résultats des tests sont reportés, résolus, rouverts et transférés à d'autres efforts de rattrapage (ER).

Scénarios de transitions d'états entre les résultats des tests et les tâches de rattrapage

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

La table suivante détaille la façon dont les états et les sous-états font la transition entre les résultats des tests de configuration et les tâches de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si l'état d'une tâche de rattrapage passe de...	... États/sous-états de destination	Les états des résultats des tests qui lui sont associés passent de...	... États/sous-états de destination	Description
Ouvrir	En cours d'examen	Ouvrir	En cours d'examen	Les États font la transition de manière bidirectionnelle.
Ouvrir	En cours de révision	Ouvrir	En cours de révision	Les États font la transition de manière bidirectionnelle.
Ouvrir	Différé/avec n'importe quel motif sélectionné pour la résolution	Ouvrir	Différé	Les résultats des tests conservent le même motif de résolution que la tâche de rattrapage.
Différé/avec n'importe quel motif de résolution	Ouvrir	Les résultats des tests restent différés		Les résultats des tests conservent la même résolution que la tâche de rattrapage.
Ouvrir	Résolu/Corrigé	Ouvrir	Résolu	Les États/ sous-États font la transition de manière bidirectionnelle.
Ouvrir	Résolu et Résolu à Fermé/Corrigé	Ouvrir	Résolu	Si une tâche de rattrapage passe à l'état Fermé/Fixe, elle peut revenir à l'état Ouvert. Si la tâche passe à l'état Ouvert, les résultats des tests qui lui sont associés passent de Résolu à Ouvert.
Ouvrir	Résolu	Ouverts	Résolu	Les États/ sous-États font la transition de manière bidirectionnelle.
Ouvrir	Résolu/Annulé	Ouvrir	Résolu	Les États/ sous-États font la transition

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si l'état d'une tâche de rattrapage passe de...	... États/sous-états de destination	Les états des résultats des tests qui lui sont associés passent de...	... États/sous-états de destination	Description
				de manière bidirectionnelle.
Ouvrir	Résolu et Résolu à Fermé	Ouvrir	Résolu	Si une tâche de rattrapage passe automatiquement à l'état Fermé, ses résultats des tests associés peuvent revenir à l'état Ouvert.
Ouvrir	Résolu et Résolu à Fermé/Résultat non valide	Ouvrir	Résolu et Résolu à Fermé/Résultat non valide	Si une tâche de rattrapage passe à l'état Résolu, elle peut repasser à l'état Ouvert. Si une tâche de rattrapage passe à l'état Fermé/Résultat non valide, elle et ses résultats des tests associés ne peuvent pas être rouverts.
Ouvrir	Fermé/Fixe	Les résultats des tests restent ouverts		

Traduction automatique

Remarque :

- À partir de la version 14.12 de Conformité de la configuration, l'option **Résultat non valide** est supprimée dans la **résolution** déposée dans le modal Fermer.
- À partir de la version 14.12 du , le workflow **Approbation de l'état** de la tâche de Conformité de la configurationrattrapage est déconseillé et remplacé par l'Approbation de l'état de la tâche de rattrapage du flux dans le concepteur de flux.

Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage

Il existe une relation synchronisée entre les champs d'état des tâches de rattrapage et les champs d'état des demandes de changement (CHG) dans l'application Conformité de la configuration .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Au fur et à mesure qu'une demande de changement avance dans son cycle de vie, elle déplace automatiquement l'état de toutes les tâches de rattrapage connexes. La synchronisation d'état est activée par défaut par une propriété système de votre instance lorsque vous téléchargez l'application depuis le début de la Conformité de la configurationServiceNow Store version 12.0.

Lorsque la synchronisation d'état est activée, le champ État CHG change automatiquement le champ État de la tâche de rattrapage dans les cas suivants :

- Lorsqu'une nouvelle demande de changement est créée pour une tâche de rattrapage, si elle n'est pas en **attente d'implémentation**, l'état de la tâche de rattrapage passe à **En attente d'implémentation**.
- Lorsqu'une demande de changement existante est associée à une tâche de rattrapage, si elle n'est pas en **attente d'implémentation**, l'état de la tâche de rattrapage passe à **En attente d'implémentation**.
- Une fois que les tâches d'une demande de changement sont terminées (`implémentées`) et que le CHG est passé à l'état de **révision** , la tâche de rattrapage passe à **l'état Résolu**.

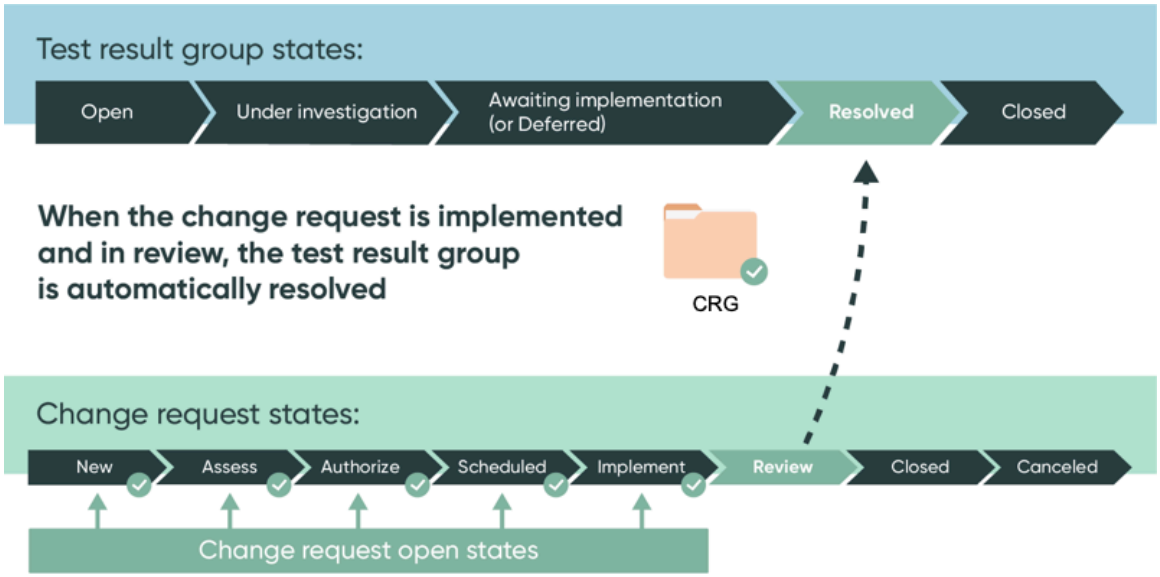
Pour plus d'informations et des exemples de synchronisation d'état, consultez les sections suivantes.

Remarque : Vous pouvez toujours déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre sur leurs enregistrements respectifs lorsque la synchronisation d'état est activée, mais lorsque le système enregistre qu'une demande de changement a changé d'état, ou que vous ajoutez une demande de changement ou que vous la supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la tâche de rattrapage de la zone **Fermée**.

Synchronisation de l'état vers l'avant

L'image suivante illustre comment les états CHG déplacent automatiquement les états des tâches de rattrapage dans un cycle de vie vers l'avant, c'est-à-dire **d'Ouvert** à **Résolu**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez créer de nouvelles demandes de changement pour n'importe quelle tâche de rattrapage dont l'état n'est pas **Résolu** ou **Fermé**. La synchronisation d'état déplace automatiquement le TRG de façon bidirectionnelle entre les états **Ouvert**, **En cours d'examen**, **En attente d'implémentation** et **Résolu** . Ce déplacement est basé sur certaines valeurs du champ d'état de la demande de changement. La synchronisation d'état entre la demande de changement et la tâche de rattrapage est invoquée automatiquement, sauf si la case à cocher (**Ajouter des CI au CR)** s'affiche sur un formulaire et que vous choisissez de la décocher.

La tâche de rattrapage ne passe pas à **l'état Résolu** lorsqu'un CHG est dans ses états ouverts. Tout CHG dans des états antérieurs à la **révision** dans son cycle de vie, tels que **Nouveau**, **Évaluer**, **Autoriser**, **Planifié** ou **Implémenter**, comme illustré dans la figure précédente, est considéré comme un état ouvert pour le CHG. Les états ouverts ne déplacent pas le champ État sur la tâche de rattrapage, car les enquêtes ou les tâches sur le CHG ne sont pas terminées. La synchronisation d'état est invoquée lorsqu'un CHG est créé pour la tâche de rattrapage ou associé à celle-ci, ou lorsque l'état d'une relation existante change sur le CHG. Les états CHG terminés sont **Examiner** et **Fermé** avec succès. Lorsqu'un CHG est fermé avec succès, ses codes fermés sont : **Réussi** ou **Réussi avec problèmes**, auquel cas la tâche de rattrapage passe à **Résolu**.

Synchronisation d'état en amont

Comme un CHG est traité au cours de son cycle de vie, il peut être annulé à un moment donné. Dans ce cas, si le CHG est **annulé** ou **fermé** (avec un code de fermeture **En échec**), la tâche de rattrapage revient automatiquement à l'état **En cours d'examen**. La tâche de rattrapage revient à **l'état En cours d'examen**, car il n'existe aucun plan actif pour corriger la vulnérabilité.

Si une tâche de rattrapage est à l'état **Résolu** et que vous créez un nouveau CHG ou l'associez à un CHG existant dans l'un des états ouverts initiaux, la tâche de rattrapage revient automatiquement à **l'état En attente d'implémentation**. La tâche de rattrapage revient à cet état, car davantage de travail est maintenant affecté au CHG.

Tâches de remédiation avec plus d'un CHG

Si plusieurs CHG sont associés à une tâche de rattrapage en **attente d'implémentation** , la synchronisation de l'état est basée sur l'état du CHG au plus tôt de son cycle de vie. Par

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

exemple, supposons que quatre CHG sont associés à une tâche de rattrapage, CHG1, CHG2, CHG3 et CHG4, comme illustré dans la table suivante.

Numéro CHG	État du CHG
1	**Implémenter**
2	**Annulé**
3	Fermé (code de fermeture de **En échec**)
4	Fermé (code de fermeture **en échec**)

Dans ce cas, la synchronisation de l'état entre le CHG et la tâche de rattrapage est basée sur CHG1, qui est dans l'état le plus ancien des quatre CHG (**Implémenter**). Dans ce cas, la tâche de rattrapage reste en **attente d'implémentation**.

Dans un autre exemple, si une tâche de rattrapage est à l'état **Résolu** et qu'un CHG existant a été implémenté et est à l'état **Révision** , et qu'un nouveau CHG est créé, la tâche de rattrapage revient de **Résolu** à **En attente d'implémentation**. La synchronisation de l'état est basée sur le CHG dans l'état **Nouveau** , qui est le CHG dans l'état le plus ancien.

Numéro CHG	État du CHG
1	Revue
2	Nouveau

De plus, lorsque les tâches de rattrapage ont plusieurs CHG, l'état de la tâche de rattrapage change automatiquement dans les cas suivants :

- Lorsqu'un CHG passe à **l'état Révision**, si tous les autres CHG associés à la tâche de rattrapage sont à l'état **Révision** ou **Fermé** (avec un code de fermeture réussi), la tâche de rattrapage passe automatiquement à **l'état Résolu**. Tous les autres CHG associés qui sont annulés ou fermés sans succès sont ignorés.
- Lorsqu'un CHG passe à l'état **Annulé** ou **Fermé** (code de fermeture En **échec**), si tous les autres CHG associés à la tâche de rattrapage sont dans le même état, la tâche de rattrapage revient automatiquement à **l'état En cours d'examen**.

Pour en savoir plus sur les états des tâches de rattrapage et sur ce que vous pouvez faire dans chaque état, reportez-vous à la section Conformité de la configuration États.

Séparation de domaine et Conformité de la configuration

L'application Séparation de domaine est prise en charge dans Conformité de la configuration. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Niveau de prise en charge : Standard

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Comment fonctionne Séparation de domaine dans Conformité de la configuration

Avec Domain Separation, vous pouvez standardiserConformité de la configuration les procédures, pour l'ensemble de la clientèle que vous servez, avec des coûts d'exploitation réduits et une meilleure qualité de service.

Des espaces de travail client distincts pour les workflows, les tableaux de bord, les rapports, etc., garantissent que les données client sont séparées et ne sont jamais exposées à d'autres clients.

Prise en charge de Domain Separation dans Conformité de la configuration les versions par version

Version	Niveau de prise en charge	Notes
Orlando	Standard	
Paris	Standard	
Québec	Standard	
Rome	Standard	
San Diego	Standard	
Tokyo	Standard	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prise en charge de Domain Separation dans Conformité de la configuration les versions par version (suite)

Version	Niveau de prise en charge	Notes
Utah	Standard	
Vancouver	Standard	

Séparation de domaine pour l'application Conformité de la configuration couvre les fonctionnalités du produit suivantes :

- Ingère les résultats des tests des scanners tiers (Qualys) dans le domaine approprié.

  Les données ingèrent dans le même domaine que celui de l'utilisateur d'intégration, dont les informations d'identification sont utilisées pour l'intégration.

- Analyse à nouveau des hôtes spécifiques à partir du domaine à partir Conformité de la configuration duquel la demande a été effectuée.
- Utilise le processus de recherche de CI CMDB pour s'assurer que les informations CI des scanners correspondent aux CI dans CMDB du domaine de l'utilisateur d'intégration.
- Calcule les scores de risque au niveau du résultat du test selon le calculateur de score de risque défini dans le même domaine que celui de l'utilisateur d'intégration.
- Il est possible de définir, d'affecter et de rester dans le même domaine que le domaine de l'utilisateur d'intégration.
- Les tâches de rattrapage créées à l'aide du document Les règles de tâche de rattrapage restent dans le même domaine que l'endroit où les règles de tâche de rattrapage sont créées.
- Le workflow du report passe par le processus d'approbation dans le même domaine pour lequel le report est demandé.
- Les rapports et les tableaux de bord affichent les états des résultats des tests, tels que l'âge des résultats des tests, les résultats des tests ouverts par CI, les résultats des tests par impact dans le domaine auquel ils appartiennent.
- Les connaissances provenant d'analyseurs tiers (Qualys) peuvent être ingérées dans le domaine global et les données peuvent être partagées entre plusieurs clients.

Remarque : Dans tous les cas ci-dessus, les principes fondamentaux de la séparation de la visibilité dans des domaines séparés dans la NOW Platform s'appliquent.

Cas d'utilisation

L'application Conformité de la configuration gère le cycle de vie d'un résultat de test de bout en bout. Les cas d'utilisation suivants prennent en charge la séparation par domaine :

- **Ingérer les** résultats des tests à partir de Qualys
  - Ingérer des données à partir de plusieurs instances
  - Dédupliquer les résultats des tests
  - Correspondre avec le CI CMDB
- **Enrichissement** des résultats des tests avec les scores de risque

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Enrichissement des actifs (CMDB)
- Score du risque

- **Regrouper** les résultats des tests et affecter la tâche de rattrapage
  - Regrouper automatiquement les résultats des tests
  - Affecter automatiquement la tâche de rattrapage
- **Corriger**
  - Tâche de rattrapage affectée en tant que tâche de rattrapage
  - Cycle de vie complet de la correction
  - Workflow du report
- **Mesurer** la posture de sécurité de l'organisation et le programme de gestion de la conformité
  - Tendance des résultats, par conformité, catégorie, criticité et technologie
  - État et répartition sur les politiques, les tests, les hôtes, les résultats des tests et le score de risque

Configuration

La configuration de Séparation de domaine pour Conformité de la configuration ne nécessite aucune étape supplémentaire. Toutes les Conformité de la configuration tables acquièrent la colonne Domaine une fois que l'instance est séparée par domaine. Vous pouvez diriger les données d'importation d'intégration des résultats des tests vers des domaines spécifiques. Pour plus d'informations, consultez Créer des importations séparées par domaine pour une intégration. Pour en savoir plus sur les précautions et les réglages supplémentaires, reportez-vous à la section Paramètres supplémentaires pour Séparation de domaine.

Données séparées par domaine

Les données peuvent être séparées par domaine, ce qui signifie :

- Les résultats des tests ingérés à partir d'analyseurs tiers restent dans le même domaine que le domaine de l'utilisateur d'intégration et ne sont accessibles à partir d'aucun autre domaine.
- Les résultats des tests ou les hôtes d'un domaine ne peuvent pas être affichés à partir d'autres domaines.
- L'algorithme de notation des risques et les règles de tâche de rattrapage ne peuvent être consultés par aucune personne extérieure au domaine.
- Les workflows de report créés dans un domaine ne sont pas visibles dans un autre domaine.
- Toutes les notifications par e-mail sont contenues dans le domaine auquel elles appartiennent.

Comment les analystes de conformité gèrent-ils leurs propres données d'application ?

- Les analystes créent leurs propres règles d'installation d'application, de gestion des applications multisources et de recherche de CI.
- Les analystes peuvent configurer des intégrations spécifiques exclusivement pour une utilisation au sein du domaine.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

- Les analystes peuvent créer leurs propres workflows de gestion des reports et des changements.
- Les analystes peuvent créer leurs propres règles de tâche de rattrapage, une logique de notation des risques pour classer les résultats par ordre de priorité précis, affecter automatiquement les tâches de rattrapage et les affecter au groupe d'affectation approprié.
- Les utilisateurs du domaine créent une tâche de rattrapage manuel, puis la ferment.

Logique métier et processus qui peuvent être séparés par domaine par le propriétaire de l'instance

- Conformité de la configuration Utilisateurs et groupes
- Conformité de la configuration intégrations (à partir de la version Madrid)
- Configuration complète (gestion des utilisateurs et des groupes, installation des applications, gestion des applications multisources, règles de recherche de CI, règles de tâche de rattrapage, calculateurs de risque, etc.)
- Cycle de vie complet du rattrapage, y compris le report

Information associée

Séparation de domaine pour les fournisseurs de services

Champs Résultats des tests

Les résultats des tests sont automatiquement créés lors des importations d'intégration de vulnérabilité tierce.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Conformité de la configuration ne crée ni ne met à jour les résultats des tests, mais les importe dans le cadre d'une intégration tierce. Une fois qu'ils sont visibles dans , ils sont corrigés à Conformité de la configurationl'aide de **groupes de résultats des tests**.

Champs de résultats des tests

Champ	Description
Numéro	Numéro attribué au résultat de test au cours du processus d'importation.
Source	Nom du système de l'application d'intégration tierce ou nom saisi dans l'application pour l'API utilisée pour communiquer avec Conformité de la configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID source	Identificateur affecté au résultat du test par l'intégration tierce.
Score du risque	Score basé sur la *Criticality* valeur du test. Si vous ne l'avez pas installé et configuré, une valeur moyenne de 50 est utilisée.
Résolution	Résolution du résultat du test, calculée à partir des groupes associés.
Résultat	État de l'analyse. Réussite ou échec. Si ce test appartient à plusieurs tâches de rattrapage, son état est déterminé suivant un ordre de priorité.
État	État du résultat du test, calculé à partir des groupes associés.
Groupe d'affectation	Groupe sélectionné pour travailler sur ce résultat de test.
Affecté à	Personne du groupe d'affectation sélectionné pour travailler sur ce résultat de test.
Type d'affectation	Type d'affectation. Les choix possibles sont les suivants : • Règle • Manuel • Aucun
Règle d'affectation	Quelle règle d'affectation a été utilisée avec ce résultat de test, le cas échéant.
Premier observé	Heure et date auxquelles le résultat du test a été vu pour la première fois.
Dernier observé	Heure et date auxquelles le résultat du test a été observé pour la dernière fois.
Test	Contrôle auquel ce résultat appartient.
Élément de configuration	Élément de configuration associé à ce résultat de test.
Technologie	Technologie associée à ce résultat de test.
Description	
Description	Description détaillée du résultat du test tel que défini dans l'application de scanner tiers.
Valeurs attendues	
Valeurs attendues	Description et valeurs attendues telles que définies dans l'application de scanner tierce.
Valeurs réelles	
Valeurs réelles	Description et valeurs réelles telles que définies dans l'application de scanner tierce.
Rattrapage	
Rattrapage	Action de rattrapage telle que définie dans l'application de scanner tiers.

Voici les listes connexes des éléments vulnérables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Description
Tâches de remédiation	Tâches de rattrapage associées à ce résultat de test.
Historique des résultats des tests	Liste des enregistrements passés contenant des résultats différents.

Conformité de la configuration Cartes de criticité

Conformité de la configuration Le mappage de criticité transforme les champs de criticité de la source en champs au format Conformité de la configuration.

Le Conformité de la configuration système de base est livré avec un mappage standard Qualys Cloud Platform à standard ServiceNow . La création ou la modification d'une carte de criticité est destinée uniquement aux mappages tiers personnalisés ou non standard dans votre environnement.

Conformité de la configuration États

Avec Conformité de la configuration, vous pouvez afficher un modèle d'état pour connaître l'état de la tâche de rattrapage à un moment donné. Les états des tâches de rattrapage contrôlent les états des résultats des tests par priorité.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

États des tâches de résolution

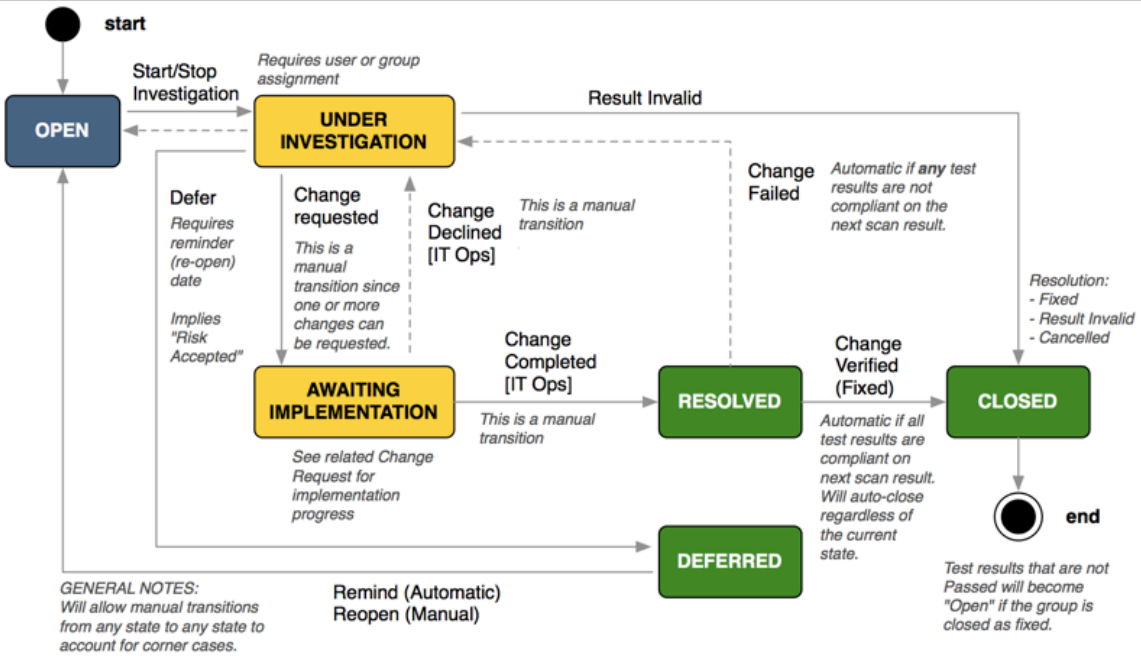
Les tâches de rattrapage ont de nombreux états possibles. La transition automatique est disponible à partir de l'état Résolu en fonction des résultats de l'analyse suivante. Si tous les résultats des tests sont transmis lors de l'analyse suivante, la tâche de rattrapage est fermée. Sinon, il passe à l'état En cours d'examen. Le système vérifie cet état Fermé, mais il réévalue l'état de la tâche de rattrapage si un résultat de test est ajouté ou supprimé de la tâche de rattrapage. Les notes de travail sont mises à jour pour refléter la transition.

La figure suivante montre comment l'état d'une tâche de rattrapage passe de l'état Ouvert à l'état Fermé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux d'état de Configuration Compliance (avant v15.0)



Remarque :

- Chaque formulaire de tâche de rattrapage contient des boutons **Suivre** et **Mettre à jour** , qui sont standard pour ServiceNow les tâches.
- À partir de la version 15.0 de Conformité de la configuration, les éléments suivants ont été supprimés :
  - **Bouton Fermer**
  - le champ **Résolution** du modal Résoudre.

Le tableau suivant répertorie les Conformité de la configuration états.

États de Conformité de la configuration

État	Description
Ouvrir	État à la création.
En cours d'examen	Déclenché par le bouton **Démarrer l'examen** . À partir de cet état, vous pouvez : Créer une demande de changement Pour plus d'informations, consultez Créer une demande de changement dans Conformité de la configuration. Demande d'exception Indiquez un motif et sélectionnez une date de réouverture. Supprimer Confirmez la suppression. Supprime la tâche de rattrapage. Marquer comme faux positif Indiquez un motif et prenez des notes. Marque la tâche de rattrapage comme un faux positif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États de Conformité de la configuration (suite)

État	Description
Différé	Déclenché par le bouton **Différer** . À partir de cet état, vous pouvez : Rouvrir Revenez à un état Ouvert. Supprimer Confirmez la suppression. Supprime la tâche de rattrapage. Les informations sur le report s'affichent sous l'onglet **connexe Différer/ Fermer** . À la date de report, la tâche de rattrapage rouvre pour le rattrapage.
En attente d'implémentation	Déclenché par le bouton **En attente d'implémentation** . À partir de cet état, vous pouvez : Créer un incident de sécurité Pour plus d'informations, consultez Créer un incident de sécurité. Créer une demande de changement Pour plus d'informations, consultez Créer une demande de changement dans Conformité de la configuration. Résoudre Dans les **notes de résolution**, ajoutez la raison pour laquelle vous résolvez la tâche de rattrapage. L'état devient Résolu. Les notes s'affichent sous l'onglet **Résolution** associée. Supprimer Confirmez la suppression. Supprime la tâche de rattrapage.
Résolu	Déclenché à partir du bouton **Résoudre** . À partir de cet état, vous pouvez : Créer un incident de sécurité Pour plus d'informations, consultez Créer un incident de sécurité. Rouvrir Revenez à un état Ouvert. Supprimer Confirmez la suppression. Supprime la tâche de rattrapage. Les notes s'affichent sous l'onglet **Notes** associées. Les informations sur la résolution s'affichent sous l'onglet **Résolution** connexe. Les notes reflètent dans les **notes de travail** tous les résultats des tests associés à la tâche de rattrapage.
Fermé	Déclenché à partir du bouton **Fermer** ou **Marquer comme faux positif** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États de Conformité de la configuration (suite)

État	Description
	À partir de la version 14.12 de , vous pouvez fermer une tâche de Conformité de la configurationrattrapage en la marquant comme faux positif. À partir de cet état, vous pouvez : Rouvrir Revenez à un état Ouvert. Supprimer Confirmez la suppression. Supprime la tâche de rattrapage. Les informations sur la fermeture s'affichent sous l'onglet connexe **Différer/Fermer** . Les notes reflètent dans les **notes de travail** tous les résultats des tests associés à la tâche de rattrapage.

- Si la tâche de rattrapage est marquée comme fermée ou fixe et si le résultat du test ajouté n'est pas lui-même fermé ou fixe, l'état du résultat du test ne change pas et l'état de la tâche de rattrapage passe à Ouvert.
- Lorsque vous créez une nouvelle tâche de rattrapage ou que vous divisez une tâche de rattrapage, les champs **Motif etJusqu'à sont** réévalués pour les tâches de rattrapage, nouvelles et anciennes. Lorsque l'état de tous les résultats des tests est défini sur Différé, la valeur des champs **Motif et Jusqu'à** est déployée sur la tâche de rattrapage.
  - Si tous les résultats des tests d'une tâche de rattrapage sont différés et ont le même **motif**, le même **motif** est affecté à la tâche de rattrapage. Dans le cas contraire, le champ **Motif** est remplacé par **Aucun**.
  - La date dans le champ **Jusqu'à** est mise à jour avec la date jusqu'à la plus proche de toutes les tâches de rattrapage auxquelles appartiennent les résultats des tests.

  Remarque : Cette évaluation est effectuée par la *`Rollup test result values to test result group and configuration test`* tâche planifiée, qui s'exécute toutes les heures.

- Si le **dernier observé** est supérieur à la **date de résolution** d'un résultat de test résolu, le résultat du test est rouvert. Dans une tâche de rattrapage résolue, si au moins un résultat de test est rouvert pendant l'ingestion, la tâche de rattrapage passe à l'état En cours d'examen.

États des résultats des tests

L'état d'une tâche de rattrapage modifie également l'état des résultats des tests qui lui sont associés. Ce mécanisme comporte deux cas de figure :

Résultats des tests qui appartiennent à une seule tâche de rattrapage

Les résultats correspondent à l'état de la tâche de rattrapage, à trois exceptions près :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si la tâche de rattrapage passe de l'état à Fermé et de la résolution (sous-état) à Fixe, l'élément ignore ce changement et revient à l'état Ouvert.
- Si la tâche de rattrapage passe de l'état à Fermé et de sa résolution (sous-état) à Annulé, l'élément ignore ce changement et revient à l'état Ouvert.
- Si l'état de la source du résultat des tests est Fixe (mis à jour par une analyse ou une importation), lorsque la tâche de rattrapage change d'état, le résultat du test passe à Fermé (Fixe), quel que soit l'état de la tâche de rattrapage.

Résultats des tests appartenant à plusieurs tâches de rattrapage

Les résultats des tests ne correspondent pas automatiquement à l'état de la tâche de rattrapage. Au lieu de cela, il effectue une recherche parmi tous les groupes associés pour trouver l'état ayant la priorité la plus élevée à appliquer. Il s'agit de l'état de priorité :

Fermé (sous-état : résultat non valide) Fermé (sous-état : faux positif) > **Différé** > **Résolu** > **En attente d'implémentation** > **En cours d'examen** > **ouvert**

Remarque : **Fermé (sous-état : Fixe)** et **Fermé (sous-état : Annulé)** sont deux cas particuliers.

Remarque : À partir de la version 15.0 de Conformité de la configuration, le sous-état **Résultat non valide** est déconseillé.

Exemples d'états de tâches de rattrapage

Par exemple :

État des tâches de remédiation	État du résultat des tests
Groupe A : **Ouvrir** > **En cours d'examen** Groupe B : **Ouvert**	**En cours d'examen** Lorsque le groupe A est En cours d'examen et que le groupe B est Ouvert, le résultat du test passe à En cours d'examen, car après la recherche, entre le groupe A et le groupe B, le groupe A a l'état ayant la priorité la plus élevée.
Groupe A : **En cours d'examen** Groupe B : **Ouvrir** > **En cours d'examen**	**En cours d'examen** Lorsque le groupe B est En cours d'examen et que le groupe A est En cours d'examen, le résultat du test reste défini sur En cours d'examen, car après la recherche, entre le groupe A et le groupe B, ils ont l'état avec la même priorité.
Groupe A : **En cours d'examen** Groupe B : **En cours d'examen** > **En attente d'implémentation**	**En attente d'implémentation** Lorsque le groupe B est En attente d'implémentation et que le groupe A est En cours d'examen, le résultat du test passe à En attente d'implémentation, car après la recherche, entre le groupe A et le groupe B, le groupe B a l'état ayant la priorité la plus élevée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État des tâches de remédiation	État du résultat des tests
Groupe A : **En cours d'examen** > **Différé** Groupe B : **En attente d'implémentation**	**Différé** Lorsque le groupe A est Différé et que le groupe B est En attente d'implémentation, le résultat du test passe à Différé, car après la recherche, l'élément 1 a découvert qu'entre le groupe A et le groupe B, le groupe A a l'état ayant la priorité la plus élevée
Groupe A : **Différé** Groupe B : **En attente d'implémentation** > **Fermé (résultat non valide)**	**Fermé (résultat non valide)** > **Différé** Lorsque le groupe B est fermé et que la résolution (sous-état) est Résultat non valide et que le groupe A est différé, le résultat du test passe à Fermé (résultat non valide), car après la recherche, entre le groupe A et le groupe B, le groupe B a l'état ayant la priorité la plus élevée.
Groupe A : **Différé** Groupe B : **Fermé (résultat non valide)** > **Ouvrir (via Rouvrir)**	**Différé** Lorsque le groupe B est rouvert et que son état devient Ouvert, et que le groupe A est Différé, le résultat du test passe à Différé, car après la recherche, entre le groupe A et le groupe B, le groupe A a l'état ayant la priorité la plus élevée.
Groupe A : **Différé** Groupe B : **En attente d'implémentation** > **Fermé (faux positif)**	**Fermé (faux positif)** Lorsque le groupe B est fermé et que la résolution (sous-état) est un faux positif et que le groupe A est différé, le résultat du test passe à Fermé (faux positif), car après la recherche, entre le groupe A et le groupe B, le groupe B a l'état ayant la priorité la plus élevée.

État du résultat de test : cas particuliers

État de la tâche de résolution	État du résultat du test
Groupe A : **En cours d'examen** Groupe B : **En attente d'implémentation** > **Fermé (Fixe ou Annulé)**	**En cours d'examen** Lorsque le groupe B est Fermé (sous-état Fixe ou sous-état Annulé) et que le groupe A est En cours d'examen, le résultat du test passe de En attente d'implémentation (auparavant, la priorité la plus élevée) à En cours d'examen (actuellement, la priorité la plus élevée).
Groupe A : tout état Groupe B : n'importe quel état	Si l'état de la source du résultat des tests est Fixe (mis à jour par une analyse ou une importation), lorsque la tâche de rattrapage change d'état, le résultat du test passe à Fermé (Fixe), quels que soient les états des autres tâches de rattrapage associées. La recherche des résultats des tests

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État du résultat de test : cas particuliers (suite)

État de la tâche de résolution	État du résultat du test
	pour l'état de la tâche de rattrapage n'a pas lieu.

Résolution des Conformité de la configuration problèmes d'importation

Résolvez les problèmes liés à l'importation d'intégration tierce.

Importer la résolution du problème

Problème	Résolution
les résultats des tests sont manquants	Vérifiez l'intégration *`Start Time`* de **Qualys PC Results** . Il n'est peut-être pas assez en retrait. Consultez Modifier la date de début des résultats de l'application PC Qualys.
L'intégration échoue	Vérifiez l'état **d'exécution de l'intégration de vulnérabilité** . Les entrées individuelles du processus d'intégration contiennent le XML importé, qui peut être examiné à la recherche d'informations inattendues. Accédez à la **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Résultats QualysPC** > **Exécutions de l'intégration de vulnérabilité** Onglet connexe. Choisissez la dernière exécution. Examinez l'état et les remarques des entrées dans la liste connexe **Processus d'intégration de vulnérabilité** pour détecter les anomalies. .

Modifier la date de début des résultats de l'application PC Qualys

S'il manque des données pour la date de début dans l'importation des résultats Qualys PC, elles peuvent être modifiées.

Avant de commencer

Rôle requis : sn_vul_qualys.admin

Procédure

1. Accédez à la **Tout** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
2. Cliquez sur **Intégration de Qualys PC Results** .
3. Cliquez sur **Détails de l'intégration**.
4. Définissez le champ **Heure de début** sur une valeur passée, de sorte que tous les résultats des tests analysés et détectés depuis cette date soient détectés.

> **Remarque :** Si la date est vide, aucune donnée n'est renvoyée lors de la première exécution. Définissez la valeur sur un maximum d'un mois dans le passé. Ce paramètre empêche de grandes quantités de données de dépasser les limites de débit de l'API Qualys et déclenche des délais d'exécution.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Envoyer** ou **Mettre à jour**.
6. Facultatif : Cliquez sur **Exécuter maintenant** pour l'exécuter immédiatement.

Règles de recherche de CI pour Microsoft Defender for Cloud Integration pour Opérations de sécurité et Palo Alto Prisma Cloud

Vous pouvez utiliser les règles de recherche d'éléments de configuration (CI) pour les Microsoft Defender for Cloud Integration intégrations et Palo Alto Prisma Cloud afin de trouver une correspondance correcte avec les types de ressources couramment utilisés dans le Base de données de gestion des configurations (CMDB).

Vue d'ensemble

Le module Règles de recherche de CI contient les règles qui vous aident à définir les champs qui comportent les données correspondantes dans le Base de données de gestion des configurations (CMDB)fichier . Vous pouvez utiliser ces règles pour identifier les applications et les versions d'application. Tous les Microsoft Defender for Cloud Integration actifs sont identifiés de manière unique par la combinaison de leur ID d'objet, de leur compte dans le cloud et de leur centre de données logique dans la ServiceNow plateforme. ServiceNow Discovery remplit l'ID de ressource dans la colonne `Object_id` du dans différents formats pour les différents types de CMDB ressources.Palo Alto Prisma Cloud La table suivante présente les formats d'ID d'objet des types de ressources couramment utilisés que le service de détection utilise pour remplir la colonne `Object_id` du CI. Tout scanner qui souhaite rechercher une ressource d'un type de ressource particulier doit effectuer une recherche en utilisant le format d'ID d'objet approprié. Vous pouvez obtenir le bon format d'ID d'objet en examinant la colonne d'ID d'objet de la classe CI correspondante CMDB , puis en essayant de construire l'ID d'objet à l'aide des valeurs reçues du scanner.

Format d'ID d'objet pour différents types de ressources

Type de ressource	Format
AWS::EC2::Instance	ID d'objet
AWS::ElasticLoadBalancing::LoadBalancer	Nom de l'équilibreur de charge
AWS::S3::Bucket	arn :aws :s3 :::<Nom de la catégorie>

La correspondance CI pour un résultat de test peut ne pas être trouvée avec précision dans le Base de données de gestion des configurations (CMDB) à moins que le même format du `object_id` ne soit utilisé dans la règle de recherche. La plupart du temps, les règles de recherche de CI OOB trouvent une correspondance pour les types de ressources les plus couramment utilisés pour Microsoft Defender for Cloud Integration et Palo Alto Prisma Cloud. Si les règles de recherche de CI suivantes ne trouvent pas les CI dans les CMDB résultats de vos tests, vous pouvez créer une règle de recherche de CI pour un type de ressource. Pour plus d'informations sur la création d'une règle de recherche de CI, consultez Créer une règle de recherche de CI.

Règles de recherche de CI

Les règles de recherche de CI suivantes sont spécifiques aux Microsoft Defender for Cloud Integration et Palo Alto Prisma Cloud.

Catégorie S3

Cette règle de recherche tente de trouver le CI dans le CMDB par la valeur obtenue en concaténant `arn :aws :s3 :::` et le nom de la ressource. La valeur obtenue est recherchée dans la colonne `object_id` de la table

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

`cmdb_ci_cloud_object_storage` . Cette règle de recherche s'applique uniquement lorsque le type de ressource est `AWS ::S3 ::Bucket`.

Nom

Cette règle de recherche tente de trouver le CI dans le CMDB par nom. Le nom, qui est recherché dans la colonne `Object_id` de la classe CI, correspond à un type de ressource dans la table `sn_capi_resource_type` .

Remarque : Pour l'application Palo Alto Prisma Cloud, cette règle de recherche de CI s'exécute uniquement pour les types de ressources `AWS ::RDS ::D BInstance`, `AWS ::ElasticLoadBalancing ::LoadBalancer` et `AWS ::CloudTrail ::Trail.` Vous pouvez ajouter les types de ressources pour lesquels vous souhaitez exécuter cette règle de recherche de CI.

ID de ressource

Cette règle de recherche tente de trouver le CI dans le CMDB par l'ID de ressource. L'ID de ressource, qui est recherché dans la colonne `Object_id` de la classe CI, correspond à un type de ressource dans la table `sn_capi_resource_type` .

Remarque : Vous pouvez définir la priorité d'une règle de recherche de CI dans le champ **Commande** . La règle de recherche de CI ayant la valeur d'ordre la moins élevée est exécutée en premier.

Vulnerability Response commun

Le module d'extension Vulnerability Response Common est installé lorsque vous installez l'application Vulnerability Response.

À partir de la version 20.0 de Vulnerability Response, vous pouvez utiliser le cadre de travail des rapports agrégés dans Vulnerability Response Common pour créer des rapports concernant les vulnérabilités d'hôte, d'application, de conteneur et les erreurs de configuration.

Cadre de travail pour les rapports agrégés

À l'aide du cadre de travail des rapports agrégés, vous pouvez créer des rapports pour les données qui impliquent des requêtes à la volée complexes et de longue durée pour de meilleures performances.

Le cadre de travail des rapports agrégés améliore les performances en :

- en utilisant moins de ressources et en rendant les rapports plus rapidement,
- l'agrégation des données et la réutilisation des agrégations et des répartitions (Group By) et
- Réduction des requêtes à la base de données

Lorsque vous avez plus d'un million d'éléments vulnérables, utilisez le cadre de travail fourni dans Vulnerability Response Common en plus des rapports standard.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Administrateur Now Platform (admin) : installer et activer cette Solution Analyse des performances et Reporting, et apporter les modifications nécessaires aux propriétés système.
- Analyse des performances administrateur (pa_admin) : examinez les agrégations, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.
- Administrateur (sn_vul_cmn.admin) : créer des agrégations.
- VR write(sn_vul_cmn.write) : modifiez les données dans les agrégations et les résultats agrégés.
- Lecture VR (sn_vul_cmn.read) : examinez les données dans les agrégations et les résultats agrégés.
- Analyste de vulnérabilité (sn_vul.vulnerability_analyst) : examiner les résultats agrégés.

Information associée

Configurer une agrégation pour les données sources

Exécuter plusieurs agrégations simultanément

Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Créer un rapport à l'aide d'une agrégation

Configurer une agrégation pour les données sources

Pour analyser les performances d'une facette spécifique d'un processus business enregistré dans une ServiceNow table, créez une agrégation spécifique à la facette et créez un rapport pour cette agrégation.

Avant de commencer

Rôle requis : sn_vul_cmn.admin

Procédure

1. Accédez à la **Tout** > **Rapports agrégés** > **Définitions d'agrégations** > **Tout** et cliquez sur **Nouveau**.
2. Dans le champ **Nom** , donnez à l'agrégation un nom descriptif.
3. Dans le champ **Description** , décrivez brièvement l'agrégation.
4. Renseignez les champs de l'onglet **Source** .

Champs de l'onglet source

Champ	Description
Table	Table à partir de laquelle vous souhaitez extraire les données pour le rapport. Cette liste déroulante contient uniquement les tables communes de sécurité des applications, app-vul, app-vulc, app-vul-container et de vulnérabilité des applications.
Fonction d'agrégat	Fonction à appliquer à la colonne sélectionnée dans **Champ**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ **Nombre** : nombre d'enregistrements. ◦ **Somme** : somme totale des valeurs de la colonne sélectionnée dans **Champ**. ◦ **Moyenne** : moyenne de toutes les valeurs d'une colonne sélectionnée dans **Champ**. ◦ **Maximum** : valeur maximale dans la colonne sélectionnée dans **Champ**. ◦ **Minimum** : valeur minimale de la colonne sélectionnée dans **Champ**. ◦ **Nombre distinct** : valeurs uniques dans la colonne sélectionnée dans **Champ**.
Champ	Colonne sur laquelle vous souhaitez appliquer la fonction. **Remarque :** Ce champ n'apparaît pas lorsque vous sélectionnez **Nombre** dans le champ **Fonction d'agrégation** .

5. Dans l'onglet **Conditions supplémentaires** , fournissez la condition dans le champ **Conditions** pour sélectionner un ensemble particulier d'enregistrements pour lequel vous souhaitez obtenir les résultats agrégés.
6. Dans l'onglet **Grouper par** , sélectionnez les colonnes de la table selon lesquelles vous souhaitez regrouper ou empiler les données.
   Vous pouvez sélectionner jusqu'à deux répartitions.

   Si vous sélectionnez la colonne **de date** dans n'importe quel champ Grouper par, le champ **Tendance par** s'affiche. Vous pouvez obtenir les résultats d'agrégation classés par semaine, jour, minutes, etc. en sélectionnant les options dans le champ **Tendance par** .
7. Dans l'onglet **Calendrier** , sélectionnez ou créez un calendrier d'agrégation, qui définit la fréquence à laquelle vous pouvez exécuter l'agrégation pour extraire les données.
   Pour créer un calendrier d'agrégation, reportez-vous à Exécuter plusieurs agrégations simultanément.

   Remarque : Vous ne pouvez pas planifier l'exécution d'agrégation pour une définition d'agrégation inactive.
8. Cliquez sur **Envoyer** pour créer l'agrégation.
   L'agrégation apparaît dans la liste Agrégation. À la fréquence prédéfinie, l'agrégation est exécutée et un enregistrement est créé avec une date et une heure d'exécution dans la liste connexe Exécutions planifiées pour chaque exécution.
9. Accédez à la **Tout** > **Résultats agrégés** et ouvrez votre agrégation pour afficher les résultats agrégés et les exécutions planifiées.
   Les résultats agrégés sont répertoriés dans la liste connexe **Résultats agrégés** . En cas d'échec de l'exécution de l'agrégation, consultez la colonne **Notes** de la liste connexe **Exécutions planifiées** pour plus d'informations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Facultatif : Sélectionnez **Exécuter maintenant** pour collecter les résultats de l'agrégation, quel que soit le calendrier d'agrégation.
    Si vous arrêtez l'exécution planifiée alors qu'elle est en cours, aucune modification n'est apportée aux résultats agrégés. Vous pouvez également supprimer ou désactiver une agrégation.

Que faire ensuite

Créez un rapport à l'aide de votre agrégation. Pour plus d'informations sur la création d'un rapport à l'aide d'une agrégation, reportez-vous à la section Créer un rapport à l'aide d'une agrégation.

Information associée

- Cadre de travail pour les rapports agrégés
- Exécuter plusieurs agrégations simultanément
- Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément
- Créer un rapport à l'aide d'une agrégation

Exécuter plusieurs agrégations simultanément

Vous pouvez planifier l'exécution de plusieurs agrégations à l'aide d'un seul calendrier d'agrégation.

Avant de commencer

Rôle requis : sn_vul_cmn.admin

Pourquoi et quand exécuter cette tâche

Supposons que vous souhaitiez exécuter six agrégations en même temps. Créez un calendrier d'agrégation et ajoutez-y toutes les agrégations. Ces agrégations sont exécutées à la fréquence et à l'heure définies.

Procédure

1. Accédez à la **Tout** > **Rapports agrégés** > **Calendrier**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Calendrier d'agrégation.

Champ	Description
Nom de calendrier	Nom du calendrier d'agrégation.
Travail de planification	Exécution de script planifiée qui définit la fréquence à laquelle les agrégations doivent s'exécuter. Vous pouvez créer une tâche planifiée en cliquant sur le bouton **Nouveau** .

4. Sélectionnez **Soumettre**.
   Le calendrier d'agrégation apparaît dans la liste Calendrier d'agrégation.
5. Ouvrez votre calendrier d'agrégation.
6. Sélectionnez **Modifier**, ajoutez les agrégations à la **liste d'agrégation**, puis sélectionnez **Enregistrer**.
   Les agrégations sélectionnées apparaissent dans la liste connexe Agrégations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous ajoutez une agrégation inactive à un calendrier, l'exécution planifiée ne commencera pas.

7. Sélectionnez **Mettre à jour**.
   Ces agrégations sont exécutées à la fréquence définie dans le calendrier d'agrégation.

Information associée

- Cadre de travail pour les rapports agrégés
- Configurer une agrégation pour les données sources
- Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément
- Créer un rapport à l'aide d'une agrégation

Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Un nouveau processeur ou une tâche en arrière-plan, le processeur Agrégatd Reporting Framework, est fourni avec le système de base, qui exécute les travaux planifiés associés à la table Agrégatd Reports Framework. Cela permet à l'ensemble du sous-système de s'exécuter en arrière-plan et à une meilleure utilisation des ressources système lorsqu'elles sont disponibles.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Configuration de la tâche en arrière-plan – Calculateur de résultat d'agrégation commune de Vulnerability Response**.
2. Définissez le nombre d'agrégations que vous souhaitez exécuter simultanément dans le **champ Nombre maximal de threads simultanés** déposés et sélectionnez **Enregistrer**.
   Par défaut, quatre agrégations sont exécutées simultanément.
3. Accéder à la liste Pools de processeurs de tâches en arrière-plan, **sn_sec_cmn_background_job_processor_pool.list**et sélectionnez **Nouveau** pour créer un processeur de tâches en arrière-plan pour le cadre de travail des rapports agrégés.
   Pour plus d'informations sur la création d'un pool de processeurs de tâches en arrière-plan, consultez Traitement parallèle avancé pour les tâches en arrière-plan dans Vulnerability Response .

Remarque : Le nombre de processeurs de tâches en arrière-plan doit être égal au nombre maximal de threads simultanés fournis dans le formulaire Configuration de la **tâche en arrière-plan – Calculateur de résultats d'agrégation commune de Vulnerability Response** . Reportez-vous à l'étape 2.

Information associée

- Cadre de travail pour les rapports agrégés
- Configurer une agrégation pour les données sources
- Exécuter plusieurs agrégations simultanément
- Créer un rapport à l'aide d'une agrégation

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un rapport à l'aide d'une agrégation

Pour visualiser et analyser les données spécifiques à une agrégation que vous avez créée, générez un rapport en fournissant une condition pour l'agrégation dans le générateur de conditions.

Avant de commencer

Rôle requis : pa_admin

Procédure

1. Accédez à la **Tout** > **Rapports** > **Créer**.
2. Renseignez les champs de l'onglet **Données** .

Champs de l'onglet Données

Champ	Description
Nom du rapport	Le nom du rapport.
Type de source	Type de la source à partir de laquelle les données sont extraites. Sélectionnez **Table**.
Table	Nom de la table pour laquelle l'agrégation est créée. Sélectionnez la table des résultats agrégés, **Résultat agrégé [sn_vul_cmn_aggregate_result].**

3. Dans le générateur de conditions, définissez la condition de l'agrégation pour laquelle vous souhaitez générer un rapport.

Condition dans le générateur de conditions

Réf.	Description
Champ	Sélectionnez **Agrégation**.
Opérateur	Sélectionnez **est**.
Valeur	Nom de l'agrégation.

4. Dans l'onglet **Données** , cliquez sur **Suivant**.
5. Dans l'onglet **Types** , sélectionnez la façon dont vous souhaitez visualiser les données et cliquez sur **Suivant**.
   Pour en savoir plus sur les types de rapports, reportez-vous à la section Création de rapports .

   Les visualisations prises en charge sont histogramme, graphique à secteurs et carte thermique. Vous pouvez modifier les graphiques linéaires et d'autres visualisations de tendances pour utiliser les visualisations prises en charge avec un résultat agrégé afin de représenter les mêmes données. La vue de liste n'est pas prise en charge.
6. Renseignez les champs de l'onglet **Configurer** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Grouper par	Sélectionnez **Groupé par 1** que vous avez sélectionné dans l'onglet **Grouper par** pour l'agrégation.
Empiler par	Sélectionnez **Groupé par 2** que vous avez sélectionné dans l'onglet **Grouper par** pour l'agrégation.
Agrégation	Appliquer **la fonction Minimum** ou **Maximum** à **la valeur**.

7. Dans l'onglet **Style** , renseignez les champs comme il convient et cliquez sur **Run (Exécuter**). Pour plus d'informations sur les champs des onglets **Configurer** et **Style** , consultez la vidéo Création d'un rapport .
8. Dans le générateur de conditions, définissez la condition de l'agrégation pour laquelle vous souhaitez générer un rapport, puis cliquez sur **Exécuter**.

   Le rapport s'affiche.
9. Pour trier les valeurs sur l'axe X, sélectionnez **Ajouter un tri**.

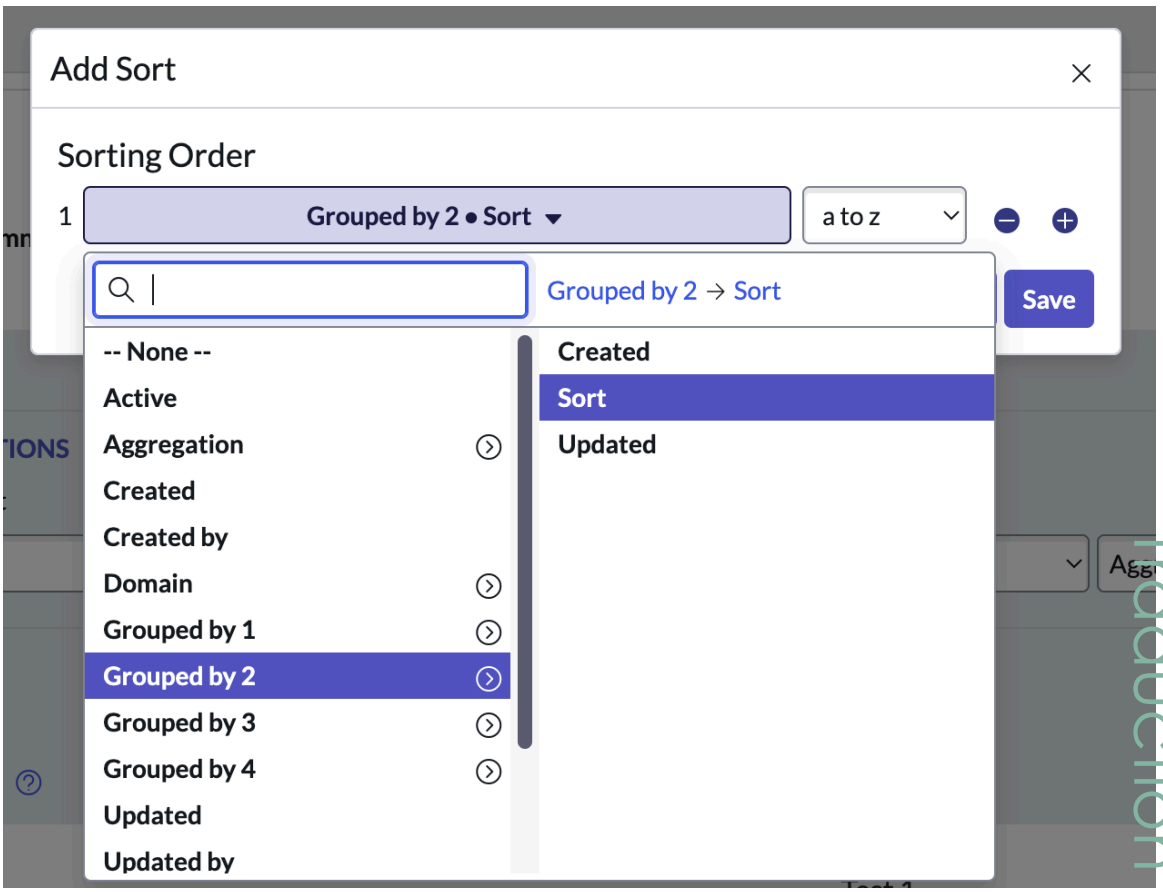
   a. Pour les chaînes, indiquez la condition **Groupée par > a-z ou z-a** pour trier les chaînes par ordre alphabétique.

   b. Pour les valeurs de type de données Entier et Date, indiquez la condition sous la **forme Groupé par.trier > a-z ou z-a** pour trier les valeurs par ordre croissant et décroissant respectivement.

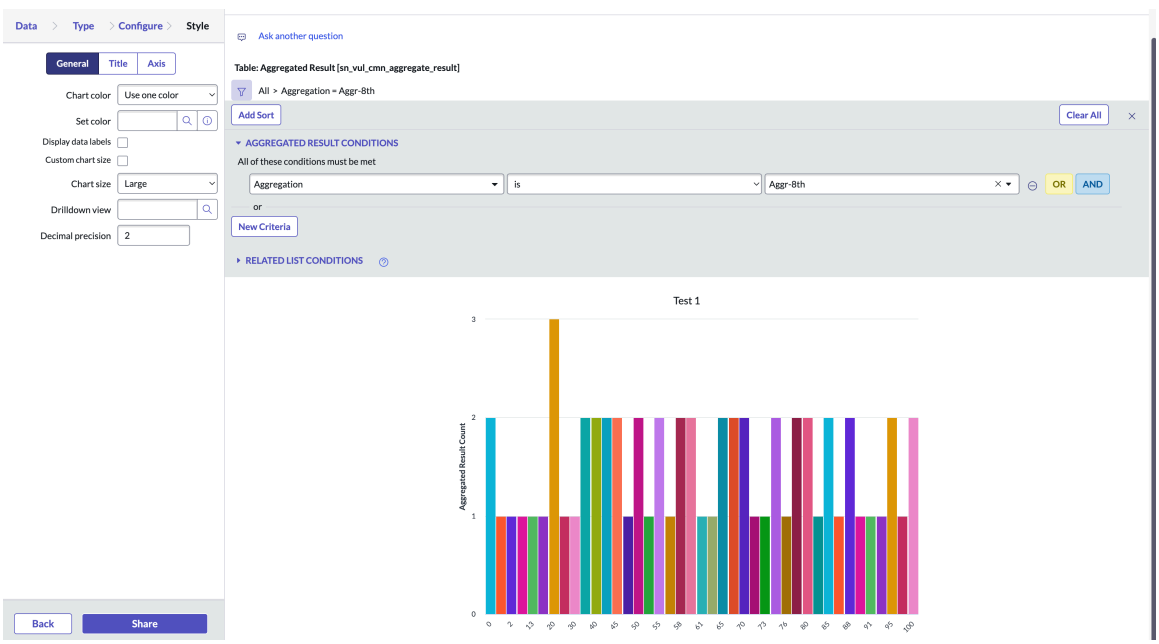
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tri des entiers sur l'axe des X



c. Sélectionnez **Exécuter**.
Les valeurs de nombre entier et de date sont triées sur l'axe X.



10. Cliquez sur **Enregistrer** pour enregistrer votre rapport.
Le rapport généré pour une agrégation s'affiche dans l'onglet **Résultats** du formulaire **d'agrégation** respectif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. Facultatif : Ajoutez votre rapport à un tableau de bord.
    Pour en savoir plus sur l'ajout d'un rapport à un tableau de bord, consultez Ajouter un rapport à un tableau de bord réactif .

    Le tableau **de bord Gestion de la vulnérabilité [agrégé],** composé de rapports créés à l'aide de l'infrastructure de génération de rapports mise en cache, est fourni avec le système de base. Pour afficher ce tableau de bord, accédez à **Tout** > **Analyse des performances** > **Tableaux de bord** > **Tout** > **Gestion de la vulnérabilité [agrégé]**. Les agrégations actives correspondant aux rapports de ce tableau de bord sont expédiées avec le système de base.

12. Partagez votre rapport avec d'autres utilisateurs.
    Pour plus d'informations sur le partage de rapports, voir Distribuer des rapports .

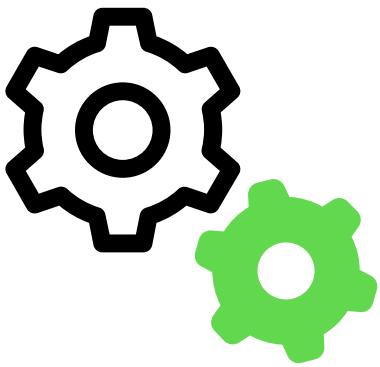
Information associée

- Configurer une agrégation pour les données sources
- Cadre de travail pour les rapports agrégés
- Exécuter plusieurs agrégations simultanément
- Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Réponse aux vulnérabilités Espaces de travail

Les espaces de travail Vulnerability Response offrent une vue consolidée des fonctionnalités qui vous permet d'effectuer plusieurs tâches à partir du même volet en augmentant votre productivité et en gagnant du temps.

Réponse aux vulnérabilités Espaces de travail

Espace de travail du gestionnaire de vulnérabilité	Espace de travail de remédiation informatique	Espace de travail de l'évaluation de la vulnérabilité
		
En savoir plus sur l'espace de travail du gestionnaire de vulnérabilité	En savoir plus sur l'espace de travail de remédiation informatique	En savoir plus sur l'espace de travail de l'évaluation de la vulnérabilité

Avant de commencer

Avant de pouvoir utiliser les espaces de travail :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous devez effectuer quelques tâches de configuration. Pour plus d'informations, consultez Configurer les espaces de Réponse aux vulnérabilités travail.
- Passez en revue les informations importantes sur les mises à jour des tâches de rattrapage, des règles de tâche de rattrapage et des termes et concepts clés relatifs aux espaces de travail, dans Réponse aux vulnérabilités Espaces de travail et mises à jour des tâches de rattrapage et des règles de tâche de rattrapage.

Dépannage et demande d'aide

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

Appliquer des correctifs à Orchestration avec les Réponse aux vulnérabilités espaces de travail

Vous pouvez gérer les correctifs et les déploiements de correctifs pour les vulnérabilités critiques de grands groupes de vos actifs avec l'orchestration de correctifs avec Réponse aux vulnérabilités.

Orchestration des correctifs dans les espaces de travail

L'orchestration des correctifs avec l'application Réponse aux vulnérabilités utilise des importations planifiées à partir d'intégrations de solutions tierces, de fournisseurs de correctifs et de scanners de vulnérabilité.

L'orchestration des correctifs avec l'application Réponse aux vulnérabilités est prise en charge à la fois dans l'environnement classique et dans les Réponse aux vulnérabilités espaces de travail. Les données corrélées sont déployées et affichées à la fois dans les espaces de travail et dans l'environnement classique. Pour obtenir une vue d'ensemble sur les fonctionnalités, les exigences et les informations relatives à l'orchestration des correctifs dans l'environnement classique, reportez-vous à la section Orchestration des correctifs avec Réponse aux vulnérabilités.

- Pour plus d'informations sur les intégrations prises en charge avec les fournisseurs de correctifs, consultez Présentation de l'intégration de l'orchestration des correctifs HCL BigFix avec Réponse aux vulnérabilités et Présentation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités.
- Pour en savoir plus sur la planification des correctifs dans les enregistrements de formulaire dans les espaces de travail, reportez-vous aux rubriques Planifier les correctifs avec l'intégration Microsoft SCCM avec Réponse aux vulnérabilités et Planifier les correctifs avec l'intégration Patch Réponse aux vulnérabilités Orchestration HCL BigFix.

Versions disponibles des applications et dépendances requises pour l'intégration d'orchestration de correctifs

Pour afficher les données d'orchestration des correctifs et les mises à jour disponibles (correctifs) dans les espaces de travail de Réponse aux vulnérabilités, les applications suivantes sont requises. Toutes les applications répertoriées sont disponibles dans le ServiceNow® Storefichier . Certaines applications nécessitent des abonnements distincts. Consultez Orchestration des correctifs avec Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles requis

Outre les rôles sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin requis pour les Réponse aux vulnérabilités espaces de travail, les utilisateurs ont besoin de rôles spécifiques aux intégrations d'orchestration de correctifs que vous utilisez pour afficher les données et planifier les correctifs. Consultez les intégrations prises en charge suivantes pour en savoir plus sur ces rôles.

Consultez Présentation de l'intégration de l'orchestration des correctifs HCL BigFix avec Réponse aux vulnérabilités et Présentation de l'intégration de l'orchestration de correctifs à Microsoft SCCM Réponse aux vulnérabilités.

Appliquer des correctifs aux données dans les Réponse aux vulnérabilités espaces de travail

Dans l'espace de travail de remédiation informatique, vous pouvez afficher les données de correctifs dans les espaces de travail :

- Dans la vue d'accueil, cliquez sur Tableaux de résultats pour afficher les enregistrements des solutions préférées sur les VI, des CI vulnérables et des correctifs préférés sur les VI.
- Dans la vue de liste, affichez tous les enregistrements de mise à jour de correctifs (VPU) et les éléments vulnérables qui vous sont affectés et qui ont des correctifs à partir des liens disponibles.

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- Mise à jour de correctif (VPU)
- Tâche de rattrapage (RT)
- Élément détecté (SDI)

Dans l' Espace de travail du gestionnaire de vulnérabilité, vous pouvez afficher les correctifs :

- À partir de la vue d'accueil sur les rubriques de surveillance de l'onglet Éléments vulnérables, vous pouvez afficher les correctifs préférés et potentiels, les dates planifiées des correctifs et d'autres informations.
- À partir de la vue de liste sur les enregistrements d'efforts de rattrapage, vous pouvez afficher les données de correctifs sur les enregistrements VIT dans l'onglet Éléments vulnérables.

Réponse aux vulnérabilités Espaces de travail et mises à jour des tâches de rattrapage et des règles de tâche de rattrapage

Les tâches de rattrapage regroupent les éléments vulnérables dans les Réponse aux vulnérabilités espaces de travail.

Termes clés pour les Réponse aux vulnérabilités espaces de travail

Espaces de travail Vulnerability Response ou espaces de travail

Réponse aux vulnérabilités prend en charge les espaces de Réponse aux vulnérabilités travail. Vous pouvez utiliser l'expérience classique Interface utilisateur principale ou les espaces de travail.

Interface utilisateur classique (héritée)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fait référence à l'expérience Interface utilisateur principale . Vous pouvez tout de même effectuer certaines actions et afficher quelques listes dans l'environnement classique.

Espace de travail du gestionnaire de vulnérabilité

Dans cet espace de travail, les gestionnaires surveillent les vulnérabilités ciblées et sélectionnent les éléments vulnérables et les résultats des tests qui les intéressent le plus à affecter au service informatique.

Espace de travail de remédiation informatique

Dans cet espace de travail, les équipes informatiques peuvent se concentrer sur les vulnérabilités les plus importantes qui leur sont affectées par la sécurité. Dans cet espace de travail, les propriétaires de rattrapage ont facilement accès aux informations centrées sur l'informatique qui incluent les éléments de configuration (CI) distincts et impactés, les solutions et la progression du rattrapage.

Espace de travail de l'évaluation de la vulnérabilité

Dans cet espace de travail, les analystes de vulnérabilité peuvent effectuer une évaluation de la vulnérabilité au cours de l'analyse de vulnérabilité zero-day. Une fois qu'une vulnérabilité zero-day est identifiée, ils peuvent évaluer l'impact potentiel et le risque associés à la vulnérabilité. Les analystes peuvent analyser le système, les applications ou les composants réseau affectés pour comprendre la gravité et les vecteurs d'attaque possibles au sein de l'organisation.

Rubrique de surveillance

Les rubriques de visualisation définissent un segment des éléments vulnérables que les gestionnaires et analystes de vulnérabilité souhaitent surveiller dans l'espace de travail du gestionnaire de vulnérabilité. Les rubriques de visualisation présentent un ensemble de rapports de vue d'ensemble ciblée qui se rapportent à un segment de VI et des résultats de tests avec des statistiques relatives aux tendances, aux CI et aux vulnérabilités. Les tableaux de bord relatifs à ces rubriques peuvent être utilisés pour surveiller les tendances. Les tableaux de bord peuvent également aider les gestionnaires à :

- Afficher l'avancement du rattrapage sur les éléments critiques
- Déterminer l'existence de vulnérabilités sur les systèmes critiques
- Voir quand un nouvel exploit sort
- Générez une réponse rapide pour résoudre un ensemble particulier de vulnérabilités

Effort de rattrapage (ER)

Les efforts de rattrapage sont créés par les gestionnaires de vulnérabilité lorsqu'ils déterminent qu'il est temps pour le service informatique de corriger les vulnérabilités répertoriées dans une rubrique de surveillance. Les gestionnaires et analystes de vulnérabilités peuvent choisir la façon dont ils souhaitent créer des tâches de rattrapage, par groupe d'affectation et par vulnérabilité, par exemple. Les tâches de rattrapage font partie de l'effort de rattrapage.

Tâche de rattrapage (VUL)

Les équipes informatiques utilisent des tâches de rattrapage pour corriger les vulnérabilités qui leur sont affectées par la sécurité. Les tâches de rattrapage sont des listes des actions requises pour corriger les vulnérabilités. Les tâches de rattrapage sont créées automatiquement lorsque les gestionnaires de sécurité créent des efforts de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aménagement des espaces de travail

Dans les versions précédentes de Réponse aux vulnérabilités, vous disposiez de deux options pour surveiller un ensemble d'éléments vulnérables (VI) en tant qu'analyste de la sécurité et des vulnérabilités :

- Tableau de bord Vue d'ensemble, qui résume tous les VI
- Tâches de rattrapage

Les éléments vulnérables ont été triés automatiquement dans les tâches de remédiation en fonction de vos règles de tâche de rattrapage prédéfinies. Les tâches de rattrapage ont été conçues pour aider les équipes informatiques à corriger les blocs gérables d'éléments vulnérables.

Cette automatisation a permis de regrouper automatiquement un très grand nombre de VI pour une affectation et une correction en bloc. Cependant, les analystes et les gestionnaires de vulnérabilités ont trouvé difficile de surveiller l'ensemble des éléments vulnérables des tâches de remédiation. Outre les problèmes de performances avec les grands groupes, il peut être difficile de créer des règles de tâche de rattrapage fonctionnelles qui filtrent uniquement les vulnérabilités que vous avez trouvées les plus critiques.

Les Réponse aux vulnérabilités espaces de travail :

- Aidez les gestionnaires de sécurité à filtrer, à surveiller les VI actifs et les résultats des tests au fil du temps, et à corriger les vulnérabilités qu'ils jugent les plus importantes.
- Fournissez aux équipes informatiques des informations centrées sur l'informatique en un seul endroit qu'elles peuvent utiliser pour corriger les vulnérabilités qui leur sont affectées par la sécurité.

Mises à jour des tâches de rattrapage dans les espaces de travail

Dans l'espace de travail Gestionnaire de vulnérabilité, les analystes et les gestionnaires de vulnérabilités utilisent les rubriques de visualisation et les efforts de rattrapage comme deux nouvelles méthodes de surveillance et d'affectation de VI pour le rattrapage.

Les groupes de vulnérabilité sont renommés Tâches de remédiation. Ce changement s'applique aux étiquettes des listes, des enregistrements et des règles dans l'interface utilisateur héritée et dans les espaces de travail. Les tâches de rattrapage sont configurées de manière à ce que les équipes informatiques puissent les utiliser dans l'espace de travail de remédiation informatique. La liste suivante illustre comment, en tant que gestionnaire des vulnérabilités ou analyste des vulnérabilités, vous pouvez surveiller les vulnérabilités et les résultats des tests, les filtrer et les affecter :

1. Dans Vulnerability Manager Workspace, les responsables surveillent les vulnérabilités importées sur les rubriques de surveillance. Les gestionnaires et les analystes utilisent des rubriques de surveillance pour surveiller un ensemble dynamique d'éléments vulnérables filtrés au fil du temps qu'ils considèrent comme les plus critiques.
2. Grâce aux rubriques de surveillance, les responsables de la sécurité peuvent déterminer quand et quel type de VI transférer aux équipes informatiques dans le cadre des efforts de remédiation (RE). Il s'agit de listes statiques des VI que la sécurité souhaite que les équipes informatiques corrigent.

   En ce qui concerne les efforts de rattrapage, les gestionnaires disposent de quatre options pour regrouper les éléments vulnérables en tâches de rattrapage (VUL). Les tâches de rattrapage sont automatiquement affectées aux équipes informatiques en fonction des groupes d'affectation associés à l'origine aux VI.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Les équipes informatiques travaillent sur des tâches de remédiation dans IT Remediation Workspace sans avoir à trier toutes les VI.

   Une tâche de rattrapage passe par les mêmes états que la tâche de rattrapage dans les versions précédentes de Réponse aux vulnérabilités. Lorsque tous les VI d'une tâche de rattrapage sont fermés, la tâche de rattrapage est fermée et passe l'état **Inactif**.

   La progression du rattrapage est mise à jour sur les visualisations de données dans les rubriques de surveillance et sur la page d'accueil du rattrapage informatique.

Mises à jour des règles de tâche de rattrapage dans les espaces de travail

Les règles des groupes de vulnérabilité sont appelées règles de tâche de rattrapage. Cette modification s'applique aux étiquettes des listes, des enregistrements et des règles dans l'interface utilisateur héritée et dans les espaces de travail.

Les noms de table, par exemple [sn_vul_m2m_vul_group_item], ne sont pas modifiés.

Si vous avez créé des règles de groupes de vulnérabilité dans une version antérieure de , elles sont toujours disponibles, étiquetées en tant que règles de tâche de Réponse aux vulnérabilitésrattrapage.

Toutefois, dans les espaces de travail, les règles de groupe de vulnérabilité ne sont plus utilisées comme méthode principale d'organisation d'un grand volume d'éléments vulnérables en groupes de vulnérabilité. Vous préférerez peut-être laisser vos règles de tâche de rattrapage inactives pendant que vous vous habituez aux espaces de travail.

Au lieu de cela, vous préférerez peut-être commencer à utiliser progressivement les espaces de Réponse aux vulnérabilités travail.

1. Si vous effectuez une mise à niveau à partir d'une version précédente de Réponse aux vulnérabilités votre VG existant, les règles sont conservées. Ils sont toujours à votre disposition dans les espaces de travail. La règle de groupe par défaut, Vulnérabilité, est inactive par défaut.
2. Configurez des règles d'affectation et, si vous le souhaitez, des règles de risque, puis effectuez une importation.
3. En tant que responsable ou analyste des vulnérabilités, vous pouvez choisir des segments à surveiller dans les rubriques de surveillance de l'espace de travail du gestionnaire de vulnérabilité. Vous pouvez utiliser les rubriques de visualisation en tant que fonctionnalités autonomes. Sélectionnez n'importe quel sous-ensemble de VI et utilisez le tableau de bord correspondant pour surveiller les tendances. Grâce à eux, vous pouvez décider où et quand concentrer les efforts de rattrapage.
4. En tant que gestionnaire ou analyste des vulnérabilités, vous créez des efforts de rattrapage à partir des rubriques de surveillance lorsque vous décidez qu'il est temps de corriger un sous-ensemble d'éléments vulnérables. Une tâche de rattrapage est également créée automatiquement pour être transférée au service informatique lorsque vous créez un effort de rattrapage.
5. Au fil du temps, en tant que gestionnaire ou analyste des vulnérabilités, vous découvrirez peut-être des modèles de routine que vous pouvez gérer automatiquement avec des règles de tâches de remédiation.

Pour afficher vos règles de tâche de rattrapage, accédez à **Réponse aux vulnérabilités** > **Administration** > **Règles de la tâche de rattrapage**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus sur les règles d'affectation, les règles de tâche de rattrapage, les efforts de rattrapage et les éléments vulnérables dans les Réponse aux vulnérabilités espaces de travail

- Les enregistrements de tâches de rattrapage (VUL) sont affichés dans des listes et des enregistrements dans l'environnement classique et dans les espaces de travail.
- Une tâche de rattrapage passe par les mêmes états qu'un groupe de vulnérabilité. Lorsque tous les éléments vulnérables d'une tâche de rattrapage sont fermés, la tâche de rattrapage passe à l'état Inactif.
- Pour aider vos équipes à effectuer le rattrapage, un élément vulnérable ne peut faire l'objet que d'un seul effort de rattrapage. Une fois qu'il est dans un effort de rattrapage, un élément vulnérable ne sera pas ajouté aux autres efforts de rattrapage que vous créez.
- Si vous supprimez un effort de rattrapage, celui-ci devient inactif et tous les VI actifs sont disponibles pour de nouveaux efforts de rattrapage.
- Un élément vulnérable peut se trouver dans plusieurs tâches de rattrapage.
- Les tâches de rattrapage sont affectées automatiquement aux équipes informatiques en fonction du groupe d'affectation associé à un élément vulnérable dans un effort de rattrapage. Si vous créez une tâche de rattrapage à la demande, vous sélectionnez le groupe d'affectation.
- Si vous effectuez une mise à niveau à partir d'une version précédente de , vos règles d'affectation Réponse aux vulnérabilitésont été conservées dans l'interface utilisateur héritée.
- Si vous effectuez une mise à niveau à partir d'une version précédente de , vos utilisateurs et groupes actuels sont hérités et vous sont accessibles dans les espaces de Réponse aux vulnérabilitéstravail.

Pour en savoir plus sur les cycles de vie des mesures correctives, reportez-vous à Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Vulnerability Response.

Configuration et paramétrage des Réponse aux vulnérabilités espaces de travail

Pour en savoir plus sur les règles d'affectation et les règles de tâche de rattrapage, consultez Configurer les espaces de Réponse aux vulnérabilités travail et Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Si vous êtes un nouveau client et que vous ne les avez pas encore ajoutés, vous devez configurer les utilisateurs et les groupes de manière à ce que les éléments vulnérables et les tâches de rattrapage soient affectés aux groupes de rattrapage souhaités. Les règles d'affectation de Vulnerability Response sont utilisées pour affecter le travail aux groupes.

Configurer les espaces de Réponse aux vulnérabilités travail

Avant de pouvoir utiliser les espaces de travail, confirmez que vous avez effectué les tâches de configuration suivantes.

Avant de commencer

Rôle requis : admin pour l'affectation de rôles aux utilisateurs et aux groupes, et les utilisateurs aux groupes.

sn_vul.vulnerability_admin pour l'édition, la création de règles et la configuration de l'application Réponse aux vulnérabilités .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Confirmez que vous avez effectué les tâches de configuration suivantes. Reportez-vous aux étapes suivantes de la liste pour en savoir plus sur la manière d'effectuer ces tâches.

Tâche	Description
☐	Si ce n'est pas déjà fait, affectez aux utilisateurs et aux groupes les rôles appropriés afin qu'ils aient accès aux espaces de travail. Rôle requis : admin. Reportez-vous aux étapes ci-dessous pour plus d'informations.
☐	Configurez des règles d'affectation afin que les éléments vulnérables soient affectés aux groupes appropriés pour le rattrapage. Rôle requis : sn_vul.vulnerability_admin. Pour en savoir plus sur les règles d'affectation, reportez-vous à Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation. Vous créez et modifiez des règles d'affectation dans l'environnement classique.
☐	(Facultatif) : modifiez ou créez vos règles de tâche de rattrapage. Rôle requis : sn_vul.vulnerability_admin. **Remarque :** D'un point de vue fonctionnel, les règles de tâche de rattrapage fonctionnent de la même manière que dans les versions précédentes de Réponse aux vulnérabilités. Toutefois, contrairement aux groupes de vulnérabilité qui ont été créés automatiquement à partir de vos règles de tâche de rattrapage, les tâches de rattrapage sont créées lorsque vous créez des efforts de rattrapage. Pour regrouper les éléments vulnérables dans le cadre d'un effort de rattrapage en tâches de rattrapage, vous disposez des options suivantes : • Par groupe d'affectation • Par groupe d'affectation et élément de configuration • Par groupe d'affectation et par vulnérabilité • Aucun : utilisez cette option si vous souhaitez ajouter manuellement des VI à une tâche de rattrapage. Consultez Créer une tâche de remédiation sur demande dans Vulnerability Manager Workspace pour plus d'informations. Pour plus d'informations sur la façon dont les VI sont automatiquement regroupés et sur la façon dont les règles de groupe sont réappliquées dans l'environnement classique, reportez-vous à la section Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage.
☐	Modifiez les règles de cibles de rattrapage. Rôle requis : sn_vul.vulnerability_admin. Ajoutez des règles de cible de rattrapage dans l'environnement classique. Pour en savoir plus sur les règles de cibles de rattrapage,

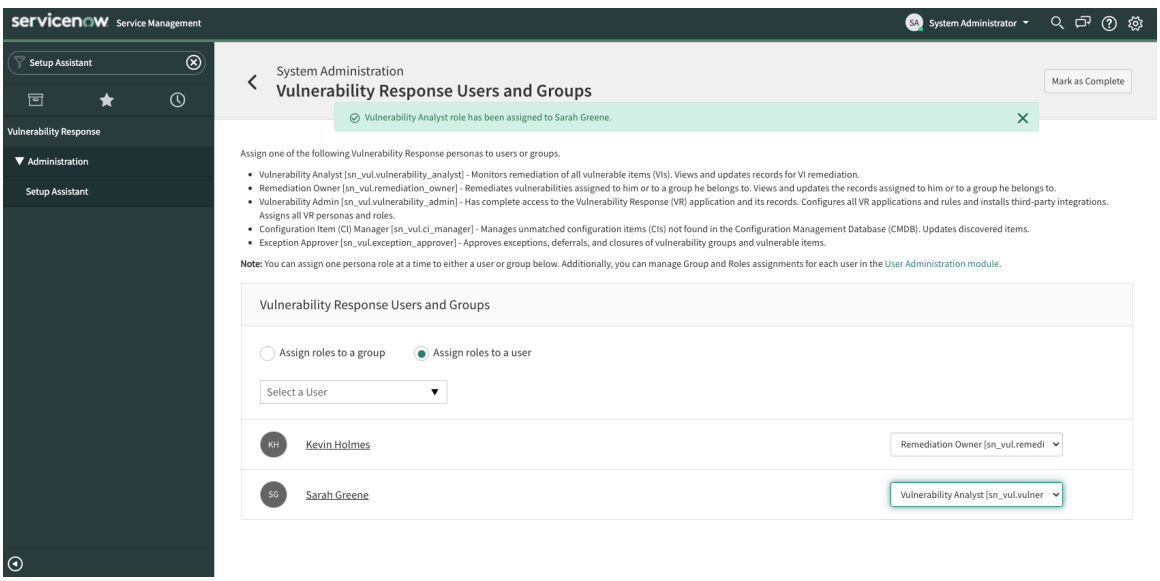
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	reportez-vous à Créer ou modifier Réponse aux vulnérabilités des règles de cibles de rattrapage.

Procédure

1. Après avoir installé et activé l'application Réponse aux vulnérabilités , dans l'environnement classique en tant qu'utilisateur disposant du rôle administrateur, accédez à **Tout** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.



2. Dans l'Assistant de configuration, affectez des utilisateurs aux groupes suivants.

   Remarque : 1 000 est la limite du nombre de groupes d'utilisateurs auxquels un utilisateur peut être affecté dans les espaces de travail Vulnerability Response.

   Les groupes suivants sont fournis avec l'application Réponse aux vulnérabilités et sont utilisés dans les espaces de travail. Vous pouvez leur affecter des utilisateurs dans l'assistant de configuration :

   - Propriétaire du rattrapage : ce groupe est destiné aux propriétaires du rattrapage informatique dans l'espace de travail du rattrapage IT. Les utilisateurs dotés de ce rôle corrigent les vulnérabilités qui leur sont affectées dans les tâches de rattrapage.

     Remarque :

     Si vous souhaitez que les propriétaires de rattrapage créent et visualisent les demandes de changement et affichent les données des éléments de configuration (CI) vulnérables dans IT Remediation Workspace et dans l'environnement classique, affectez-leur le rôle itil. Vous préférerez peut-être affecter le rôle itil à des utilisateurs individuels plutôt qu'à tous les membres d'un groupe. Le rôle cmdb_read est également une option permettant aux utilisateurs d'afficher les données CI dans les espaces de travail.

   - À partir de la version 16.1, vous pouvez configurer des rappels par e-mail à vos propriétaires de rattrapage informatique. Pour configurer des notifications par e-mail vers les espaces de travail, reportez-vous à la section Configurer des notifications par e-mail dans les Réponse aux vulnérabilités espaces de travail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Administrateur de vulnérabilité : ce groupe est destiné aux gestionnaires de vulnérabilité. Ce rôle configure l'application Réponse aux vulnérabilités dans l'assistant de configuration. Ce rôle a également l'autorisation de traiter les demandes d'exception et les faux positifs.
- Analyste de vulnérabilité : ce groupe s'adresse aux gestionnaires de sécurité, aux gestionnaires de vulnérabilité et aux analystes de l'espace de travail du gestionnaire de vulnérabilité. Ce rôle surveille les vulnérabilités, crée des rubriques de surveillance et des efforts de correction, et surveille la progression des corrections.
- Approbateur faux positif : les utilisateurs de ce groupe traitent les demandes de faux positif pour les éléments vulnérables ou les tâches de rattrapage. Une demande de faux positif nécessite un processus d'approbation à un seul niveau. Vous pouvez gérer l'affectation d'utilisateurs à ce groupe en dehors de l'Assistant de configuration dans **l'Administration utilisateurs**.
- Approbateur d'exception : une demande d'exception pour un élément vulnérable ou une tâche de rattrapage est approuvée à l'aide d'un workflow d'approbation à deux niveaux par défaut. La demande d'exception nécessite deux niveaux d'approbateurs. Ajoutez des utilisateurs aux deux groupes d'approbation : Approbateur d'exception de niveau 1 et Approbateur d'exception de niveau 2. Une fois la demande approuvée par l'approbateur de niveau 1, elle est envoyée à l'approbateur de deuxième niveau. Vous gérez l'affectation d'utilisateurs à ce groupe en dehors de l'Assistant de configuration dans **l'Administration utilisateurs**.

> **Remarque :** Ajoutez des utilisateurs aux groupes d'approbation avant de soumettre des demandes de faux positifs et d'exceptions. Si vous créez des demandes avant d'affecter des utilisateurs ayant une autorisation d'approbation, il est possible qu'ils ne voient pas ces demandes.

Vous pouvez également cliquer sur le lien **Administration utilisateurs** pour gérer et affecter les rôles granulaires suivants à vos utilisateurs et groupes existants. Ces rôles permettent aux utilisateurs d'effectuer des actions spécifiques au sein de l'application Réponse aux vulnérabilités et des espaces de travail.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- Pour créer et afficher des demandes de changement dans l'espace de travail de remédiation informatique et dans l'environnement classique, affectez-leur le rôle itil.

Consultez Réponse aux vulnérabilités Profils et rôles granulaires et Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration pour en savoir plus sur l'affectation de rôles de profil aux utilisateurs et aux groupes.

3. Les tâches de rattrapage sont automatiquement transférées aux groupes d'affectation de rattrapage informatique pour traitement lorsqu'elles sont créées.
   - Par groupe d'affectation
   - Par groupe d'affectation et élément de configuration
   - Par groupe d'affectation et par vulnérabilité
   - Aucun : utilisez cette option si vous souhaitez ajouter manuellement des VI à une tâche de rattrapage.

   > **Remarque :** Pour la version 18.0 de Réponse aux vulnérabilités, l'option **Aucun** n'est pas disponible.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous effectuez une mise à niveau à partir d'une version précédente de , vos groupes d'affectation Réponse aux vulnérabilitéssont conservés. Toutefois, vous préférerez peut-être modifier ces groupes afin que les éléments vulnérables soient associés à des groupes d'affectation spécifiques jusqu'à ce que vous vous habituiez au fonctionnement des rubriques de surveillance et des efforts de rattrapage. Par exemple, vous pouvez créer des groupes d'affectation par produit ou par région, mais vous pouvez utiliser n'importe quel critère qui convient le mieux à votre organisation.

Vous pouvez également utiliser des règles d'affectation pour affecter des tâches de rattrapage à des groupes. Vous préférez peut-être exécuter uniquement des règles de priorité élevée pour les éléments suivants :

- Éléments nécessitant une manutention spéciale
- Éléments où le risque est critique ou où un VI doit être géré par la conformité réglementaire

Les règles d'affectation suivantes, fournies avec l'application, sont actives par défaut :

- Règle d'affectation de CI mise hors service
- Affecter au groupe de support CI
- Règle d'affectation de station de travail
- Règle d'affectation de base de données
- Règle d'affectation de l'application Web
- Règle d'affectation de Windows Server
- Règle d'affectation serveur non Windows
- Règle d'affectation Contact de secours

Pour en savoir plus sur les règles d'affectation, reportez-vous à Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation. Vous créez et modifiez des règles d'affectation dans l'environnement classique.

4. Facultatif : Modifiez ou créez vos règles de tâche de rattrapage.

(Optional) Dans les espaces de travail, les tâches de rattrapage sont créées lorsque vous créez des efforts de rattrapage. Pour regrouper les éléments vulnérables dans le cadre d'un effort de rattrapage en tâches de rattrapage, vous disposez des options suivantes :

- Par groupe d'affectation
- Par groupe d'affectation et élément de configuration
- Par groupe d'affectation et par vulnérabilité
- Aucun : utilisez cette option si vous souhaitez ajouter manuellement des VI à une tâche de rattrapage. Consultez Créer une tâche de remédiation sur demande dans Vulnerability Manager Workspace pour plus d'informations.

> **Remarque :** Dans la version 18.0 de Réponse aux vulnérabilités, l'option **Aucun** n'est pas disponible.

Pour plus d'informations sur la façon dont les VI sont automatiquement regroupés et sur la façon dont les règles de groupe sont réappliquées dans l'environnement classique, reportez-vous à la section Réponse aux vulnérabilités Tâches de rattrapage et vue d'ensemble des règles de tâche de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

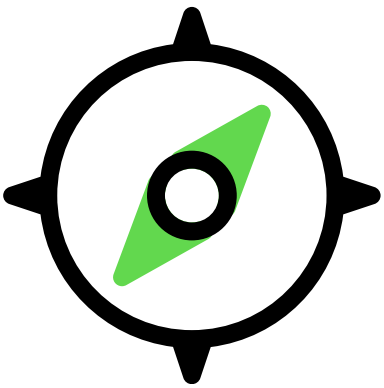
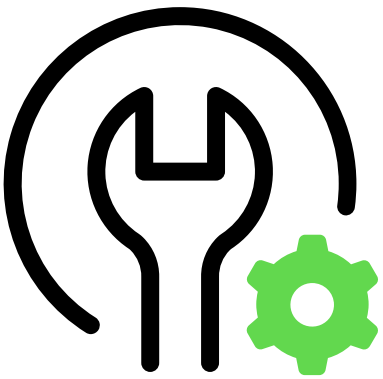
Espace de travail du gestionnaire de vulnérabilités

Il Espace de travail du gestionnaire de vulnérabilités permet aux gestionnaires et analystes de vulnérabilités de surveiller les vulnérabilités qui les intéressent le plus et de décider stratégiquement des vulnérabilités qu'ils envoient aux équipes informatiques pour qu'elles les corrigent.

Vue d'ensemble

V18.0 Démo de Vulnerability Manager Workspace

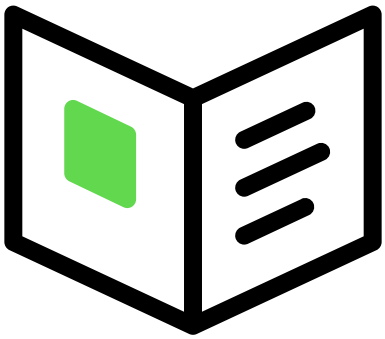
Premiers pas

Explorer	Surveiller et gérer	Corriger
		
En savoir plus sur les fonctionnalités de Vulnerability Manager Workspace	Apprenez à surveiller et à gérer les éléments vulnérables (VIT, AVIT ET CVIT) et les résultats des tests dans l'espace de travail du gestionnaire de vulnérabilité	Apprenez à corriger les éléments vulnérables (VIT, AVIT ET CVIT) et à tester les résultats dans l'espace de travail du gestionnaire de vulnérabilité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Référence



En savoir plus sur les informations supplémentaires requises pour utiliser Vulnerability Manager Workspace

Dépannage et demande d'aide

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

Exploration de l'Espace de travail du gestionnaire de vulnérabilités

En tant que gestionnaire et analyste des vulnérabilités, obtenez une vue unifiée de tous les types de vulnérabilités dans le Espace de travail du gestionnaire de vulnérabilités. Vous pouvez afficher les vulnérabilités et les problèmes de configuration de l'hôte, de l'application et du conteneur, créer des rubriques de surveillance concernant ces vulnérabilités et erreurs de configuration, et créer des tâches de rattrapage.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

Vous pouvez afficher le Espace de travail du gestionnaire de vulnérabilités en accédant à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.

L'espace de travail du gestionnaire de vulnérabilité se compose des pages suivantes :

Page d'accueil

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Se compose de filtres prédéfinis qui sont utilisés pour visualiser le résumé des enregistrements.

Pour en savoir plus sur la page d'accueil, reportez-vous à la section Vue d'ensemble de la page d'accueil.

Remarque : À partir de la version 21.0 de , les rubriques de Réponse aux vulnérabilitéssurveillance apparaissent sur la page Rubriques de surveillance.

Page Rubriques de surveillance

Se compose d'une liste de rubriques de surveillance, qui sont classées en quatre modules : vulnérabilités d'hôte, vulnérabilités d'applications, vulnérabilités de conteneurs et résultats des tests de configuration.

Pour en savoir plus sur les rubriques de la montre, reportez-vous à la section Vue d'ensemble des rubriques de surveillance.

Page Tableaux de bord

Comprend les tableaux de bord Gestion de la vulnérabilité, Gestion de la vulnérabilité (PA), Approbations de vulnérabilité, CISO, Vue d'ensemble de la gestion de la vulnérabilité des conteneurs, Gestion de la vulnérabilité des applications, Réponse de vulnérabilité unifiée et Intégrité.

Pour plus d'informations, consultez Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités.

Remarque : La page Tableaux de bord apparaît à partir de la version 19.0 de Réponse aux vulnérabilités.

Page de liste

Elles se composent des pages de liste personnalisées et par défaut pour les efforts de rattrapage, les tâches de rattrapage, les éléments vulnérables de l'hôte, les éléments vulnérables de l'application, les éléments vulnérables du conteneur, les résultats des tests de configuration, les exceptions, les approbations et les bibliothèques.

Pour plus d'informations, consultez Vue d'ensemble des listes.

Vue d'ensemble de la page d'accueil

À partir de la Réponse aux vulnérabilités version 21.0, la page d'accueil de fournit Espace de travail du gestionnaire de vulnérabilités un résumé des enregistrements actifs en présentant des visualisations de l'évaluation des risques, de la progression du rattrapage, des affectations à des groupes d'affectation, des enregistrements dans les tâches de rattrapage et des vulnérabilités des ressources du cloud.

À partir de la version 21.0 de Vulnerability Response, les rubriques de surveillance apparaissent sur la page Rubriques de surveillance. Pour plus d'informations, consultez Vue d'ensemble des rubriques de surveillance.

Sur la page d'accueil, vous pouvez afficher les visualisations des éléments vulnérables de l'hôte préfiltrés, des éléments vulnérables du conteneur, des éléments vulnérables de l'application et des résultats des tests de configuration. Vous pouvez également afficher des visualisations pour un ensemble d'enregistrements souhaités en créant et en appliquant des filtres. Pour en savoir plus sur la création, la mise à jour, l'application et la suppression de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

filtres, reportez-vous à la section Créez et appliquez des filtres pour visualiser le résumé des enregistrements actifs.

Conseil :

Si vous définissez la *sn_vul_cmn_ws.navigate_to_workspace* propriété système sur true, lors de la sélection des liens de filtre prédéfinis dans le volet de navigation, ces liens s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités avec sélection automatique du filtre enregistré correspondant.

Par exemple, si vous sélectionnez **Risque élevé** en accédant à **Tout** > **Réponse aux vulnérabilités** > **Éléments vulnérables**, ce lien est redirigé vers la page d'accueil dans le Espace de travail du gestionnaire de vulnérabilités avec sélection automatique du filtre **Risque élevé** .

Sur la page d'accueil, vous pouvez effectuer les opérations suivantes :

- accéder à la liste des enregistrements actifs dans l'interface utilisateur classique en sélectionnant le lien **Afficher la liste classique** à partir de la version 22.0 de Réponse aux vulnérabilités.
- Affichez la liste des enregistrements actifs dans le Espace de travail du gestionnaire de vulnérabilités en sélectionnant le nombre d'enregistrements actifs en regard de la liste déroulante **Afficher par** à partir de la version 22.0 de Réponse aux vulnérabilités.
- afficher les dernières informations en sélectionnant l'option **Actualiser** dans le menu à trois points d'un widget.

Vulnérabilités d'hôte

L'onglet **Vulnérabilités de l'hôte** contient des visualisations qui fournissent un résumé global des vulnérabilités actives de l'hôte.

Rôles requis :

- sn_vul.vulnerability_analyst et sn_vul.vulnerability_admin pour afficher les visualisations en appliquant des filtres et créer des filtres.
- sn_vul.read_all rôle granulaire permettant d'afficher les visualisations en appliquant des filtres.

Le tableau suivant décrit les visualisations de l'onglet Vulnérabilités de l'hôte de la page d'accueil. Sélectionnez ces visualisations pour obtenir la liste des enregistrements correspondants.

Visualisations dans l'onglet Vulnérabilités de l'hôte de la page d'accueil

Visualisation	Type	Description
Par groupe d'affectation et état du rattrapage	Barre de distribution	Enregistrements actifs affectés à divers groupes d'affectation regroupés par état de rattrapage.
Par état	Histogramme	Enregistrements actifs classés par différents états (Ouvert, En cours d'examen, En attente d'implémentation, En cours de révision, Résolu et Différé).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations dans l'onglet Vulnérabilités de l'hôte de la page d'accueil (suite)

Visualisation	Type	Description
Par cote de risque	Graphique à secteurs	Enregistrements actifs classés par cote de risque (1 - Critique, 2 - Élevé, 3 - Moyen, 4 - Faible et 5 - Aucun)
Dans une tâche de rattrapage	Anneau demi-cercle	Enregistrements actifs qui font partie de la tâche de rattrapage et qui ne font pas partie de celle-ci.
Avec les exploits existants	Anneau demi-cercle	Enregistrements actifs avec et sans exploits connus.
Par face à l'extérieur	Anneau demi-cercle	Enregistrementsactifs classés en fonction de l'exposition des actifs à Internet.
Par classe CI	Histogramme	Enregistrements actifs classés par classes CI.
Par ressource de cloud	Couronne	Enregistrementsactifs classés par diverses ressources cloud.
Éléments différés par motif	Couronne	Enregistrements différés actifs regroupés par motif.

Vulnérabilités du conteneur

L'onglet **Vulnérabilités du conteneur** contient des visualisations qui fournissent un résumé global des éléments vulnérables actifs du conteneur.

Rôles requis :

- sn_vul_container.vulnerability_analyst et sn_vul_container.vulnerability_admin pour afficher les visualisations en appliquant des filtres et créer des filtres.
- sn_vul_container.read_all rôle granulaire permettant d'afficher les visualisations en appliquant des filtres.

Le tableau suivant décrit les visualisations de l'onglet Vulnérabilités de l'hôte de la page d'accueil. Sélectionnez ces visualisations pour obtenir la liste des enregistrements correspondants.

Visualisations dans l'onglet Vulnérabilités du conteneur de la page d'accueil

Visualisation	Type	Description
Par groupe d'affectation et état du rattrapage	Barre de distribution	Enregistrements actifs affectés à divers groupes d'affectation regroupés par état de rattrapage.
Par état	Histogramme	Enregistrements actifs classés par différents états (Ouvert, En cours d'examen, En attente d'implémentation, En

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations dans l'onglet Vulnérabilités du conteneur de la page d'accueil (suite)

Visualisation	Type	Description
		cours de révision, Résolu et Différé).
Par cote de risque	Graphique à secteurs	Enregistrements actifs classés par cote de risque (1 - Critique, 2 - Élevé, 3 - Moyen, 4 - Faible et 5 - Aucun)
Dans une tâche de rattrapage	Anneau demi-cercle	Enregistrements actifs qui font partie de la tâche de rattrapage et qui ne font pas partie de celle-ci.
Avec les exploits existants	Anneau demi-cercle	Enregistrements actifs avec et sans exploits connus.
Par face à l'extérieur	Anneau demi-cercle	Enregistrementsactifs classés en fonction de l'exposition des actifs à Internet.
Images de Docker	Nombre	Nombre d'images Docker uniques.
Par image de base	Couronne	Enregistrements actifs classés par type d'image.
Éléments différés par motif	Couronne	Enregistrements différés actifs regroupés par motif.

Vulnérabilités d'applications

L'onglet **Vulnérabilités de l'application** contient des visualisations qui fournissent un résumé global des vulnérabilités de l'application.

Rôles requis :

- sn_vul.app_sec_manager pour afficher les visualisations en appliquant des filtres et créer des filtres.
- sn_vul.app_read_all rôle granulaire permettant d'afficher les visualisations en appliquant des filtres.

Le tableau suivant décrit les visualisations de l'onglet Vulnérabilités de l'hôte de la page d'accueil. Sélectionnez ces visualisations pour obtenir la liste des enregistrements correspondants.

Visualisations dans l'onglet Vulnérabilités de l'application de la page d'accueil

Visualisation	Type	Description
Par groupe d'affectation et état du rattrapage	Barre de distribution	Enregistrements actifs affectés à divers groupes d'affectation regroupés par état de rattrapage.
Par état	Histogramme	Enregistrements actifs classés par différents états (Ouvert,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations dans l'onglet Vulnérabilités de l'application de la page d'accueil (suite)

Visualisation	Type	Description
		En cours d'examen, En attente d'implémentation, En cours de révision, Résolu et Différé).
Par cote de risque	Graphique à secteurs	Enregistrements actifs classés par cote de risque (1 - Critique, 2 - Élevé, 3 - Moyen, 4 - Faible et 5 - Aucun)
Dans une tâche de rattrapage	Anneau demi-cercle	Enregistrements actifs qui font partie de la tâche de rattrapage et qui ne font pas partie de celle-ci.
Avec les exploits existants	Anneau demi-cercle	Enregistrements actifs avec et sans exploits connus.
Par face à l'extérieur	Anneau demi-cercle	Enregistrementsactifs classés en fonction de l'exposition des actifs à Internet.
Par classe CI	Histogramme	Enregistrements actifs classés par classes CI.
Par ressource de cloud	Couronne	Enregistrementsactifs classés par diverses ressources cloud.
Éléments différés par motif	Couronne	Enregistrements différés actifs regroupés par motif.

Résultats des tests de configuration

L'onglet **Résultats des tests de configuration** contient des visualisations qui fournissent un résumé global des mauvaises configurations actives des actifs de votre organisation.

Rôles requis :

- sn_vulc.admin pour afficher les visualisations en appliquant des filtres et créer des filtres.
- sn_vulc. Rôle granulaire de lecture pour afficher les visualisations en appliquant des filtres.

Le tableau suivant décrit les visualisations de l'onglet Résultats des tests de configuration de la page d'accueil. Sélectionnez ces visualisations pour obtenir la liste des enregistrements correspondants.

Visualisations dans l'onglet Résultats des tests de configuration de la page d'accueil

Visualisation		Description
Par groupe d'affectation et état du rattrapage	Barre de distribution	Enregistrements actifs affectés à divers groupes d'affectation regroupés par état de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations dans l'onglet Résultats des tests de configuration de la page d'accueil (suite)

Visualisation		Description
Par état	Histogramme	Enregistrements actifs classés par différents états (Ouvert, En cours d'examen, En attente d'implémentation, En cours de révision, Résolu et Différé).
Par cote de risque	Graphique à secteurs	Enregistrements actifs classés par cote de risque (1 - Critique, 2 - Élevé, 3 - Moyen, 4 - Faible et 5 - Aucun)
Par technologie	Histogramme	Enregistrements actifs classés par technologie.
Par test	Histogramme	Enregistrements actifs classés par tests.
Par face à l'extérieur	Anneau demi-cercle	Enregistrementsactifs classés en fonction de l'exposition des actifs à Internet.
Par classe CI	Histogramme	Enregistrements actifs classés par classes CI.
Par ressource de cloud	Couronne	Enregistrementsactifs classés par diverses ressources cloud.
Éléments différés par motif	Couronne	Enregistrements différés actifs regroupés par motif.

Vue d'ensemble des rubriques de surveillance

Une rubrique Regarder est un ensemble de visualisations de données qui vous permet de surveiller un ensemble filtré d'enregistrements au fil du temps sur un tableau de bord susceptible d'être d'un intérêt ou d'une priorité particulière pour votre organisation.

À partir de la version 21.0 de , les rubriques de Réponse aux vulnérabilitéssurveillance apparaissent sur la page Rubriques de surveillance.

Les données affichées sur les visualisations de données des rubriques de surveillance sont mises à jour dynamiquement à mesure que les données de vulnérabilité changent lors de l'importation. Utilisez les tableaux de bord pour surveiller les tendances, le champ d'application et les types de vulnérabilités, ainsi que vos éléments de configuration pour la rubrique de surveillance sélectionnée. Ces informations vous aident à déterminer l'impact des vulnérabilités de chaque rubrique de surveillance sur votre environnement. Pour en savoir plus sur les onglets d'éléments connexes et leurs visualisations dans une rubrique de visualisation, reportez-vous Liste d'éléments connexes et visualisations dans une rubrique de surveillanceà .

Les rubriques de surveillance suivantes sont fournies avec le système de base dans le module Vulnérabilités de l'hôte :

- Vulnérabilités sur les actifs externes
- Vulnérabilités avec exploits disponibles

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vulnérabilités sur les serveurs Windows
- Vulnérabilités sur les serveurs LINUX
- Vulnérabilités critiques en retard
- Vulnérabilités critiques ne faisant pas partie des tâches de rattrapage

Remarque : Si une visualisation des données montre qu'il n'y a aucun VI pour cette catégorie, mais qu'une liste de VI s'affiche lorsque vous cliquez sur l'icône graphique, cochez la colonne avec le nom de la rubrique de surveillance dans la liste qui s'affiche. Vérifiez que la valeur de tous les VI répertoriés dans la colonne de la rubrique de surveillance (par exemple, accessible sur Internet) est `fausse`. Dans cet exemple, cette valeur indique qu'il n'existe aucun VI orientés vers Internet pour cette rubrique de surveillance.

Pour démarrer le rattrapage ou lorsqu'un besoin critique se fait sentir pour les enregistrements qui se trouvent dans une rubrique de surveillance, vous pouvez créer un effort de rattrapage à partir d'une rubrique de visualisation. Pour plus d'informations, consultez Créer un effort de rattrapage dans Vulnerability Manager Workspace.

Information associée

Liste d'éléments connexes et visualisations dans une rubrique de surveillance

Utiliser des rubriques de visualisation dans Espace de travail du gestionnaire de vulnérabilités

Créer une rubrique de surveillance dans Vulnerability Manager Workspace

Modifier ou supprimer une rubrique de surveillance

Désactiver ou activer une rubrique de surveillance

Liste d'éléments connexes et visualisations dans une rubrique de surveillance

À partir de la version 18.0, vous pouvez créer des rubriques de surveillance classées en quatre modules : Vulnérabilités d'hôte, Vulnérabilités de conteneur, Vulnérabilités d'applications et Résultats des tests de configuration. Les onglets d'éléments connexes d'une rubrique de surveillance diffèrent pour chaque module.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

Le volet de navigation de la page de destination contient les modules suivants :

- Vulnérabilités de l'hôte : affiche les rubriques de surveillance qui incluent les éléments vulnérables de l'hôte.
- Vulnérabilités du conteneur : affiche les rubriques de surveillance qui incluent les éléments vulnérables du conteneur.
- Vulnérabilités de l'application : affiche les rubriques de surveillance qui incluent les éléments vulnérables de l'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Résultats des tests de configuration : affiche les rubriques de surveillance qui incluent les éléments de configuration.
- Inactif : affiche les rubriques de surveillance inactives des quatre modules.

Le tableau suivant répertorie les onglets d'éléments connexes disponibles pour différents modules de rubrique de surveillance :

Rubrique de surveillance et ses éléments connexes

Rubrique de surveillance	Onglets Éléments connexes
Vulnérabilités d'hôte	Vue d'ensemble, CI impactés, vulnérabilités distinctes et éléments vulnérables
Vulnérabilités du conteneur	Vue d'ensemble, CI impactés, vulnérabilités distinctes et éléments vulnérables
Vulnérabilités d'applications	Vue d'ensemble et éléments vulnérables
Résultats des tests de configuration	Vue d'ensemble, CI impactés, tests de configuration distincts et résultats des tests de configuration

Le tableau suivant fournit une description des onglets d'éléments connexes et des visualisations dans une rubrique de visualisation.

Onglets et visualisation d'éléments connexes dans une rubrique de surveillance

Onglet et visualisation des éléments connexes	Description
Vue d'ensemble	
Éléments vulnérables actifs au fil du temps	Nombre d'éléments vulnérables actifs (VI) au fil du temps. Vous pouvez surveiller les tendances de ces données au cours des 30 derniers jours. Vous pouvez également filtrer les données à l'aide des filtres Catégorie d'actif.
VI dans des efforts de rattrapage	Nombre de VI actifs sur le nombre total de VI qui font déjà l'objet d'efforts de rattrapage actifs.
Efforts de rattrapage actifs	Liste des efforts de rattrapage actifs.
CI impactés	
CI distincts	Nombre d'éléments de configuration (CI) (actifs) impactés par ces vulnérabilités.
VI par classe de CI	Nombre d'éléments vulnérables (VI) pour chaque Base de données de gestion des configurations (CMDB) classe CI. **Remarque :** Ce widget apparaît uniquement pour les rubriques de surveillance dans le module Vulnérabilités de l'hôte, de l'application et du conteneur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglets et visualisation d'éléments connexes dans une rubrique de surveillance (suite)

Onglet et visualisation des éléments connexes	Description
Problèmes de configuration par classe CI	Nombre de CI pour chaque Base de données de gestion des configurations (CMDB) classe CI. **Remarque :** Ce widget s'affiche uniquement pour les rubriques de surveillance dans le module Problèmes de configuration.
VI accessibles sur Internet	Nombre d'éléments vulnérables actifs par rapport au nombre total d'éléments vulnérables de vos actifs exposés à Internet. **Remarque :** Ce widget apparaît uniquement pour les rubriques de surveillance dans le module Vulnérabilités de l'hôte, de l'application et du conteneur.
Problèmes de configuration sur Internet	Nombre de CI actifs sur le nombre total de CI de vos actifs exposés à Internet. **Remarque :** Ce widget s'affiche uniquement pour les rubriques de surveillance dans le module Problèmes de configuration.
Vulnérabilités distinctes	
VI avec exploits existants	VI actifs avec des exploits connus.
Vulnérabilités distinctes	Nombre de vulnérabilités individuelles distinctes associées à vos actifs. Les différentes vulnérabilités peuvent être filtrées en fonction du type de problème.
Éléments vulnérables avec vulnérabilités PCI	Nombre d'actifs individuels distincts qui ont des VI actifs présentant des vulnérabilités de l'industrie des cartes de paiement (PCI).
Éléments vulnérables	
Éléments vulnérables d'hôte	Liste de tous les éléments vulnérables de l'hôte. Vous pouvez filtrer cette liste afin d'afficher uniquement les enregistrements que vous souhaitez voir. **Remarque :** Cette liste s'affiche uniquement pour les rubriques de surveillance du module Vulnérabilités de l'hôte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglets et visualisation d'éléments connexes dans une rubrique de surveillance (suite)

Onglet et visualisation des éléments connexes	Description
Éléments vulnérables de l'application	Liste de tous les éléments vulnérables de l'application. Vous pouvez filtrer cette liste afin d'afficher uniquement les enregistrements que vous souhaitez voir. **Remarque :** Cette liste s'affiche uniquement pour les rubriques de surveillance dans le module Vulnérabilités d'application.
Éléments vulnérables de conteneurs	Liste de tous les éléments vulnérables du conteneur. Vous pouvez filtrer cette liste pour l'afficher afin que seuls les enregistrements que vous souhaitez afficher s'affichent. **Remarque :** Cette liste s'affiche uniquement pour les rubriques de surveillance du module Vulnérabilités du conteneur.
Onglet Vue d'ensemble dans une rubrique de surveillance sous le module Résultats des tests de configuration	
Résultats des tests de configuration actifs au fil du temps	Nombre de résultats des tests de configuration actifs au fil du temps. Vous pouvez surveiller les tendances de ces données au cours des 30 derniers jours.
Résultats des tests de configuration dans les efforts de rattrapage	Nombre de résultats des tests de configuration actifs par rapport au nombre total d'enregistrements qui sont déjà dans les efforts de rattrapage actifs.
Efforts de rattrapage actifs	Liste des efforts de rattrapage actifs.
Onglet Tests de configuration distincts dans une rubrique de surveillance sous le module Résultats des tests de configuration	
Résultats des tests de configuration via la criticité du test	Résultats des tests de configuration basés sur la criticité des problèmes.
Tests de configuration distincts	Nombre de tests de configuration distincts.
Onglet Résultats des tests de configuration dans une rubrique de surveillance sous le module Résultats des tests de configuration	Liste des résultats des tests de configuration.

Vous pouvez obtenir les derniers détails d'une rubrique de surveillance en cliquant sur le bouton **Actualiser** . Le dernier état d'actualisation et le dernier horodatage sont affichés sous le nom de la rubrique de surveillance. Lorsque vous actualisez une rubrique de visualisation, tous les détails de la rubrique de visualisation, y compris les graphiques et les efforts de rattrapage, sont mis à jour. Une rubrique de surveillance est actualisée automatiquement lorsqu'elle est créée ou mise à jour.

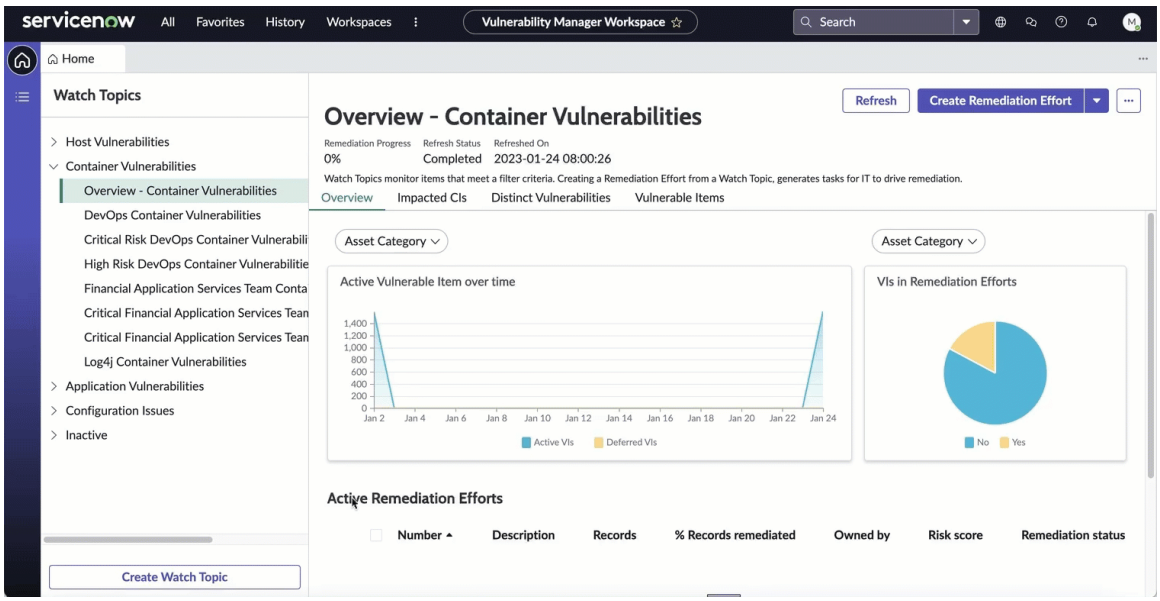
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Étant donné que vous ne pouvez pas actualiser une rubrique de visualisation inactive, le bouton **Actualiser** est inactif pour une rubrique de visualisation inactive.

Cliquez sur un tracé de données sur l'un des widgets pour afficher des informations supplémentaires sur les enregistrements.

Example: Version 18.0 Visualisations de données dans une rubrique de surveillance



Vue d'ensemble des efforts de rattrapage

Un effort de rattrapage est un ensemble d'enregistrements associés à une rubrique de visualisation. Les enregistrements répertoriés dans un effort de rattrapage sont statiques. Ils ne sont pas mis à jour par les nouvelles données d'importation ou les modifications que vous apportez aux rubriques de surveillance.

Une fois **Actif** sélectionné dans la liste **Efforts de rattrapage** , cliquez sur un lien d'effort de rattrapage pour l'ouvrir.

Les éléments de liste connexes de l'enregistrement des efforts de rattrapage vous permettent d'afficher la progression et l'état globaux du rattrapage sur les enregistrements qui lui sont associés.

- Sous l'onglet **Vue d'ensemble** , surveillez les enregistrements associés à cet effort de rattrapage qui ont été fermés au fil du temps. À droite de l'enregistrement, cliquez sur l'icône de filtre sur le graphique pour afficher les filtres appliqués à la visualisation des données.
- Dans l'onglet **Détails** , affichez les détails de l'effort de rattrapage, y compris sa rubrique de surveillance associée et son état (actif ou inactif). Vous pouvez désactiver un effort de rattrapage à partir de cette page. Si vous désactivez l'effort de rattrapage avant la fermeture de tous les enregistrements, tous les enregistrements actifs peuvent être ajoutés aux nouveaux efforts de rattrapage.
- Dans l'onglet **Tâches de rattrapage** , affichez les tâches de rattrapage associées à cet effort de rattrapage. Affichez le pourcentage des enregistrements associés à cette tâche qui sont rattrapés.
- Dans l'onglet **Éléments vulnérables** , affichez les enregistrements associés à cet effort de rattrapage. Lorsque tous les enregistrements d'une tâche de rattrapage sont terminés

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

et fermés, l'effort de rattrapage passe à l'état Inactif. Lorsqu'un effort de rattrapage est inactif, tous les enregistrements fermés associés à cet effort ne peuvent pas être ajoutés à de nouveaux efforts de rattrapage.

Remarque : À partir de la version 18.0, l'onglet **Éléments vulnérables** apparaît pour les efforts de rattrapage associés aux rubriques de surveillance dans les modules Vulnérabilités d'hôte, Vulnérabilités d'applications et Vulnérabilités de conteneurs.

- Dans l'onglet **Résultats des tests de configuration** , affichez les résultats des tests de configuration associés à l'effort de rattrapage.

Remarque : À partir de la version 18.0, l'onglet **Résultats des tests de configuration** s'affiche pour les efforts de rattrapage associés aux rubriques de surveillance dans le module Résultats des tests de configuration.

Pour plus de détails et pour connaître les actions d'interface utilisateur que vous pouvez effectuer à partir d'un effort de rattrapage, reportez-vous à la section Utiliser les enregistrements d'efforts de rattrapage.

Information associée

Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Vulnerability Response

Créer un effort de rattrapage dans Vulnerability Manager Workspace

Créer une tâche de remédiation sur demande dans Vulnerability Manager Workspace

Créer un effort de rattrapage récurrent dans les espaces de travail Vulnerability Response

Transférer des enregistrements aux efforts de rattrapage dans les Réponse aux vulnérabilités espaces de travail

Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Vulnerability Response

Les états des enregistrements et leurs tâches de rattrapage (RT) associées sont impactés si les enregistrements sont reportés, résolus, rouverts et transférés à d'autres efforts de rattrapage (ER).

Rôles requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Création d'efforts de rattrapage

L'impact sur les états et les cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dépend de la façon dont un effort de rattrapage est créé, du moment où il est créé et de sa désactivation.

Dans la liste située en haut à droite d'une rubrique de visualisation, vous pouvez créer un effort de rattrapage en cliquant sur **Créer un effort de rattrapage** ou **Créer un effort récurrent**. Vous pouvez créer un effort de rattrapage récurrent par rubrique de surveillance. Si vous créez un effort de rattrapage récurrent, les efforts de rattrapage suivants pour la rubrique

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de surveillance associée sont créés automatiquement en fonction des critères que vous définissez. Dans les deux cas :

- Pour faciliter le rattrapage, seuls les enregistrements actifs sont ajoutés aux efforts de rattrapage.
- Tous les enregistrements faisant l'objet d'un nouvel effort de rattrapage sont placés dans de nouvelles tâches de rattrapage. Les enregistrements peuvent exister dans plusieurs tâches de rattrapage, mais un seul enregistrement peut être associé à un effort de rattrapage.

Remarque : Un effort de rattrapage est désactivé automatiquement lorsqu'il n'existe aucun enregistrement actif.

Transfert d'enregistrements ou transfert d'enregistrements

Vous pouvez transférer des enregistrements d'un effort de rattrapage à un autre lors de la création d'un effort de rattrapage en cochant la case **Transférer les enregistrements correspondants à partir d'autres efforts de rattrapage actifs** . Pour en savoir plus sur le transfert des enregistrements, reportez-vous à la section Transférer des enregistrements aux efforts de rattrapage dans les Réponse aux vulnérabilités espaces de travail. Si les enregistrements sont transférés d'un effort de rattrapage ou déplacés dans des efforts de rattrapage récurrents :

À un nouvel effort de rattrapage dans la même rubrique de surveillance

- Toutes les tâches de rattrapage de l'ancien effort de rattrapage sont déplacées vers le nouvel effort de rattrapage.
- Les nouvelles tâches de rattrapage sont créées en fonction des critères de regroupement choisis pour les enregistrements qui ne faisaient auparavant partie d'aucune tâche de rattrapage.
- L'ancien effort de rattrapage est désactivé.

Vers un nouvel effort de rattrapage dans une rubrique de surveillance différente

Tous les enregistrements de l'ancien effort de rattrapage sont déplacés vers le nouvel effort de rattrapage et les tâches de rattrapage sont créées en fonction des critères de regroupement choisis.

- Si tous les enregistrements des tâches de rattrapage associées à l'ancien effort de rattrapage sont transférés, ces tâches de rattrapage sont fermées-annulées.
- Si seul un sous-ensemble d'enregistrements est transféré, les tâches de rattrapage associées à l'ancien effort de rattrapage sont fractionnées et restent actives.

Les tâches de rattrapage fermées associées à l'ancien effort de rattrapage ne sont pas affectées.

Remarque : Vous ne pouvez pas transférer les enregistrements d'efforts de rattrapage récurrents vers de nouveaux efforts de rattrapage. Toutefois, vous pouvez transférer des enregistrements d'efforts de rattrapage existants et non récurrents vers de nouveaux efforts de rattrapage. Pour plus d'informations sur le transfert d'enregistrements, reportez-vous à la rubrique Transférer des enregistrements aux efforts de rattrapage dans les Réponse aux vulnérabilités espaces de travail

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités

Dans le Espace de travail du gestionnaire de vulnérabilités, vous pouvez afficher les tableaux de bord dans l'interface Next Experience utilisateur et utiliser ces tableaux de bord pour suivre et analyser les vulnérabilités.

Rôles requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Accéder aux tableaux de bord du Espace de travail du gestionnaire de vulnérabilités en naviguant jusqu'à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et en sélectionnant l'icône **Tableaux de bord** . Le tableau de bord par défaut s'affiche en fonction de votre rôle.

La table suivante montre le tableau de bord par défaut qui s'affiche pour un rôle spécifique.

Tableau de bord par défaut

Tableau de bord par défaut	Rôle
Tableau de bord unifié	sn_vul_cmn_vulnerability_admin ou sn_vul_cmn_vulnerability_analyst
Tableau de bord de PA de vulnérabilité	sn_vul_vulnerability_admin ou sn_vul_vulnerability_analyst
Vue d'ensemble de l'application	sn_vul_app_sec_manager
Vue d'ensemble du conteneur	sn_vul_container_vulnerability_admin ou sn_vul_container_analyst

Vous pouvez afficher les tableaux de bord suivants pour les tâches que vous souhaitez effectuer en les sélectionnant dans la liste déroulante de la page Tableaux de bord.

Tableaux de bord dans Vulnerability Manager Workspace

Tableau de bord	Description
Gestion de la vulnérabilité (PA)	Suivez le volume, les performances et la progression des vulnérabilités de l'hôte, depuis l'analyse et la détection initiales jusqu'au confinement ou à la correction. Pour plus d'informations, consultez Vulnerability Management (PA) tableau de bord.
Approbations de vulnérabilité	Affichez le nombre de demandes d'approbation approuvées, rejetées et en attente pour vous. Pour plus d'informations, consultez Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableaux de bord dans Vulnerability Manager Workspace (suite)

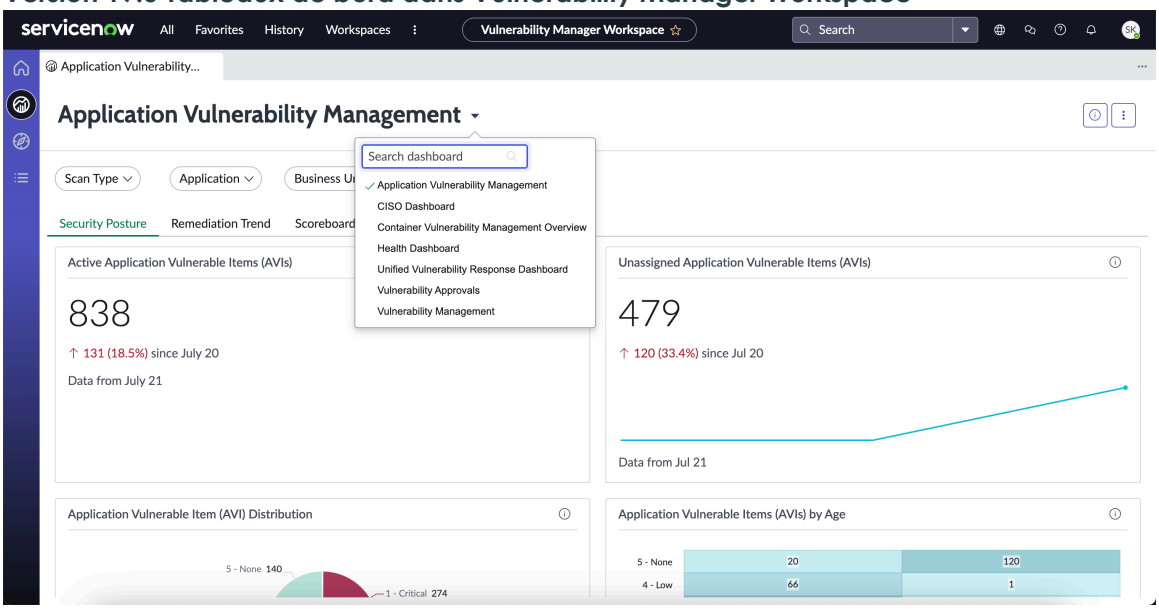
Tableau de bord	Description
Tableau de bord des CISO	Révèle la posture de sécurité globale de votre organisation, y compris la vulnérabilité de sécurité et les incidents. Pour plus d'informations, consultez Tableau de bord Vulnerability Management des CISO.
Vue d'ensemble de la gestion de la vulnérabilité du conteneur	Suivez le volume, les performances et la progression des vulnérabilités du conteneur, depuis l'analyse et la détection initiales jusqu'au confinement ou à la correction. Pour plus d'informations, consultez Tableau de bord de Réponse aux vulnérabilités pour conteneurs.
Tableau de bord Application Vulnerability Management	Suivez le volume, les performances et la progression des vulnérabilités des applications, depuis l'analyse et la détection initiales jusqu'au confinement ou à la correction. Pour plus d'informations, voir Gestion de la vulnérabilité des applications (PA) tableau de bord
Tableau de bord de Vulnerability Response unifié	Fournit une visibilité à partir de plusieurs scanners de vulnérabilités et outils de sécurité pour fournir une vue complète des vulnérabilités et des risques d'une organisation. Pour plus d'informations, consultez Solutions d'analyse et de reporting pour le tableau de bord de Vulnerability Response unifié.
Tableau de bord d'intégrité de Vulnerability Response	Affiche le score d'intégrité global de l'application Vulnerability Response. Pour plus d'informations, consultez Tableau de bord d'intégrité de SecOps Vulnerability Response.

L'image suivante montre la page Tableaux de bord dans le Espace de travail du gestionnaire de vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Version 19.0 Tableaux de bord dans Vulnerability Manager Workspace



Vous pouvez également créer un tableau de bord personnalisé en sélectionnant l'icône Plus d'options Plus ⋮, puis en sélectionnant **Créer un nouveau tableau de bord**.

Vue d'ensemble des listes

La vue de liste de l'espace de travail du gestionnaire de vulnérabilité permet aux gestionnaires et analystes de la vulnérabilité et de la sécurité de voir la progression du rattrapage sur les enregistrements, d'explorer les enregistrements Vulnerability Response et d'afficher l'état de leurs demandes d'approbation et exceptions.

Ces listes et liens vous permettent d'accéder facilement aux enregistrements et aux tâches. Il contient deux onglets :

- **Onglet Listes** : affiche les listes par défaut pour les efforts de rattrapage, les tâches de rattrapage, les éléments vulnérables, les solutions, les exceptions et les résultats des tests de configuration.
- **Onglet Mes listes** : affiche toutes les listes que vous avez renommées à partir de l'onglet Liste et toutes les listes que vous créez.

  Vous pouvez également créer votre propre liste pour surveiller la progression du rattrapage. Pour plus d'informations, consultez Créer une liste personnalisée des enregistrements.

Onglet Listes

Les listes suivantes s'affichent :

- Efforts de rattrapage (ER) : affiche les ER actives et toutes les RE affectées à vos groupes.
- Tâches de rattrapage (VUL) : affiche les tâches de rattrapage actives et toutes les tâches de rattrapage affectées à vos groupes.

> **Remarque :** À partir de la version 18.0, la liste des tâches de rattrapage affiche les tâches de rattrapage créées dans l'interface utilisateur et l'espace de travail classiques pour Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Éléments vulnérables de l'hôte : affiche les éléments vulnérables de l'hôte (VI) actifs et tous les VI de l'hôte du module Vulnérabilités de l'hôte.
- Éléments vulnérables de l'application : affiche les éléments vulnérables de l'application (AVIT) actifs et tous les AVIT du module des vulnérabilités de l'application.
- Éléments vulnérables du conteneur : affiche les éléments vulnérables (CVIT) actifs du conteneur et tous les CVIT du module Vulnérabilités du conteneur.
- Résultats des tests de configuration : affiche les résultats des tests de configuration actifs et tous les résultats des tests de configuration du module Résultats des tests de configuration.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

- Solutions : affiche toutes les solutions pour les éléments vulnérables.
- Exceptions : affiche les états d'approbation pour toutes les demandes d'exception et les faux positifs de vos groupes.
- Approbations : affiche les demandes d'approbation qui vous sont affectées pour traitement. Pour traiter vos approbations dans l'espace de travail, reportez-vous à la section Approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilités.
- Bibliothèques : affiche les bibliothèques, politiques et tests suivants.
  - CVE : affiche toutes les vulnérabilités et expositions courantes (CVE) de , Réponse aux vulnérabilités des applications, Réponse aux vulnérabilitéset Réponse aux vulnérabilités pour conteneurs.
  - TPE : affiche toutes les entrées tierces (TPE) de Réponse aux vulnérabilités.
  - CWE : affiche toutes les énumérations de faiblesses courantes (CWE) de , Réponse aux vulnérabilités des applications, Réponse aux vulnérabilitéset Réponse aux vulnérabilités pour conteneurs.
  - Vulnérabilités de l'application : affiche toutes les entrées de vulnérabilité de l'application tierce.
  - Groupes de tests : affiche tous les groupes de Conformité de la configuration tests. Vous pouvez afficher le pourcentage de conformité des CI et la conformité des résultats des tests pour un groupe de tests dans la vue d'enregistrement.
  - Tests : affiche tous les tests à partir d'un Conformité de la configurationfichier . Vous pouvez afficher le pourcentage de conformité des résultats des tests pour un test dans la vue d'enregistrement.
  - Contrôles de compensation : affiche tous les contrôles de compensation qui peuvent être utilisés pour les demandes de réduction des risques. Vous pouvez ajouter un contrôle de compensation en cliquant sur **Nouveau**. Pour plus d'informations sur l'ajout

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'un contrôle de compensation, reportez-vous à la section Ajouter un contrôle de compensation à la bibliothèque.

Remarque : La liste des contrôles compensatoires apparaît à partir de la v20.0 de Réponse aux vulnérabilités.

Information associée

Utiliser la vue de liste dans l'espace de travail du gestionnaire de vulnérabilité

Vue d'ensemble des modifications en bloc

Dans le Espace de travail du gestionnaire de vulnérabilités, la fonctionnalité de modification en bloc vous permet de mettre à jour simultanément plusieurs éléments vulnérables (VIT, AVIT, CVIT ou TR), rationalisant ainsi le processus de gestion et de correction.

La modification en bloc vous permet de sélectionner plusieurs vulnérabilités et d'appliquer des changements cohérents, tels que l'affectation de propriétaires de rattrapage, la mise à jour de l'état, l'ajout de notes de travail, la demande d'exceptions et la demande de faux positif. Cela permet d'économiser du temps et des efforts en éliminant la nécessité de modifier les éléments vulnérables individuellement, ce qui favorise une gestion efficace et cohérente des vulnérabilités.

La fonctionnalité de modification en bloc est disponible pour :

- éléments vulnérables de l'hôte (VIT) à partir de la version 21.0 de Réponse aux vulnérabilités.
- Éléments vulnérables de l'application (AVIT) et éléments vulnérables du conteneur (CVIT) à partir de la version 22.0 de Réponse aux vulnérabilités.
- résultats des tests (TR) à partir de la version 23.0 de Réponse aux vulnérabilités.

Vous pouvez effectuer les tâches suivantes à l'aide de la fonctionnalité de modification en bloc dans :Espace de travail du gestionnaire de vulnérabilités

- Affecter des enregistrements à un groupe d'affectation en bloc
- Demander une exception en bloc dans Vulnerability Manager Workspace
- Supprimer les affectations des éléments vulnérables d'hôte en bloc
- Modification en bloc pour les faux positifs dans Vulnerability Manager Workspace
- Fermer les enregistrements en bloc dans le Espace de travail du gestionnaire de vulnérabilités

Comprendre les contrôles compensatoires pour la réduction des risques

Les contrôles compensatoires sont les mesures prises pour réduire le risque posé par les vulnérabilités qui ne peuvent pas être corrigées immédiatement. Ils peuvent être utilisés pour atténuer la probabilité ou l'impact d'un exploit réussi.

Remarque : La fonctionnalité de contrôles de compensation n'est disponible que pour les vulnérabilités de l'hôte.

L'application de contrôles compensatoires peut contribuer à réduire le risque d'une vulnérabilité.

La table suivante présente les cas d'utilisation des contrôles de compensation :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation pour les contrôles de compensation

Cas d'utilisation	Contrôle de compensation
Une vulnérabilité dans un serveur Web qui permet aux attaquants d'exécuter du code arbitraire.	Implémentez un pare-feu d'application Web (WAF) pour bloquer les demandes malveillantes adressées au serveur Web.
Une vulnérabilité dans un système d'exploitation qui permet aux attaquants d'élever les privilèges à la racine.	Implémentez un contrôle d'application pour restreindre l'exécution d'applications sur le système hôte.
Une vulnérabilité dans un serveur de base de données qui permet aux attaquants d'accéder à des données sensibles.	Implémentez la segmentation du réseau pour isoler le serveur de base de données des autres hôtes et des systèmes critiques.

Pour plus d'informations sur l'impact des contrôles compensatoires sur le score de risque d'un élément vulnérable et d'une tâche de rattrapage, reportez-vous à Impact des contrôles compensatoires sur le score de risque et la date d'expiration.

Information associée

- Ajouter un contrôle de compensation à la bibliothèque
- Associer les contrôles compensatoires aux CVE ou aux TPE pour les demandes de réduction des risques
- Désactiver ou activer la réduction du risque pour une CVE ou une TPE

Solutions d'analyse et de reporting pour le tableau de bord de Vulnerability Response unifié

Le tableau de bord de Vulnerability Response unifié est un tableau de bord agrégé centralisé qui fournit une visibilité à partir de plusieurs scanners de vulnérabilité et outils de sécurité afin de fournir une vue complète des vulnérabilités et des risques d'une organisation.

Rôles requis

Les rôles et tâches suivants sont associés à cette solution. Ils sont nécessaires pour afficher et partager les rapports :

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

Information associée

- Solutions d'analyse et de génération de rapports

Tableau de bord de Vulnerability Response unifié

Le tableau de bord Unified Vulnerability Response fournit une vue complète des vulnérabilités et des risques d'une organisation. Les vulnérabilités liées à l'infrastructure, au

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

cloud, aux applications et aux conteneurs peuvent être consultées dans un tableau de bord centralisé pour une meilleure visibilité et une meilleure correction.

Rôles Now Platform requis

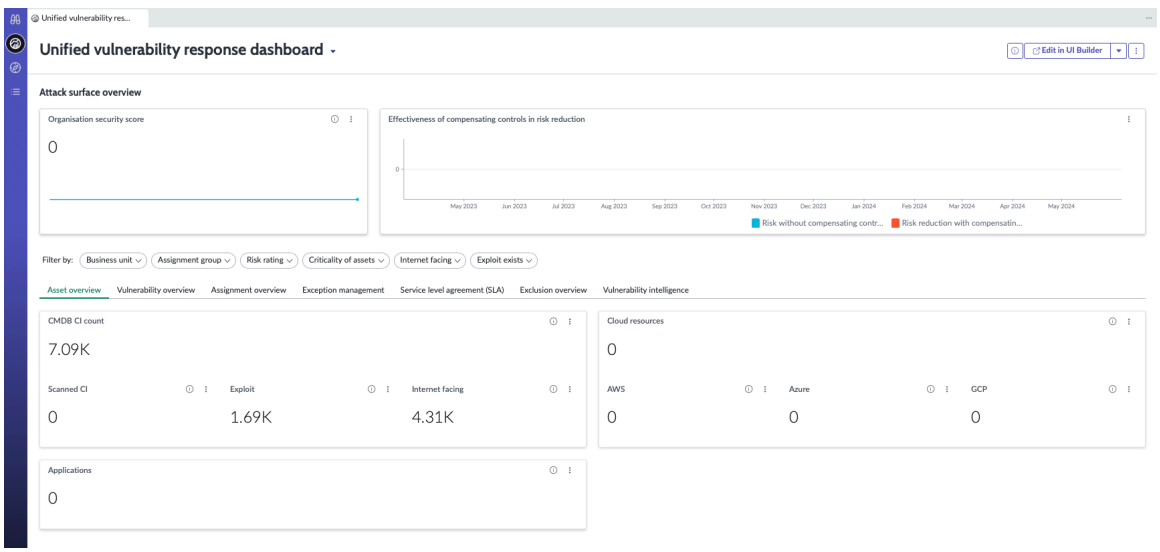
Les rôles suivants sont associés à cette solution. Ils sont nécessaires pour afficher, modifier et partager les rapports :

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

Accéder au tableau de bord de Vulnerability Response unifié

Pour ouvrir le tableau de bord, accédez à :

- **Tout** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité** et sélectionnez l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher le tableau de bord de Vulnerability Response unifié, sélectionnez la liste déroulante en regard du nom du tableau de bord.
- **Espaces de travail** > **Espace de travail d'Analyse de la plateforme** > **Tableaux de bord** > **Tableau de bord de Vulnerability Response unifié**.



Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Traduction automatique

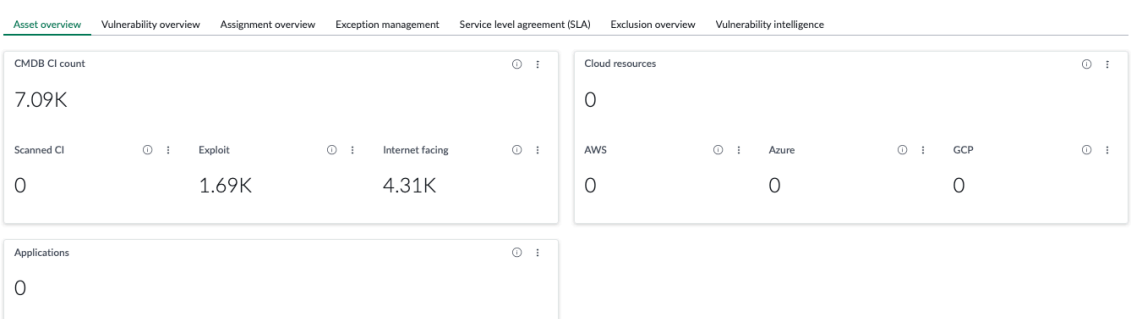
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur	Utilisation du tableau de bord
• Responsables des vulnérabilités • Analystes de vulnérabilité	• Fournit une visibilité en temps réel des risques présents dans l'infrastructure, les applications, les configurations et les conteneurs. Permet aux gestionnaires de vulnérabilité et aux analystes de vulnérabilité de hiérarchiser et de corriger les vulnérabilités en temps opportun. • Fournit une vue d'ensemble de la surface d'attaque des actifs critiques, qui peut être utilisée pour suivre la progression et les efforts de correction. • Fournit une vue d'ensemble des risques entre les unités business (BU). Vous pouvez utiliser des filtres pour sélectionner des unités de gestion et comparer la progression pour réallouer des ressources, si nécessaire. L'accès au niveau du rôle doit être fourni au responsable de la BU. • Fournit une visibilité sur l'impact potentiel des BU. Vous pouvez utiliser le filtre Vulnérabilité et exposition communes (CVE) pour identifier les expositions dans l'ensemble de l'organisation. • Fournit une visibilité sur les scores EPSS atteints par les entrées vulnérables qui existent dans le catalogue CISA KEV pour les éléments vulnérables d'application, d'hôte et de conteneur.

Onglets du tableau de bord de Vulnerability Response unifié

Ce tableau de bord vous permet de voir les vulnérabilités ou les problèmes présents dans les hôtes, le cloud, les configurations, les applications et les conteneurs. Vous pouvez afficher les vulnérabilités en fonction de l'unité business, du groupe d'affectation, de la cote de risque, de la criticité et de l'existence d'un exploit pour les vulnérabilités.

L'onglet **Vue d'ensemble des actifs** fournit l'état global des éléments de configuration (CI) dans le

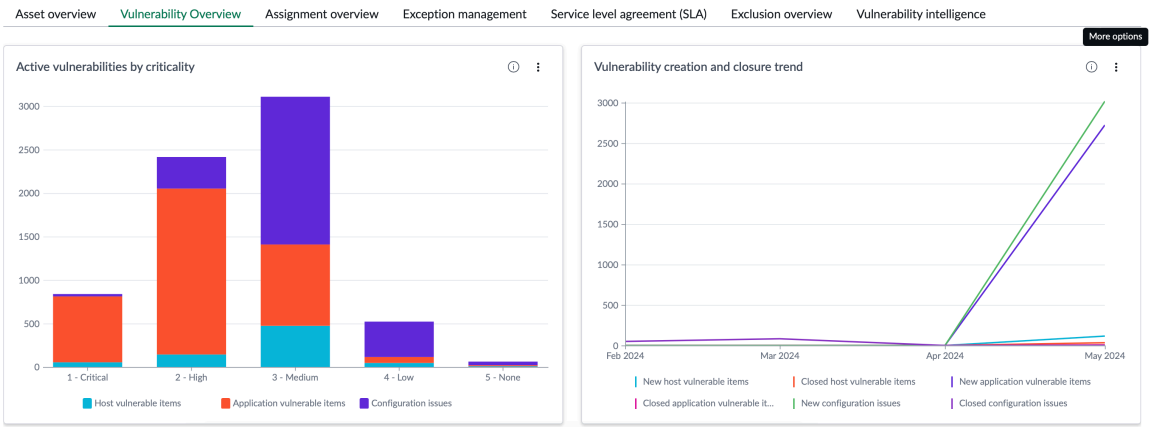


système.

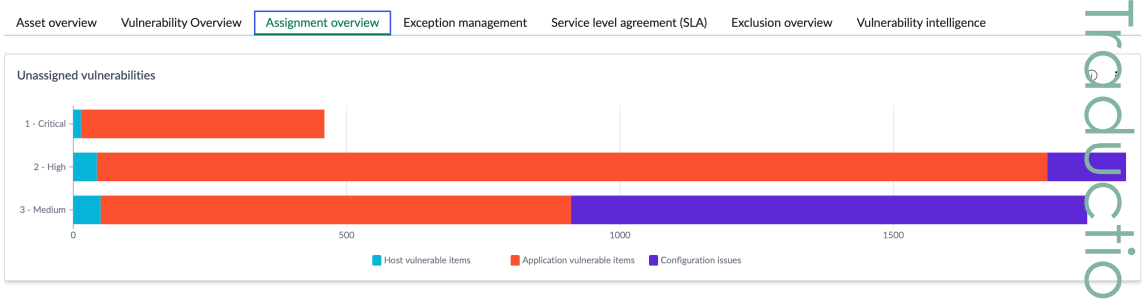
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

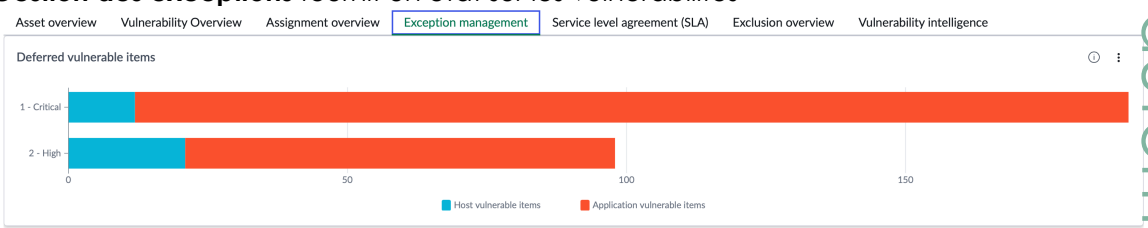
L'onglet **Vue d'ensemble** de la vulnérabilité fournit un état sur les types de vulnérabilités tels que l'hôte, l'application, le conteneur.



L'onglet **Vue d'ensemble de l'affectation** fournit un état sur l'affectation des vulnérabilités.



L'onglet **Gestion des exceptions** fournit un état sur les vulnérabilités différées.



L'onglet Accord sur les **niveaux de service (SLA)** indique l'état de l'accord sur les niveaux de service atteint par différents groupes d'affectation.

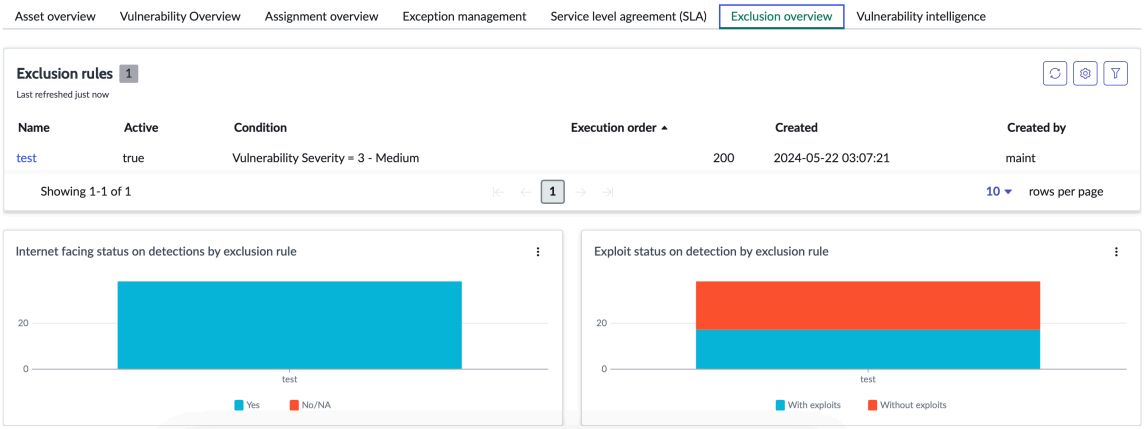


L'onglet **Vue d'ensemble de l'exclusion** indique l'état des règles d'exclusion que vous avez créées, ainsi que celles affectant les détections

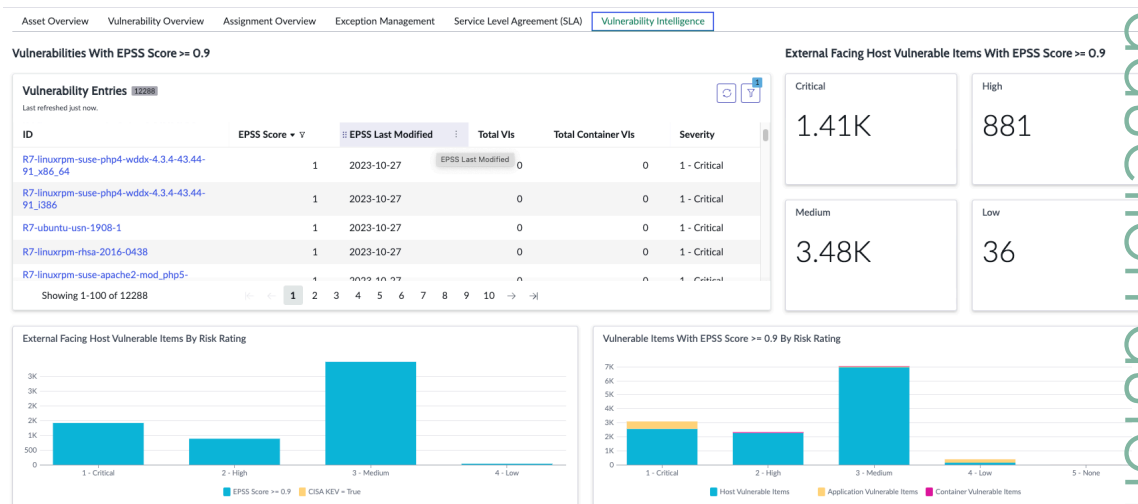
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

qui sont ouvertes sur Internet et qui disposent d'exploits disponibles.



L'onglet Renseignements sur les **vulnérabilités** fournit un état sur les scores EPSS atteints par les vulnérabilités ayant le marqueur CISA KEV vrai et un score EPSS > = 0,9 pour les éléments vulnérables d'application, d'hôte et de conteneur.



Filtres

Vous pouvez filtrer les widgets en fonction des éléments suivants :

- Unité business
- Groupe d'affectation
- Cote de risque
- État critiques des actifs
- Accessible sur Internet
- Existence de l'exploit

Lorsqu'un filtre est sélectionné, les données de tous les widgets sont mises à jour. Toutefois, si un filtre n'est pas applicable pour un widget, un symbole en forme de croix s'affiche à côté du nom du filtre.

Remarque : Seuls les filtres Unité business et Groupe d'affectation sont disponibles dans Tokyo. Tous les filtres sont disponibles à partir de maintenant Utah .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indicateurs

Actifs analysés

Indicateur de formule pour les actifs analysés au cours des 60 derniers jours. Contient les actifs d'éléments détectés analysés, les actifs de version d'application analysés, les actifs d'images de conteneurs détectés analysés en tant qu'indicateurs de contribution.

Actifs : l'exploit existe

Indicateur de formule pour les actifs où un exploit existe dans les vulnérabilités. Contient les actifs de l'hôte - l'exploit existe, les actifs de l'application - l'exploit existe, les actifs du conteneur - l'exploit existe en tant qu'indicateurs de contribution.

Actif Infra : accessible sur Internet

Indicateur pour extraire le nombre d'actifs, qui sont accessibles sur Internet.

Éléments détectés basés sur le type de ressources dans le cloud

Indicateur pour l'extraction du nombre d'actifs ayant une catégorie d'actifs telle que le cloud.

Images de base

Indicateur pour l'extraction du nombre d'images de base.

Type d'actif CISA KEV

Indicateur de formule, qui donne le nombre d'éléments vulnérables de conteneurs et d'hôtes pour lesquels la vulnérabilité a le marqueur CISA KEV (BOD 22-01) défini sur vrai. Contient le CVR existant CISA et les éléments vulnérables existants CISA en tant qu'indicateurs de contribution.

Éléments vulnérables existants CISA : non affectés

Indicateur de formule, qui donne le nombre d'éléments vulnérables de conteneurs et d'hôtes pour lesquels le marqueur CISA KEV (BOD 22-01) est défini sur vrai et pour lesquels les éléments vulnérables ne sont pas affectés. Contient des éléments vulnérables du conteneur non affectés et des éléments vulnérables de l'hôte non affectés comme indicateurs de contribution.

Éléments vulnérables existants CISA : cible manquée

Indicateur de formule, qui donne le nombre d'éléments vulnérables de conteneurs et d'hôtes pour lesquels le marqueur CISA KEV (BOD 22-01) est défini sur vrai et pour lesquels les éléments vulnérables ont manqué la cible. Contient les éléments vulnérables existants CISA, CVR existe CISA en tant qu'indicateurs de contribution.

VIT d'hôtes actifs

Nombre d'éléments vulnérables de l'hôte actifs (VIT).

VIT d'application actifs

Nombre d'éléments vulnérables de l'application (AVIT) actifs.

VIT de conteneurs actifs

Nombre d'éléments vulnérables actifs du conteneur (CVIT).

Nouveaux VIT

Nombre de VIT qui ont ouvert un jour.

Nouveaux AVIT

Nombre d'AVIT qui ont ouvert un jour.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nouveaux CVIT

Nombre de CVIT qui se sont ouverts au cours d'une journée.

Nouveaux résultats des tests

Nombre de résultats des tests (TR) qui ont été créés sur une journée.

AVIT fermés

Nombre de VIT fermés sur une journée.

VIT fermés

Nombre d'AVIT fermés sur une journée.

CVIT fermés

Nombre de CVIT clôturés sur une journée.

Résultats des tests fermés

Nombre de TR fermés sur une journée.

Problèmes de configuration ouverts : résultats des tests

Nombre de tous les résultats des tests ouverts, qui sont à l'état d'échec.

Score de risque de l'organisation

Score de risque d'une organisation à partir de la table Déployer le score de risque de l'application.

Élément vulnérable de l'application non affecté

AVIT sans groupe d'affectation ni affecté à.

Élément de vulnérabilité de l'hôte non affecté

VIT sans groupe d'affectation ni affecté à.

Éléments vulnérables du conteneur non affectés

CVIT sans groupe d'affectation ni affecté à.

Problèmes de configuration non affectés

TR sans groupe d'affectation ou affecté à.

VIT différés

VIT à l'état différé.

AVIT différés

AVIT à l'état différé.

CVIT différés

CVIT à l'état différé.

SLA hôte : fermé

Âge moyen des VIT fermés.

SLA de l'application : fermé

Âge moyen des AVIT fermés.

SLA de conteneur : fermé

Âge moyen des CVIT fermés.

SLA de résultat de test : réussi

Âge moyen clôturé des TR réussis.

SLA de l'hôte : fermé (critique et élevé)

Âge moyen des VIT fermés critiques et élevés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

SLA de l'application : fermé (critique et élevé)

Âge moyen clôturé des AVIT critiques et élevés.

SLA de conteneur : fermé (critique et élevé)

Âge moyen des CVIT critiques et élevés fermés.

SLA de résultat de test : réussi (critique et élevé)

Âge moyen de fermeture des TR critiques et élevés réussis.

Regrouper MTTR

Âge moyen des VIT, AVIT, CVIT et TR fermés.

SLA manqué

Âge moyen des VIT, AVIT, CVIT et TR fermés et ciblés manqués.

Vulnérabilités avec des scores EPSS >= 0,9

Nombre d'entrées de vulnérabilité avec des scores EPSS supérieurs ou égaux à 0,9.

Répartitions

- Type de VIT (unifié)
- Accessible sur Internet (unifié)
- Évaluation du risque (unifiée)
- L'exploit existe (unifié)
- Types de ressources dans le cloud de l'élément détectés (unifié)
- CISA existe (unifié)
- Classe CMDB (unifiée)
- Unité business (unifiée)
- Criticité opérationnelle (unifié)
- Raison de l'ajournement (unifiée)
- Groupe d'affectation (unifié)
- État du rattrapage (unifié)

Visualisations des données

Onglet Vue d'ensemble de l'actif

Titre	Type	Description
Vue d'ensemble de la surface d'attaque	Score unique 	Nombre représentant le score agrégé de sécurité d'une organisation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

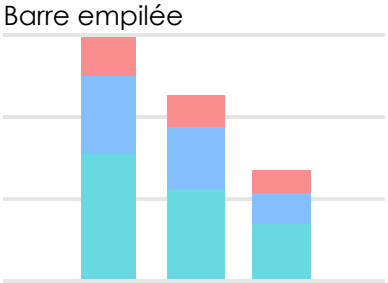
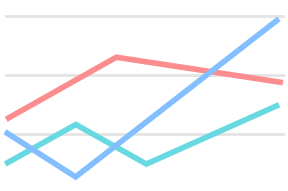
Onglet Vue d'ensemble de l'actif (suite)

Titre	Type	Description
Nombre CI CMDB	Score unique 	Nombre de CI de l'organisation qui sont enregistrés et suivis dans le Base de données de gestion des configurations (CMDB). Fournit une répartition des CI suivants : • CI analysés : nombre de CI analysés • Exploit : nombre d'exploits disponibles • Accessible sur Internet : nombre de CI accessibles sur Internet
Ressource du cloud	Score unique 	Nombre de CI avec une catégorie d'actif telle que le cloud. Fournit une répartition des actifs dans le cloud suivants : • AWS • Azure • GCP
Image de Docker	Score unique 	Nombre d'images Docker, y compris le nombre d'images de base.
Applications	Score unique 	Nombre d'applications dans l'organisation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

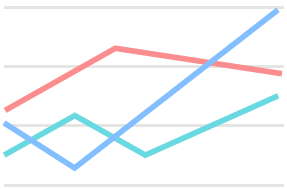
Onglet Vue d'ensemble de la vulnérabilité

Titre	Type	Description
KEV CISA	Graphique circulaire	Nombre de vulnérabilités associées au catalogue et au CISA marqueur CISA comme vrai. Fournit une répartition basée sur les éléments suivants : • Vulnérabilité CISA : types de vulnérabilités avec le marqueur CISA comme vrai • CI hôtes : accessible sur Internet : CI accessibles sur Internet • VIT non affectés : VIT non affectés avec le marqueur CISA comme vrai • Cible VIT manquée : VIT qui ont manqué la cible avec le marqueur CISA comme vrai
Vulnérabilités actives par criticité	Barre empilée 	Nombre de VIT, AVIT et CVIT actifs en fonction de la criticité.
Tendance de création et de fermeture de vulnérabilité	Ligne multiple 	Nombre de vulnérabilités nouvelles et fermées pour toutes les applications. Fournit une tendance pour les trois derniers mois.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

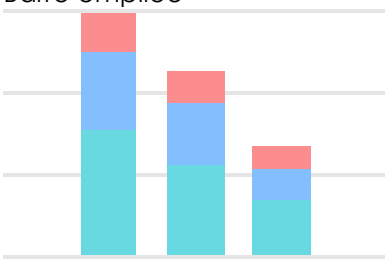
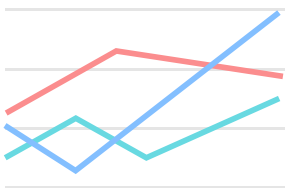
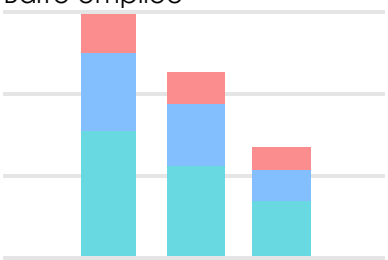
Onglet Vue d'ensemble de la vulnérabilité (suite)

Titre	Type	Description
Mauvaise configuration par plateforme cloud	Ligne multiple 	Nombre de problèmes de configuration basés sur la cote de risque pour chaque actif dans le cloud.
Conformité du cloud	Table	Liste des ressources dont la catégorie d'actif est Cloud avec les détails suivants : • Nom de la ressource • Classe • Problèmes de vulnérabilité : nombre de problèmes présents dans la ressource qui sont agrégés en fonction de l'évaluation du risque. • Problèmes de configuration : nombre de ressources présentant des problèmes de configuration ainsi que la cote de risque. • Compte dans le cloud : ID de compte dans le cloud. • Région du cloud : emplacement des ressources dans le cloud. • Fournisseur dans le cloud : nom du fournisseur dans le cloud.

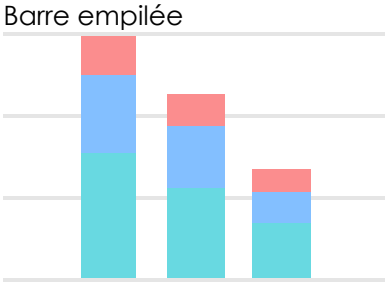
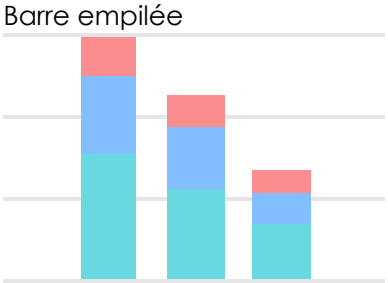
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble de l'affectation

Titre	Type	Description
VIT non attribués	Barre empilée 	Nombre de vulnérabilités qui ne sont affectées à aucun groupe ou individu, ainsi que la cote de risque.
MTTR par groupe d'affectation - 10 premiers	Ligne multiple 	Temps moyen nécessaire à un groupe d'affectation pour identifier et corriger les vulnérabilités ou les problèmes de sécurité. Les 10 premiers groupes d'affectation qui ont le délai moyen de rattrapage le plus élevé sont affichés.
10 principaux groupes d'affectation sans SLA (critique et vulnérabilité élevée)	Barre empilée 	10 principaux groupes d'affectation n'ayant pas respecté la date cible de rattrapage des vulnérabilités critiques et élevées.

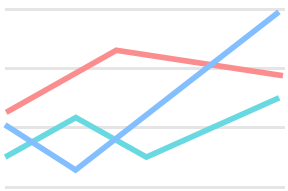
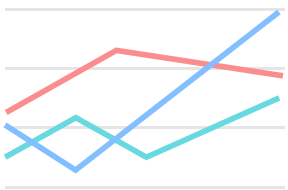
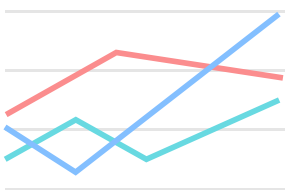
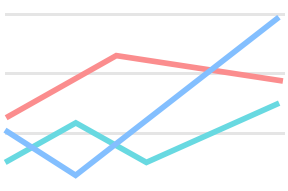
Onglet Gestion des exceptions

Titre	Type	Description
VIT différés	Barre empilée 	Nombre de vulnérabilités à l'état différé, basé sur l'évaluation du risque.
VIT critiques et différés élevés par groupe d'affectation	Barre empilée 	Nombre de vulnérabilités avec des cotes de risque critique et élevé à l'état Différé, classé en fonction des groupes d'affectation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

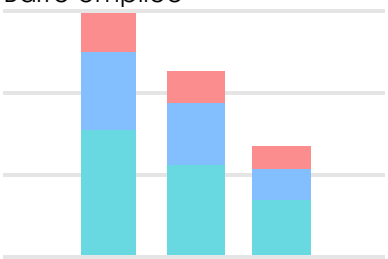
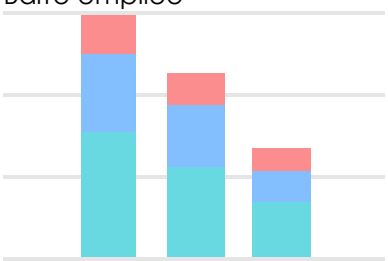
Onglet Accord sur les niveaux de service (SLA)

Titre	Type	Description
Vulnérabilité de l'hôte : exécution de SLA par groupe d'affectation	Ligne multiple 	Temps nécessaire par un groupe d'affectation pour corriger les vulnérabilités de l'hôte. Fournit une tendance pour les 10 derniers mois.
Problèmes de conformité : exécution de SLA par groupe d'affectation	Ligne multiple 	Temps nécessaire par un groupe d'affectation pour corriger les problèmes de conformité. Fournit une tendance pour les 10 derniers mois.
Vulnérabilité de l'application : exécution de SLA par groupe d'affectation	Ligne multiple 	Temps nécessaire par un groupe d'affectation pour corriger les vulnérabilités d'une application. Fournit une tendance pour les 10 derniers mois.
Vulnérabilité de conteneur : exécution de SLA par groupe d'affectation	Ligne multiple 	Temps nécessaire par un groupe d'affectation pour corriger les vulnérabilités d'un conteneur. Fournit une tendance pour les 10 derniers mois.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble de l'exclusion

Titre	Type	Description
Règles d'exclusion	Table	Liste de toutes les règles d'exclusion que vous avez créées.
Règles d'exclusion par rapport à Internet	Barre empilée 	Règles d'exclusion ayant un impact sur les détections qui appartiennent aux actifs accessibles sur Internet.
Règles d'exclusion par rapport à un exploit existant	Barre empilée 	Règles d'exclusion ayant un impact sur les détections vulnérables aux exploits existants.

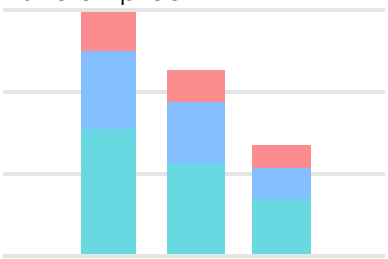
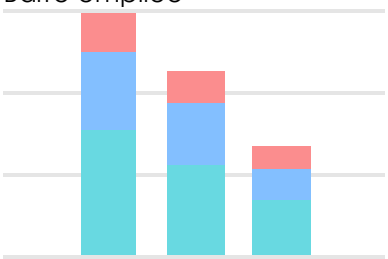
Onglet Renseignements sur les vulnérabilités

Titre	Type	Description
Vulnérabilités avec un score EPSS>= 0,9	Table	Vue de liste complète de toutes les entrées vulnérables (CVE ou TPE) dont le score EPSS est supérieur ou égal à 0,9, ainsi que les détails suivants. • ID : ID CVE de la vulnérabilité • Score de l'EPSS • Dernière modification de l'EPSS • CISA KEV BOD 22-01 : indique si l'entrée existe dans la CISA KEV BOD (Binding Operational Directive 22-01) • Total des VI : nombre total de VI qui existent pour cette entrée de vulnérabilité. • Total des VI de conteneurs : nombre total de VI de conteneurs qui

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Renseignements sur les vulnérabilités (suite)

Titre	Type	Description
		existent pour cette entrée de vulnérabilité. • Sévérité
Éléments vulnérables d'hôte externes avec un score EPSS >= 0,9	Score unique 	Nombre indiquant le nombre agrégé d'éléments vulnérables de l'hôte orientés vers l'extérieur avec un score EPSS supérieur ou égal à 0,9. Fournit des scores uniques triés par gravité de la cote de risque.
Éléments vulnérables de l'hôte orientés vers l'extérieur, par niveau de risque	Barre empilée 	Nombre d'éléments vulnérables de l'hôte orientés vers l'extérieur, par cote de risque. Les barres de pile sont classées par score EPSS > = 0,9 et CISA KEV = vrai.
Éléments vulnérables avec un score EPSS >= 0,9 par niveau de risque	Barre empilée 	Nombre de vulnérabilités avec un score EPSS supérieur ou égal à 0,9, triées par cote de risque. Fournit une répartition par éléments vulnérables d'hôte, éléments vulnérables d'application et éléments vulnérables de conteneur.

Travaux planifiés pour la collecte de données

Travaux de collecte de données permet de collecter automatiquement les scores d'indicateurs et de répartitions automatisés. Les travaux planifiés suivants sont exécutés pour collecter automatiquement les scores sur de nouvelles données.

Avertissement : Par défaut, les travaux de collecte de données suivants sont désactivés dans le système de base :

- Collecte de données quotidienne du tableau de bord unifié
- Collecte de données hebdomadaire du tableau de bord unifié
- Collecte de données historiques du tableau de bord unifié

Avant d'activer les tâches, consultez la base de connaissances .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Fréquence	Description
Collecte de données historiques du tableau de bord unifié	Une fois	Collecte les scores et les instantanés des enregistrements existants.
Collecte de données hebdomadaire du tableau de bord unifié	Hebdomadaire	Collecte des données chaque semaine.
Collecte de données quotidienne du tableau de bord unifié	Quotidien	Collecte des données tous les jours.
Déployer les scores de risque vers l'organisation	Quotidien	Collecte le score de risque agrégé pour une organisation.
Renseigner les nombres quotidiens de conformité du cloud	Quotidien	Collecte les données pour la conformité du cloud.
Tâche quotidienne de l'EPSS	Quotidien	Collecte les données de l'EPSS à partir de First.org.

Une nouvelle table Déployer le score des risques de l'application [sn_vul_cmn_rollup_app_risk_score] est créée dans le champ d'application commun de vulnérabilité. Cette table est renseignée à l'aide des calculateurs de déploiement suivants via les travaux planifiés tous les jours.

Nom du calculateur de déploiement	Description
Déploiement du score de risque de l'organisation	Cumule les scores de risque pour tous les éléments vulnérables et les problèmes de configuration dans une organisation. Il fournit un score de risque global pour une organisation.
Déploiement de l'élément vulnérable	Cumule les scores de risque pour tous les éléments vulnérables dans une organisation afin de contribuer au score de risque global d'une organisation.
Déploiement de l'élément vulnérable d'application	Cumule les scores de risque pour tous les éléments vulnérables de l'application dans une organisation afin de contribuer au score de risque global d'une organisation.
Déploiement de l'élément vulnérable de conteneur	Cumule les scores de risque pour tous les éléments vulnérables du conteneur dans une organisation afin de contribuer au score de risque global d'une organisation.
Déploiement du résultat de test	Cumule les scores de risque de tous les résultats de test d'une organisation afin de contribuer au score de risque global d'une organisation.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom du calculateur de déploiement	Description
Cumul des scores de l'EPSS des NVD aux TPE	Cumule les scores de l'EPSS des NVD aux TPE, afin de contribuer au score de risque global d'une organisation.

La surveillance et la gestion des éléments vulnérables et des résultats des tests dans le Espace de travail du gestionnaire de vulnérabilités

Le Espace de travail du gestionnaire de vulnérabilités vous permet de surveiller les éléments vulnérables (VIT, AVIT ET CVIT) et les résultats des tests à l'aide de rubriques de visualisation, et de suivre et gérer leur progression de rattrapage en créant des efforts de rattrapage.

Créez et appliquez des filtres pour visualiser le résumé des enregistrements actifs

En tant que gestionnaire et analyste des vulnérabilités, vous pouvez filtrer les enregistrements pour visualiser leur résumé dans le Espace de travail du gestionnaire de vulnérabilitésfichier .

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Page d'accueil**.
2. Sur la page d'accueil, sélectionnez dans l'un des onglets Vulnérabilités d'hôte, Vulnérabilités de conteneurs, Vulnérabilités d'applications ou Résultats des tests de configuration.
3. Renseignez les champs du modal Filtres enregistrés.

Modal Filtres enregistrés

Champ	Description
Nom du filtre	Nom du filtre
Conditions	Condition permettant de pré-répertorier les enregistrements pour lesquels vous souhaitez afficher les visualisations.

4. Sélectionnez **Enregistrer**.
   Le filtre créé s'affiche dans la liste déroulante **Afficher par** .
5. Sélectionnez le filtre créé dans le champ **Afficher par** pour afficher les visualisations des enregistrements filtrés.
   Pour plus d'informations sur les widgets, consultez Vue d'ensemble de la page d'accueil.
6. Pour mettre à jour ou supprimer un filtre :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Sélectionnez l'icône Engrenage icône .

b. Dans le formulaire Filtres enregistrés, sélectionnez **Utiliser les filtres existants** et renseignez les champs, puis sélectionnez **Mettre à jour**.

Formulaire Filtres enregistrés

Champ	Description
Sélectionner un filtre	Liste des filtres existants.
Nom du filtre	Nom descriptif du filtre.
Conditions	Les conditions du filtre existant. Modifiez la condition pour un nouvel ensemble d'enregistrements.

c. Pour supprimer un filtre, sélectionnez **Supprimer**.

Utiliser des rubriques de visualisation dans Espace de travail du gestionnaire de vulnérabilités

Utilisez les rubriques de surveillance dans pour Espace de travail du gestionnaire de vulnérabilités afficher les vulnérabilités filtrées à partir de vos données importées à partir des critères que vous définissez. Utilisez ces informations pour déterminer comment les vulnérabilités de chaque rubrique de surveillance peuvent impacter votre environnement.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Dans les rubriques de visualisation, vous pouvez effectuer les tâches suivantes :

- Surveillez le nombre d'efforts de rattrapage et d'enregistrements d'éléments vulnérables pour suivre la progression de votre rattrapage de vulnérabilité.
- Modifiez ou supprimez vos rubriques de surveillance existantes et créez des rubriques.
- Créez les efforts de rattrapage et transférez automatiquement les tâches de rattrapage à vos équipes informatiques uniquement pour les vulnérabilités que vous souhaitez corriger.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

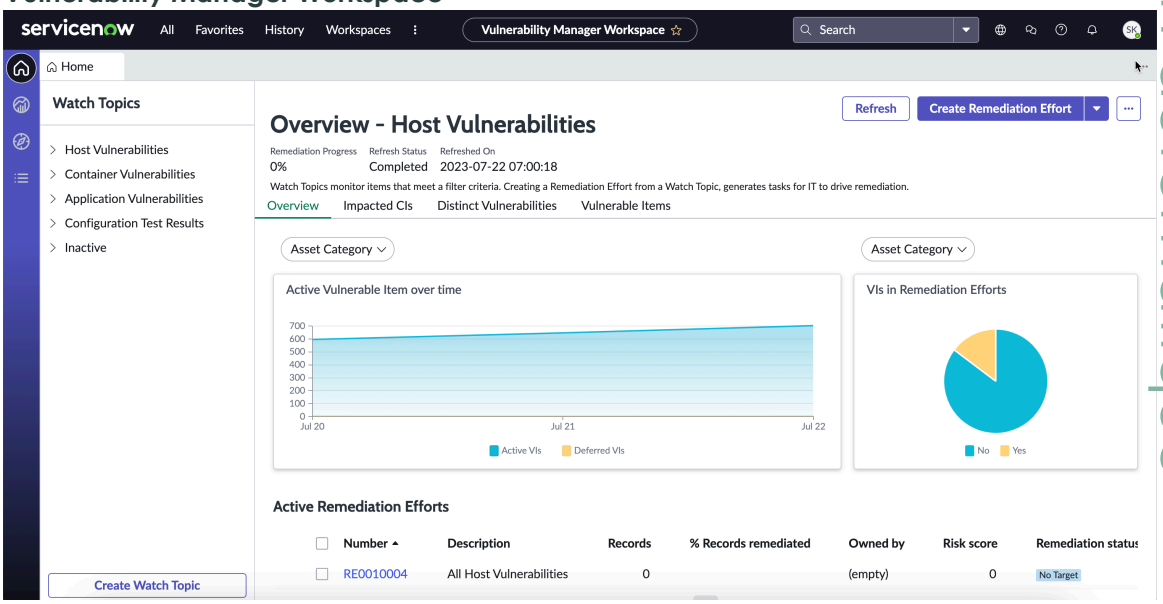
Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sélectionnez une rubrique de visualisation.

   Lorsque vous sélectionnez une rubrique de visualisation, l'onglet **Vue d'ensemble** s'affiche par défaut.

   Pour plus d'informations sur les rubriques de surveillance, reportez-vous à la section Vue d'ensemble des rubriques de surveillance.

   ### Onglet Vue d'ensemble de la version 19.0 sur la page d'accueil de Vulnerability Manager Workspace

   Les tableaux de bord sont dynamiques et les nouvelles données de vulnérabilité sont mises à jour lors de l'importation.

3. Sélectionnez un **onglet Éléments connexes** pour afficher plus de données.

   Pour les mises à jour de la liste des éléments connexes et des visualisations dans une rubrique de surveillance à partir de la version 18.0, reportez-vous à Liste d'éléments connexes et visualisations dans une rubrique de surveillance.

4. Effectuez les actions d'interface utilisateur sur la page Rubriques de visualisation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
Créer une rubrique de surveillance	Créez votre propre rubrique de surveillance en utilisant votre propre ensemble de conditions pour les vulnérabilités qui vous semblent importantes. Pour en savoir plus sur la création d'une rubrique de visualisation, reportez-vous à la section Créer une rubrique de surveillance dans Vulnerability Manager Workspace.
Modifier ou supprimer une rubrique de surveillance existante	Pour en savoir plus sur la modification ou la suppression d'une rubrique de visualisation, reportez-vous à la section Modifier ou supprimer une rubrique de surveillance.
Désactiver ou activer une rubrique de surveillance	À partir de la version 18.0, vous pouvez désactiver ou activer une rubrique de visionnage. Pour plus d'informations sur la désactivation ou l'activation d'une rubrique de visionnage, consultez la sectionDésactiver ou activer une rubrique de surveillance .
Actualiser une rubrique de surveillance	À partir de la version 18.0, vous pouvez obtenir les détails les plus récents d'une rubrique de surveillance en cliquant sur le bouton **Actualiser** . Le dernier état d'actualisation et le dernier horodatage sont affichés sous le nom de la rubrique de surveillance. ◦ Une rubrique de surveillance est actualisée automatiquement lorsqu'elle est créée ou mise à jour. ◦ Lorsque vous actualisez une rubrique de visualisation, tous les détails de la rubrique de visualisation, y compris les graphiques et les efforts de rattrapage, sont mis à jour. **Remarque :** Étant donné que vous ne pouvez pas actualiser une rubrique de visualisation inactive, le bouton **Actualiser** est inactif pour une rubrique de visualisation inactive.
Créer un effort de rattrapage	◦ Créez un effort de rattrapage. Un effort de rattrapage contient les tâches de rattrapage qui sont affectées à vos équipes informatiques. Vous pouvez utiliser cet outil pour piloter et suivre la progression du rattrapage, de l'affectation à la résolution. ◦ Lorsque vous créez un effort de rattrapage, tous les éléments vulnérables actifs sont automatiquement extraits s'ils ne

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
	font pas déjà partie d'un effort de rattrapage existant pour cette rubrique de surveillance. ◦ Les tâches de rattrapage sont affectées automatiquement aux équipes informatiques en fonction du groupe d'affectation de VI. ◦ Un exemple d'effort de rattrapage à partir de la rubrique de surveillance Vulnérabilités sur les serveurs Windows pourrait être Vulnérabilités sur les serveurs Windows au deuxième trimestre 2021. Les tâches de rattrapage de cet effort sont ensuite affectées aux groupes d'affectation répertoriés dans les enregistrements associés.
Créer un effort récurrent	Créez des efforts de rattrapage récurrents selon un calendrier qui vous aide à suivre les vulnérabilités susceptibles de nécessiter votre attention immédiate et continue. Pour en savoir plus sur la création d'efforts récurrents, reportez-vous à la section Créer un effort de rattrapage récurrent dans les espaces de travail Vulnerability Response. **Remarque :** À partir de la version 18.0, vous ne pouvez pas créer d'effort récurrent pour une rubrique de surveillance inactive.
Affiner les filtres d'une colonne d'une liste	Passez la souris sur le titre d'une colonne et cliquez sur le menu à trois points verticaux pour définir les filtres de cette colonne. Par exemple, supposons que vous souhaitiez filtrer davantage vos éléments de configuration associés aux enregistrements. Vous pouvez sélectionner la colonne Élément de configuration pour afficher les conditions de filtre disponibles. Vous pouvez définir des conditions pour filtrer vos ressources afin de ne voir que les ressources qui contiennent des données PCI.
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Filtrez les éléments ou faites correspondre les éléments d'une ligne dans une colonne. Par exemple, supposons que vous souhaitiez afficher uniquement les enregistrements qui présentent une vulnérabilité spécifique. Avec l'onglet de liste d'éléments connexes des éléments vulnérables sélectionné, dans la liste des enregistrements, sélectionnez la ligne d'un enregistrement dans la colonne Résumé. Sélectionnez le menu à trois points

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
	verticaux qui s'affiche et sélectionnez l'une des options suivantes : ◦ **Afficher les éléments correspondants** : affiche tous les autres enregistrements qui présentent cette vulnérabilité. ◦ **Filtrer :** affiche tous les enregistrements qui ne présentent pas cette vulnérabilité.

5. Facultatif : Sélectionnez un enregistrement pour afficher plus de détails.

Créer une rubrique de surveillance dans Vulnerability Manager Workspace

Les gestionnaires et analystes de vulnérabilités peuvent créer des rubriques de surveillance à l'aide d'un ensemble de conditions pour filtrer les sous-ensembles d'éléments vulnérables qu'ils souhaitent surveiller.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Dans l'onglet Vue d'ensemble des rubriques de surveillance, un rapport de tendance mis à jour tous les soirs, ainsi que d'autres rapports, montrent l'état actuel des enregistrements de cette rubrique de surveillance.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
   La page d'accueil (de destination) s'affiche avec les rubriques de surveillance actuelles.
2. Facultatif : Vous pouvez également cliquer sur les trois points à droite du bouton Créer un effort de rattrapage, puis sur Modifier pour modifier une rubrique de surveillance existante.

Remarque : Vous remarquerez peut-être un délai avant l'affichage des données actuelles pour une rubrique de surveillance après avoir modifié le filtrage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. En bas à gauche de la page, cliquez sur **Créer une rubrique de visualisation**.
4. Renseignez les champs du modal qui s'affiche.
   Pour plus d'informations sur les champs modaux Créer une rubrique de surveillance, consultezChamps du formulaire Créer une rubrique de surveillance .
5. À partir de la version 18.0, vous pouvez définir des conditions pour la catégorie d'enregistrement sélectionnée.

Option dans la liste déroulante Catégorie	Étapes
Vulnérabilités d'hôte	Dans la **condition d'élément vulnérable**, définissez des conditions pour identifier les vulnérabilités de l'hôte. Les vulnérabilités de l'hôte sont détectées en fonction des conditions définies.
Vulnérabilités d'applications	Dans la **condition d'élément vulnérable de l'application**, définissez des conditions pour identifier les vulnérabilités de l'hôte. Les vulnérabilités de l'application (ou AVIT) sont détectées en fonction des conditions définies.
Vulnérabilités du conteneur	Dans la **condition d'élément vulnérable de conteneur**, définissez des conditions pour identifier les vulnérabilités de l'hôte. Les vulnérabilités du conteneur (CVIT) sont détectées en fonction des conditions définies.
Résultats des tests de configuration	Dans la **condition des résultats des tests de configuration**, définissez des conditions pour identifier les problèmes de configuration. Les résultats des tests de configuration sont détectés en fonction des conditions définies.

Remarque : Si vous ne définissez aucune condition dans votre rubrique de suivi, aucune donnée n'est extraite du tableau de bord.

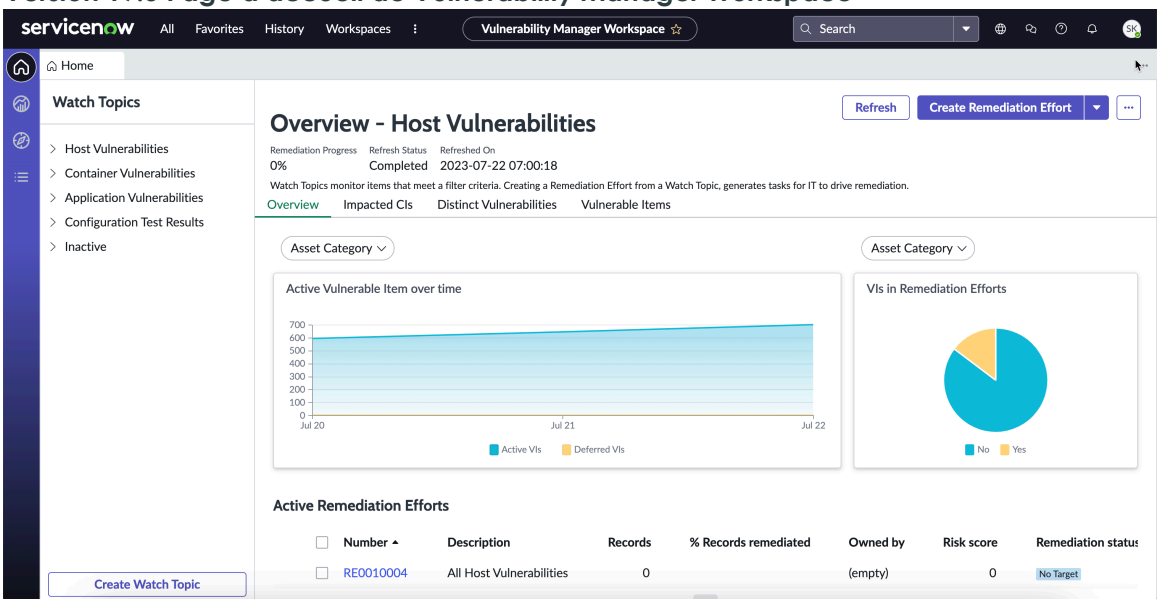
6. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Votre nouvelle rubrique de surveillance s'affiche sur la page de destination de l'accueil. À partir de la version 18.0, les rubriques de surveillance sont classées par type d'enregistrement dans le volet de navigation.

Version 19.0 Page d'accueil de Vulnerability Manager Workspace



Que faire ensuite

Créez un effort de rattrapage.

Modifier ou supprimer une rubrique de surveillance

En tant qu'administrateur ou analyste de vulnérabilités, vous pouvez modifier ou supprimer une rubrique de surveillance existante.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Si vous modifiez une rubrique de surveillance existante :

- Les données du tableau de bord sont mises à jour pour refléter vos changements.
- Les enregistrements qui font actuellement l'objet des efforts de rattrapage existants restent inchangés.
- Les enregistrements qui ne sont actuellement pas dans l'état Efforts de rattrapage s'affichent en fonction des critères que vous saisissez dans le générateur de conditions.

Si vous supprimez une rubrique de visualisation avant que tous ses enregistrements associés ne soient corrigés, les enregistrements qui s'affichent avec cette rubrique de surveillance ne sont pas affectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
   La page d'accueil (de destination) s'affiche avec les rubriques de surveillance actuelles.
2. Ouvrez la rubrique de surveillance que vous souhaitez modifier.
3. Cliquez sur les trois points, puis sur **Modifier**.

   Remarque : Vous ne pouvez pas modifier une rubrique de surveillance inactive.

4. Dans le modal Modifier la rubrique de surveillance, modifiez les champs.
5. Cliquez sur **Envoyer**.

   Remarque : Vous remarquerez peut-être un délai avant l'affichage des données actuelles pour une rubrique de surveillance après avoir modifié le filtrage.

   Vous pouvez également modifier les efforts de rattrapage récurrents existants. S'il existe un effort de rattrapage récurrent pour une rubrique de surveillance, **l'option Modifier l'effort récurrent** est disponible dans le menu. Sélectionnez cette option pour modifier l'effort récurrent.

   Les modifications que vous apportez et enregistrez dans l'enregistrement des efforts de rattrapage n'affectent pas les autres efforts de rattrapage que vous avez déjà créés à partir de la rubrique de surveillance.

6. Facultatif : Pour supprimer une rubrique de visualisation, sélectionnez le menu à trois points sur la rubrique de visualisation et sélectionnez **Supprimer**.

Désactiver ou activer une rubrique de surveillance

À partir de la version 18.0, vous pouvez désactiver ou activer une rubrique de visionnage.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

- Toutes les rubriques de surveillance inactives sont affichées dans le module **Inactif** du volet de navigation.
- Vous ne pouvez pas créer un effort de rattrapage ou un effort de rattrapage récurrent pour une rubrique de surveillance inactive.
- Vous ne pouvez pas actualiser une rubrique de surveillance inactive.
- Les détails d'une rubrique de surveillance inactive et de ses efforts de rattrapage associés ne sont pas mis à jour.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
   La page d'accueil (de destination) s'affiche avec les rubriques de surveillance actuelles.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Ouvrez la rubrique de surveillance que vous souhaitez désactiver.
3. Cliquez sur les trois points, puis sur **Désactiver**.
   La rubrique de surveillance apparaît dans le module Inactif.
4. Pour activer une rubrique de visualisation, sélectionnez-la dans le module Inactif, sélectionnez le menu à trois points et sélectionnez **Activer**.
   La rubrique de surveillance activée se déplace vers le module approprié dans le volet de navigation.

Utiliser les enregistrements d'efforts de rattrapage

Lorsque les gestionnaires et analystes de vulnérabilité créent des efforts de remédiation (ER), les tâches de remédiation (VUL) sont automatiquement affectées aux équipes informatiques pour la remédiation.

Avant de commencer

Vous devez créer un effort de rattrapage avant de pouvoir l'utiliser pour surveiller la progression du rattrapage sur les tâches de rattrapage.

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Procédure

1. Si ce n'est pas fait, cliquez sur l'icône Liste dans l'angle supérieur gauche.

   La vue de liste contenant les enregistrements d'efforts de rattrapage actifs s'affiche.
2. Sur la page de destination Vue de liste, avec les efforts de rattrapage actifs sélectionnés dans les listes filtrées, cliquez sur un enregistrement pour l'ouvrir.
   L'enregistrement s'affiche. Vous pouvez afficher les tâches et enregistrements de rattrapage associés à l'effort de rattrapage sélectionné.
3. Consultez la table suivante pour connaître les actions que vous pouvez effectuer sur l'enregistrement d'effort de rattrapage.

   Une fois l'enregistrement créé, les tâches de rattrapage et l'affichage d'un grand nombre d'enregistrements peuvent prendre quelques minutes.

Action d'interface utilisateur	Description
Ajouter une balise	À droite de l'en-tête, cliquez sur l'icône de petite balise. Vous pouvez ajouter du texte qui vous aidera davantage à identifier cet enregistrement. Par exemple, vous pouvez ajouter une balise indiquant que cet enregistrement contient des données PCI ou d'autres données critiques.
Ajouter une note de travail à l'enregistrement	Tout à droite de l'écran, cliquez sur l'icône **Activité** (icône d'allègement) et saisissez

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
	une note de travail. Cliquez sur l'icône pour basculer le panneau.
Mettre à jour l'enregistrement	Dans l'onglet **Détails** , pour tous les champs modifiables, cliquez sur un champ pour le sélectionner, apportez vos modifications, puis cliquez sur **Enregistrer** pour mettre à jour l'enregistrement.
Lorsqu'il est affiché, cliquez sur l'icône de filtre pour affiner les données sur la page affichée	Lorsque l'un des onglets Tâches de rattrapage, Éléments vulnérables ouRésultats des tests de configuration est sélectionné, à l'extrême droite, cliquez sur l'icône de filtre pour afficher les filtres qui s'appliquent à l'onglet. Dans le panneau qui s'affiche, cliquez sur **Vue avancée** pour ajouter ou modifier les conditions de filtre des éléments de la page. Cliquez sur **Mettre à jour** pour enregistrer vos modifications. Par exemple, dans l'onglet **Éléments vulnérables** , vous pouvez ajouter le champ Âge et saisir une plage pour afficher uniquement les enregistrements d'une période spécifique. Les enregistrements qui correspondent aux conditions que vous définissez sont affichés dans la liste.
Affiner les filtres pour les éléments d'une colonne	Sélectionnez une colonne, puis cliquez sur le menu à trois points verticaux, développez-la et entrez des conditions pour affiner et regrouper les données dans la colonne.
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Supposons, par exemple, que vous souhaitiez afficher uniquement les enregistrements qui présentent une vulnérabilité spécifique. Dans la liste des enregistrements, sélectionnez la ligne de l'enregistrement dans la colonne **Résumé** . Cliquez sur le menu à points vertical qui s'affiche et choisissez-en un : ◦ **Afficher la correspondance** : afficher tous les autres enregistrements qui présentent cette vulnérabilité. ◦ **Filtrer :** afficher tous les enregistrements qui n'ont pas cette vulnérabilité.

4. Dans les onglets Tâches de remédiation, Éléments vulnérables et Résultats des tests de configuration, vous pouvez explorer des enregistrements individuels de tâche de rattrapage (VUL), d'élément vulnérable (VIT) et de résultat de test (CTR).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Si vous souhaitez créer une tâche de rattrapage sur demande à partir d'un effort de rattrapage, reportez-vous à la section Créer une tâche de remédiation sur demande dans Vulnerability Manager Workspace. Vous pouvez également Créer une liste personnalisée des enregistrements vous aider à surveiller la progression du rattrapage.

Créer un effort de rattrapage dans Vulnerability Manager Workspace

Un enregistrement d'effort de rattrapage est une liste statique d'enregistrements que vous créez à partir d'une rubrique de surveillance dans l'espace de travail du gestionnaire de vulnérabilité.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Vous utilisez les efforts de rattrapage pour transférer les tâches utilisées par les équipes informatiques pour corriger les vulnérabilités. À partir de la version 16.1 :

- Vous pouvez modifier les efforts de rattrapage existants.
- Créez des efforts de rattrapage qui sont créés automatiquement aux dates et heures que vous définissez.
- Transférer des enregistrements des efforts de rattrapage existants vers un nouvel effort de rattrapage.

À partir de la version 18.0, comme vous ne pouvez pas créer d'effort de rattrapage pour une rubrique de visualisation inactive, le bouton **Créer un effort de rattrapage** est inactif.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page de destination (accueil), sélectionnez une rubrique de surveillance pour laquelle vous souhaitez créer un effort de rattrapage.
3. Pour afficher les enregistrements associés à la rubrique de surveillance sélectionnée, sous l'en-tête de l'enregistrement, cliquez sur **Éléments vulnérables** onglet.

   Les enregistrements s'affichent.

   Dans l'en-tête sous l'onglet Éléments vulnérables, vous pouvez afficher le nombre total d'enregistrements de cette rubrique de visualisation.

   Les colonnes et données suivantes s'affichent :

Colonnes de l'onglet Éléments vulnérables

Colonne	Description
Numéro	Numéro de l'enregistrement.
Résumé	Description de la vulnérabilité.
Élément de configuration	Actif associé à la vulnérabilité.
Cote de risque	Score de risque quantifié séparant les enregistrements en trois catégories : Critique, Élevé, Moyen, Faible et Aucun.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Description
État	État de l'enregistrement.
État du rattrapage	État du rattrapage pour un enregistrement.
Groupe d'affectation	Groupes d'affectation responsables du rattrapage. L'affectation des enregistrements aux groupes est basée sur les règles d'affectation que vous créez.
Effort de rattrapage	S'il est affecté à un effort de rattrapage, chaque enregistrement répertorie l'effort de rattrapage qui lui est affecté. Une fois ajouté à un effort de rattrapage, un enregistrement ne sera pas ajouté aux autres efforts de rattrapage que vous créez.
Groupe d'affectation	Groupes d'affectation responsables du rattrapage. L'affectation des enregistrements aux groupes est basée sur les règles d'affectation que vous créez.
Effort de rattrapage	S'il est affecté à un effort de rattrapage, chaque enregistrement répertorie l'effort de rattrapage qui lui est affecté. Une fois ajouté à un effort de rattrapage, un enregistrement ne sera pas ajouté aux autres efforts de rattrapage que vous créez.
Dans une tâche de rattrapage	Si `vrai`, cette valeur indique qu'un enregistrement est déjà dans une tâche de rattrapage. Les enregistrements peuvent faire partie de plusieurs tâches de rattrapage, mais un enregistrement ne peut être ajouté qu'à un seul effort de rattrapage.
Existence de l'exploit	Indique s'il existe un exploit connu pour un enregistrement.
Dernières ouvertures	Date à laquelle l'enregistrement a été ouvert pour la dernière fois dans votre Now Platform. Si l'enregistrement a été fermé puis rouvert, il s'agit de la dernière réouverture de l'enregistrement.

4. Pour créer un effort de rattrapage, cliquez sur **Créer un effort de rattrapage**.

   Lorsque vous créez un effort de rattrapage, les enregistrements déjà dans les efforts de rattrapage existants ne sont pas ajoutés aux nouveaux efforts de rattrapage que vous créez à partir de cette rubrique de surveillance.

   Au fur et à mesure que les enregistrements sont mis à jour ou que de nouveaux enregistrements sont créés dans les rubriques de visualisation, vous pouvez créer des efforts de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Vous pouvez Créer un effort de rattrapage récurrent dans les espaces de travail Vulnerability Responseégalement .

   Le bouton **Modifier** est disponible dans le menu pour les efforts de rattrapage existants. Vous pouvez modifier les champs et les conditions à partir d'un modal affiché. Les modifications que vous apportez et enregistrez dans l'enregistrement des efforts de rattrapage n'affectent pas les autres efforts de rattrapage que vous avez déjà créés à partir de la rubrique de visualisation.

6. À l'étape 1 du modal Créer un effort de rattrapage, renseignez les champs.

   Dans le champ Brève description, saisissez un texte qui décrit l'effort de rattrapage récurrent et vous aide à le localiser et à le suivre dans la liste des efforts.

   Dans le champ Description, saisissez plus de texte sur le contexte de l'effort pour vous aider à le localiser facilement dans la liste des efforts de rattrapage.

   À partir de la version 17.1, tout en créant un effort de rattrapage pour les rubriques de surveillance qui contiennent des vulnérabilités d'hôte, vous pouvez actualiser automatiquement les éléments vulnérables en double sur les tâches de rattrapage créées. Pour actualiser automatiquement les éléments vulnérables en double, vous devez cocher la case **Actualiser automatiquement les éléments vulnérables en double pour les tâches de rattrapage créées** .

   Remarque : À partir de la version 18.0, cette case à cocher apparaît à l'étape 2.

7. À l'étape 2, Génération de tâches, choisissez une méthode dans la liste pour regrouper les enregistrements dans les tâches de rattrapage que vous générez à partir de cet effort de rattrapage après sa création.

Option	Description
Par groupe d'affectation	Les enregistrements avec le même groupe d'affectation sont regroupés dans une seule tâche de rattrapage.
Par groupe d'affectation et élément de configuration	Les enregistrements ayant le même groupe d'affectation et le même élément de configuration sont regroupés dans une seule tâche de rattrapage.
Par groupe d'affectation et (vulnérabilité ou test de configuration)	Les enregistrements ayant le même groupe d'affectation et le même élément de configuration sont regroupés dans une seule tâche de rattrapage.
Aucune (aucune tâche de rattrapage n'est créée).	Utilisez cette méthode si vous souhaitez ajouter manuellement des enregistrements à une tâche de rattrapage pour cet effort. Consultez Créer une tâche de remédiation sur demande dans Vulnerability Manager Workspace. **Remarque :** À partir de la version 18.0, l'option **Aucun** n'est plus disponible.

Remarque : Pour la version 18.0, l'option **Aucun** n'est pas disponible.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

8. À l'étape 3, Transférer, vérifiez le nombre d'enregistrements que vous souhaitez ajouter à l'effort de rattrapage et voyez combien d'enregistrements sont disponibles pour le transfert à partir d'autres efforts de rattrapage actifs.

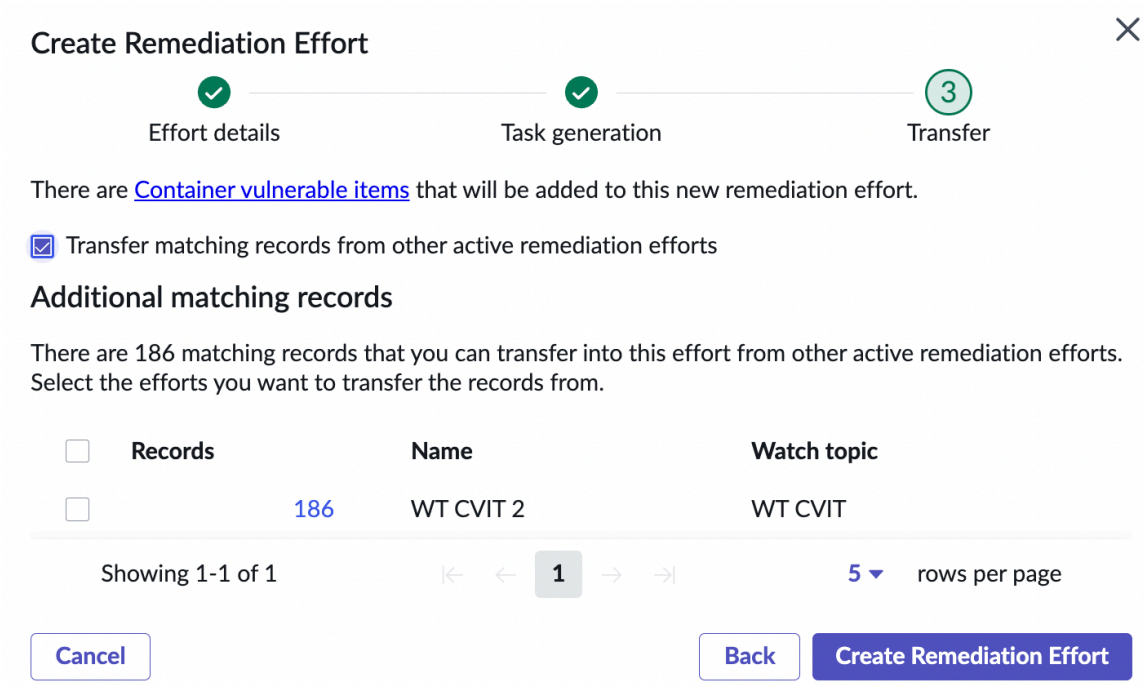
   S'il n'existe aucun nouvel enregistrement actif à ajouter, le texte suivant s'affiche :

   ```
   Il n'existe aucun enregistrement actif disponible à ajouter à ce nouvel effort de rattrapage.
   ```

   Tous les enregistrements supplémentaires disponibles pour le transfert vers cet effort sont répertoriés sous `Enregistrements correspondants supplémentaires` .

   À partir de la version 18.0, cochez la case **Transférer les enregistrements correspondants à partir d'autres efforts de rattrapage actifs** , puis cochez les cases des enregistrements que vous souhaitez transférer à partir d'autres efforts de rattrapage actifs.

   Version 18.0 Créer un effort de rattrapage

   Une fois que vous avez cliqué sur **Créer un effort de rattrapage**, le nouvel effort de rattrapage s'affiche quelques instants plus tard. Selon le nombre d'enregistrements, le remplissage du nouvel enregistrement peut prendre un certain temps. Un message indique si l'enregistrement est toujours en cours de remplissage.

   Le nouvel effort de rattrapage est créé avec tous les enregistrements disponibles à partir de la rubrique de surveillance utilisée pour le créer, en plus des enregistrements que vous avez sélectionnés pour le transfert à partir des efforts existants.

   Si vous sélectionnez les enregistrements à transférer à partir d'un effort existant, et que l'effort existant transfère tous ses enregistrements dans votre nouvel effort, l'effort de rattrapage à partir duquel vous avez déplacé les enregistrements est fermé. Pour en savoir plus sur la façon dont les tâches de rattrapage associées aux efforts de rattrapage sont impactées par le transfert d'enregistrements, reportez-vous à Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Vulnerability Response.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si aucun enregistrement n'est disponible à partir de la rubrique de surveillance ou s'il n'y a pas d'enregistrement sélectionné pour le transfert, le bouton **Créer un effort de rattrapage** est désactivé.

La *Populate Efforts* tâche planifiée s'exécute toutes les 10 minutes pour renseigner les données dans les widgets en fonction de la condition sélectionnée.

Cliquez sur l'onglet Progression du rattrapage pour afficher les progrès du rattrapage. Cliquez sur n'importe quel élément pour afficher les détails, notamment le type d'enregistrement, le score de risque, la cote de risque, le pourcentage d'enregistrements rattrapés, les enregistrements à l'état différé et non différé et le nombre total d'enregistrements, les conditions utilisées dans la rubrique de surveillance et l'état du rattrapage. Les informations sur l'état du rattrapage, telles que la cible et l'état du rattrapage, sont déployées à partir de la table Éléments vulnérables. Le score de risque d'enregistrement le plus élevé est déployé à partir de la table Calculateurs de vulnérabilité, tandis que le score de risque est déployé à partir de **Calculateurs de déploiement de vulnérabilité** > **Déploiement d'effort de correction**.

L'onglet Tâches de rattrapage affiche les tâches pour tous les types de problèmes. Les champs sont renseignés lorsque les travaux planifiés suivants s'exécutent. Ils sont exécutés automatiquement toutes les 15 minutes :

- Déployer les valeurs d'éléments vulnérables de l'application vers la vulnérabilité et le groupe.
- Déployer les valeurs d'éléments vulnérables de conteneur dans la vulnérabilité et le groupe.
- Cumulez les valeurs des résultats des tests vers le groupe de résultats de test et le test de configuration.
- Déployer les valeurs d'éléments vulnérables dans la vulnérabilité et le groupe.

Dans la vue Listes, vous pouvez afficher les efforts de rattrapage, les tâches de rattrapage, les éléments vulnérables, les résultats des tests de configuration, etc. Vous pouvez ouvrir une tâche de rattrapage ou un élément vulnérable et afficher la page Détails. Cliquez sur les ellipses More Actions (Actions supplémentaires), puis sur **Start Investigation (Démarrer l'examen**) pour résoudre une tâche de rattrapage.

9. Facultatif : Vous pouvez également modifier les efforts de rattrapage récurrents existants.

   (Optional) S'il existe un effort de rattrapage récurrent pour une rubrique de visualisation, **l'option Modifier l'effort récurrent** est disponible dans le menu en haut à droite d'une rubrique de visualisation. Choisissez cette option pour modifier l'effort récurrent.

   Les modifications que vous apportez et enregistrez dans l'enregistrement des efforts de rattrapage n'affectent pas les autres efforts de rattrapage que vous avez déjà créés à partir de la rubrique de visualisation.

Créer une tâche de remédiation sur demande dans Vulnerability Manager Workspace

Créez une tâche de rattrapage sur demande à partir d'un effort de rattrapage. Si vous créez une tâche de rattrapage à la demande, vous choisissez les enregistrements que vous souhaitez ajouter manuellement.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Pour la version 18.0 de Réponse aux vulnérabilités, vous ne pouvez pas créer une tâche de rattrapage à partir de la vue d'enregistrement d'un effort de rattrapage.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. En haut à gauche de l'espace de travail avec la page d'accueil affichée, cliquez sur l'icône **Vue de listes** pour afficher la page de destination Liste.
3. Sous Efforts de rattrapage, cliquez sur **Actif** ou **Tous**.
4. Dans la liste qui s'affiche, cliquez sur un enregistrement pour l'ouvrir.
   L'onglet Vue d'ensemble de l'enregistrement s'affiche.
5. Cliquez sur l'onglet **Éléments vulnérables** .
   La liste des enregistrements s'affiche.
6. Pour créer une tâche de rattrapage, dans la colonne Nombre, sélectionnez les enregistrements que vous souhaitez ajouter.
7. Cliquez sur **Créer une tâche de rattrapage**.
8. Renseignez les champs de la fenêtre modale qui s'affiche.

Champ	Description
Description brève	Saisissez un texte qui peut vous aider à identifier facilement ces tâches de rattrapage à partir de vos tâches de rattrapage existantes.
Groupe d'affectation	Choisissez un groupe d'affectation pour les tâches. Utilisez le filtre pour vous aider à localiser le groupe souhaité.

9. Cliquez sur **Créer**.
10. La nouvelle tâche de rattrapage s'affiche avec les enregistrements actifs que vous avez sélectionnés.

Créer un effort de rattrapage récurrent dans les espaces de travail Vulnerability Response

Vous pouvez créer et planifier des efforts de rattrapage récurrents qui sont générés automatiquement aux dates et heures que vous définissez.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez créer automatiquement des efforts de rattrapage récurrents selon un calendrier qui vous aide à suivre les vulnérabilités susceptibles de survenir et qui nécessitent une attention immédiate et continue.

À partir de la version 18.0, l'option **Créer un effort récurrent** est inactive, car vous ne pouvez pas créer d'effort de rattrapage récurrent pour une rubrique de surveillance inactive. Si vous désactivez une rubrique de visualisation pour laquelle un effort récurrent est déjà planifié, un nouvel effort de rattrapage n'est pas créé tant que la rubrique de surveillance

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

n'est pas activée. De plus, les détails **Récurrence de l'effort** et **Date de récurrence suivante** disparaissent en haut à droite. Une fois la rubrique de surveillance activée, un effort de rattrapage est créé au niveau du calendrier à venir.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page de destination (accueil), sélectionnez une rubrique de surveillance pour laquelle vous souhaitez créer un effort de rattrapage récurrent.

   Vous pouvez créer un effort de rattrapage récurrent par rubrique de surveillance.

   Remarque : Vous ne pouvez pas transférer les enregistrements d'efforts de rattrapage récurrents vers de nouveaux efforts de rattrapage. Toutefois, vous pouvez transférer des enregistrements d'efforts de rattrapage existants et non récurrents vers de nouveaux efforts de rattrapage. Pour plus d'informations sur le transfert d'enregistrements, reportez-vous à la rubrique Transférer des enregistrements aux efforts de rattrapage dans les Réponse aux vulnérabilités espaces de travail

3. Dans une rubrique de visualisation, en haut à droite de la liste Créer un effort de rattrapage, sélectionnez **Créer un effort récurrent**.

   Le modal Créer un effort récurrent s'affiche.

4. À l'étape 1, Détails de l'effort, renseignez les champs requis.

   Dans le champ Brève description, saisissez le texte qui décrit l'effort de rattrapage récurrent qui vous aide à le localiser et à le suivre à partir de la liste d'efforts.

   Dans le champ Description, saisissez plus de texte sur le contexte de l'effort pour vous aider à le localiser facilement dans la liste des efforts de rattrapage. Par exemple, `les vulnérabilités sur les actifs externes`.

   À partir de la version 17.1, tout en créant un effort de rattrapage pour les rubriques de surveillance qui contiennent des vulnérabilités d'hôte, vous pouvez actualiser automatiquement les éléments vulnérables en double sur les tâches de rattrapage créées. Pour actualiser automatiquement les éléments vulnérables en double, vous devez sélectionner l'option **Actualiser automatiquement les éléments vulnérables en double pour les tâches de rattrapage créées** .

   Remarque : À partir de la version 18.0, cette case à cocher apparaît à l'étape 2.

5. Cliquez sur **Suivant**.
   Les détails de la génération des tâches s'affichent.
6. À l'étape 2, Génération de tâches, choisissez une méthode dans la liste pour regrouper les éléments vulnérables dans les tâches de rattrapage que vous générez à partir de cet effort de rattrapage après sa création.
   - Par groupe d'affectation
   - Par groupe d'affectation et élément de configuration
   - Par groupe d'affectation et par vulnérabilité
   - Aucune (aucune tâche de rattrapage n'est créée). Utilisez cette méthode si vous souhaitez ajouter manuellement des enregistrements à une tâche de rattrapage pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

cet effort. Consultez Créer une tâche de remédiation sur demande dans Vulnerability Manager Workspace.

Remarque : Pour la version 18.0 de Réponse aux vulnérabilités, l'option **Aucun** n'est pas disponible.

7. Cliquez sur **Suivant** pour continuer.
8. À l'étape 3, Récurrence, sélectionnez la fréquence.

Option	Description
Par trimestre (tous les 3 mois)	Planifie l'effort de rattrapage une fois tous les trois mois. **Remarque :** Si le mois que vous sélectionnez n'a que 30 jours, l'effort de rattrapage est créé à cette dernière date du mois.
Mensuel	Planifie l'effort de rattrapage une fois par mois.
Hebdomadaire	Planifie l'effort de rattrapage une fois par semaine. **Remarque :** Cette option est disponible à partir de la version 19.0 de Réponse aux vulnérabilités.
Quotidien	Planifie l'effort de rattrapage tous les jours. **Remarque :** Cette option est disponible à partir de la version 19.0 de Réponse aux vulnérabilités.

a. Définissez le calendrier de récurrence.

Utilisez les listes pour sélectionner le mois/jour/heure/minute dans lequel vous souhaitez que l'effort de rattrapage soit créé. Le fuseau horaire pour la planification est par défaut votre fuseau horaire.

Remarque : Si vous rencontrez de nombreuses vulnérabilités, vous préférerez peut-être définir la création en dehors des heures de travail.

Si vous souhaitez que la tâche soit créée le dernier jour du mois, la tâche planifiée crée l'effort de rattrapage récurrent le dernier jour du mois. Un message s'affiche si le mois n'a pas 31 jours.

b. Facultatif : Sélectionnez **Transférer les vulnérabilités** vers les vulnérabilités actives dans cet effort de rattrapage pour les reporter à chaque effort de rattrapage ultérieur créé.

9. Cliquez sur **Planifier la récurrence**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un message indique que l'enregistrement de rattrapage récurrent a été créé. Le nouvel effort de rattrapage n'est pas affiché immédiatement, il est créé lorsque vous l'avez planifié. Il apparaît dans vos listes une fois qu'il est créé par la tâche planifiée.

La date de création de l'effort de rattrapage est indiquée dans la rubrique de surveillance correspondante. Pour en savoir plus sur l'impact du transfert d'enregistrements sur les tâches de rattrapage associées aux efforts de rattrapage, reportez-vous Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Vulnerability Responseà .

Transférer des enregistrements aux efforts de rattrapage dans les Réponse aux vulnérabilités espaces de travail

Vous pouvez transférer des enregistrements d'efforts de rattrapage existants vers de nouveaux efforts de rattrapage.

Avant de commencer

Si vous êtes confronté à une menace zero-day ou à une vulnérabilité très critique que vous souhaitez résoudre rapidement, vous pouvez consolider tous les enregistrements actifs que vous avez déjà pour cette vulnérabilité en un seul effort de correction. Toutefois, chaque enregistrement ne peut faire l'objet que d'un seul effort et les enregistrements peuvent se chevaucher entre les rubriques de surveillance. Ainsi, pour les rassembler tous, vous devez transférer ces enregistrements de plusieurs efforts existants en un seul effort de correction.

Supposons, par exemple, que vous ayez créé un effort de rattrapage qui comporte une vulnérabilité hautement prioritaire. Étant donné que cette vulnérabilité est répandue et qu'elle a potentiellement un impact sur d'autres zones de votre environnement, il se peut que des enregistrements déjà associés à cette vulnérabilité fassent déjà partie des efforts de rattrapage existants. Pour combiner ces enregistrements afin qu'ils soient tous réunis dans un seul effort de rattrapage, vous pouvez transférer tous les enregistrements des efforts de rattrapage existants vers un nouvel effort de rattrapage.

Remarque : Vous ne pouvez pas transférer les enregistrements d'efforts de rattrapage récurrents vers de nouveaux efforts de rattrapage. Pour plus d'informations, consultez Créer un effort de rattrapage récurrent dans les espaces de travail Vulnerability Response.

Rôle requis : sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page de destination (accueil), sélectionnez une rubrique de surveillance pour laquelle vous souhaitez créer un effort de rattrapage récurrent.
3. Cliquez sur **Créer un effort de rattrapage**.
   Le modal Créer un effort de rattrapage s'affiche.
4. À la première étape, Détails de l'effort, renseignez les champs requis.

   Dans le champ Brève description, saisissez un texte qui décrit l'effort de rattrapage récurrent qui vous aide à le localiser et à le suivre à partir de la liste d'efforts.

   Dans le champ Description, saisissez plus de texte sur le contexte de l'effort pour vous aider à le localiser facilement dans la liste des efforts de rattrapage. Par exemple, `Vulnérabilités Log4J actives`.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans le champ Nom, saisissez un nom pour votre nouvel effort de rattrapage. Par défaut, le nom de la rubrique de surveillance s'affiche.

b. Dans le champ Description, saisissez un texte qui vous aidera à localiser facilement cet effort de rattrapage dans la liste des efforts de rattrapage.

À partir de la version 17.1, tout en créant un effort de rattrapage pour les rubriques de surveillance qui contiennent des vulnérabilités d'hôte, vous pouvez actualiser automatiquement les éléments vulnérables en double sur les tâches de rattrapage créées. Pour actualiser automatiquement les éléments vulnérables en double, vous devez sélectionner l'option **Actualiser automatiquement les éléments vulnérables en double pour les tâches de rattrapage créées** .

Remarque : À partir de la version 18.0, cette case à cocher apparaît à l'étape 2.

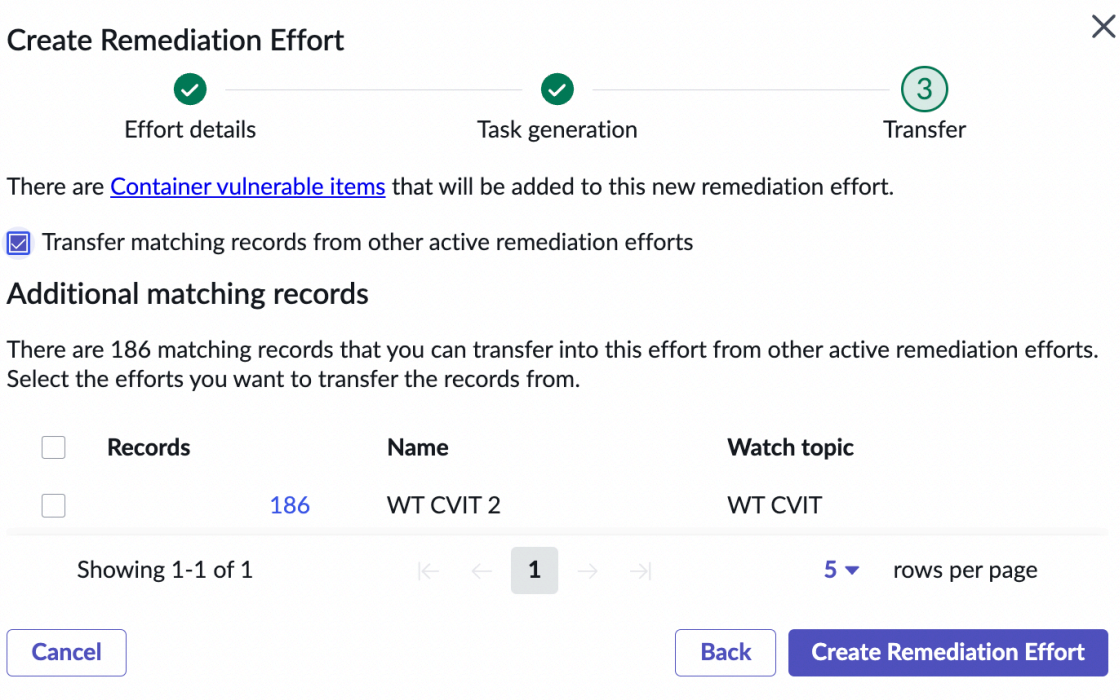
5. Cliquez sur **Suivant**.
   Les détails de la génération des tâches s'affichent.
6. À l'étape 2, Génération de tâches, choisissez une méthode dans la liste pour regrouper les enregistrements dans les tâches de rattrapage que vous générez à partir de cet effort de rattrapage après sa création.
   - Par groupe d'affectation
   - Par groupe d'affectation et élément de configuration
   - Par groupe d'affectation et par vulnérabilité
   - Aucune (aucune tâche de rattrapage n'est créée). Utilisez cette méthode si vous souhaitez ajouter manuellement des enregistrements à une tâche de rattrapage pour cet effort. Consultez Créer une tâche de remédiation sur demande dans Vulnerability Manager Workspace.

     Remarque : Pour la version 18.0, l'option **Aucun** n'est pas disponible.
7. Cliquez sur **Suivant**.
8. À l'étape 3, Transférer, vérifiez combien d'enregistrements seront ajoutés à l'effort de rattrapage et voyez combien d'enregistrements sont disponibles pour le transfert à partir d'autres efforts de rattrapage actifs.
9. Pour transférer des enregistrements d'autres efforts, à partir de la liste, cochez les cases en regard des enregistrements souhaités.

   À partir de la version 18.0, cochez la case **Transférer les enregistrements correspondants à partir d'autres efforts de rattrapage actifs** , puis cochez les cases en regard des enregistrements que vous souhaitez transférer à partir d'autres efforts de rattrapage actifs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Cliquez sur **Créer un effort de rattrapage**.

    Après quelques instants, le nouvel effort de rattrapage s'affiche. Selon le nombre d'enregistrements, cela peut prendre un certain temps. Un message indique que l'enregistrement est en cours de remplissage.

    Le nouvel effort de rattrapage est créé avec tous les enregistrements disponibles à partir de la rubrique de surveillance utilisée pour le créer, en plus des enregistrements que vous avez sélectionnés pour le transfert à partir des efforts existants.

    Si vous sélectionnez les enregistrements à transférer à partir d'un effort existant, et que l'effort existant transfère tous ses enregistrements dans votre nouvel effort, l'effort de rattrapage à partir duquel vous avez déplacé les enregistrements est fermé.

    Remarque : S'il n'y a pas d'enregistrements disponibles à partir de la rubrique de surveillance ni d'enregistrements sélectionnés pour le transfert, le bouton **Créer un effort de rattrapage** est désactivé.

    Pour plus d'informations sur la façon dont les tâches de rattrapage associées aux efforts de rattrapage sont impactées par le transfert d'enregistrements, voir Transfert d'enregistrements ou transfert d'enregistrements.

Ajouter un contrôle de compensation à la bibliothèque

En tant que gestionnaire ou analyste de vulnérabilité, ajoutez une liste de contrôles compensatoires à la bibliothèque de contrôles compensatoires dans l'espace de travail du gestionnaire de vulnérabilités, qui peuvent être appliquées pour la réduction du risque des éléments vulnérables et des tâches de rattrapage.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Certains contrôles de compensation couramment utilisés sont livrés avec le système de base. Vous pouvez afficher ces contrôles de compensation en accédant à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Listes** > **Bibliothèques** > **Contrôles de compensation**. Vous pouvez activer ou désactiver ces contrôles de compensation selon vos besoins.

Remarque : La fonctionnalité de contrôles de compensation n'est disponible que pour les vulnérabilités de l'hôte.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, sous **Bibliothèques, sélectionnez Contrôles de compensation**.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire Créer des contrôles de compensation.

Champs du formulaire Créer des contrôles de compensation

Champ	Description
Nom	Nom du contrôle de compensation, qui apparaît en tant qu'option dans la liste déroulante **Contrôles de compensation** du modal Demande d'exception.
Description	Informations brèves qui fournissent des détails sur le contrôle de compensation.
Actif	État du contrôle de compensation. Seuls les contrôles actifs apparaissent dans la liste **déroulante Contrôles de compensation** du modal Demande d'exception.

5. Sélectionnez **Enregistrer**.
6. Dans la liste Contrôles de compensation sous Bibliothèques, sélectionnez le contrôle de compensation souhaité et sélectionnez **Modifier**, activer ou désactiver un contrôle de compensation et cliquez sur **Enregistrer** pour modifier les contrôles de compensation. Tous les contrôles compensatoires actifs s'affichent sous forme d'option dans la liste déroulante **Contrôles compensatoires** du modal Demande d'exception pour les demandes de réduction des risques.

Que faire ensuite

À partir de la version 21.0 de Réponse aux vulnérabilités, vous pouvez associer des contrôles de compensation à des CVE ou des TPE après avoir ajouté un contrôle de compensation à la bibliothèque. Pour plus d'informations sur l'association de contrôles de compensation, reportez-vous à la section Associer les contrôles compensatoires aux CVE ou aux TPE pour les demandes de réduction des risques.

Information associée

Comprendre les contrôles compensatoires pour la réduction des risques

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Associer les contrôles compensatoires aux CVE ou aux TPE pour les demandes de réduction des risques

Impact des contrôles compensatoires sur le score de risque et la date d'expiration

Associer les contrôles compensatoires aux CVE ou aux TPE pour les demandes de réduction des risques

En tant que gestionnaire ou analyste des vulnérabilités, vous pouvez associer des contrôles compensatoires pertinents à une entrée de vulnérabilité commune (CVE) ou à une entrée tierce (TPE) dans l'espace de travail du gestionnaire de vulnérabilité, qui peuvent être utilisées pour réduire le risque posé par une vulnérabilité.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

- Si vous n'associez pas les contrôles compensatoires à un CVE ou un TPE, tous les contrôles actifs apparaissent dans le champ Sélectionner les contrôles compensatoires du formulaire Demande d'exception.
- Si vous associez un contrôle de compensation à un CVE, ce contrôle de compensation est automatiquement associé au TPE, qui est mappé au CVE.

Remarque : La fonctionnalité de contrôles de compensation n'est disponible que pour les vulnérabilités de l'hôte.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Listes, sous Bibliothèques, ouvrez l'un des éléments suivants pour lesquels vous souhaitez associer les contrôles :
   - **CVE** de la liste des CVE.
   - **TPE** de la liste des TPE.
3. Sélectionnez **Associer des contrôles**.

   Remarque : Le bouton **Associer des contrôles** n'apparaît que lorsque la réduction du risque est activée pour une CVE ou une TPE. En d'autres termes, vous ne pouvez associer des contrôles compensatoires que lorsque la réduction du risque est activée pour une CVE ou une TPE. Si le bouton **Associer des contrôles** n'est pas visible, sélectionnez **Activer la réduction du risque**.

4. Dans le modal Associer des contrôles, sélectionnez les contrôles compensatoires qui peuvent être appliqués aux vulnérabilités associées aux CVE ou TPE pour réduire les risques.
5. Sélectionnez **Soumettre**.
   - Les contrôles de compensation associés apparaissent dans l'onglet Contrôles de compensation applicables de la vue d'enregistrement des CVE et TPE.
   - Lorsqu'un propriétaire du rattrapage demande une réduction des risques, ces contrôles compensatoires associés apparaissent dans le champ Sélectionner les contrôles compensatoires du modal Demande d'exception.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

- Comprendre les contrôles compensatoires pour la réduction des risques
- Désactiver ou activer la réduction du risque pour une CVE ou une TPE
- Ajouter un contrôle de compensation à la bibliothèque
- Impact des contrôles compensatoires sur le score de risque et la date d'expiration

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

En tant que gestionnaire et analyste des vulnérabilités, vous pouvez désactiver ou activer les demandes de réduction des risques pour les vulnérabilités de l'hôte à partir d'une entrée de vulnérabilité commune (CVE) ou d'une entrée tierce (TPE) dans l'espace de travail du gestionnaire de vulnérabilité.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
La réduction du risque pour une CVE et un TPE est activée par défaut.

Remarque : La fonctionnalité de contrôles de compensation n'est disponible que pour les vulnérabilités de l'hôte.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
   Sur la page Listes, sous Bibliothèques, ouvrez l'un des éléments suivants pour lequel vous souhaitez désactiver les demandes de réduction du risque :
   - **CVE** de la liste des CVE.
   - **TPE** de la liste des TPE.
2. Sélectionnez **Désactiver la réduction du risque**.
   Le propriétaire de la correction ne peut pas demander de réduction du risque pour les éléments vulnérables de l'hôte associés à ces CVE ou TPE. En d'autres termes, la case à cocher Demande de réduction des risques n'apparaît pas lorsque le **motif** est sélectionné en tant que `contrôle d'atténuation en place` sur le modal Demande d'exception.
3. Pour activer les demandes de réduction du risque pour les éléments vulnérables de l'hôte, sélectionnez **Activer la réduction du risque**.

Information associée

- Comprendre les contrôles compensatoires pour la réduction des risques
- Ajouter un contrôle de compensation à la bibliothèque
- Associer les contrôles compensatoires aux CVE ou aux TPE pour les demandes de réduction des risques
- Impact des contrôles compensatoires sur le score de risque et la date d'expiration

Analyser à nouveau les enregistrements et les tâches de rattrapage dans Vulnerability Manager Workspace

Pour vérifier que vos tâches et enregistrements de rattrapage ont été résolus entre les cycles d'analyse planifiés, lancez de nouvelles analyses à partir de votre Now Platform ordinateur à la demande.

Rôle requis : sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, vos correctifs et vos autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Les Rapid7 analyseurs et Qualys sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Ré-analyse** n'est pas disponible.

Pour activer ces analyseurs, en tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin :

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Localisez le produit de scanner que vous souhaitez activer et cliquez sur l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher Activé.
4. Cliquez sur **Mettre à jour**.

   Le produit que vous avez activé s'affiche dans le champ Source sur les enregistrements d'élément vulnérable et de tâche de rattrapage après l'importation suivante, et **Analyser de nouveau** est disponible en tant qu'action d'interface utilisateur.

La nouvelle analyse est prise en charge pour les enregistrements et les tâches de rattrapage avec les intégrations suivantes dans Vulnerability Manager Workspace. Consultez les rubriques suivantes pour plus d'informations :

- Analyser Rapid7 à nouveau les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail
- Analyser Qualys à nouveau les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail
- Analyser Tenable.io à nouveau et Tenable.sc les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail

Pour lancer de nouvelles analyses dans l'espace de travail du gestionnaire de vulnérabilité à partir d'enregistrements d'éléments vulnérables et de tâches de rattrapage, les enregistrements nécessitent un scanner pris en charge comme source.

Vous préférez peut-être créer une liste filtrée qui affiche les enregistrements par source. Voir Créer une liste personnalisée des enregistrements pour un exemple de création d'une liste.

Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités

À partir de la version 23.0 de Vulnerability Response, évaluez les affectations, la date cible de rattrapage, les tâches de rattrapage et le score de risque pour un ensemble d'enregistrements (VIT, AVIT, CVIT ou TR) dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneur
- sn_vulc.vulnerability_analyst et sn_vulc.admin pour les résultats des tests de configuration

Pourquoi et quand exécuter cette tâche

Avant la version 23.0 de Vulnerability Response, il était nécessaire d'appliquer les règles à tous les enregistrements pour obtenir les dernières affectations, dates cibles de rattrapage, scores de risque et tâches de rattrapage, ce qui était un processus chronophage. À partir de la version 23.0, vous pouvez évaluer et mettre à jour de manière sélective ces propriétés pour des enregistrements spécifiques, réduisant ainsi le temps de traitement. De plus, vous pouvez affiner le processus de rattrapage en fonction de ces propriétés mises à jour.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, ouvrez la liste Actif ou Tout dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de l'application
   - Éléments vulnérables de conteneurs
   - Résultats des tests de configuration
3. Cochez la case des enregistrements souhaités et cliquez sur le bouton **Réévaluer** .
4. Dans le modal Réévaluer et mettre à jour les propriétés de rattrapage, sélectionnez les propriétés que vous souhaitez mettre à jour pour les enregistrements sélectionnés.

Propriété	Description
Affectations	Met à jour les affectations dans le champ Groupe d'affectation en fonction des dernières règles d'affectation.
Score du risque	Met à jour le score de risque dans le champ Score de risque conformément aux dernières règles de score de risque.
Tâches de rattrapage	Met à jour les tâches de rattrapage en fonction des dernières règles de tâche de rattrapage.
Date cible de rattrapage	Met à jour la date cible de rattrapage en fonction des dernières règles de cibles de rattrapage.

Remarque : Lorsque vous sélectionnez une propriété, ses propriétés dépendantes sont sélectionnées automatiquement.

5. Sélectionnez **Appliquer**.

Résultats

Les propriétés sont mises à jour pour les enregistrements sélectionnés. Vous pouvez consulter les **notes de travail** des enregistrements pour connaître les valeurs précédentes et les plus récentes des propriétés de rattrapage mises à jour.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser la vue de liste dans l'espace de travail du gestionnaire de vulnérabilité

La vue de liste de l'espace de travail du gestionnaire de vulnérabilité permet aux gestionnaires et analystes de la vulnérabilité et de la sécurité de voir la progression du rattrapage sur les enregistrements, d'explorer les enregistrements Vulnerability Response et d'afficher l'état de leurs demandes d'approbation et exceptions.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. En haut à gauche de l'espace de travail avec la page d'accueil affichée, cliquez sur l'icône **Liste** .
3. Facultatif : Cliquez sur **Mes listes** pour créer une liste.
   Pour en savoir plus sur la création d'une liste, reportez-vous à la section Créer une liste personnalisée des enregistrements.
4. Reportez-vous au tableau suivant pour connaître les actions que vous pouvez effectuer sur la page Liste.

Action d'interface utilisateur	Description
Ouvrir un effort de rattrapage	
À gauche de la colonne Nombre avec une liste affichée, passez la souris sur une ligne et cliquez sur la petite icône d'information **(i)** d'un enregistrement.	Les détails des enregistrements sont affichés dans le panneau latéral droit de la page. Les détails sont les suivants : ◦ Groupe d'affectation ◦ Vulnérabilité ◦ Affecté à ◦ Brève description ◦ Description Vous pouvez modifier les champs. Si la case à cocher Actif s'affiche, vous pouvez activer ou désactiver l'enregistrement. Cliquez sur Mettre à **jour** pour enregistrer vos modifications.
Actualiser la liste	Avec l'icône d'actualisation en haut à droite de la page, rechargez la page actuelle.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
Rétablir la largeur des colonnes	Cliquez sur l'icône en forme d'engrenage pour ajuster la largeur des colonnes de vos listes. Une copie de la liste d'origine est enregistrée sous **Vos listes**.
Copier l'URL de la page affichée	Copiez l'URL pour l'utiliser ailleurs.
Exporter la page	Dans la fenêtre modale, saisissez le fichier et les types de livraison, puis cliquez sur **Exporter**.
Affinez les filtres pour les données de la page.	Sélectionnez une colonne et développez le menu à trois points verticaux pour afficher les options qui filtrent davantage les données de la colonne. Par exemple, vous préférerez peut-être filtrer la colonne Groupe d'affectation de la liste des tâches de rattrapage actives par un groupe d'affectation spécifique.
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes : ◦ Afficher les éléments correspondants : affiche uniquement les éléments qui correspondent à la cellule sélectionnée dans la colonne. ◦ Filtrer : filtre les éléments de la colonne qui correspondent à la cellule sélectionnée dans la colonne.

5. Créez un élément vulnérable de l'application à partir des listes **Actif** ou **Tous** ci-dessous *Application Vulnerable items* en cliquant sur le bouton **Nouveau** en haut à droite.

Créer une liste personnalisée des enregistrements

Vous pouvez créer une liste personnalisée dans l'espace de travail du gestionnaire de vulnérabilité.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sélectionnez l'icône **Liste** , puis cliquez sur **Mes listes**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez **Nouvelle liste**.
4. Dans le modal Nouvelle liste, cliquez sur **Démarrer à partir de l'élément existant** et recherchez dans la liste de choix de liste une liste existante à utiliser comme modèle.
5. Modifiez le nom de la liste.
6. Ajoutez des filtres.
   Par exemple, vous pouvez créer une liste des enregistrements actifs pour un scanner particulier que vous souhaitez surveiller pour les nouvelles analyses. Vous pouvez utiliser les filtres suivants : `Actif est vrai` et `Source contient (nom de votre scanner)`.
7. Modifiez les colonnes que vous souhaitez afficher dans votre liste.
8. Cliquez sur **Créer**.
   Votre nouvelle liste s'affiche.
9. Vous pouvez également cliquer sur **Créer le vôtre**, entrer un nom, puis **sélectionner la source**.
10. Commencez à saisir du texte dans le champ et sélectionnez parmi les sources qui s'affichent pour votre nouvelle liste.
11. Cliquez sur **Créer**.
    Votre nouvelle liste s'affiche.

    Remarque : Si vous quittez le module de liste, la liste affichée lorsque vous quittez est la liste que vous voyez à votre retour.

12. Pour supprimer une liste, avec la liste affichée, cliquez sur l'icône d'engrenage en haut à droite de la page.

Actualiser une tâche de rattrapage dans Vulnerability Manager Workspace

Le bouton **Mettre à jour l'état** permet d'inspecter les enregistrements pour voir s'il existe des enregistrements supplémentaires appartenant à une tâche de rattrapage (VUL, AVUL, CVUL ou CRG). Utilisez-la si une mise à jour est justifiée en dehors de la tâche planifiée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, sous la liste Tâches de rattrapage, ouvrez tout enregistrement dont l'état est Ouvert ou En cours d'examen.
3. Sélectionnez le menu à trois points et sélectionnez l'option **Mettre à jour le statut** .

Résultats

Les nouveaux enregistrements correspondants apparaissent sous les onglets Éléments vulnérables, Éléments vulnérables de l'application, Éléments vulnérables du conteneur ou Résultats des tests de configuration.

Activer ou désactiver l'importation de résultats des tests pour un groupe de Qualys tests

À partir de la version 23.0 de , contrôlez l'importation des résultats des tests pour les tests d'un Qualys groupe de Réponse aux vulnérabilitéstests à l'aide du bouton **Activer/Désactiver l'importation**, disponible dans la vue d'enregistrement du groupe de tests.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Listes**.
2. Dans les bibliothèques, sous la liste Groupes de tests, ouvrez un Qualys groupe de tests dans la vue d'enregistrement.
3. Désactivez l'importation des résultats des tests associés à un Qualys groupe de tests en cliquant sur le bouton **Désactiver l'importation** .
   À partir de l'ingestion de données à venir, les résultats des tests ne sont pas importés pour le groupe de Qualys tests.
   La valeur du champ **L'importation est-elle désactivée** devient *vrai*.
4. Facultatif : Activez l'importation des résultats des tests en cliquant sur le bouton **Activer l'importation** .

Approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilités

Approuvez ou rejetez les demandes soumises par les propriétaires du rattrapage.

Avant de commencer
Rôles requis :

Rôles d'approbateur requis pour diverses demandes d'approbation

Type d'approbation	Niveaux d'approbation requis	Rôles d'approbateur	Information supplémentaire
Approbations de faux positifs	Un	• sn_vul.false_positive_approver Rôle granulaire pour les éléments vulnérables (VIT). • Rôle sn_vul.app_false_positive_approver pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.false_positive_approver rôle pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.false_positive_approver pour les résultats des tests de configuration Ou Les approbateurs doivent faire partie du groupe	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles d'approbateur requis pour diverses demandes d'approbation (suite)

Type d'approbation	Niveaux d'approbation requis	Rôles d'approbateur	Information supplémentaire
		d'utilisateurs Approbateur faux positif.	
Approbations d'exceptions (reports)	Deux	• Un approbateur est requis dans le groupe Approbateur - Niveau 1 • Un approbateur est requis dans le groupe Approbateur - Niveau 2	Une demande d'exception pour un enregistrement ou une tâche de rattrapage est approuvée à l'aide d'un workflow d'approbation à deux niveaux par défaut. La demande d'exception nécessite deux niveaux d'approbateurs. Une fois que la demande est approuvée par l'approbateur de niveau 1, elle est envoyée à l'approbateur de deuxième niveau et est alors visible dans la file d'attente de l'approbateur 2.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles d'approbateur requis pour diverses demandes d'approbation (suite)

Type d'approbation	Niveaux d'approbation requis	Rôles d'approbateur	Information supplémentaire
Annuler l'affectation des approbations	Un approbateur est requis dans le groupe Approbateur – Niveau 1	• sn_vul.unassign_appr pour les AVIT et les VIT • sn_vul_container.una pour les CVIT • sn_vulc.unassign_app pour les problèmes de configuration (CI)	**Remarque :** Par défaut, une configuration d'approbation est fournie et un groupe d'approbation de désaffectation est créé. Les utilisateurs (Désaffecter l'approbateur : niveau 1) de ce groupe peuvent approuver la demande. Ce groupe contient un rôle d'approbateur de désaffectation, sn_vul.unassign_approver, par défaut. Vous pouvez modifier ou créer un nouveau groupe et mettre à jour la configuration de l'approbation. Pour configurer des règles d'approbation, accédez au module Règles d'approbation respectif, sélectionnez l'une des règles d'approbation suivantes, puis accédez à la configuration d'approbation dans l'onglet **Configurations d'approbation** : • *Vulnerable item. find change request* pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles d'approbateur requis pour diverses demandes d'approbation (suite)

Type d'approbation	Niveaux d'approbation requis	Rôles d'approbateur	Information supplémentaire
Approbations de réduction des risques	Deux	• Un approbateur est requis dans le groupe Approbateur - Niveau 1 • Un approbateur est requis dans le groupe Approbateur - Niveau 2	Le flux d'approbation pour la réduction des risques est le même que pour les approbations d'exceptions (reports).

Consultez Réponse aux vulnérabilités Profils et rôles granulaires et Affecter les rôles de profil à l'aide de l'Assistant Réponse aux vulnérabilités de configuration pour en savoir plus sur l'affectation de rôles de profil aux utilisateurs et aux groupes.

Remarque : Ajoutez des utilisateurs aux groupes d'approbation avant de soumettre des demandes d'approbation. Si vous créez des demandes avant d'ajouter des utilisateurs aux groupes d'approbation, les demandes peuvent ne pas être visibles par les utilisateurs disposant de l'autorisation d'approbation.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
   Si un approbateur n'a pas accès à l'espace de travail, les approbations peuvent être traitées à l'adresse **Réponse aux vulnérabilités** > **Mes approbations** dans l'environnement classique.
2. Sélectionnez l'icône Vue de listes (
   La page Liste s'affiche.
3. Dans la liste filtrée des approbations, sélectionnez **Mes affectations**.
4. Recherchez une demande que vous souhaitez traiter, puis sélectionnez le lien dans la colonne État.
   L'enregistrement d'approbation de changement d'état de la vulnérabilité (VCA#) s'affiche.
5. Choisissez l'une des options suivantes pour approuver ou rejeter la demande.

Option	Description
Cliquez sur l'onglet Détails, saisissez du texte dans le champ Commentaires, puis cliquez sur Rejeter	◦ Un message s'affiche indiquant qu'il y a une approbation rejetée pour l'enregistrement d'approbation du changement d'état de la vulnérabilité. ◦ L'état de l'enregistrement Approbation de changement d'état de la vulnérabilité passe à Rejeté. ◦ L'état de la tâche de rattrapage ou de l'enregistrement reste le même.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	◦ L'enregistrement d'approbation de changement d'état de la vulnérabilité n'est plus affiché dans votre vue de liste d'approbations dans l'espace de travail.
Dans l'onglet **Demande** ou **Détails** , cliquez sur Approuver	◦ Un message s'affiche indiquant que l'enregistrement d'approbation du changement d'état de la vulnérabilité est approuvé. ◦ L'état de la tâche de rattrapage ou de l'enregistrement passe à Différé. ◦ Les enregistrements actifs sur les tâches de rattrapage passent à l'état Différé. ◦ L'enregistrement d'approbation de changement d'état de la vulnérabilité n'est plus affiché dans votre vue de liste d'approbations.

Configurer des notifications par e-mail dans les Réponse aux vulnérabilités espaces de travail

Identifiez les utilisateurs pour les rappels automatiques par e-mail envoyés aux utilisateurs du groupe d'utilisateurs Propriétaire du rattrapage.

Avant de commencer

Rôle requis : administrateur

Cette fonctionnalité génère automatiquement un résumé d'e-mail pour les utilisateurs du groupe d'utilisateurs du propriétaire du rattrapage. Ajoutez tous les utilisateurs que vous souhaitez voir recevoir des notifications par e-mail, conformément aux instructions de la section Utiliser la synthèse d'e-mail dans les espaces de travail Vulnerability Response.

Vérifiez que les utilisateurs ont une adresse e-mail active saisie dans leur enregistrement utilisateur et que vous les avez ajoutés au groupe d'utilisateurs Propriétaire du rattrapage.

Si vous souhaitez modifier la fréquence de livraison, le jour ou l'heure des e-mails, ou désactiver la fonctionnalité, procédez comme suit.

Procédure

1. Accédez à la **Tout** > **Travaux planifiés**.
2. Localisez le **synthèses de rattrapage Générer** et cliquez dessus pour ouvrir l'enregistrement.

   Vous préférerez peut-être laisser les champs dans leurs paramètres par défaut jusqu'à ce que vous vérifiiez que les notifications sont envoyées. Par défaut, les e-mails sont envoyés chaque semaine, le lundi matin à 9h00, dans le fuseau horaire de l'instance qui exécute la tâche.

3. Modifiez les champs de formulaire.
   Pour plus d'informations sur les champs de formulaire, consultezGénérer des champs de formulaire de synthèse de rattrapage .
4. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Si vous avez vérifié que toutes les informations répertoriées précédemment sont correctes et que vous avez des utilisateurs dans le groupe d'utilisateurs Propriétaire du rattrapage mais que les e-mails ne sont pas envoyés comme prévu, vérifiez qu'il existe des canaux activés pour recevoir des notifications par e-mail. Consultez Créer des canaux de notification .

Corriger les éléments vulnérables et les résultats des tests dans le Espace de travail du gestionnaire de vulnérabilités

Dans le Espace de travail du gestionnaire de vulnérabilités, vous pouvez corriger des éléments vulnérables et des résultats de test en les intégrant dans une rubrique de surveillance en définissant une condition, et vous pouvez suivre leur progression de rattrapage en créant des efforts de rattrapage.

L'utilisation de la modification en bloc dans Espace de travail du gestionnaire de vulnérabilités

Dans le Espace de travail du gestionnaire de vulnérabilités, vous pouvez mettre à jour l'état des enregistrements, demander des exceptions et des faux positifs, et affecter des enregistrements à un groupe d'affectation de plusieurs éléments vulnérables (VIT, AVIT ou CVIT) simultanément à l'aide de la fonctionnalité de modification en bloc.

La fonctionnalité de modification en bloc est disponible pour :

- éléments vulnérables de l'hôte (VIT) à partir de la version 21.0 de Réponse aux vulnérabilités.
- Éléments vulnérables de l'application (AVIT) et éléments vulnérables du conteneur (CVIT) à partir de la version 22.0 de Réponse aux vulnérabilités.
- Résultats des tests à partir de la version 23.0 de Réponse aux vulnérabilités.

Mettre à jour l'état des enregistrements en bloc dans le Espace de travail du gestionnaire de vulnérabilités

Mettez à jour simultanément l'état de plusieurs enregistrements (VIT, AVIT ou CVIT) en fonction de leur état d'avancement du rattrapage à l'aide de la fonctionnalité de modification en bloc du Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneur

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, ouvrez la liste Actif ou Tout dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
3. Effectuez l'une des actions suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Seuls les éléments sélectionnés** dans le champ **Sélection d'enregistrement** .
- Appliquez des filtres si vous souhaitez utiliser l'option **Tous les éléments vulnérables qui correspondent au filtre** dans le champ **Sélection d'enregistrement** .

4. Sélectionnez le bouton **Modifier en bloc** .
5. Dans le modal de modification en bloc, renseignez les champs suivants pour mettre à jour l'état des enregistrements.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ Uniquement les éléments sélectionnés : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ Tous les éléments vulnérables qui correspondent au filtre : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ◦ Tâche de rattrapage : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ◦ Entrée de vulnérabilité : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une entrée vulnérable commune (CVE), puis sélectionnez les CVE dans le champ **Entrée de vulnérabilité** . **Remarque :** Les enregistrements avec CI non valide ou CI désactivé ne sont pas mis à jour.
État	Changement de **l'état** dans l'enregistrement. Les choix possibles sont les suivants : ◦ Ne pas mettre à jour ◦ Ouvrir ◦ En cours d'examen ◦ En attente d'implémentation ◦ DifféréDemander une exception en bloc dans Vulnerability Manager Workspace ◦ FerméModification en bloc pour les faux positifs dans Vulnerability Manager Workspace ◦ Résolu **Remarque :** Seuls les enregistrements pour lesquels la transition d'état est valide sont mis à jour.
Notes de travail	Texte que vous saisissez pour décrire les changements.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sélectionnez **Modifier**.

   Une tâche asynchrone de modification en bloc met à jour les enregistrements sélectionnés.

Modifier en bloc les éléments vulnérables de l'hôte avec des correctifs et des solutions

Recommandez un correctif ou une solution pour plusieurs éléments vulnérables de l'hôte simultanément à l'aide de la fonctionnalité de modification en bloc du Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin et tout rôle doté du rôle granulaire sn_vul.bulk_edit.

Pourquoi et quand exécuter cette tâche

Dans le modal de modification en bloc, tout en ajoutant une solution et un correctif préférés, vous pouvez également annuler l'affectation ou affecter simultanément plusieurs éléments vulnérables d'hôte (VIT) à un groupe d'affectation.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.

   Remarque : Les enregistrements sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.

2. Sur la page Liste, sous Éléments vulnérables de l'hôte, ouvrez la liste Actif ou Tous.
3. Effectuez l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Seuls les éléments sélectionnés** dans le champ **Sélection d'enregistrement** .
   - Appliquez des filtres si vous souhaitez utiliser l'option **Tous les éléments vulnérables qui correspondent au filtre** dans le champ **Sélection d'enregistrement** .
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Seuls les éléments sélectionnés** dans le champ Sélection d'enregistrement du modal de modification en bloc.
   - Appliquez des filtres si vous souhaitez utiliser l'option **Tous les éléments vulnérables qui correspondent au filtre** dans le champ Sélection d'enregistrement du modal de modification en bloc.
4. Sélectionnez le bouton **Modifier en bloc** .
5. Dans le modal de modification en bloc, renseignez les champs pour recommander un correctif ou une solution pour plusieurs éléments vulnérables de l'hôte.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Uniquement les éléments sélectionnés : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ Tous les éléments vulnérables qui correspondent au filtre : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ◦ Tâche de rattrapage : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ◦ Entrée de vulnérabilité : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une entrée vulnérable commune (CVE), puis sélectionnez les CVE dans le champ **Entrée de vulnérabilité** . **Remarque :** ◦ Les enregistrements avec CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements (VIT) à l'état Ouvert, En cours d'examen ou En attente d'implémentation sont mis à jour.
État	Changement de **l'état** des éléments vulnérables de l'hôte. Vous pouvez ajouter la solution et le correctif préférés uniquement lorsque vous choisissez les états suivants. ◦ Ne pas mettre à jour ◦ Ouvrir ◦ En cours d'examen ◦ En attente d'implémentation
Solution privilégiée	Solution ciblée pour le rattrapage de tous les éléments vulnérables sélectionnés pour la modification en bloc. Sélectionnez le changement pour le champ **Solution privilégiée** dans l'élément vulnérable. Les choix proviennent d'une liste de recherche des solutions préférées disponibles pour les VIT sélectionnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ◦ L'ensemble des solutions privilégiées disponibles est une intersection de toutes les solutions potentielles des vulnérabilités dans tous les VIT sélectionnés. ◦ Lors de la sélection de **Sélection d'enregistrement** > **Entrée de vulnérabilité** pour une modification en bloc, tous les VIT pour la vulnérabilité sont définis sur la solution préférée sélectionnée. **Remarque :** Cette opération ne définit pas la **solution privilégiée** au niveau de l'entrée de vulnérabilité. La définition de la **solution privilégiée** au niveau d'entrée de vulnérabilité définira la **solution privilégiée** pour tous les nouveaux VIT à l'avenir. La modification en bloc ne modifie que l'ensemble actuel des VIT. ◦ Les vulnérabilités distinctes par rapport aux critères de sélection sont limitées à 500. S'il existe plus de 500 vulnérabilités distinctes, un message d'avertissement s'affiche vous demandant de sélectionner des VIT avec des critères différents pour définir la **solution privilégiée**. ◦ Le nombre total de solutions pouvant être affichées dans la liste de recherche est limité à 170. S'il y a plus de 170 solutions, un message d'avertissement s'affiche. La valeur mise à jour est affichée dans la vue de liste Élément vulnérable.
Correctif préféré	Correctif ciblé pour corriger tous les éléments de vulnérabilité sélectionnés pour la modification en bloc. **Remarque :** ◦ Vous devez installer Patch Orchestration pour afficher la liste des correctifs préférés. ◦ L'ensemble des correctifs préférés disponibles est une intersection de tous les correctifs potentiels pour tous les VIT sélectionnés. ◦ Les vulnérabilités distinctes par rapport aux critères de sélection sont limitées à 500. S'il existe plus de 500 vulnérabilités distinctes, un message d'avertissement s'affiche vous demandant de sélectionner des VIT avec différents critères pour définir le **correctif préféré**. ◦ Le nombre total de correctifs pouvant être affichés dans la liste de recherche est limité à 170. S'il y a plus de 170 correctifs, un message d'avertissement s'affiche.
Annuler l'affectation	Tous les éléments sélectionnés ne sont pas affectés au groupe d'affectation et au propriétaire du rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ◦ Ce champ s'affiche lorsque vous sélectionnez l'état Ne pas mettre à jour. ◦ Lorsque vous annulez l'affectation d'enregistrements, une tâche de rattrapage est créée et envoyée pour approbation. Pour plus d'informations, voir Supprimer les affectations des éléments vulnérables d'hôte en bloc
Groupe d'affectation	Groupe d'affectation pour les enregistrements. Tous les groupes d'affectation actifs apparaissent dans ce champ. **Remarque :** Ce champ est désactivé lorsque vous cochez la case Annuler l'affectation.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Sélectionnez **Modifier**.

Résultats
Une tâche asynchrone de modification en bloc met à jour les éléments vulnérables de l'hôte (VIT) sélectionnés. La solution et le correctif préférés sont ajoutés aux éléments vulnérables de l'hôte (VIT) pertinents. Ouvrez un élément vulnérable de l'hôte et affichez la solution et le correctif préférés dans la section Rattrapage de l'onglet Détails.

Affecter des enregistrements à un groupe d'affectation en bloc

Affectez simultanément plusieurs enregistrements (VIT, AVIT, CVIT ou TR) à un groupe d'affectation à l'aide de la fonctionnalité de modification en bloc du Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer
Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Procédure
1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, ouvrez la liste Actif ou Tout dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
   - Résultats des tests de configuration
3. Effectuez l'une des actions suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Seuls les éléments sélectionnés** dans le champ Sélection d'enregistrement .
- Appliquez des filtres si vous souhaitez utiliser l'option **Tous les enregistrements qui correspondent au filtre** dans le champ Sélection d'enregistrement .

4. Sélectionnez le bouton **Modifier en bloc** .
5. Renseignez les champs du formulaire pour affecter les enregistrements à un groupe d'affectation.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ *Uniquement les éléments sélectionnés* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ *Tous les enregistrements qui correspondent au filtre* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ◦ *Tâche de rattrapage* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ◦ *Entrée de vulnérabilité* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une vulnérabilité, puis sélectionnez un CVE ou un TPE dans le champ **Entrée de vulnérabilité**. **Remarque :** Ce champ apparaît pour les éléments vulnérables de l'hôte, les éléments vulnérables de l'application et les éléments vulnérables du conteneur. ◦ *Test de configuration* : sélectionnez cette option si vous souhaitez mettre à jour les résultats des tests spécifiques à un test, puis sélectionnez un test dans le champ **Test de configuration** . **Remarque :** Cette option s'affiche uniquement pour les résultats des tests de configuration. **Remarque :** ◦ Les enregistrements avec CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements à l'état Ouvert, En cours d'examen, En attente d'implémentation ou Différé sont mis à jour.
Groupe d'affectation	Groupe d'affectation pour les enregistrements. Tous les groupes d'affectation actifs apparaissent dans ce champ. **Remarque :** Ce champ est désactivé lorsque vous cochez la case Annuler l'affectation des VIT.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.

Résultats
Ouvrez un enregistrement pour lequel vous avez mis à jour le groupe d'affectation et accédez à l'onglet Vue d'ensemble, le groupe d'utilisateurs auquel l'enregistrement est affecté apparaît dans le champ **Groupe d'affectation** .

Supprimer les affectations des éléments vulnérables d'hôte en bloc

Supprimez-vous ou retirez vos groupes des champs **Affecté à** et **Groupe d'affectation** sur les éléments vulnérables de l'hôte (VIT) ou les tâches de rattrapage (VUL) si vous déterminez que les enregistrements ne sont pas dans votre champ d'application pour le rattrapage, ou si vous pensez que les enregistrements ont été affectés de manière incorrecte à vous ou à vos groupes.

Avant de commencer
Rôle requis : sn_vul.vulnerability_analyst et sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
La fonctionnalité Annuler l'affectation s'applique aux enregistrements dont l'état n'est pas Fermé ou Résolu. Lorsque vous supprimez des affectations d'éléments vulnérables d'hôte à l'aide de la fonctionnalité de modification en bloc, seuls les enregistrements pertinents sont mis à jour.

Procédure
1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, sous Éléments vulnérables de l'hôte, ouvrez la liste Actif ou Tous.
3. Effectuez l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Seuls les éléments sélectionnés** dans le #unique_785_Connect_42_record-slection-field-unassign champ.
   - Appliquez des filtres si vous souhaitez utiliser l'option **Tous les éléments vulnérables qui correspondent au filtre** dans le #unique_785_Connect_42_record-slection-field-unassign champ.
4. Sélectionnez le bouton **Modifier en bloc** .
5. Renseignez les champs du formulaire pour supprimer des affectations en bloc.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ Uniquement les éléments sélectionnés : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ Tous les éléments vulnérables qui correspondent au filtre : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Tâche de rattrapage : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ◦ Entrée de vulnérabilité : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une entrée vulnérable commune (CVE), puis sélectionnez les CVE dans le champ **Entrée de vulnérabilité** . **Remarque :** ◦ Les enregistrements avec CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements à l'état Ouvert, En cours d'examen, En attente d'implémentation ou Différé sont mis à jour.
État	Sélectionnez l'état Ne pas mettre à jour.
Annuler l'affectation	Tous les éléments vulnérables sélectionnés sont désaffectés du groupe d'affectation et du propriétaire du rattrapage. **Remarque :** ◦ Ce champ s'affiche lorsque vous sélectionnez l'état Ne pas mettre à jour. ◦ Lorsque vous annulez l'affectation d'enregistrements, une tâche de rattrapage est créée et envoyée pour approbation.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.
   Une tâche de rattrapage est créée avec les éléments vulnérables d'hôte (VIT) sélectionnés.

   Votre demande est soumise pour approbation et l'approbateur reçoit une notification par e-mail concernant votre demande.

   L'état des éléments vulnérables de l'hôte (VIT) et de la tâche de rattrapage (VUL) passe à En cours de révision. Si une tâche de rattrapage est mise à jour avec cette fonctionnalité, les champs **Affecté à** et **Groupe d'affectation** de tous ses VIT associés sont également effacés lors de l'approbation de votre demande.

Résultats
Dans Vulnerability Manager Workspace, sur la page Liste, accédez à **Demandes d'exception** > **Tout** et ouvrez l'enregistrement d'approbation de changement d'état (VCA#) correspondant et vérifiez l'état de votre demande dans la colonne État d'approbation :

État d'approbation	Résultat
Approuvé	Les champs **Affecté à** et **Groupe d'affectation** de tous les éléments vulnérables de l'hôte sont effacés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État d'approbation	Résultat
Rejeté	Les champs **Affecté à** et **Groupe d'affectation** de tous les éléments vulnérables de l'hôte ne sont pas mis à jour.

Dans le **flux d'activité** d'un enregistrement ou d'une tâche de rattrapage, vous pouvez afficher l'ensemble du workflow de votre demande.

Demander une exception en bloc dans Vulnerability Manager Workspace

Demandez une exception pour plusieurs enregistrements (VIT, AVIT, CVIT ou TR) simultanément à l'aide de la fonctionnalité de modification en bloc au lieu de sélectionner manuellement chaque enregistrement.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Lorsque vous demandez une exception pour un ou plusieurs enregistrements à partir du modal de modification en bloc, une tâche de rattrapage est créée avec les enregistrements sélectionnés.

Remarque : Les éléments vulnérables de l'application (AVIT) des scanners avec le paramètre **Gérer les exceptions dans ServiceNow** défini sur faux ne sont pas mis à jour.

- Si vous sélectionnez des AVIT à partir de différents analyseurs, certains avec le paramètre **Gérer les exceptions dans ServiceNow** défini sur vrai et d'autres sur faux, les AVIT liés aux scanners avec le paramètre **Gérer les exceptions dans ServiceNow** défini sur faux ne sont pas mis à jour.
- Si vous sélectionnez des AVIT uniquement parmi les analyseurs pour lesquels le paramètre **Gérer les exceptions dans ServiceNow** est défini sur false, l'option *Différer* n'apparaît pas dans le champ **État** du modal de modification en bloc.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, ouvrez la liste Actif ou Tout dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
   - Résultats des tests de configuration
3. Effectuez l'une des actions suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option *Seuls les éléments sélectionnés* dans le champ Sélection d'enregistrement .
- Appliquez des filtres si vous souhaitez utiliser l'option *Tous les enregistrements qui correspondent au filtre* dans le champ Sélection d'enregistrement .

4. Sélectionnez le bouton **Modifier en bloc** .
5. Renseignez les champs suivants du formulaire pour demander une exception pour plusieurs enregistrements (VIT, AVIT, CVIT ou TR) simultanément.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ *Uniquement les éléments sélectionnés* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ *Tous les enregistrements qui correspondent au filtre* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ◦ *Tâche de rattrapage* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ◦ *Entrée de vulnérabilité* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une vulnérabilité , puis sélectionnez un CVE ou un TPE dans le champ **Entrée de vulnérabilité** . **Remarque :** Ce champ apparaît pour les éléments vulnérables de l'hôte, les éléments vulnérables de l'application et les éléments vulnérables du conteneur. ◦ *Test de configuration* : sélectionnez cette option si vous souhaitez mettre à jour les résultats des tests spécifiques à un test, puis sélectionnez un test dans le champ **Test de configuration** . **Remarque :** Cette option s'affiche uniquement pour les résultats des tests de configuration. **Remarque :** ◦ Les enregistrements avec CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements à l'état Ouvert, En cours d'examen ou En attente d'implémentation sont mis à jour.
État	Sélectionnez l'état *Différé* pour demander une exception pour les enregistrements sélectionnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ◦ Lorsque vous sélectionnez cette option, les champs Motif, Description brève, Jusqu'au et Informations supplémentaires s'affichent. ◦ Lorsque vous différez des enregistrements, une tâche de rattrapage est créée et cette tâche est envoyée pour approbation.
Motif	Motif du report des enregistrements : ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre **Remarque :** Le champ **Motif** s'affiche lorsque vous sélectionnez l'état Différé ou Fermé.
Description brève	Brève note décrivant les raisons de la demande de report. Ces informations sont reflétées dans le champ **Description** de la tâche de rattrapage créée pour une demande de report. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé et Fermé : faux positif.
Jusqu'à	Date à laquelle l'enregistrement demeure différé. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé.
Information supplémentaire	Toute autre information nécessaire. Ces informations sont reflétées dans le champ Informations supplémentaires de l'onglet Vue d'ensemble de la tâche de rattrapage créée pour les demandes de report et les demandes de faux positifs fermés. Si votre demande de report est approuvée, ces informations supplémentaires apparaissent sous forme de notes de report pour VIT et pour la tâche de rattrapage. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé et Fermé : faux positif.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.
7. Dans le modal Répondre au questionnaire, répondez aux questions et cliquez sur **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une tâche de rattrapage contenant les enregistrements que vous avez sélectionnés est créée. Votre demande est soumise pour approbation et l'état des enregistrements passe à En cours de révision.

Remarque : Le modal **Répondre au questionnaire** s'affiche uniquement lorsque le questionnaire est activé pour les demandes d'exception dans le formulaire Gestion des exceptions. Pour plus d'informations sur la configuration d'un questionnaire pour les demandes d'exception, consultez , Configurer la gestion des exceptions pour Réponse aux vulnérabilités des applicationset Configurer la gestion des exceptions pour Réponse aux vulnérabilitésConfigurer la gestion des exceptions pour Réponse aux vulnérabilités pour conteneurs.

L'approbateur reçoit une notification par e-mail au sujet de votre demande.

Résultats

Dans Vulnerability Manager Workspace, sur la page Liste, accédez à **Exception :** > **Tout**, ouvrez l'enregistrement d'approbation de changement d'état (VCA#) correspondant et vérifiez l'état de votre demande dans la colonne État d'approbation :

État d'approbation	Résultat
Approuvé	L'état de la tâche de rattrapage passe à Différé avec le motif indiqué comme sous-état. L'état et le motif sont déployés jusqu'aux enregistrements.
Rejeté	L'état de la tâche de rattrapage et de ses enregistrements ne change pas.

Dans le **flux d'activité** d'un enregistrement ou d'une tâche de rattrapage, vous pouvez afficher l'ensemble du workflow de votre demande.

Modification en bloc pour les faux positifs dans Vulnerability Manager Workspace

Marquez un ou plusieurs enregistrements (VIT, AVIT, CVIT ou TR) comme faux positifs simultanément en utilisant la fonctionnalité de modification en bloc de Vulnerability Manager Workspace au lieu de sélectionner manuellement chaque élément.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Lorsque vous émettez une demande de faux positif pour un ou plusieurs enregistrements à partir du modal de modification en bloc, une tâche de rattrapage est créée avec les enregistrements sélectionnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous émettez une demande de faux positif pour les éléments vulnérables de l'application (AVIT) à l'aide de la fonctionnalité de modification en bloc, les AVIT des analyseurs pour lesquels le paramètre **Gérer les faux positifs avec ServiceNow** est défini sur faux ne sont pas mis à jour.

- Si vous sélectionnez des AVIT à partir de différents analyseurs, certains avec le paramètre **Gérer les faux positifs avec ServiceNow** défini sur vrai et d'autres avec false, les AVIT liés aux analyseurs avec le paramètre **Gérer les faux positifs avec ServiceNow** défini sur faux ne sont pas mis à jour.
- Si vous sélectionnez des AVIT uniquement parmi les scanners dont le paramètre **Gérer les faux positifs avec ServiceNow** est défini sur faux, l'option *Faux positif* n'apparaît pas dans le champ **Motif** du modal de modification en bloc.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste**.

   Remarque : Les enregistrements sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.

2. Sur la page Liste, ouvrez la liste Actif ou Tout dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
   - Résultats des tests de configuration
3. Effectuez l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option *Seuls les éléments sélectionnés* dans le champ **Sélection d'enregistrement** .
   - Appliquez des filtres si vous souhaitez utiliser l'option *Tous les enregistrements qui correspondent au filtre* dans le champ **Sélection d'enregistrement** .
4. Sélectionnez le bouton **Modifier en bloc** .
5. Renseignez les champs du formulaire pour demander un faux positif pour plusieurs enregistrements.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ *Uniquement les éléments sélectionnés* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ *Tous les enregistrements qui correspondent au filtre* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ◦ *Tâche de rattrapage* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ *Entrée de vulnérabilité* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une vulnérabilité , puis sélectionnez un CVE ou un TPE dans le champ **Entrée de vulnérabilité** . **Remarque :** Ce champ apparaît pour les éléments vulnérables de l'hôte, les éléments vulnérables de l'application et les éléments vulnérables du conteneur. ◦ *Test de configuration* : sélectionnez cette option si vous souhaitez mettre à jour les résultats des tests spécifiques à un test, puis sélectionnez un test dans le champ **Test de configuration** . **Remarque :** Cette option s'affiche uniquement pour les résultats des tests de configuration. **Remarque :** ◦ Les enregistrements avec CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements à l'état Ouvert, En cours d'examen ou En attente d'implémentation sont mis à jour.
État	Sélectionnez l'état **Fermé** .
Motif	Sélectionnez le motif en tant que faux positif. **Remarque :** ◦ Lorsque vous sélectionnez cette option, les champs Brève description et Informations supplémentaires s'affichent. ◦ Une tâche de rattrapage est créée lorsque vous marquez les enregistrements comme faux positifs et que cette tâche est envoyée pour approbation. **Remarque :** Le champ **Motif** s'affiche lorsque vous sélectionnez l'état Différé ou Fermé.
Description brève	Brève note décrivant les raisons de la demande fermée ou fausse positive. Ces informations sont reflétées dans le champ **Description** de la tâche de rattrapage créée pour une demande de type Fermé-Faux positif. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé ou Fermé : faux positif.
Information supplémentaire	Toute autre information nécessaire. Ces informations sont reflétées dans le champ Informations supplémentaires de l'onglet Vue d'ensemble de la tâche de rattrapage créée pour la demande Fermé-Faux positif. Si votre demande de faux positif est approuvée, ces informations supplémentaires apparaissent sous forme de notes pour VIT et pour la tâche de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Ce champ s'affiche lorsque vous sélectionnez l'état Différé ou Fermé : faux positif.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.
7. Dans le modal Répondre au questionnaire, répondez aux questions et sélectionnez **Soumettre**.
   Une tâche de rattrapage est créée avec les enregistrements sélectionnés. Votre demande est soumise pour approbation et l'état de la tâche de rattrapage passe à En cours de révision.

   Remarque : Le modal **Répondre au questionnaire** s'affiche uniquement lorsque le questionnaire est activé pour les demandes de faux positifs dans le formulaire Gestion des exceptions. Pour plus d'informations sur la configuration d'un questionnaire pour les demandes de faux positifs, consultez , Configurer la gestion des exceptions pour Réponse aux vulnérabilités des applicationset Configurer la gestion des exceptions pour Réponse aux vulnérabilitésConfigurer la gestion des exceptions pour Réponse aux vulnérabilités pour conteneurs.

   L'approbateur reçoit une notification par e-mail au sujet de votre demande.

Résultats

Dans Vulnerability Manager Workspace, sur la page Liste, accédez à **Exception :** > **Tout**, ouvrez l'enregistrement d'approbation de changement d'état (VCA#) correspondant et vérifiez l'état de votre demande dans la colonne État d'approbation :

État d'approbation	Résultat
Approuvé	L'état de la tâche de rattrapage passe à Fermé avec le motif Faux positif. L'état et le motif sont déployés jusqu'aux enregistrements.
Rejeté	L'état de la tâche de rattrapage et de ses enregistrements ne change pas.

Dans le **flux d'activité** d'un enregistrement ou d'une tâche de rattrapage, vous pouvez afficher l'ensemble du workflow de votre demande.

Fermer les enregistrements en bloc dans le Espace de travail du gestionnaire de vulnérabilités

Fermez simultanément plusieurs enregistrements (VIT, AVIT ou CVIT) à l'aide de la fonctionnalité de modification en bloc du Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager ou sn_vul_container.vulnerability_admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, ouvrez la liste Actif ou Tout dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
3. Effectuez l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option Seuls les éléments sélectionnés dans le champ **Sélection d'enregistrement** .
   - Appliquez des filtres si vous souhaitez utiliser l'option Tous les éléments vulnérables qui correspondent au filtre dans le champ **Sélection d'enregistrement** .
4. Sélectionnez le bouton **Modifier en bloc** .
5. Renseignez les champs du formulaire pour fermer les enregistrements sélectionnés.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ Uniquement les éléments sélectionnés : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ Tous les éléments vulnérables qui correspondent au filtre : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ◦ Tâche de rattrapage : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ◦ Entrée de vulnérabilité : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une entrée vulnérable commune (CVE), puis sélectionnez les CVE dans le champ **Entrée de vulnérabilité** . **Remarque :** ◦ Les enregistrements avec CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements à l'état Ouvert, En cours d'examen ou En attente d'implémentation sont mis à jour.
État	Sélectionnez l'état Fermé.
Motif	Motif de fermeture des enregistrements :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Faux positif **Remarque :** Lorsque vous sélectionnez cette option pour marquer les enregistrements comme faux positifs, les champs Motif, Description brève et Informations supplémentaires s'affichent. Pour plus d'informations sur la modification en bloc pour les faux positifs, reportez-vous à la section Modification en bloc pour les faux positifs dans Vulnerability Manager Workspace. ◦ Annulé ◦ Fixe **Remarque :** Les motifs Annulé et Fixe ne s'appliquent pas aux CVIT.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.

   Une tâche asynchrone de modification en bloc met à jour les enregistrements pertinents.

Demander des exceptions pour les tâches et les enregistrements de rattrapage auprès du Espace de travail du gestionnaire de vulnérabilités

À partir du , les Espace de travail du gestionnaire de vulnérabilitésgestionnaires et analystes de vulnérabilités peuvent demander des exceptions et des faux positifs pour une tâche de correction (VUL, AVUL, CVUL ou CRG) et un enregistrement (VIT, CVIT, AVIT ou TR). Vous pouvez également diviser une tâche de rattrapage et créer des demandes de changement.

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables de l'hôte
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneur
- sn_vulc.admin pour les résultats des tests de configuration

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans le Espace de travail du gestionnaire de vulnérabilités, vous pouvez effectuer les actions suivantes sur les enregistrements et les tâches de rattrapage :

- Divisez une tâche de rattrapage (VUL, AVUL, CVUL et CRG).
- Demandez une exception pour un enregistrement (VIT, AVIT, CVIT ou CTR) ou une tâche de rattrapage (VUL, AVUL, CVUL ou CRG).
- Demandez une exception de politique pour les enregistrements (VIT, AVIT ou CVIT) ou la tâche de rattrapage (VUL, AVUL, CVUL ou CRG).
- Créez une demande de changement pour la tâche de rattrapage (VUL, CVUL ou CRG).
- Demandez un faux positif pour l'enregistrement (VIT, AVIT ou CVIT) ou la tâche de rattrapage (VUL, AVUL, CVUL ou CRG).

> **Remarque :** Vous pouvez émettre des demandes de faux positif pour un ensemble de résultats des tests et une tâche de rattrapage (CRG) à partir de la version 22.0 de Réponse aux vulnérabilités.

Vous initiez ces actions d'interface utilisateur à partir d'enregistrements dans , de la Espace de travail du gestionnaire de vulnérabilitésmême manière que les propriétaires de rattrapage effectuent ces tâches dans le Espace de travail de remédiation IT.

Consultez les rubriques suivantes pour plus d'informations :

- Demander un faux positif dans le Espace de travail de remédiation IT
- Demander une exception dans le Espace de travail de remédiation IT
- Demander une réduction du risque dans le Espace de travail de remédiation IT
- Fractionner une tâche de rattrapage dans Espace de travail de remédiation IT
- Créer une demande de changement dans Espace de travail de remédiation IT
- Demander une exception à l'aide GRC : gestion de la politique et de la conformité de Espace de travail de remédiation IT
- Demande de faux positif pour un ensemble de résultats des tests

Information associée

Vue d'ensemble de la gestion des exceptions

Conformité de la configuration Vue d'ensemble de la gestion des exceptions

Demander une exception en bloc dans Vulnerability Manager Workspace

Modification en bloc pour les faux positifs dans Vulnerability Manager Workspace

Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilités

Demandez une extension pour un élément vulnérable différé avant qu'il n'atteigne sa date de report jusqu'à l'échéance. En tant que propriétaire du rattrapage, vous n'avez plus besoin d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension à partir de l'environnement classique.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez la même procédure pour demander une extension pour un élément vulnérable d'application, un élément vulnérable de conteneur, un groupe de résultats de test et une tâche de rattrapage.

Procédure

1. Accédez à la **Espaces de travail** > **Espaces de travail du gestionnaire de vulnérabilité**.
2. Sélectionnez Listes.
3. Sous Éléments vulnérables de l'hôte, sélectionnez **Tous**.
4. Filtrez la liste en sélectionnant Différé dans la colonne État.
5. Sélectionnez un élément vulnérable différé.

> **Remarque :** Le bouton Demande d'extension n'est visible que lorsque l'état de l'élément vulnérable est Différé.

6. Cliquez sur le bouton **Demande de prolongation** .
7. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle l'élément vulnérable différé doit être prolongé pour le rattrapage.
Motif	Entrez la raison du report du problème. Les choix sont les suivants : ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre
Information supplémentaire	Saisissez toute autre information pertinente.

8. Sélectionnez **Demande d'extension**.
   Un e-mail est déclenché lors de l'envoi de la demande et de l'action ultérieure de l'approbateur.

> **Remarque :**
> ◦ La demande passe par deux niveaux d'approbation.
> ◦ Si un élément vulnérable différé est à nouveau étendu, le nombre de reports d'extension augmente dans le back-end.

9. Une fois la demande approuvée, les notes Jusqu'à, Motif et Report sont mises à jour.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations de référence pour Vulnerability Manager Workspace

Les rubriques suivantes vous fournissent des liens, des informations de référence, ainsi que des données de champ sur les formulaires et les enregistrements disponibles dans les espaces de travail Vulnerability Manager.

Champs du formulaire Créer une rubrique de surveillance

La table suivante décrit les champs du formulaire Créer une rubrique de surveillance dans l'espace de travail du gestionnaire de vulnérabilité.

Champ	Description
Nom	Nom de votre rubrique de surveillance, par exemple `VI critiques`.
Propriété de	Nom de l'utilisateur propriétaire de la rubrique de visualisation.
Ordre d'affichage	Entrez une valeur comprise entre 100 et 1 000. 100 est la valeur par défaut. Les valeurs inférieures commençant par 100 sont affichées par ordre croissant dans les listes.
Groupe propriétaire	Nom du groupe propriétaire de la rubrique de surveillance.
Actif	Activez ou désactivez la rubrique de visualisation. Il est sélectionné par défaut (Actif).
Liste de surveillance	Ajoutez les noms des utilisateurs qui reçoivent des notifications et peuvent afficher la rubrique de visualisation.
Description	Texte qui décrit votre rubrique de visualisation. Ce texte s'affiche dans le champ Description lorsque vous créez un effort de rattrapage à partir de cette rubrique de surveillance.
Catégorie	Type d'enregistrement pour lequel la rubrique de surveillance est créée. **Remarque :** Le champ **Catégorie** apparaît à partir de la version 18.0.
Aperçu	Cliquez sur **Aperçu** pour afficher une liste du nombre d'enregistrements renvoyés par vos conditions de filtre. **Remarque :** À partir de la version 18.0, le bouton **Aperçu** n'est plus disponible.

Information associée

Créer une rubrique de surveillance dans Vulnerability Manager Workspace

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire d'exception de demande GRC

La table suivante répertorie la description des champs du formulaire d'exception de demande GRC.

Formulaire Demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si aucune politique n'est sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date de début de l'exception. La valeur par défaut est la date du jour. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert. **Remarque :** Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale (jours) de l'exception** que vous avez définie pour la politique dans Politique et conformité. Pour plus d'informations, reportez-vous à la section Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ doit être renseigné par le propriétaire du rattrapage.

Générer des champs de formulaire de synthèse de rattrapage

La table suivante répertorie les champs du formulaire Générer une synthèse de rattrapage.

Générer des champs de synthèse de rattrapage

Champ	Description
Case à cocher Actif	Cette case à cocher est activée par défaut. Si vous ne souhaitez pas envoyer de notifications par e-mail, désactivez ce champ.
Exécuter	L'option hebdomadaire est la valeur par défaut. Choisissez une option dans la liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Générer des champs de synthèse de rattrapage (suite)

Champ	Description
Jour	Lundi est la valeur par défaut. Choisissez une option dans la liste.
Heure	Fixez une heure pour la remise des e-mails. Sélectionnez un fuseau horaire si vous voulez un fuseau horaire différent de celui utilisé par l'instance exécutant la tâche.

Impact des contrôles compensatoires sur le score de risque et la date d'expiration

À partir de la version 20.0 de Vulnerability Response, en tant que propriétaire de rattrapage, vous pouvez demander une réduction des risques pour un élément vulnérable de l'hôte ou une tâche de rattrapage. Le responsable ou l'analyste des vulnérabilités peut également approuver ces demandes de réduction des risques.

Pour plus d'informations sur la façon de demander une réduction des risques et d'approuver l'approbation de réduction des risques, consultez Demander une réduction du risque dans le Espace de travail de remédiation IT respectivement et Approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilités

Lorsqu'une demande de réduction des risques est approuvée, le score des risques est réduit en fonction de la **valeur souhaitée** (cote de risque) dans l'enregistrement d'approbation du changement d'état (VCA#). Le score de risque le plus élevé de la cote de risque souhaitée est affecté à l'enregistrement lorsque votre demande de réduction des risques est approuvée. L'exemple suivant montre comment le score de risque et le score de risque d'origine sont mis à jour lorsque des contrôles de compensation sont appliqués. Les scores de risque les plus élevés par défaut des évaluations de risque sont utilisés dans l'exemple suivant.

Impact des contrôles compensatoires sur le score de risque et le score de risque d'origine

Scénario	Cote de risque	Score du risque	Score de risque d'origine (score de risque calculé)
Données antérieures à la version 20.0	2 : élevé	80	Le champ n'est pas disponible avant la version 20.0.
Après la mise à niveau vers la version 20.0	2 : élevé	80	Zéro
Le score de risque calculé passe à 90 pendant l'ingestion	1 - Critique	90	Zéro
Lorsque vous appliquez des contrôles de compensation	3 : moyen	69	90
Le score de risque calculé passe à 70 pendant l'ingestion	3 : moyen	69	70

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Impact des contrôles compensatoires sur le score de risque et le score de risque d'origine (suite)

Scénario	Cote de risque	Score du risque	Score de risque d'origine (score de risque calculé)
Le score de risque calculé passe à 50 pendant l'ingestion	3 : moyen	50	50
Le score de risque calculé passe à 80 pendant l'ingestion	3 : moyen	50	80
Lorsque les contrôles de compensation expirent le **Date de fin pour la réduction du risque**	2 : élevé	80	Zéro

Impact des contrôles compensatoires sur une tâche de rattrapage

Lorsque votre demande de réduction des risques est approuvée pour une tâche de rattrapage, l'impact des contrôles compensatoires sur ses éléments vulnérables est le suivant :

- Les contrôles de compensation appliqués à la tâche de rattrapage sont appliqués à ses éléments vulnérables (autres que ceux à l'état Fermé) dont le score de risque est supérieur au score de risque correspondant à la **valeur souhaitée** dans l'approbation de changement d'état d'une tâche de rattrapage. Et le score de risque de ces éléments vulnérables est réduit en fonction de la **valeur souhaitée**.
- La **date de fin pour la réduction du risque** reste inchangée pour les éléments vulnérables sur lesquels un contrôle compensatoire est déjà appliqué. Elle n'est pas mise à jour avec la **date de fin pour la réduction du risque** de la tâche de rattrapage.
- La **date de fin pour la réduction du risque** n'est étendue aux éléments vulnérables que lorsqu'un contrôle compensatoire n'est appliqué à aucun élément vulnérable auparavant. Si vous appliquez à nouveau les contrôles compensatoires sur la tâche de rattrapage, la **Date de fin pour la réduction du risque** n'est pas reportée sur les éléments vulnérables, car la **date de fin existante pour la réduction du risque** des éléments vulnérables est prioritaire.
- Lorsqu'un nouvel élément vulnérable est ajouté à une tâche de rattrapage à laquelle des contrôles compensatoires sont déjà appliqués, le risque n'est pas réduit à l'élément vulnérable.

Impact d'un contrôle compensatoire sur un élément vulnérable

Lorsque votre demande de réduction des risques est approuvée pour un élément vulnérable :

- Lenouveau score de risque s'affiche dans le champ **Score de risque** et l'ancien score de risque (score de risque calculé) est déplacé vers le champ **Score de risque d'origine** . Ce changement est en vigueur jusqu'à la date spécifiée dans le champ **Date de fin pour la réduction du risque** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lorsqu'un élément vulnérable a déjà des contrôles de compensation appliqués, lors de l'ingestion:
  - Si le score de risque calculé est supérieur au score de risque, le score de risque reste le même et le score de risque d'origine est mis à jour avec le score de risque calculé.
  - Si le score de risque calculé est inférieur au score de risque, le score de risque et le score de risque d'origine sont mis à jour avec le score de risque calculé.
- En cas de modification d'un élément de configuration(CI) pour un élément vulnérable pour lequel un contrôle de compensation est déjà appliqué :
  - Le CI est mis à jour pour un élément vulnérable par défaut, car la *sn_sec_cmn.update_on_ci_change* propriété système est définie sur vrai.

    Le contrôle de compensation est toujours applicable pour l'élément vulnérable.
  - L'élément vulnérable est fermé et un nouvel élément vulnérable est créé si la *sn_sec_cmn.update_on_ci_change* propriété système est définie sur false.

    Le contrôle compensatoire appliqué à l'ancien élément vulnérable est appliqué au nouvel élément vulnérable et la **date de fin pour la réduction du risque**, le **score de risque d'origine** et le **score de risque** restent les mêmes.
- Lorsqu'un élément vulnérable est rouvert par le scanner et qu'un contrôle de compensation lui est déjà appliqué, le même contrôle de compensation est appliqué après sa réouverture.

Information associée

Comprendre les contrôles compensatoires pour la réduction des risques

Ajouter un contrôle de compensation à la bibliothèque

Associer les contrôles compensatoires aux CVE ou aux TPE pour les demandes de réduction des risques

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

#unique_126_Connect_42_li-risk-reduction-vmws

Espace de travail de remédiation IT

Les équipes informatiques affichent les tâches et informations centrées sur l'informatique, telles que les solutions et les éléments de configuration affectés. Les équipes informatiques peuvent gagner du temps dans la résolution des vulnérabilités en créant facilement des demandes de changement, en analysant à nouveau les éléments vulnérables et en soumettant des demandes d'exception à partir de l'espace de travail de remédiation informatique.

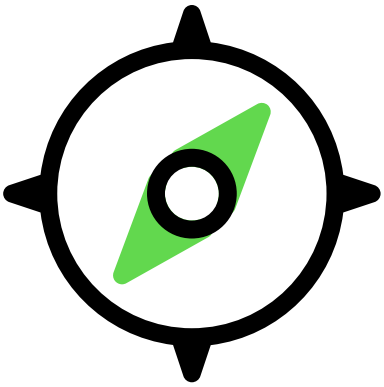
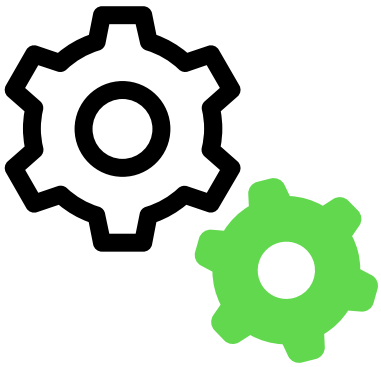
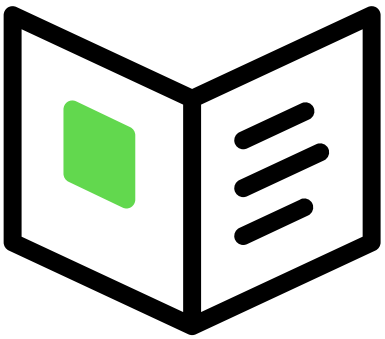
Vue d'ensemble

v18.0 Démo de l'espace de travail de remédiation informatique

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Premiers pas

Explorer	Corriger	Référence
		
En savoir plus sur l'espace de travail de remédiation informatique	Apprenez à corriger des vulnérabilités et des erreurs de configuration à partir de l'espace de travail de remédiation informatique	En savoir plus sur les informations supplémentaires requises pour utiliser l'espace de travail de remédiation informatique

Dépannage et demande d'aide

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

Exploration de l'Espace de travail de remédiation IT

Le Espace de travail de remédiation IT est destiné aux propriétaires de rattrapage informatique et aux groupes informatiques. Il est composé de vues d'accueil et de listes, ainsi que de visualisations de données sur lesquelles vous pouvez cliquer et qui vous permettent de voir les tâches de rattrapage qui vous ont été affectées et le nombre d'enregistrements qui vous sont affectés et qui ont des solutions.

Rôle requis : sn_vul.remediation_owner, sn_vul.app_security_champion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il Espace de travail de remédiation IT se compose des pages de destination, listes et formulaires suivants :

Page de destination (accueil)

La page de destination Accueil se compose d'une liste des tâches de rattrapage qui vous sont affectées et des enregistrements qui vous sont affectés et qui ont des solutions.

Vous pouvez cliquer sur une tâche de rattrapage pour afficher les détails et démarrer une enquête. Dans la vue Listes, vous pouvez afficher les efforts de rattrapage, les tâches de rattrapage, les éléments vulnérables, les résultats des tests de configuration, etc. Vous pouvez ouvrir une tâche de rattrapage et cliquer sur **M'affecter** pour vous affecter la tâche et commencer l'examen.

Remarque : Si vous ne vous affectez pas la tâche dans la tâche de rattrapage, vous ne pouvez afficher aucune action d'interface utilisateur au niveau de l'élément vulnérable.

Cliquez sur les ellipses More Actions (Actions supplémentaires), puis sur **Start Investigation (Démarrer l'examen**) pour résoudre une tâche de rattrapage.

Un tableau de résultats supplémentaire, **CI vulnérables** , s'affiche dans la vue d'accueil. La visualisation des données CI vulnérables vous montre les éléments de configuration qui ont des VI qui vous sont affectés ou qui sont affectés à vos groupes. Consultez Affichez les éléments de configuration présentant des vulnérabilités dans le Espace de travail de remédiation IT pour plus d'informations.

La page qui s'affiche contient les informations suivantes :

- Tâches de rattrapage actives qui vous sont affectées.
- Enregistrements qui vous sont affectés et qui ont des solutions préférées.
- Liste des tâches de rattrapage qui vous sont affectées.

Pour plus d'informations sur ce que vous pouvez faire à partir de cette page, reportez-vous à la section Utiliser les enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT.

Page Tableaux de bord

La page Tableaux de bord comprend le tableau de bord Rattrapage de vulnérabilité. Pour en savoir plus sur la page Tableaux de bord, reportez-vous à la section Vue d'ensemble des tableaux de bord.

Page de liste

Cette vue se compose de pages de liste personnalisées et par défaut pour les tâches de rattrapage, les éléments vulnérables, les solutions et les demandes d'exceptions qui vous sont affectés.

- Listes : listes par défaut pour les tâches de remédiation, les éléments vulnérables de l'hôte, les éléments vulnérables de l'application, les éléments vulnérables du conteneur et les résultats des tests de configuration qui vous sont affectés, à vous et à votre groupe, les solutions et les demandes d'exception.
- Mes listes : cette vue affiche toutes les listes que vous avez renommées à partir de la page de destination Liste et toutes les listes que vous créez.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La vue de liste affiche des liens vers les travaux qui vous sont affectés, à vous et à vos groupes, les éléments vulnérables qui vous sont affectés à vous et à vos groupes, les solutions et vos demandes d'exception.

Vous pouvez également créer vos propres listes pour vous aider à surveiller la progression de votre rattrapage.

La liste **des CI vulnérables** s'affiche dans la vue de liste. La liste des solutions s'affiche si l'application Gestion des solutions en matière de vulnérabilité est installée. Cette carte vous montre les données de solution, les solutions potentielles et préférées, des fournisseurs tiers concernant vos éléments vulnérables.

Pour plus d'informations sur ce que vous pouvez faire à partir de cette page, reportez-vous à la section Utilisez la vue de liste dans le Espace de travail de remédiation IT.

Affichez un exemple de workflow dans Espace de travail de remédiation IT

Affichez un exemple de workflow de bout en bout dans le Espace de travail de remédiation IT. Découvrez comment les spécialistes informatiques peuvent utiliser l'espace de travail pour surveiller les éléments vulnérables critiques et corriger les vulnérabilités qui leur sont affectées.

Avant de commencer

Rôle requis : sn_vul.remediation_owner, sn_vul.app_security_champion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Procédure

Cliquez sur l'image suivante pour afficher les étapes du workflow.
Démo de l'espace de travail de remédiation informatique

L'image comprend les tâches suivantes :

- À partir de la page d'accueil (page de destination du propriétaire de rattrapage informatique), affichez les tâches de rattrapage qui vous sont affectées. Basculez entre les tâches qui vous sont affectées et celles de votre groupe. Affichez les tâches de rattrapage qui disposent de solutions.
- Cliquez sur la vue **de liste** pour afficher les listes des tâches qui vous sont affectées.
- Dans la vue de liste avec la liste **Affecté à mon groupe** sélectionnée, identifiez et affectez-vous le travail.
- Sur un enregistrement de tâche de rattrapage ouvert :
  - Cliquez sur l'onglet **Vue d'ensemble** pour afficher les éléments vulnérables (VI) et les éléments de configuration (CI) affectés qui sont associés à l'enregistrement.
  - Cliquez sur l'onglet **Solutions** pour afficher les solutions préférées et potentielles.
  - Cliquez sur l'onglet **Détails** pour modifier les champs modifiables.
  - Cliquez sur les actions d'interface utilisateur : **Marquer comme faux positif**, **Créer un changement**, **Fractionner la tâche**, **Demande d'exception**. Suivez les invites dans les boîtes de dialogue pour vous aider dans votre rattrapage.

Vue d'ensemble des tableaux de bord

La page Tableaux de bord de fournit Espace de travail de remédiation IT le tableau de bord de rattrapage de vulnérabilité dans l'interface Next Experience utilisateur qui peut être utilisé pour se concentrer sur les tâches de rattrapage et les éléments vulnérables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En tant que propriétaire du rattrapage (sn_vul.remediation_owner), vous pouvez accéder au tableau de bord **du rattrapage des vulnérabilités** en naviguant vers **Espaces de travail** > **Espace de travail de remédiation informatique** et en sélectionnant l'icône Tableaux de bord. Pour en savoir plus sur le tableau de bord Rattrapage des vulnérabilités, reportez-vous à la section Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.

Vous pouvez créer un tableau de bord personnalisé en sélectionnant ⋮ d'options et en sélectionnant **Créer un nouveau tableau de bord**.

Utilisation du Espace de travail de remédiation IT

L'espace de travail de remédiation informatique fournit une liste consolidée des vulnérabilités de l'hôte, des applications et des conteneurs ainsi que des erreurs de configuration qui vous sont affectées, à vous et à votre groupe. Vous pouvez utiliser cet espace de travail pour corriger et demander des exceptions pour les vulnérabilités et les erreurs de configuration.

Utiliser la synthèse d'e-mail dans les espaces de travail Vulnerability Response

Utilisez les notifications par e-mail pour afficher la progression de votre rattrapage et vous rappeler quand les tâches approchent ou dépassent le SLA.

Avant de commencer

Rôle requis : sn_vul.remediation_owner, sn_vul.app_security_champion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Pourquoi et quand exécuter cette tâche

En tant que propriétaire du rattrapage, entrez dans votre zone de travail et consultez votre notification par e-mail comme un résumé de votre travail. Voyez ce que vous avez accompli, ce qui s'en vient et ce qui est en retard. Utilisez la notification pour vous aider à organiser et à classer par ordre de priorité vos actions de rattrapage critiques. Cliquez sur un lien dans l'e-mail pour accéder directement à votre espace de travail. Les notifications peuvent aider les spécialistes informatiques à avoir un aperçu de l'état de leur travail. En tant que gestionnaire des vulnérabilités, aidez vos spécialistes informatiques à accéder à la plateforme directement à partir de leur service de messagerie pour les tâches de correction.

Pour en savoir plus sur la configuration de cette fonctionnalité, reportez-vous Configurer des notifications par e-mail dans les Réponse aux vulnérabilités espaces de travail à la section .

Par défaut, l'e-mail affiche les tâches que vous avez fermées, le nombre total de tâches actives qui vous sont affectées, à vous et à vos groupes, les tâches nouvellement affectées, les VIT fermés, ainsi que d'autres informations.

Procédure

1. Accédez à votre e-mail, localisez une notification et cliquez dessus pour l'ouvrir.
   La notification s'affiche avec des informations sur l'état de votre travail.
2. Cliquez sur **Accéder à l'espace de travail** pour accéder à votre zone de travail.

Utilisez la vue de liste dans le Espace de travail de remédiation IT

Avec la vue de liste de , Espace de travail de remédiation ITvous pouvez afficher les tâches de rattrapage et les enregistrements qui vous sont affectés, à vous et à vos groupes. Vous pouvez également suivre vos demandes d'exception et de faux positifs pour les tâches de rattrapage, les éléments vulnérables et les résultats des tests, et afficher les solutions.

Avant de commencer

Rôle requis :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte (VIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de l'application (AVIT)
- sn_vul.app_security_champion pour les éléments vulnérables du conteneur (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (TR)

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
2. Cliquez sur l'icône Liste.
   La vue de liste s'affiche.
   - Cliquez sur une liste filtrée pour afficher le nombre total de tâches ou d'enregistrements de rattrapage actifs affectés à vous ou à votre groupe. Consultez Utiliser les enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT pour plus d'informations sur ce que vous pouvez faire à partir de ces enregistrements.
   - Affichez le nombre total de VI qui vous sont affectés ou qui sont affectés à vos groupes qui disposent de solutions. Cliquez sur les **solutions préférées sur la carte des VI** pour afficher la liste.
   - Consultez les CI vulnérables qui vous sont affectés, ainsi qu'à vos groupes et qui présentent des vulnérabilités, dans l'onglet **CI vulnérables** ou dans la vue de listes des CI vulnérables qui vous sont affectés, ainsi qu'à votre groupe.
3. Facultatif : Cliquez sur **Mes Listes**.

   (Optional) Pour créer une liste, procédez comme suit :

   a. En bas à gauche de la page, cliquez sur **Nouvelle liste**.

   b. Dans le modal Nouvelle liste, cliquez sur **Démarrer à partir de l'élément existant** et recherchez dans la liste de choix de liste une liste existante à utiliser comme modèle.

   c. Modifiez le nom de la liste.

   d. Ajoutez des filtres.
   Par exemple, vous souhaiterez peut-être créer une liste d'éléments vulnérables actifs pour un scanner particulier que vous souhaitez surveiller. Par exemple, vous pouvez utiliser les filtres : `Actif est vrai` et `Source contient (nom de votre scanner).`

   e. Modifiez les colonnes que vous souhaitez afficher dans votre liste.

   f. Cliquez sur **Créer**.
   Votre nouvelle liste s'affiche.

   g. Vous pouvez également cliquer sur **Créer le vôtre**, entrer un nom, puis **sélectionner la source**.

   h. Commencez à saisir du texte dans le champ et sélectionnez parmi les sources affichées pour votre nouvelle liste.

   i. Cliquez sur **Créer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Votre nouvelle liste s'affiche.

Remarque : Si vous quittez le module de liste, la liste affichée lorsque vous quittez est la liste que vous voyez à votre retour. Pour supprimer les listes personnalisées que vous créez, avec la liste affichée, à droite du volet, cliquez sur l'icône d'engrenage.

4. Reportez-vous à la table suivante pour savoir ce que vous pouvez faire à partir de la vue de liste.

Tâche	Description
Cliquez sur Mes listes	Créez de nouvelles listes et affichez les listes que vous avez créées. Dans la fenêtre modale qui s'affiche, créez une autre version d'une liste existante ou une nouvelle version. Les listes que vous créez s'affichent dans l'onglet Ma liste. Pour supprimer une liste, avec la liste affichée, cliquez sur l'icône en forme d'engrenage située à l'extrême droite de la page.
Vous affecter des enregistrements de tâches de rattrapage	Sous l'onglet **Listes, avec l'option Affecté à mon groupe** sélectionnée, cliquez sur un enregistrement de tâche de rattrapage (VUL) pour l'ouvrir. Sur l'enregistrement qui s'affiche, cliquez sur **M'affecter**. Cette option n'est disponible que si aucune tâche de rattrapage ne vous est déjà affectée.
Ouvrir une tâche de rattrapage (VUL)	Une fois qu'un enregistrement de tâche de rattrapage est affiché, cliquez sur un élément de liste connexe pour ouvrir et afficher les détails suivants : ◦ Vue d'ensemble : affichez la progression du rattrapage et d'autres détails sur les tâches de rattrapage. ◦ Solutions : affichez les solutions préférées et potentielles que vous pouvez utiliser pour corriger la vulnérabilité. Dans l'onglet Solutions, les éléments de liste connexe enfants affichent les solutions préférées et les solutions potentielles. ◦ Détails : plus d'informations sur la vue d'ensemble, y compris la vulnérabilité associée. Vous pouvez modifier ces champs. ◦ Demandes de changement : affichez les demandes de changement associées à l'enregistrement. ◦ Approbations demandées : affichez les approbations demandées. S'il n'y a aucune approbation de demande

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	de changement, cet élément de liste connexe n'est pas affiché. ◦ Approbations de changement de l'état : affichez les demandes de faux positif et d'exception associées à cet enregistrement. S'il n'y a aucune demande, cet élément de liste connexe n'est pas affiché. Les enregistrements ouverts restent affichés sous forme d'onglets jusqu'à ce que vous les fermiez. Voyez Utiliser les enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT ce que vous pouvez faire à partir de l'enregistrement de tâche de rattrapage.
Ouvrir un enregistrement d'élément vulnérable (VIT)	Une fois qu'un enregistrement d'élément vulnérable est affiché, cliquez sur un élément de liste connexe pour ouvrir et afficher les détails suivants : ◦ Vue d'ensemble : l'actif affecté, la vulnérabilité associée, la détection initiale et d'autres détails sur l'état et la date cible. ◦ Détails : plus d'informations sur la vue d'ensemble, y compris la solution privilégiée, le cas échéant. Vous pouvez modifier ces champs. ◦ Détections : premier trouvé, dernier trouvé, adresse IP, port, protocole et informations de preuve, le cas échéant. ◦ Services impactés : criticité opérationnelle, groupe de support et service ◦ Tâches de rattrapage : tâches de rattrapage auxquelles ce VI est associé. Les enregistrements VIT ouverts restent affichés sous forme d'onglets jusqu'à ce que vous les fermiez. Voyez Utiliser les enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT ce que vous pouvez faire à partir de l'enregistrement de tâche de rattrapage.
Définir des filtres pour une colonne d'une liste	Sélectionnez une colonne et développez le menu à points verticaux pour afficher les options qui filtrent davantage les données de la colonne. Par exemple, dans une liste d'éléments vulnérables sélectionnée, vous préférerez peut-être trier la colonne Cote de risque

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	afin que seuls les éléments critiques soient affichés.
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes : ◦ Afficher les éléments correspondants : affiche uniquement les éléments qui correspondent à la cellule sélectionnée dans la colonne. ◦ Filtrer : filtre les éléments de la colonne qui correspondent à la cellule sélectionnée dans la colonne.
Dans la vue de liste, à gauche de la colonne Nombre avec une liste affichée, passez la souris sur une ligne et cliquez sur la petite icône d'information (i) d'un enregistrement.	Les détails des enregistrements sont affichés dans le panneau latéral droit de la page.

Utiliser des enregistrements dans le Espace de travail de remédiation IT

Utilisez des enregistrements pour vous aider à afficher la progression de votre rattrapage et l'impact des éléments vulnérables sur vos actifs.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte (VIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de l'application (AVIT)
- sn_vul.app_security_champion pour les éléments vulnérables du conteneur (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (TR)

Procédure

1. Dans votre Now Platform instance, accédez à **Espaces de travail** > **Espace de travail de remédiation informatique**.
   La page de destination de l'écran d'accueil s'affiche.
2. Accédez à un enregistrement d'élément vulnérable et ouvrez-le à partir de la page de destination Accueil ou de la vue Liste.

   L'onglet Détails comprend des informations dans l'en-tête du formulaire en haut qui se rapportent à la nature de la vulnérabilité, par exemple, `CVE-2013-5014 détectée sur LINUX-DAL-4331`. Sous l'en-tête du formulaire, les valeurs État, Cote de risque et Date cible de rattrapage sont affichées.
3. Consultez la table suivante pour connaître les actions d'interface utilisateur que vous pouvez effectuer sur l'enregistrement de tâche de rattrapage.

Tâche	Description
Cliquer sur un lien d'éléments connexes	◦ Vue d'ensemble : affichez des détails tels que l'état, la cote de risque, le score de risque, la source, le dernier trouvé, l'état

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	du rattrapage, la vulnérabilité associée, l'élément de configuration affecté et les informations de détection initiale. ◦ Détails : plus d'informations sur la vue d'ensemble, y compris la solution privilégiée. Vous pouvez modifier ces champs. ◦ Détections : affichez les informations de détection importées de vos scanners. ◦ Services impactés : affichez les services impactés par la vulnérabilité. ◦ Tâches de rattrapage : affichez les autres tâches de rattrapage associées à cet élément vulnérable. Les enregistrements ouverts à partir de VIT restent affichés sous forme d'onglets sous les onglets d'enregistrement jusqu'à ce que vous les fermiez.
Cliquez sur un lien pour ouvrir un enregistrement.	À partir de la liste affichée sur les enregistrements ouverts à partir des liens des éléments connexes, affichez plus de détails sur les tâches de rattrapage, les détections et les services impactés.
Cliquer sur une action d'interface utilisateur	◦ M'affecter : cette option s'affiche uniquement si la tâche de rattrapage ne vous est pas déjà affectée. ◦ Marquer comme faux positif : signalez lorsqu'un scanner détecte une vulnérabilité, mais que vous déterminez qu'aucune vulnérabilité n'existe. Envoyez une demande. ◦ Si l'élément vulnérable vous est affecté, vous pouvez analyser à nouveau le VI. ◦ Résoudre : résolvez cet élément vulnérable. Les tâches de rattrapage associées passent à l'état Résolu lorsque tous les VI sont Résolus. ◦ Demande d'exception : si une date cible est passée et que vous savez que vous avez besoin de plus de temps pour résoudre la vulnérabilité, soumettez une demande. ◦ Enregistrer : enregistre toutes les modifications et met à jour l'enregistrement.
Ajouter une note de travail ou joindre un fichier	Tout à droite de l'écran, cliquez sur l'icône **Activité** (icône d'allègement) et saisissez une note de travail. Cliquez sur l'icône pour basculer le panneau.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Vous pouvez également charger un fichier.
Définir des filtres pour une colonne d'une liste	Sélectionnez une colonne et développez le menu à points verticaux pour afficher les options qui filtrent davantage les données de la colonne. Par exemple, avec l'élément connexe Détections sélectionné, vous préférerez peut-être trier la colonne de sorte que seules les dernières détections trouvées à partir d'une certaine date soient affichées.
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes : ◦ Afficher les éléments correspondants : affiche uniquement les éléments qui correspondent à la cellule sélectionnée dans la colonne. ◦ Filtrer : filtre les éléments de la colonne qui correspondent à la cellule sélectionnée dans la colonne.

Utiliser les enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT

Les tâches de rattrapage sont créées et affectées automatiquement à partir des efforts de rattrapage. Les équipes informatiques et les propriétaires de rattrapage peuvent afficher les tâches de rattrapage dans le Espace de travail de remédiation IT.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte (VIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de l'application (AVIT)
- sn_vul.app_security_champion pour les éléments vulnérables du conteneur (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Lorsque les gestionnaires et analystes de vulnérabilité créent des efforts de rattrapage pour piloter le rattrapage, les tâches de rattrapage sont créées automatiquement et affectées aux équipes informatiques en fonction du groupe associé aux enregistrements dans un effort de rattrapage.

Consultez les CI vulnérables qui vous sont affectés, ainsi qu'à vos groupes et qui présentent des vulnérabilités, dans l'onglet **CI vulnérables** ou dans la vue de listes des CI vulnérables qui vous sont affectés, ainsi qu'à votre groupe.

Procédure

1. Dans votre Now Platform instance, accédez à **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
   La page de destination de l'écran d'accueil s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Dans la section Tâches de remédiation, cliquez sur un enregistrement de tâche de remédiation (VUL) pour l'ouvrir.
3. Facultatif : Vous pouvez également cliquer sur l'icône Liste en haut à gauche de la page d'accueil pour afficher toutes les tâches de rattrapage et les enregistrements (travail) qui vous sont affectés, à vous et à vos groupes.
   Pour plus d'informations sur l'utilisation de la vue de liste, reportez-vous à la section Utilisez la vue de liste dans le Espace de travail de remédiation IT.
4. À partir de la page d'accueil ou de la vue Liste, cliquez sur un enregistrement de tâche de rattrapage (VUL) pour l'ouvrir.

   L'image suivante montre les sections d'un enregistrement de tâche de rattrapage et les données disponibles.

   Entre les onglets **Solutions** et **Demandes de changement** des onglets de liste connexe affichés dans l'image suivante, vous pouvez cliquer sur l'onglet **Détails** pour mettre à jour certaines des informations de l'enregistrement, telles que le groupe d'affectation, par exemple. Cliquez sur **Enregistrer** pour appliquer vos modifications.

   L'onglet Détails comprend des informations dans l'en-tête du formulaire en haut qui se rapportent à la nature de la tâche, par exemple, `Vulnérabilités sur les serveurs XYZ (San Diego)`. Sous l'en-tête du formulaire, les valeurs d'état, de cote de risque, de groupe d'affectation, d'état du rattrapage et le pourcentage d'enregistrements actifs que vous avez corrigés s'affichent.
5. Consultez la table suivante pour connaître les actions d'interface utilisateur que vous pouvez effectuer à partir de l'enregistrement de la tâche de rattrapage.

Tâche	Description
Cliquez sur un lien d'éléments connexes	◦ Vue d'ensemble : affichez la progression de votre rattrapage avec le pourcentage de VI rattrapés, l'état, la cote de risque, le groupe d'affectation, les CI affectés et d'autres détails sur la tâche. Pour afficher les CI affectés, consultez l'image qui suit le tableau. ◦ Solutions : affichez les solutions préférées et potentielles que vous pouvez utiliser pour corriger la vulnérabilité. Sur l'enregistrement qui s'affiche, les éléments de liste associés enfants affichent les solutions préférées et les solutions potentielles. Voir les images sous le tableau. ◦ Détails : plus d'informations sur la vue d'ensemble, y compris la vulnérabilité associée. Vous pouvez modifier ces champs. ◦ Demandes de changement : affichez les demandes de changement associées à l'enregistrement. ◦ Approbations demandées : affichez les soumissions pour les demandes de changement. S'il n'existe aucune demande

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	d'approbation de changement, cet élément de liste connexe n'est pas affiché. ◦ Approbations de changement de l'état : affichez les demandes de faux positif et d'exception associées à cet enregistrement. S'il n'y a aucune demande, cet élément de liste connexe n'est pas affiché. Les enregistrements ouverts restent affichés sous forme d'onglets jusqu'à ce que vous les fermiez.
Cliquez sur un lien pour ouvrir un enregistrement.	À partir de la liste affichée sur les enregistrements ouverts à partir des liens des éléments connexes, affichez plus de détails sur les enregistrements, les vulnérabilités associées, les CI affectés (actifs), les données de détection, les services impactés et les enregistrements associés.
Cliquer sur une action d'interface utilisateur	◦ M'affecter : cette option s'affiche uniquement si la tâche de rattrapage ne vous est pas déjà affectée. ◦ Marquer comme faux positif : soumettez une demande si, par exemple, un scanner détecte une vulnérabilité, mais que vous déterminez qu'aucune vulnérabilité n'existe. ◦ Créer un changement : vous pouvez créer une nouvelle demande de changement ou ajouter cette tâche de rattrapage à une demande de changement existante. ◦ Fractionner la tâche - Identifiez un sous-ensemble de VI que vous souhaitez inclure dans une nouvelle tâche de rattrapage ◦ Demande d'exception : soumettez une demande si une date cible est passée et que vous savez que vous avez besoin de plus de temps pour résoudre la vulnérabilité. ◦ Résoudre : résoudre ce RT. La tâche de rattrapage passe à l'état Résolu et tous ses VI passent à l'état Résolu. ◦ Enregistrer : enregistrez toutes les modifications et mettez à jour l'enregistrement.
Ajouter une note de travail ou joindre un fichier	Tout à droite de l'écran, cliquez sur l'icône **Activité** (icône d'allègement) et saisissez une note de travail. Cliquez sur l'icône pour basculer le panneau.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Vous pouvez également charger un fichier.
Définir des filtres pour une colonne d'une liste	Sélectionnez une colonne et développez le menu vertical à trois points pour afficher les options qui filtrent davantage les données de la colonne. Par exemple, si l'élément associé à la vue d'ensemble est sélectionné, vous préférez peut-être trier la colonne Cote de risque afin que seuls les éléments critiques s'affichent.
Filtrer une colonne par une ligne sélectionnée	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes : ◦ Afficher les éléments correspondants : affiche uniquement les éléments qui correspondent à la cellule sélectionnée dans la colonne. ◦ Filtrer : filtre les éléments de la colonne qui correspondent à la cellule sélectionnée dans la colonne.

L'onglet Solutions affiche les informations sur les solutions préférées et potentielles qui correspondent le mieux à la vulnérabilité associée à l'enregistrement de tâche. Les solutions sont des correctifs que vos équipes informatiques appliquent pour résoudre les vulnérabilités.

Si l'application Gestion des solutions en matière de vulnérabilité est installée, les solutions privilégiées sont les solutions de remplacement les plus élevées appliquées aux enregistrements. La liste des solutions est basée sur les enregistrements de la tâche de rattrapage.

Pour afficher les solutions, sur l'enregistrement de tâche de rattrapage, accédez à **Solutions** > **Solutions privilégiées**.

Solutions potentielles. Toutes les solutions disponibles pour les VI sur cette tâche. Accédez à la **Solutions** > **Solutions potentielles**.

Vous pouvez afficher les CI (actifs) affectés par cette vulnérabilité sur l'enregistrement de tâche de rattrapage en accédant à **Vue d'ensemble** > **CI affectés**.

Vous affecter une tâche ou un enregistrement de rattrapage dans Espace de travail de remédiation IT

Affectez-vous une tâche de rattrapage (VUL, AVUL, CVUL ou CRG) ou un enregistrement (VIT, AVIT, CVIT ou TR) à vous-même à partir de la page Liste de l'espace Espace de travail de remédiation IT de travail.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte (VIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de l'application (AVIT)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vul.app_security_champion pour les éléments vulnérables du conteneur (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (TR)

Cette option n'est disponible que sur les enregistrements de tâche de rattrapage qui ne vous sont pas déjà affectés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique** > **Vue liste** > **Affecté à mon groupe**.
2. Cliquez sur une tâche de rattrapage (VUL, AVUL, CVUL ou CRG) pour l'ouvrir.
3. Dans les boutons d'action d'interface utilisateur à droite, cliquez sur **Me l'affecter**.

   Le bouton **Me l'affecter n'est** disponible que si l'enregistrement ne vous est pas déjà affecté.

   La tâche de rattrapage figure dans la liste Mes affectations sous Tâches de rattrapage.
4. Vous pouvez également vous affecter un enregistrement (VIT, AVIT, CVIT ou TR) en suivant les mêmes étapes à partir d'un enregistrement ouvert.
   Le bouton **Me l'affecter n'est** disponible que si l'enregistrement ne vous est pas déjà affecté.

Affichez les éléments de configuration présentant des vulnérabilités dans le Espace de travail de remédiation IT

Les améliorations suivantes ont été ajoutées aux tâches de remédiation avec la version 16.1 de l'application Réponse aux vulnérabilités .

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte (VIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de l'application (AVIT)
- sn_vul.app_security_champion pour les éléments vulnérables du conteneur (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (TR)

Le rôle itil ou cmdb_read est également requis si vous souhaitez afficher les données CI dans les espaces de travail.

Pourquoi et quand exécuter cette tâche

Consultez les éléments de configuration (CI) qui vous sont affectés et qui présentent des vulnérabilités. Cliquez sur **Vulnerable CIs scorecard (Tableau de résultats des CI vulnérables**). Cliquez sur la liste Filtres en haut à gauche pour basculer entre **Affecté à moi** et **Affecté à mes groupes**. Dans la vue de liste, cliquez sur les liens.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
   La page de destination de l'écran d'accueil s'affiche.
2. Vous pouvez également afficher ces listes à partir des liens présents dans la vue Liste ou en accédant à leurs modules, par exemple : **Tout** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
3. Choisissez-en un pour continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En fonction de ce qui est sélectionné dans l'activation/désactivation du filtre, affichez les listes des enregistrements suivants qui vous sont affectés ou qui vous sont affectés, à vous et à vos groupes.

Option	Description
Tâche de rattrapage affectée	Tâches de rattrapage (RT). Pour plus d'informations sur les actions que vous pouvez effectuer à partir d'un RT, reportez-vous à la section Utiliser les enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT.
Solution privilégiée sur les VI	Enregistrements auxquels des solutions préférées sont mappées. Si l'application Gestion des solutions en matière de vulnérabilité est installée, les solutions privilégiées sont les solutions de remplacement les plus élevées appliquées aux enregistrements. La liste des solutions est basée sur les enregistrements de l'enregistrement de tâche de rattrapage. Pour voir ce que vous pouvez faire à partir des enregistrements de solution, reportez-vous à la section Utiliser les enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT.
CI vulnérables	(CI)s avec des vulnérabilités. Après son remplissage initial, ce tableau de résultats affiche les nombres mis à jour de vos CI vulnérables après l'ajout de nouveaux éléments vulnérables ou lorsque des changements d'état sont apportés aux VI existants. Consultez les étapes suivantes pour savoir comment afficher cet enregistrement et ce que vous pouvez faire à partir de cette liste.

4. Cliquez sur le tableau **de résultats des CI vulnérables** .

   La liste des enregistrements de CI s'affiche.

5. Cliquez sur un élément de configuration pour ouvrir son enregistrement.
   L'enregistrement s'affiche.

   Les listes connexes vous permettent d'afficher les détails et divers enregistrements connexes. Les nouvelles données disponibles sur cet enregistrement avec cette version comprennent :

   - Chronologie qui affiche l'activité récente sur cet enregistrement.
   - Toutes les demandes de changement associées à ce CI.
   - Naviguez facilement vers les tableaux de résultats et affichez les tâches de rattrapage, les éléments vulnérables et les solutions préférées associés à ce CI.
   - Vouspouvez accéder aux tableaux de résultats et afficher les correctifs préférés associés à ce CI. Les correctifs préférés sont les correctifs associés aux éléments vulnérables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'onglet Correctifs de la liste connexe affiche les correctifs installés et manquants pour les CI.

- Informations sur le CI, y compris la classe, l'emplacement, l'accès sur Internet, l'environnement et le calendrier de maintenance.

Créer une demande de changement dans Espace de travail de remédiation IT

Créez une demande de changement à partir d'une tâche de rattrapage (VUL, CVUL ou CRG). Vous pouvez également ajouter une tâche de rattrapage à une demande de changement existante.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte
- sn_vul.app_security_champion pour les éléments vulnérables du conteneur
- sn_vulc.remediation_owner pour les résultats des tests de configuration

Remarque : Le rôle itli est requis si vous souhaitez soumettre des demandes de changement à partir du Espace de travail de remédiation IT.

Pourquoi et quand exécuter cette tâche

Il peut y avoir différentes raisons pour lesquelles vous souhaitez créer une demande de changement pour une tâche de rattrapage. C'est généralement parce que votre enquête nécessite une intervention manuelle pour corriger les vulnérabilités.

Pour plus d'informations sur les demandes de changement et la création de demandes de changement à partir de l'environnement classique, reportez-vous à la rubrique Gestion des changements pour Réponse aux vulnérabilités.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Sur la page Liste, dans la liste des tâches de rattrapage, recherchez une tâche de rattrapage pour laquelle vous souhaitez créer une demande de changement.
3. Dans les boutons d'action d'interface utilisateur sur la droite, développez la liste et choisissez-en une :
   - Cliquez sur **Créer un changement**
   - **Ajouter au changement existant**
4. Pour créer une demande de changement, renseignez les champs du modal qui s'affiche. Pour plus d'informations sur les champs de formulaire, consultez Créer des champs de formulaire de demande de changement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez **Créer une demande de changement**.
   L'enregistrement de la tâche de rattrapage s'affiche et un message indique que la demande de changement a été créée avec succès.

   Cliquez sur le lien connexe Demandes de changement sur un enregistrement pour afficher toutes les demandes de changement associées à l'enregistrement.

6. Pour ajouter cette tâche de rattrapage à une demande de changement existante, procédez comme suit.

   a. Cliquez sur la flèche vers le bas pour développer la liste sur le bouton **Créer un changement** .

   b. Sélectionnez **Ajouter au changement existant**.

   c. Dans le modal qui s'affiche, cliquez sur l'icône de recherche pour afficher la liste des demandes de changement existantes.

   d. Pour ajouter des conditions à la liste afin de cibler la liste des demandes de changement, cliquez sur l'icône de filtre (entonnoir) dans le coin supérieur droit du modal.

   e. Dans le nouveau volet qui s'affiche, cliquez sur **Vue avancée**.

   f. Utilisez le Créateur de conditions pour créer vos conditions.

   g. Sélectionnez **Mettre à jour**.

   h. Dans la liste, cliquez sur une demande de changement pour la sélectionner.
   Une fenêtre modale mise à jour s'affiche avec votre choix.

   i. Facultatif : Dans le modal, cochez la case Ajouter des CI au CR pour ajouter des éléments de configuration de tous les éléments vulnérables actifs à la demande de changement.

   j. Sélectionnez **Ajouter un changement**.
   L'enregistrement de rattrapage s'affiche et un message indique que la demande de changement a été créée et soumise pour approbation.

   - Cliquez sur le lien **Afficher le changement** dans le message pour ouvrir l'enregistrement de demande de changement (CHG).
   - Sélectionnez le lien de menu **Élément connexe Demandes de changement** sur l'enregistrement de tâche de rattrapage pour afficher toutes les demandes de changement associées à l'enregistrement.

   Alternativement, dans l'environnement classique, accédez à **Libre-service** > **Mes demandes**. Une fois que vous avez soumis le changement et qu'il est implémenté, si la synchronisation d'état est activée, la tâche de rattrapage passe automatiquement à `l'état Résolu`. Pour en savoir plus sur les états et la synchronisation des états dans les demandes de changement, reportez-vous à la section Créer une demande de changement à partir d'une tâche de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fractionner une tâche de rattrapage dans Espace de travail de remédiation IT

À partir d'un enregistrement de tâche de rattrapage, identifiez un sous-ensemble d'éléments vulnérables ou de résultats des tests, puis créez une nouvelle tâche de rattrapage pour ceux-ci.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte (VIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de l'application (AVIT)
- sn_vul.app_security_champion pour les éléments vulnérables du conteneur (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Vous pouvez sélectionner des éléments vulnérables individuels dans la liste affichée dans l'onglet Éléments vulnérables et les déplacer vers une nouvelle tâche de rattrapage.

Les cas d'utilisation de fractionnement de VI de tâches de rattrapage existantes en de nouvelles tâches peuvent inclure les exemples suivants :

- Vous souhaitez créer une demande de changement ou des demandes de changement pour un groupe divisé.
- Vous souhaitez réaffecter un groupe fractionné à un autre utilisateur de votre groupe d'affectation.
- Vous demandez un report ou une exception pour un groupe divisé, car vous savez que certaines vulnérabilités sur des éléments de configuration (CI) spécifiques ne peuvent pas être corrigées avant la date cible.

Pour plus d'informations sur les demandes de changement et le fractionnement d'une tâche de Réponse aux vulnérabilités rattrapage dans l'environnement classique et pour les versions antérieures à la version 15.0, reportez-vous à la section Diviser une tâche de rattrapage.

À partir de la version 19.0 de , vous pouvez diviser les tâches pour les groupes de résultats des Réponse aux vulnérabilitéstests.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

À partir de la version 18.0, vous pouvez diviser les tâches pour les éléments de vulnérabilité d'application et les éléments de vulnérabilité de conteneur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Une fois qu'une tâche de rattrapage est affichée, cliquez sur l'onglet **Éléments vulnérables** , s'il n'est pas déjà sélectionné.
2. Dans la liste, sélectionnez les éléments vulnérables que vous souhaitez déplacer vers une nouvelle tâche de rattrapage.
3. Cliquez sur **Fractionner la tâche**.
4. La boîte de dialogue qui s'affiche, le nombre de VI que vous avez sélectionnés dans la liste s'affiche.
5. Cliquez à nouveau sur **Fractionner la tâche** .
   Le message de confirmation suivant s'affiche avec un lien vers la nouvelle tâche de rattrapage.

   Vous pouvez également utiliser le créateur de conditions pour filtrer les VI.
6. Recherchez une tâche de rattrapage que vous souhaitez diviser.
7. Dans les boutons d'action d'interface utilisateur à droite, cliquez sur **Diviser la tâche**.
   Après quelques instants, le générateur de conditions s'affiche.
8. Dans la fenêtre modale qui s'affiche, utilisez le créateur de conditions pour identifier le sous-ensemble d'éléments vulnérables que vous souhaitez ajouter à une nouvelle tâche de rattrapage.
9. Cliquez sur **Fractionner la tâche**.
   Si un message s'affiche indiquant qu'aucun élément vulnérable ne correspond à vos conditions, vous devez ajuster vos critères et cliquer à nouveau sur **Fractionner la tâche** .
   Modifiez le champ Brève description selon vos besoins. Ce champ peut vous aider à trouver votre nouvelle tâche de rattrapage après sa création.

   Si les VI correspondent à vos conditions, le nombre de VI correspondants s'affiche dans un message, comme illustré dans l'image précédente.
10. Facultatif : Cliquez sur le lien **Visualiser les éléments** pour afficher les VI qui correspondent à vos conditions de filtre.
    La nouvelle tâche de rattrapage s'affiche sous la forme d'un nouvel onglet en haut de l'enregistrement.

Demander un faux positif dans le Espace de travail de remédiation IT

Émettre une demande de faux positif pour un élément vulnérable de l'hôte (VIT), un élément vulnérable de l'application (AVIT), un élément vulnérable du conteneur (CVIT) ou une tâche de rattrapage (VUL, AVUL, CVUL ou CRG) dans le Espace de travail de remédiation IT.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte (VIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de l'application (AVIT)
- sn_vul.app_security_champion pour les éléments vulnérables du conteneur (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Un faux positif est une condition dans laquelle le scanner signale qu'une vulnérabilité existe dans le système, alors qu'en réalité, il n'y a aucune vulnérabilité. Il peut y avoir plusieurs raisons, telles qu'une classification incorrecte, une logique ou un algorithme incorrect dans le scanner.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur la procédure à suivre pour demander un faux positif pour un ensemble de résultats de tests, reportez-vous à la section Demande de faux positif pour un ensemble de résultats des tests.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Localisez une tâche de rattrapage (VUL, AVUL, CVUL ou CRG) ou un élément vulnérable (VIT, AVIT ou CVIT) que vous souhaitez marquer comme faux positif.
3. Dans les boutons d'action d'interface utilisateur à droite, sélectionnez **Marquer comme faux positif**.
4. Dans la boîte de dialogue qui s'affiche, saisissez des informations sur la demande et sélectionnez **Demander l'approbation**.
5. Dans le modal Répondre au questionnaire, répondez aux questions pour fournir des informations supplémentaires sur votre demande à l'approbateur et sélectionnez **Soumettre**.

   Remarque : Le modal Répondre au questionnaire s'affiche uniquement lorsque la case à cocher **Activer le questionnaire pour marquer comme faux positif** est sélectionnée dans le formulaire Configuration de gestion des exceptions. Pour plus d'informations, reportez-vous à Configurer la gestion des exceptions pour Réponse aux vulnérabilités,Configurer la gestion des exceptions pour Réponse aux vulnérabilités des applications, Configurer la gestion des exceptions pour Réponse aux vulnérabilités pour conteneursetConfigurer la gestion des exceptions pour Conformité de la configuration.

   L'état de l'élément vulnérable (VIT, AVIT ou CVIT) ou de la tâche de rattrapage (VUL, AVUL ou CVUL) passe à En cours de révision.

   Votre demande est soumise pour approbation et l'approbateur reçoit une notification par e-mail concernant votre demande.

Résultats

Vous recevrez une notification par e-mail après l'approbation ou le rejet de votre demande.

Que faire ensuite

Dans l'espace de travail de remédiation informatique, sur la page Liste, accédez à **Demandes d'exception** > **Mes demandes** et ouvrez l'enregistrement d'approbation de changement d'état (VCA#) correspondant et vérifiez l'état de votre demande dans la colonne État d'approbation :

État d'approbation	Enregistrement (VIT, AVIT ou CVIT)	Tâche de rattrapage (VUL, AVUL, CVUL ou CRG)
Approuvé	L'état de l'enregistrement passe à Fermé avec le motif comme Faux positif.	L'état de la tâche de rattrapage passe à Fermé avec le motif comme Faux positif. En conséquence, l'état est étendu aux enregistrements de la tâche de rattrapage. Accédez à l'onglet Détails d'une tâche de rattrapage et définissez la date d'expiration du faux positif

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État d'approbation	Enregistrement (VIT, AVIT ou CVIT)	Tâche de rattrapage (VUL, AVUL, CVUL ou CRG)
		dans le champ **Jusqu'à** si nécessaire. La tâche de rattrapage revient à l'état Ouvert après la date spécifiée et l'état est reporté aux résultats des tests.
Rejeté	L'état de l'enregistrement ne change pas.	L'état de la tâche de rattrapage et de ses enregistrements revient à l'état précédent.

Dans le **flux d'activité** d'un enregistrement ou d'une tâche de rattrapage, vous pouvez afficher l'ensemble du workflow de la demande de faux positif.

Information associée

Vue d'ensemble des faux positifs

Demande de faux positif pour un ensemble de résultats des tests

À partir de la version 22.0 de Réponse aux vulnérabilités, vous pouvez émettre une demande de faux positif pour un ensemble de résultats des tests dans le cadre d'une tâche de rattrapage, dans le Espace de travail de remédiation IT.

Avant de commencer

Rôle requis : sn_vulc.remediation_owner

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Sur la page Liste, ouvrez une Conformité de la configuration tâche de rattrapage.
3. Dans l'élément connexe Vue d'ensemble, sous l'onglet Résultats des tests, sélectionnez les résultats des tests que vous souhaitez marquer comme faux positifs.

   Remarque : Vous pouvez demander un faux positif pour un ensemble de résultats des tests dans une tâche de rattrapage uniquement si :

   - Au moins un résultat de test sélectionné est à l'état Actif.
   - La tâche de rattrapage a au moins deux résultats des tests.
   - Tous les résultats des tests ne sont pas sélectionnés.

4. Sélectionnez le bouton **Marquer comme faux positif** dans l'onglet Résultats des tests de configuration.
5. Dans la boîte de dialogue qui s'affiche, saisissez des informations sur la demande et sélectionnez **Demander l'approbation**.
6. Dans le modal Répondre au questionnaire, répondez aux questions pour fournir des informations supplémentaires sur votre demande à l'approbateur et sélectionnez **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le modal Répondre au questionnaire s'affiche uniquement lorsque la case à cocher **Activer le questionnaire pour marquer comme faux positif** est sélectionnée dans le formulaire Configuration de gestion des exceptions. Pour en savoir plus sur la configuration d'un questionnaire, reportez-vous à la section Configurer la gestion des exceptions pour Conformité de la configuration.

Les résultats des tests sélectionnés sont déplacés vers une nouvelle tâche de rattrapage et votre demande est soumise pour approbation. Le numéro de tâche apparaît dans le **flux d'activité** de l'ancienne tâche de rattrapage. L'approbateur reçoit une notification par e-mail au sujet de votre demande.

Résultats

Vous recevrez une notification par e-mail sur l'approbation ou le rejet de votre demande.

Dans le **flux d'activité** d'un résultat de test ou d'une tâche de rattrapage, vous pouvez afficher l'intégralité du workflow de la demande de faux positif.

Que faire ensuite

1. Dans le Espace de travail de remédiation IT, sur la page Liste, accédez à **Demandes d'exception** > **Mes demandes**.
2. Ouvrez l'enregistrement d'approbation de changement d'état correspondant (VCA#) et vérifiez l'état de votre demande dans la colonne État d'approbation :

État d'approbation	Résultat
Approuvé	L'état de la nouvelle tâche de rattrapage passe à Fermé avec le motif comme Faux positif.
Rejeté	L'état de la nouvelle tâche de rattrapage devient Ouvert.

3. Une fois la demande approuvée, accédez à l'onglet Détails de la nouvelle tâche de rattrapage et définissez la date d'expiration du faux positif dans le champ **Jusqu'à** ce que nécessaire.

   La tâche de rattrapage revient à l'état Ouvert après la date spécifiée et l'état est rétrogradé aux résultats des tests.

Demander une exception dans le Espace de travail de remédiation IT

Depuis un enregistrement de tâche de rattrapage, demandez une exception pour une tâche de rattrapage.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte (VIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de l'application (AVIT)
- sn_vul.app_security_champion pour les éléments vulnérables du conteneur (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (TR)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Certaines vulnérabilités peuvent ne pas disposer d'un correctif, d'un correctif ou d'une solution existante. Vous pouvez également déterminer qu'une tâche de rattrapage ne peut pas être résolue à sa date cible. Lorsque votre rattrapage ne peut pas être conforme à une politique, une norme ou une directive de sécurité ou de gestion des vulnérabilités publiée, vous pouvez demander une exception.

Vous pouvez demander des exceptions pour les tâches de rattrapage et les éléments vulnérables à partir de l'espace de travail de remédiation informatique qui vous sont affectés.

À partir de la version 19.0 de , vous pouvez demander des exceptions pour les résultats des Réponse aux vulnérabilitéstests.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

À partir de la version 18.0, vous pouvez demander des exceptions pour les éléments de vulnérabilité d'application et les éléments de vulnérabilité de conteneur.

Pour plus d'informations sur la demande d'exceptions dans l'environnement classique, reportez-vous à la section Demander une exception pour une tâche de rattrapage.

Procédure

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
2. Localisez une tâche de rattrapage pour laquelle vous souhaitez demander une exception.
3. Dans les boutons d'action d'interface utilisateur à droite, cliquez sur **Demande d'exception**.
4. Dans la boîte de dialogue qui s'affiche, renseignez la date de fin de l'exception, sélectionnez un motif dans la liste et ajoutez toute autre information requise.
5. Cliquez sur **Demander une exception**.
6. Dans le modal **Répondre au questionnaire** , répondez aux questions et cliquez sur **Soumettre**.

   Remarque : À partir de la version 18.0, vous pouvez répondre au questionnaire pour fournir des informations supplémentaires sur votre demande d'approbation. Le modal **Répondre au questionnaire** s'affiche uniquement lorsque la case à cocher **Activer le questionnaire pour demander une exception** est cochée dans le formulaire **Configuration de gestion des exceptions** .

   Un message s'affiche indiquant que votre demande a été soumise avec succès pour approbation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une demande d'exception pour une tâche de rattrapage est approuvée à l'aide d'un workflow d'approbation à deux niveaux par défaut. Une fois la demande approuvée par l'approbateur de niveau 1, elle est envoyée à l'approbateur de niveau 2.

- L'enregistrement de tâche de rattrapage ou VI passe à l'état En cours de révision lorsque la demande d'exception est ouverte.
- L'enregistrement de tâche de rattrapage ou le VI passe à l'état Différé si la demande est approuvée.
- L'enregistrement de la demande d'exception est fermé une fois votre demande d'exception approuvée.

Pour afficher l'état de vos demandes d'approbation, sous Demandes d'exception sur la page Liste, cliquez sur **Mes demandes**. Le numéro de la demande (VCA#) s'affiche lorsque vous ouvrez l'enregistrement du VI ou de la tâche de rattrapage à partir de la liste.

- Si la demande est rejetée, l'enregistrement de demande (VCA#) affiche **Rejeté** dans la colonne État d'approbation de votre vue de liste sous Mes demandes.
- Vous devez soumettre une nouvelle demande d'exception si vous souhaitez toujours différer cet élément.

Demander une exception à l'aide GRC : gestion de la politique et de la conformité de Espace de travail de remédiation IT

Demandez une exception de politique pour l'élément vulnérable de l'hôte (VIT), l'élément vulnérable de l'application (AVIT), l'élément vulnérable du conteneur (CVIT) ou la tâche de rattrapage (VUL, AVUL, CVUL ou CRG) à partir du Espace de travail de remédiation IT.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables de l'hôte (VIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de l'application (AVIT)
- sn_vul.app_security_champion pour les éléments vulnérables du conteneur (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 19.0	Terminologie à partir de la version 19.0
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de tests

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Dans le navigateur d'application, sélectionnez l'icône de liste ( ).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sur la page Liste, sous Éléments vulnérables d'hôte, Éléments vulnérables d'applications, Éléments vulnérables de conteneurs ou Tâches de remédiation, sélectionnez l'enregistrement pour lequel vous souhaitez demander une exception.
   L'enregistrement que vous sélectionnez doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
4. Cliquez sur le bouton **Demander une exception** .
5. Renseignez les champs du formulaire.
   Pour plus d'informations sur les champs de formulaire, consultez Champs du formulaire Demande d'exception pour les exceptions de politique.
6. Sélectionnez **Demander une exception**.
7. Dans le modal Répondre au questionnaire, répondez aux questions pour fournir des informations supplémentaires sur votre demande et sélectionnez **Soumettre**.

   Remarque : Le modal Répondre au questionnaire s'affiche uniquement lorsque les détails du questionnaire sont ajoutés au registre d'intégration respectif.

   Un message s'affiche indiquant que votre demande a été soumise avec succès pour approbation.

   Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez la configuration facultative de Gestion de la politique et de la conformité .

Demander une réduction du risque dans le Espace de travail de remédiation IT

À partir de la version 20.0 de , vous pouvez demander la réduction du risque pour un élément vulnérable de Réponse aux vulnérabilitésl'hôte ou une tâche de rattrapage dans le Espace de travail de remédiation IT.

Avant de commencer
Rôle requis : sn_vul.remediation_owner

Pourquoi et quand exécuter cette tâche
A partir de la v21.0 de Réponse aux vulnérabilités:

- Vous pouvez demander une réduction des risques pour une tâche de rattrapage si ses éléments de vulnérabilité sont associés à une même entrée de vulnérabilité commune (CVE) ou à une entrée tierce (TPE) pour laquelle la réduction du risque est activée.
- Vous ne pouvez pas demander une réduction du risque pour une tâche de rattrapage avec des éléments vulnérables associés à différentes CVE, même si la réduction du risque est activée pour les CVE.

Remarque : La fonctionnalité de contrôles de compensation n'est disponible que pour les vulnérabilités de l'hôte.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Sur la page Liste, ouvrez un élément vulnérable d'hôte ou une tâche de rattrapage.
3. Sélectionnez le menu à trois points et sélectionnez **Demande d'exception**.
4. Renseignez les champs de la fenêtre contextuelle Demande d'exception.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modal de demande d'exception

Champ	Description
Motif	Motif de votre demande d'exception. Sélectionnez *le contrôle d'atténuation en place pour la demande de* réduction des risques. Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à la section Définir le mappage de motif de politique.
Demande de report	Différer l'enregistrement. Ce champ est sélectionné par défaut. **Remarque :** Ce champ s'affiche uniquement lorsque l'option *Contrôle d'atténuation en place* est sélectionnée dans le champ **Motif** .
Demande de réduction des risques	Vous permet de demander la réduction du score de risque. **Remarque :** Cette case à cocher s'affiche uniquement lorsque l'option *Contrôle d'atténuation en place* est sélectionnée dans le champ **Motif** .
Cote de risque actuelle	Gravité actuelle du risque. **Remarque :** Ce champ s'affiche uniquement lorsque la case **Demande de réduction des risques** est cochée.
Cote de risque souhaitée	Nouvelle cote de risque que vous souhaitez affecter à l'enregistrement. Le score de risque le plus élevé dans cette plage de cote de risque est appliqué à l'enregistrement lorsque votre demande est approuvée. **Remarque :** Ce champ s'affiche uniquement lorsque la case **Demande de réduction des risques** est cochée.
Sélectionner les contrôles de compensation	Motif de votre demande de réduction de la cote de risque.
Jusqu'à	Date d'expiration de la demande de report ou de réduction de risque. Quand la demande d'exception expire :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ L'enregistrement revient à l'état Ouvert. ◦ Les contrôles compensatoires expirent. ◦ Le score calculé sera à la place d'un score réduit.
Notes de justification	Détails liés à la raison pour laquelle cette demande est effectuée.

5. Sélectionnez **Demander une exception**.
6. Dans le modal Répondre au questionnaire, répondez aux questions pour fournir des informations supplémentaires sur votre demande et sélectionnez **Soumettre**.

   Remarque : Le modal Répondre au questionnaire s'affiche uniquement lorsque le questionnaire est activé pour la gestion des exceptions. Pour plus d'informations, consultez Configurer la gestion des exceptions pour Réponse aux vulnérabilités.

   Un message s'affiche indiquant que votre demande a été soumise avec succès pour approbation. Une notification de votre demande est envoyée à l'approbateur.

   - Si vous demandez un report et une réduction du risque :
     - Deux approbations de changement d'état (VCA#) sont créées pour le report et la réduction du risque.
     - L'état de l'enregistrement devient En cours de révision.
   - Si vous demandez une réduction des risques uniquement :
     - Une approbation de changement d'état (VCA#) est créée.
     - L'état ne change pas.

   Une notification est approuvée ou rejetée de votre demande.

   Pour en savoir plus sur la façon dont la **date de fin de la réduction du risque** est mise à jour pour une tâche de rattrapage et l'élément vulnérable lorsqu'une demande de réduction des risques est approuvée, reportez-vous à Impact des contrôles compensatoires sur le score de risque et la date d'expiration.

Que faire ensuite

Vous recevez une notification lorsque votre demande est approuvée ou rejetée par l'approbateur. Pour en savoir plus sur le processus d'approbation, reportez-vous Approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilitésà .

Information associée

Comprendre les contrôles compensatoires pour la réduction des risques

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

Ajouter un contrôle de compensation à la bibliothèque

Impact des contrôles compensatoires sur le score de risque et la date d'expiration

Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Lancez de nouvelles analyses à Espace de travail de remédiation IT partir de votre Now Platform service à la demande.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, vos correctifs et vos autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

La nouvelle analyse est prise en charge pour les intégrations suivantes dans le Espace de travail de remédiation IT. Consultez les rubriques suivantes pour plus d'informations :

- Analyser Qualys à nouveau les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail
- Analyser Rapid7 à nouveau les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail
- Analyser Tenable.io à nouveau et Tenable.sc les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail

Rôles requis : sn_vul.remediation_owner pour le Espace de travail de remédiation IT.

Analyser Qualys à nouveau les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Lancez de nouvelles analyses du Qualys produit à la demande depuis Espace de travail de remédiation IT votre Now Platform instance.

Avant de commencer

Pour lancer une nouvelle analyse du produit à Qualys partir de l'environnement classique, reportez-vous à la section Lancer une nouvelle analyse pour le Qualys Vulnerability Integration.

Les Qualys scanners sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Ré-analyse** n'est pas disponible.

Pour activer ces analyseurs, en tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin :

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Localisez le produit de scanner que vous souhaitez activer et cliquez sur l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher Activé.
4. Cliquez sur **Mettre à jour**.

   Le produit que vous avez activé s'affiche dans le champ Source sur les enregistrements d'éléments vulnérables et de tâches de rattrapage après la prochaine importation, et **l'action Analyser de nouveau** est disponible.

Pour plus d'informations sur la configuration de votre Qualys scanner, reportez-vous aux sections Configurer des dispositifs de scanner et Configurations et modifications avancées de Qualys.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous pouvez lancer de nouvelles analyses à la demande pour les éléments vulnérables et les tâches de rattrapage qui ont le Qualys produit comme source dans Espace de travail de remédiation IT votre Now Platformfichier .
- Sur un enregistrement de tâche de **rattrapage**, l'enregistrement peut être dans n'importe quel état autre que Fermé et tous les VI associés doivent provenir du Qualys produit.
- Pour lancer de nouvelles analyses dans IT Remediation Workspace à partir d'enregistrements d'éléments vulnérables et de tâches de rattrapage, ces enregistrements doivent vous être affectés.

Rôles requis :

- sn_vul.remediation_owner pour le Espace de travail de remédiation IT.
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin dans Vulnerability Manager Workspace.

Procédure

1. Accédez à un élément vulnérable ou à une tâche de rattrapage qui vous a été affectée et ouvrez-le.

   Remarque : Si vous choisissez un effort de rattrapage pour lancer une nouvelle analyse, tous les éléments vulnérables associés à cet enregistrement sont analysés.

2. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**.
3. Dans la fenêtre modale Analyser de nouveau, choisissez un profil d'option.
   Un profil d'option est requis lorsque vous lancez une Qualys analyse à partir de votre Now Platform® fichier . Les profils d'option contiennent Qualys des paramètres d'analyse.

Option	Description
Utiliser le profil d'option par défaut	Il s'agit du profil d'option défini par défaut pour l'instance d'intégration. Vous sélectionnez ce profil lors de la configuration de votre Qualys scanner. Consultez Configurer des dispositifs de scanner pour plus d'informations.
Spécifier le profil d'option	Dans la liste Profil d'option, choisissez un profil à utiliser pour l'analyse. Vous pouvez sélectionner le profil d'option que vous souhaitez utiliser pour les analyses afin de faire correspondre les éléments de configuration.

4. Dans la fenêtre modale Analyser de nouveau, cliquez sur **Demander une nouvelle analyse**.
   Le message « `La demande d'analyse est en cours de traitement` » s'affiche.
5. Cliquez sur le lien **Afficher l'état** dans le message pour afficher la progression de l'analyse.

   L'enregistrement d'analyse (VSCAN#) s'affiche. Sous l'en-tête de l'enregistrement avec le numéro d'analyse, les listes d'éléments connexes affichent les informations suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La liste Détails affiche le numéro d'analyse de l'analyse parente, la source de l'analyse et l'état. Affichez les analyses terminées et échouées dans la section Synthèse de l'analyse.
- La liste Analyses affiche toutes les analyses enfants et leurs états. Lorsque toutes les analyses enfants sont terminées, l'état de l'analyse parente passe à Terminé.
- La liste Source affiche l'élément vulnérable utilisé pour l'analyse, l'élément de configuration et la vulnérabilité associés, l'état du VI et son état de rattrapage.

Votre Now Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine correctement ou jusqu'à l'expiration de la période de suivi définie, selon la première éventualité.

Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de votre Now Platform® nouvelle analyse a cessé, et non à la date à laquelle la nouvelle analyse elle-même s'est arrêtée.

Tous les VI qui sont passés ou passeront à l'état Fermé/Fixe sont importés avec la prochaine importation planifiée des Qualys intégrations.

Analyser Rapid7 à nouveau les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Lancez de nouvelles analyses du Rapid7 produit sur demande à partir de l'espace de travail de remédiation informatique de votre Now Platform instance.

Avant de commencer

Pour lancer une nouvelle analyse du produit à partir de l'environnement classique, reportez-vous à la section Lancer une nouvelle analyse pour l'intégration de Rapid7 vulnérabilité. Cette rubrique comprend également des informations sur la façon de planifier les analyses avec les paramètres d'intégration sur l'instance d'intégration Rapid7 .

Les Rapid7 scanners sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont Rapid7 une application comme source, le bouton **Ré-analyse** n'est pas disponible.

Pour activer ces analyseurs, en tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin :

1. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Localisez le produit de scanner que vous souhaitez activer et cliquez sur l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher Activé.
4. Cliquez sur **Mettre à jour**.

   Le produit que vous avez activé s'affiche dans le champ Source sur les enregistrements d'éléments vulnérables et de tâches de rattrapage après la prochaine importation, et **l'action Analyser de nouveau** est disponible.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous pouvez lancer de nouvelles analyses à la demande pour les éléments vulnérables et les tâches de rattrapage qui ont le produit comme source à partir de l'espace Rapid7 InsightVM de travail de remédiation informatique dans votre Now Platform.
- Sur un enregistrement de tâche de **rattrapage**, l'enregistrement peut être dans n'importe quel état autre que Fermé et tous les VI associés doivent provenir du Rapid7 produit.
- Pour lancer de nouvelles analyses dans IT Remediation Workspace à partir d'enregistrements d'éléments vulnérables et de tâches de rattrapage, ces enregistrements doivent vous être affectés.

Rôles requis :

- sn_vul.remediation_owner pour l'espace de travail de remédiation informatique
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin dans Vulnerability Manager Workspace

Procédure

1. Accédez à un élément vulnérable ou à une tâche de rattrapage qui vous a été affectée et ouvrez-le.

   Remarque : Si vous choisissez un effort de rattrapage pour lancer une nouvelle analyse, tous les éléments vulnérables associés à cet enregistrement sont analysés.

2. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**.
3. Dans la fenêtre modale Confirmer la nouvelle analyse, cliquez sur **Demander une nouvelle analyse**.
   Le message « `La demande d'analyse est en cours de traitement` » s'affiche.
4. Cliquez sur le lien **Afficher l'état** dans le message pour afficher la progression de l'analyse.

   L'enregistrement d'analyse (VSCAN#) s'affiche. Sous l'en-tête de l'enregistrement avec le numéro d'analyse, les listes d'éléments connexes affichent les informations suivantes :

   - La liste Détails affiche le numéro d'analyse de l'analyse parente, la source de l'analyse et l'état. Affichez les analyses terminées et échouées dans la section Synthèse de l'analyse.
   - La liste Analyses affiche toutes les analyses enfants et leurs états. Lorsque toutes les analyses enfants sont terminées, l'état de l'analyse parente passe à Terminé.
   - La liste Source affiche l'élément vulnérable utilisé pour l'analyse, l'élément de configuration et la vulnérabilité associés, l'état du VI et son état de rattrapage.

   Votre Now Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine correctement ou jusqu'à l'expiration de la période de suivi définie, selon la première éventualité.

   Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de votre Now Platform® nouvelle analyse a cessé, et non à la date à laquelle la nouvelle analyse elle-même s'est arrêtée.

   Tous les VI qui sont passés ou passeront à l'état Fermé/Fixe sont importés avec la prochaine importation planifiée des Rapid7 intégrations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Analyser Tenable.io à nouveau et Tenable.sc les éléments vulnérables depuis les Réponse aux vulnérabilités espaces de travail

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Lancez de nouvelles analyses dans et produits Tenable.ioTenable.sc sur demande à partir de l'espace de travail de remédiation informatique de votre Now Platform instance.

Avant de commencer

Pour lancer une nouvelle analyse des Tenable.io produits et Tenable.sc et à partir de l'environnement classique de Réponse aux vulnérabilités, consultez Lancer une nouvelle analyse pour l'intégration Tenable.sc et Lancer une nouvelle analyse pour l'intégration Tenable.io.

Pour effectuer de nouvelles analyses à partir de votre Now Platform, vous avez besoin de vos informations d'identification Tenable. Pour plus d'informations sur la configuration de vos Tenable.io scanners et Tenable.sc l'importation de vos informations d'identification à partir de Tenable, consultez Configurer l'intégration de vulnérabilité tenable à l'aide de l'assistant de configuration.

- Vous pouvez lancer de nouvelles analyses à la demande pour les éléments vulnérables et les tâches de rattrapage qui ont le ou Tenable.sc comme produit à partir de l'espace Tenable.io de travail de remédiation informatique dans votre Now Platform.
- Sur un enregistrement de tâche de **rattrapage**, l'enregistrement peut être dans n'importe quel état autre que Fermé et tous les VI associés doivent provenir du Tenable.io ou du Tenable.sc produit.
- Pour lancer de nouvelles analyses dans les enregistrements de l'élément vulnérable d'origine et des Espace de travail de remédiation IT tâches de rattrapage, ces enregistrements doivent vous être affectés.

Rôles requis :

- sn_vul.remediation_owner pour le Espace de travail de remédiation IT
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin dans Vulnerability Manager Workspace

Procédure

1. Accédez à un élément vulnérable ou à une tâche de rattrapage qui vous a été affectée et ouvrez-le.

   Remarque : Si vous choisissez un effort de rattrapage pour lancer une nouvelle analyse, tous les éléments vulnérables associés à cet enregistrement sont analysés.

2. Dans l'angle supérieur droit d'un enregistrement, cliquez sur **Analyser à nouveau**. Vous êtes invité à choisir l'instance ou les instances pour la nouvelle analyse et les informations d'identification du scanner que vous souhaitez utiliser pour accéder au scanner. Les informations d'identification affichées sont celles importées par et Analyser les intégrations d'informations d'identification Tenable.ioTenable.sc .
3. Dans la fenêtre modale, cliquez sur l'icône de recherche.

   Dans la fenêtre modale Sélectionner les informations d'identification d'analyse qui s'affichent, utilisez les filtres des en-têtes de colonne pour sélectionner le nom, l'instance et/ou les instances, ainsi que les types d'informations d'identification que vous souhaitez utiliser.

   Consultez le tableau suivant pour plus d'informations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Description
Nom	Choisissez le nom du ou des identifiants souhaités. Passez la souris sur le titre de la colonne. Utilisez le menu vertical à trois points dans le titre de la colonne pour filtrer les noms de vos informations d'identification.
Instance d'intégration	Choisissez un ou Tenable.scl'instance Tenable.io d'intégration Tenable.sc à partir de laquelle vous souhaitez lancer la nouvelle analyse. Toutes vos instances d'intégration pour Tenable.io ou Tenable.sc sont affichées. Si un VI existe dans plusieurs instances d'intégration, vous pouvez utiliser ce filtre pour limiter ou développer les instances que vous souhaitez analyser. **Remarque :** Si vous choisissez d'analyser à nouveau les VI à partir d'un enregistrement de tâche de rattrapage pour une seule instance d'intégration, seuls les VI actifs associés à cette tâche de rattrapage, pour cette instance, à l'aide des informations d'identification que vous sélectionnez sont analysés.
Type	Il s'agit des informations d'identification de scanner disponibles importées depuis le ou Tenable.sc les Tenable.io produits. Passez la souris sur le titre de la colonne. Utilisez le menu à trois points verticaux dans le titre de la colonne pour ouvrir le modal et sélectionner les types d'informations d'identification souhaités.

Traduction automatique

4. Dans la fenêtre modale Analyser à nouveau mise à jour, cliquez sur **Demander une nouvelle analyse**.
   Le message « `La demande d'analyse est en cours de traitement` » s'affiche.
5. Cliquez sur le lien **Afficher l'état** dans le message pour afficher la progression de l'analyse.

   L'enregistrement d'analyse (VSCAN#) s'affiche. Sous l'en-tête de l'enregistrement avec le numéro d'analyse, les listes d'éléments connexes affichent les informations suivantes :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La liste Détails affiche le numéro d'analyse de l'analyse parente, la source de l'analyse et l'état. Affichez les analyses terminées et échouées dans la section Synthèse de l'analyse.
- La liste Analyses affiche toutes les analyses enfants et leurs états. Lorsque toutes les analyses enfants sont terminées, l'état de l'analyse parente passe à Terminé.
- La liste Source affiche l'élément vulnérable utilisé pour l'analyse, l'élément de configuration et la vulnérabilité associés, l'état du VI et son état de rattrapage.

Votre Now Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine correctement ou jusqu'à l'expiration de la période de suivi définie, selon la première éventualité.

Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de votre Now Platform® nouvelle analyse a cessé, et non à la date à laquelle la nouvelle analyse elle-même s'est arrêtée.

Tous les VI qui sont passés ou passeront à l'état Fermé/Fixe sont importés avec la prochaine importation planifiée des intégrations OU Tenable.ioTenable.sc .

Espace de travail de remédiation IT Informations de référence

Les rubriques suivantes vous fournissent des liens, des informations de référence ainsi que des données de champ sur les formulaires et enregistrements disponibles dans Espace de travail de remédiation IT.

Créer des champs de formulaire de demande de changement

La table suivante répertorie les champs et leur description dans le formulaire Créer une demande de changement.

Champ	Description
Type de changement	Normal : Normal est la valeur par défaut. Standard : deux champs supplémentaires s'affichent : Catégorie de changement standard : sélectionner une catégorie dans la liste Modèle de changement standard : sélectionnez un modèle dans la liste de choix à utiliser pour cette demande de changement Urgence : priorité critique
Ajouter des CI à la demande de changement	Cette valeur est activée par défaut. Si cette option est activée, les éléments de configuration (CI) qui appartiennent aux éléments vulnérables actifs dans cet effort de rattrapage sont ajoutés à cette demande de changement.
Priorité	Élevé est la valeur par défaut. Sélectionnez une priorité dans la liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Groupe d'affectation	Le groupe d'affectation est par défaut extrait de la rubrique de visualisation. Cliquez sur l'icône de recherche et, dans la fenêtre modale, choisissez un autre groupe d'affectation.
Date de fin prévue	Cliquez sur l'icône Calendrier pour sélectionner une date de fin prévue.
Affecté à	Par défaut, l'utilisateur actuel est affecté à la tâche de rattrapage. Cliquez sur l'icône de recherche et, dans la fenêtre modale, choisissez un autre utilisateur.
Description brève	La description brève est tirée de la tâche de rattrapage. Cliquez sur le texte pour le modifier.
Description	La description est extraite de la tâche de rattrapage. Cliquez sur le texte pour le modifier.
Justification	Justification extraite de la tâche de rattrapage. Cliquez sur le texte pour le modifier.
Plan d'implémentation	Pré-renseigné avec les informations de la solution préférée si elles sont disponibles. Affichez la solution ou saisissez un plan de justification.

Information associée

Créer une demande de changement dans Espace de travail de remédiation IT

Champs du formulaire Demande d'exception pour les exceptions de politique

La table suivante répertorie les champs que vous devez remplir dans le formulaire Demande d'exception pour les exceptions de politique.

Formulaire Demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si aucune politique n'est sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date de début de l'exception. La valeur par défaut est la date du jour. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Demande d'exception (suite)

Champ	Description
	Remarque : Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale (jours) de l'exception** que vous avez définie pour la politique dans Politique et conformité. Pour plus d'informations, reportez-vous à la section Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés à la raison pour laquelle cette demande est effectuée. Ce champ doit être renseigné par le propriétaire du rattrapage.

Information associée

Demander une exception à l'aide GRC : gestion de la politique et de la conformité de Espace de travail de remédiation IT

Champs du formulaire Demande d'exception pour la réduction du risque

Le tableau suivant répertorie les champs que vous devez remplir dans le formulaire Demande d'exception pour les demandes de réduction des risques.

Formulaire Demande d'exception

Champ	Description
Motif	Motif de votre demande d'exception. Sélectionnez *le contrôle d'atténuation en place pour la demande de* réduction des risques. Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à la section Définir le mappage de motif de politique.
Demande de report	Différer l'enregistrement. Ce champ est sélectionné par défaut. **Remarque :** Ce champ s'affiche uniquement lorsque l'option *Contrôle d'atténuation en place* est sélectionnée dans le champ **Motif** .
Demande de réduction des risques	Vous permet de demander la réduction du score de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Demande d'exception (suite)

Champ	Description
	Remarque : Cette case à cocher s'affiche uniquement lorsque l'option *Contrôle d'atténuation en place* est sélectionnée dans le champ **Motif** .
Cote de risque actuelle	Gravité actuelle du risque. **Remarque :** Ce champ s'affiche uniquement lorsque la case **Demande de réduction des risques** est cochée.
Cote de risque souhaitée	Nouvelle cote de risque que vous souhaitez affecter à l'enregistrement. Le score de risque le plus élevé dans cette plage de cote de risque est appliqué à l'enregistrement lorsque votre demande est approuvée. **Remarque :** Ce champ s'affiche uniquement lorsque la case **Demande de réduction des risques** est cochée.
Sélectionner les contrôles de compensation	Motif de votre demande de réduction de la cote de risque.
Jusqu'à	Date d'expiration de la demande de report ou de réduction de risque. Quand la demande d'exception expire : • L'enregistrement revient à l'état Ouvert. • Les contrôles compensatoires expirent. • Le score calculé sera à la place d'un score réduit.
Notes de justification	Détails liés à la raison pour laquelle cette demande est effectuée.

Traduction automatique

Explorer l'espace de travail de l'évaluation de la vulnérabilité

L'espace de travail d'évaluation de la vulnérabilité est conçu pour que le gestionnaire d'événements de vulnérabilité évalue l'exposition et gère de manière proactive les événements de vulnérabilité critiques, en particulier lors d'événements de vulnérabilité critiques tels qu'un événement zero-day.

Une fois qu'une vulnérabilité critique est identifiée, les gestionnaires d'événements de vulnérabilité peuvent évaluer l'impact potentiel et le risque associés à la vulnérabilité. Les analystes peuvent analyser le système, les applications ou les composants réseau affectés pour comprendre la gravité et les vecteurs d'attaque possibles au sein de l'organisation.

L'espace de travail de l'évaluation de la vulnérabilité contient :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Page d'évaluation de l'exposition

Fournit une visibilité détaillée sur les actifs exposés aux vulnérabilités et aux logiciels vulnérables. La fonctionnalité d'évaluation de l'exposition fournit :

- Visibilité des actifs impactés pour la vulnérabilité et les logiciels affectés
- Possibilité d'effectuer des évaluations autonomes pour un seul CVE ou logiciel vulnérable
- Visibilité des actifs impactés pour les CVE de vulnérabilité exploitée connue de CISA
- Visibilité de l'exposition à partir d'un modèle de découverte et d'actifs supplémentaires.
- Capacité à créer des éléments vulnérables

Page d'évaluation de la vulnérabilité

Page Évaluation de vulnérabilité où vous pouvez gérer les événements de crise de vulnérabilité, de l'évaluation à la résolution, à l'aide du workflow Gestion des crises de vulnérabilité. Le workflow vous permet de suivre les événements de vulnérabilité d'intérêt, d'analyser le risque qui leur est associé, d'évaluer l'exposition à plusieurs inventaires (par exemple, l'inventaire des installations logicielles) et de déclarer qu'il s'agit d'une crise pour un engagement de réponse élevé. Vous pouvez ensuite associer l'enregistrement de l'évaluation des vulnérabilités à un incident de sécurité majeur et permettre à l'équipe de Security Incident Response de répondre à la crise.

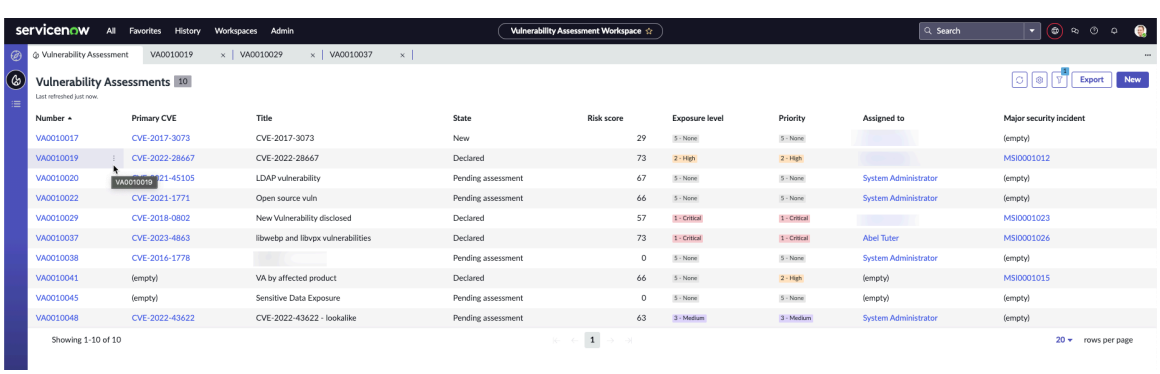
- Créer et modifier des évaluations de vulnérabilité pour les événements de vulnérabilité critique
- Enregistrer les attributs clés de la vulnérabilité pour calculer le risque
- Effectuer une évaluation de la vulnérabilité pour déterminer le niveau et la priorité d'exposition
- Déclarer l'évaluation de vulnérabilité comme un événement critique
- Associez l'évaluation de vulnérabilité à un incident de sécurité majeur en liant, en proposant ou en promouvant l'évaluation de vulnérabilité à un incident de sécurité majeur.

Page de liste

La page Liste comprend une bibliothèque contenant :

- CVE
- TPE
- CWE

L'image suivante vous montre la page d'accueil de l'espace de travail d'évaluation de la vulnérabilité.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer l'évaluation de l'exposition

L'évaluation de l'exposition utilise le cadre de travail CPE (Common Platform Enumeration), qui fait partie du système CVE (Common Vulnerabilities and Exposures), pour évaluer l'exposition de vos actifs aux logiciels vulnérables. Cette évaluation est réalisée à l'aide d'un modèle de détection de logiciels.

En utilisant un algorithme d'appariement, les CPE pertinents sont associés et mis en correspondance avec le modèle de détection de logiciels, ce qui permet d'identifier les expositions potentielles.

Vous pouvez utiliser l'évaluation de l'exposition par CVE ou un logiciel pour identifier l'exposition aux vulnérabilités potentielles pour les scénarios suivants :

- Vulnérabilités qui peuvent ne pas être identifiées par les scanners traditionnels
- Vulnérabilités zero-day avant que le scanner ne fournisse la signature pour la détection de vulnérabilité

L'évaluation de l'exposition fournit une alerte précoce pour corriger ces vulnérabilités et améliorer la maturité du programme de gestion des vulnérabilités.

Conditions préalables à l'évaluation de l'exposition

Versions disponibles

Application	Version
Module d'extension Vulnerability Crisis Management	1.0
Réponse aux vulnérabilités	20.0
Réponse aux vulnérabilités avec NVD	1.3
Intégration de Réponse aux vulnérabilités à CISA	1.2
Intégration de Vulnerability Response avec NVD **Remarque :** Pour plus d'informations, consultez Présentation des intégrations NVD.	1.3
Gestion des actifs logiciels	Module d'extension Software Asset Management Foundation ou Gestion des actifs logiciels - Professional module d'extension

Compatibilité et configuration requise

L'application Réponse aux vulnérabilités est disponible sur le ServiceNow Store. L'application Gestion des actifs logiciels pour ITSM (com.snc.asset_management) est requise pour le module d'évaluation de l'exposition. Cette application gère tous vos actifs et licences logicielles, et la SAM Foundation version de cette application fait partie de l'application Réponse aux vulnérabilités que vous téléchargez à ServiceNow Storepartir du .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : L'application Évaluation de l'exposition fonctionne avec les modules d'extension suivants :

- Module d'extension Software Asset Management Foundation (com.snc.sams)
- Gestion des actifs logiciels - Professional (com.snc.pa.samp)
- Module d'extension de gestion des actifs logiciels (com.snc.software_asset_management)

Pour vérifier que l'application SAM Foundation est installée sur votre instance, accédez à **Applications système** > **Toutes les applications disponibles** > **Tout** et recherchez com.snc.asset_management. Si l'application n'est pas installée, sélectionnez **Installer**. Comme l'application d'évaluation de l'exposition à la vulnérabilité nécessite l'accès aux données d'actif sur votre Now Platform® instance, les applications de gestion des actifs doivent avoir des données à référencer. La table des modèles de détection de logiciels (cmdb_sam_sw_discovery_model) et les installations de logiciel (cmdb_sam_sw_install) nécessitent des données.

Champs d'algorithme de correspondance pour les modèles de détection de logiciels

L'application Gestion des actifs logiciels - Professional vous permet de modifier un modèle de détection de logiciels pour normaliser manuellement le logiciel détecté qui n'a pas été entièrement normalisé (partiellement normalisé, normalisé par l'éditeur ou correspondance introuvable) sur le formulaire des modèles de détection de logiciels afin qu'il puisse être rapproché. À partir de la version 20.0, il prend en charge le modèle de Réponse aux vulnérabilités détection normalisé qui provient de Gestion des actifs logiciels - Professional. Les champs suivants sont utilisés pour l'algorithme de correspondance des modèles de détection de logiciels.

CPE (Modèle logiciel)	Fondations SAM	Professionnel SAM
Fournisseur	Clé primaire	Clé primaire
Produit	Nom d'affichage	Nom d'affichage
Version	Éditeur détecté	Éditeur détecté
Édition	Produit détecté	Produit détecté
	Version détectée	Version détectée
		Éditeur normalisé
		Produit normalisé
		Version normalisée

Remarque : L'application SAM Professional ne fait pas partie du produit principal Réponse aux vulnérabilités et ServiceNow Store nécessite un abonnement distinct.

Propriété système

Pour traiter automatiquement les vulnérabilités exploitées par CISA à des fins d'évaluation de l'exposition, définissez la propriété *sn_vul_analyst.enable_exposure_for_cisa* système sur *true*. La valeur par défaut est *false*.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Travaux planifiés

Voici les travaux planifiés.

Nom de la tâche planifiée	Description
Vérifier l'exposition potentielle à la vulnérabilité	Traite les CVE delta, les logiciels et les installations pour obtenir l'exposition. **Remarque :** Cette tâche planifiée s'exécute toutes les 12 heures. Elle s'exécute pendant une période plus longue que les autres travaux planifiés.
Insérer les CVE exploitées par CISA dans la configuration d'exposition	Sur demande. Insère les CVE CISA dans la table de configuration de l'exposition pour calculer l'exposition.
Exécuter l'évaluation de l'exposition pour les CVE configurés	Sur demande. Calcule l'exposition pour tous les enregistrements CVE dans la table Configuration de l'exposition.
Exécuter l'exposition logicielle	Sur demande. Calcule l'exposition pour tous les enregistrements logiciels dans la table de configuration de l'exposition.

Termes clés

- **Score de confiance :** Un score de confiance est une mesure de la fiabilité de la fourniture d'une recommandation pour un champ. Plus le score est élevé, plus la recommandation est fiable. Pour des exemples de calculs, reportez-vous à la section Exemple de calcul du score de confiance.
- **Nombre d'installations logicielles :** Nombre d'actifs logiciels impactés par la vulnérabilité.
- **Modèle logiciel :** Modèle logiciel associé au produit. Analysez le modèle logiciel pour voir le résultat du modèle logiciel. Pour plus d'informations, consultez Modèles de détection et installations de logiciels Module d'extension Software Asset Management Foundation .

Le champ **Nombre d'installations de logiciels** fournit le nombre total d'installations de logiciels, quel que soit leur état actif ou inactif sur le modèle de détection. À partir de la version 22.0 de Réponse aux vulnérabilités, une nouvelle propriété système, *sn_vul.filter_inactive_sw_installs*, a été introduite pour déterminer si les installations logicielles inactives doivent être filtrées pour l'évaluation de l'exposition Par défaut, la propriété est activée dans le système de base. Lorsque le filtre est activé, seules les installations actives sont affichées.

Le champ **de modèle de détection** indique spécifiquement le nombre d'installations de logiciels actives, car les installations inactives sont filtrées en fonction du filtre active=true par défaut sur la table Modèle de détection de logiciels. Le nombre indiqué dans ce champ doit correspondre au nombre filtré affiché dans le champ **Nombre d'installations de logiciel** . Le nombre indiqué dans le champ **Installation de logiciel** persiste même si vous mettez à jour la propriété système. Pour obtenir le nombre mis à jour, vous devez exécuter les travaux *Run exposure assessment for configured CVEs* planifiés et *Run software exposure that updates the count*.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluation de l'exposition par CVE

L'évaluation de l'exposition utilise les vulnérabilités et les expositions communes (CVE) pour évaluer l'exposition de vos actifs à l'aide du modèle de détection de logiciels. Vous pouvez utiliser l'évaluation de l'exposition par CVE pour identifier l'exposition aux vulnérabilités potentielles.

Pour plus d'informations sur l'évaluation de l'exposition par CVE, voir :

- Ajouter des CVE pour évaluer l'exposition
- Créer des VI pour les CVE pour l'évaluation de l'exposition
- Activer ou désactiver les CVE pour l'évaluation de l'exposition
- Exporter les CI impactés pour l'évaluation de l'exposition
- Exemple de calcul du score de confiance

Ajouter des CVE pour évaluer l'exposition

Ajoutez les vulnérabilités et les expositions communes (CVE) à la liste de configuration de l'exposition des CVE dans l'évaluation de l'exposition pour évaluer l'impact d'une nouvelle vulnérabilité ou d'une vulnérabilité zero-day.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par CVE**.
2. Sélectionnez **Ajouter**.
3. Dans la boîte de dialogue Ajouter des CVE, sélectionnez les CVE que vous souhaitez ajouter à la liste et sélectionnez l'option **Ajouter** .
   Les CVE qui figurent déjà dans la liste ne sont pas ajoutés à nouveau. Les autres sont ajoutés à la liste des CVE.

   Remarque : Sélectionnez l'icône de filtre pour accéder à la **vue avancée** et spécifiez les CVE que vous souhaitez afficher.

4. Pour évaluer l'impact des CVE qui figurent déjà dans la liste :

   a. Cochez la case des CVE que vous souhaitez réévaluer.

   b. Cliquez sur le bouton **Réévaluer** .
   Les détails mis à jour s'affichent dans les colonnes respectives.

Créer des VI pour les CVE pour l'évaluation de l'exposition

Créez des éléments vulnérables (VI) à partir de la page Évaluation de l'exposition. Les gestionnaires des événements de vulnérabilité analysent ensuite cette liste d'éléments vulnérables et recommandent des solutions et des correctifs qui aident l'équipe informatique à corriger ces vulnérabilités.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Une fois l'exposition évaluée, la liste de l'évaluation potentielle s'affiche dans l'enregistrement d'évaluation de l'exposition avec le nombre d'éléments de configuration (CI). Vous pouvez sélectionner les enregistrements et, dans l'action de liste, sélectionner **Créer des éléments vulnérables** pour créer des éléments vulnérables (VI) pour les CI où le logiciel vulnérable est présent et sur les vulnérabilités et expositions communes (CVE). Les VI sont créés en arrière-plan. Ce processus peut prendre un certain temps. Une fois les éléments créés, vous pouvez accéder à la table des VI pour afficher les enregistrements créés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par CVE**.
2. Sélectionnez les CVE requis et sélectionnez l'option **Créer des éléments vulnérables** .
3. Dans la boîte de dialogue Créer des éléments vulnérables, sélectionnez l'option **Créer des éléments vulnérables** .
4. Sélectionnez le lien **Afficher l'état** pour afficher l'état de la tâche en arrière-plan utilisée pour créer les VI.

Activer ou désactiver les CVE pour l'évaluation de l'exposition

Pour le traitement delta d'un CVE, vous pouvez l'activer, l'ajoutant ainsi à la liste active des CVE.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par CVE**.
2. Sélectionnez les CVE actifs requis et sélectionnez l'option **Désactiver** .
   Les CVE sont désactivés.

   Remarque : Pour activer le logiciel, suivez le même processus et sélectionnez l'option **Activer** .

3. Actualisez la page pour afficher l'état mis à jour (faux) dans la colonne Actif.

Exporter les CI impactés pour l'évaluation de l'exposition

Vous pouvez suivre la liste des actifs impactés pour un nouveau CVE en exportant les éléments de configuration (CI) liés à un enregistrement d'évaluation de l'exposition vers une feuille Excel. Cette feuille peut être utilisée pour partager les détails et les propriétaires des actifs afin de créer des incidents avec les actifs impactés connus pour les vulnérabilités zero-day.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par CVE**.
2. Sélectionnez le modèle de détection pour l'enregistrement dont vous souhaitez exporter les CI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'onglet Installations de logiciel contient les CI actifs associés à l'enregistrement de logiciel. Ces CI sont stockés dans la colonne **Installé le** .

3. Sélectionnez l'option **Exporter** .
4. Dans la boîte de dialogue Exporter, sélectionnez le type de fichier et le type de livraison pour exporter les CI associés.
5. Sélectionnez l'option **Exporter** .

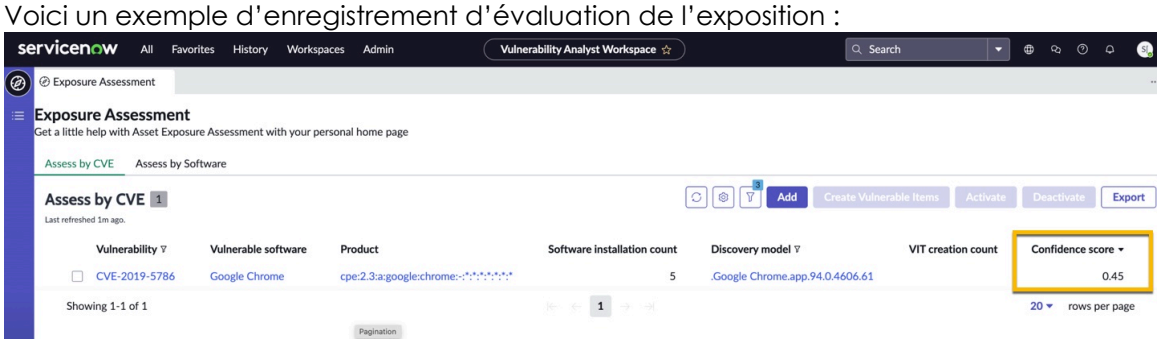
Exemple de calcul du score de confiance

Exemple de calcul de la fiabilité d'une vulnérabilité zero-day en fonction de ses informations sur les vulnérabilités et les expositions communes (CVE).

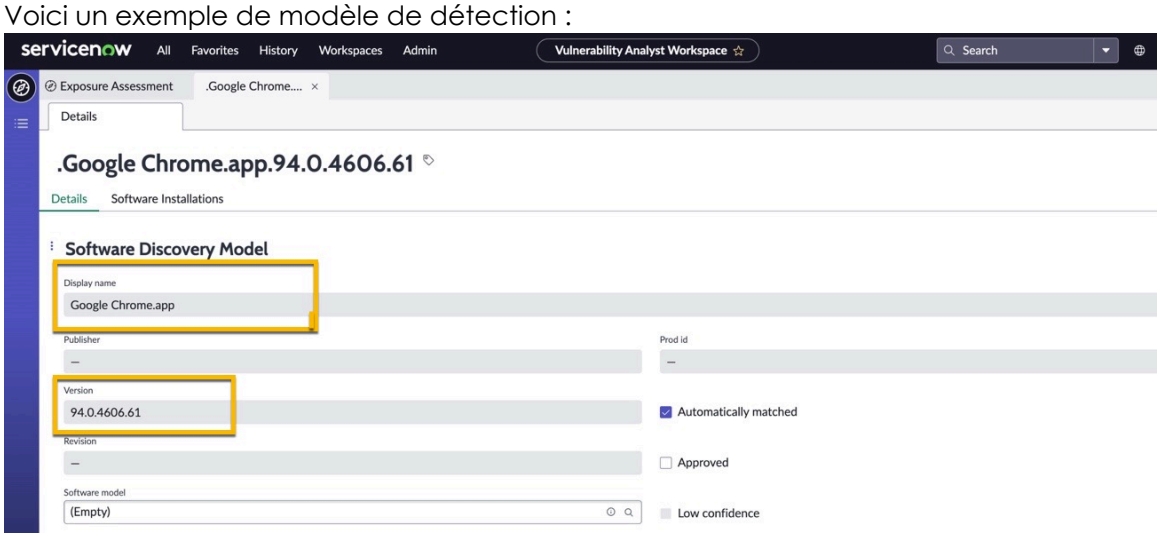
Voici un exemple de calcul du score de confiance à partir des informations CPE (Common Platform Enumeration) de **CVE-2019-5786**.

Remarque : Pour afficher les CPE, vous pouvez regrouper la colonne Vulnérabilité par vulnérabilité. Pour plus d'informations sur l'affichage des détails des logiciels vulnérables, reportez-vous à la section Afficher les détails du logiciel vulnérable.

Voici un exemple d'enregistrement d'évaluation de l'exposition :



Voici un exemple de modèle de détection :



Comment calculer le score de confiance

La plage de scores de confiance est comprise entre 0 et 1. Sur la base des informations CPE, le score de confiance est calculé à l'aide de la formule suivante :

```
((BASE SCORE) + (publisher score) +(product score) + (version score) +
 (edition score) + (display name score)) / 100
```

=

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

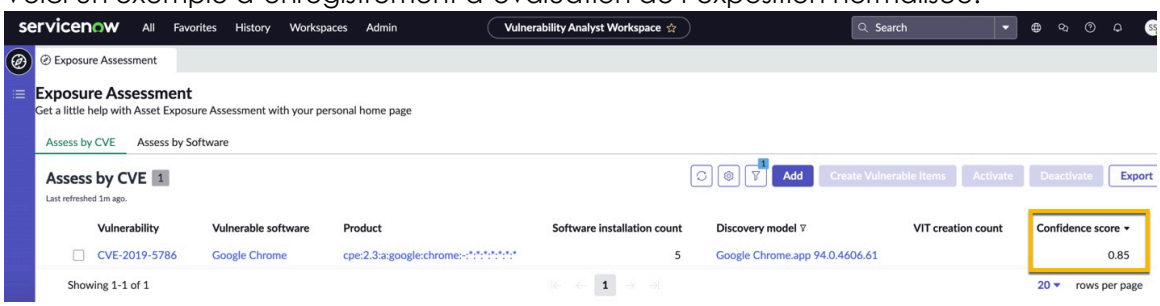
```
.45
```

Remarque : Pour consulter les valeurs utilisées pour calculer le score de confiance, reportez-vous à la section Tables de référence du score de confiance pour l'évaluation de l'exposition.

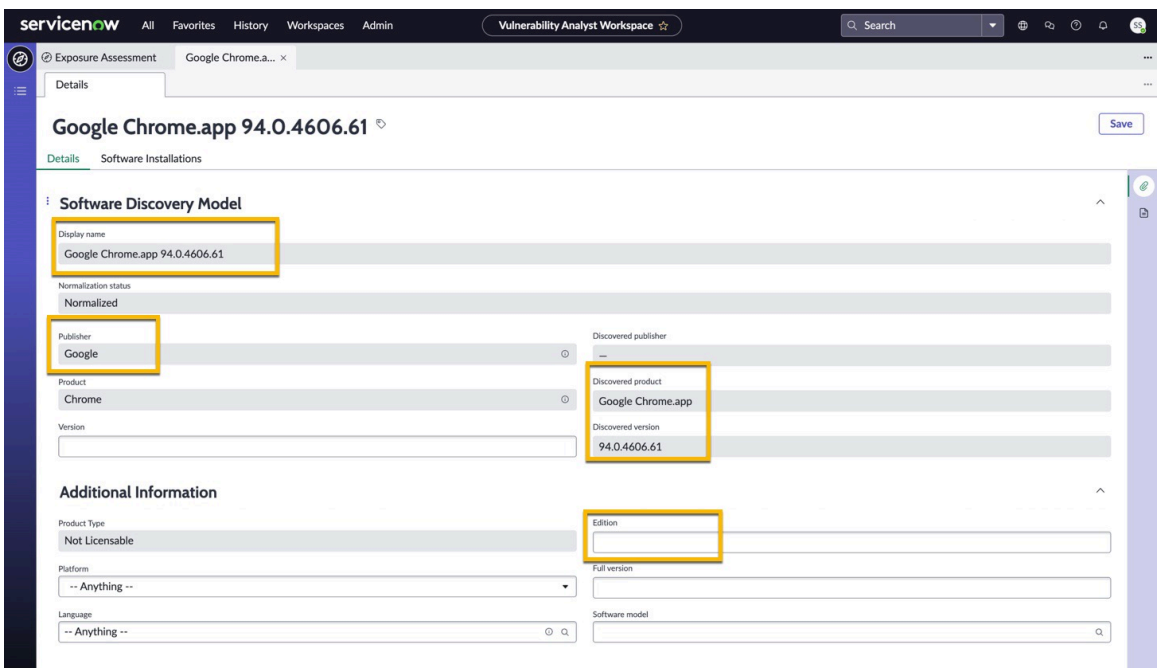
Calcul du score de confiance lorsque le modèle logiciel est mis en correspondance avec le modèle de détection normalisé

Si vous utilisez le modèle de détection normalisé, les informations supplémentaires disponibles pour le modèle de détection de logiciels fournissent un score de confiance amélioré. Voici l'exemple de calcul :

Voici un exemple d'enregistrement d'évaluation de l'exposition normalisée.



Voici un exemple de modèle de détection normalisé.




```
((BASE SCORE) + (publisher score) + (product score) + (version score) +
(edition score) + (display name score)) / 100
```

=

```
((25) + (20) + (15) + (15) + (0) + (10)) / 100
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

=

```
85 / 100
```

=

```
.85
```

Remarque : Pour consulter les valeurs utilisées pour calculer le score de confiance, reportez-vous à la section Tables de référence du score de confiance pour l'évaluation de l'exposition.

Afficher les détails du logiciel vulnérable

Affichez les détails du logiciel vulnérable, dans ce cas, Google Chrome. Il est comparé au modèle de détection et à l'énumération de plateforme commune (CPE). Cette version CPE impacte toutes les versions de Google Chrome.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à **Tout** et saisissez *sn_vul_software.LIST*.
2. Dans la liste des logiciels vulnérables, recherchez **cpe :2.3 :a :google :chrome :-:*:*:*:*:*:*:*** pour afficher les informations.

Tables de référence du score de confiance pour l'évaluation de l'exposition

Valeurs de référence utilisées pour calculer le score de confiance.

Tables de référence

Table de référence pour le calcul du score de confiance

Segment des logiciels vulnérables	Segment du modèle de détection	Score	Segment de correspondance exacte du modèle de détection	Score de correspondance exacte
Éditeur	Nom d'affichage	15	Éditeur	5
Modèle	Nom d'affichage	15	Modèle	5
Version	Nom d'affichage	10	Version	5
Édition	Nom d'affichage	3	Édition normalisée	2
Nom d'affichage	Nom d'affichage	10	Nom d'affichage	5

Table récapitulative des scores de confiance

Score	Valeur
Somme de tous les scores	75
Score de base	25

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table récapitulative des scores de confiance (suite)

Score	Valeur
Remarque : Score minimal attribué à tous les modèles de découverte correspondants.	
Score total	100

Évaluation de l'exposition par logiciel

Évaluation de l'exposition pour les vulnérabilités zero-day, lorsque les vulnérabilités et expositions communes (CVE) pour l'actif ou l'élément de configuration ne sont pas disponibles. Il utilise les informations logicielles pour évaluer l'exposition, à l'aide du modèle de détection de logiciels.

Pour plus d'informations sur l'évaluation de l'exposition par logiciel, voir :

- Ajouter un logiciel pour l'évaluation de l'exposition
- Créer des VI pour le logiciel pour l'évaluation de l'exposition
- Activer ou désactiver le logiciel pour l'évaluation de l'exposition
- Exporter les CI impactés pour les logiciels dans l'espace de travail de l'évaluation des vulnérabilités

Ajouter un logiciel pour l'évaluation de l'exposition

Ajoutez un nouveau logiciel au module Évaluation de l'exposition pour évaluer l'impact d'une nouvelle vulnérabilité ou d'une vulnérabilité zero-day.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par logiciel** > **Ajouter**.
2. Renseignez les champs du formulaire.

Champ	Description
Éditeur	Éditeur du logiciel.
Produit	Nom du produit du logiciel.
Version	Version du produit logiciel.
Édition	Édition du logiciel.

Remarque : Si vous essayez d'ajouter une exposition pour un logiciel qui existe dans la table avec l'état « faux », un enregistrement en double n'est pas créé. L'état du logiciel existant est mis à jour sur « vrai ».

3. Sélectionnez l'option **Ajouter** .
4. Pour évaluer l'impact des logiciels déjà présents dans la liste :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Cochez la case du logiciel que vous souhaitez réévaluer.

b. Cliquez sur le bouton **Réévaluer** .
Les détails mis à jour s'affichent dans les colonnes respectives.

Créer des VI pour le logiciel pour l'évaluation de l'exposition

Créez des éléments vulnérables (VI) à partir de la page Évaluation de l'exposition. Les gestionnaires des événements de vulnérabilité analysent ensuite cette liste d'éléments vulnérables et recommandent des solutions et des correctifs qui aident l'équipe informatique à corriger ces vulnérabilités.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par logiciel**.
2. Sélectionnez les enregistrements pour lesquels vous souhaitez créer des VI.
3. Sélectionnez l'option **Créer des éléments vulnérables** .
4. Dans la boîte de dialogue Créer des éléments vulnérables, sélectionnez l'une des options suivantes :
   - Vulnérabilité existante
   - Nouvelle vulnérabilité
5. Sélectionnez l'option **Créer des éléments vulnérables** .

Activer ou désactiver le logiciel pour l'évaluation de l'exposition

Pour arrêter le traitement différentiel ultérieur du logiciel, vous pouvez choisir de le désactiver, le supprimant ainsi de la liste des logiciels actifs.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par logiciel**.
2. Pour le désactiver, sélectionnez le logiciel actif requis et sélectionnez l'option **Désactiver** .
   Le logiciel est désactivé.

   Remarque : Pour activer le logiciel, suivez le même processus et sélectionnez l'option **Activer** .

3. Actualisez la page pour afficher l'état mis à jour (faux) dans la colonne Actif.

Exporter les CI impactés pour les logiciels dans l'espace de travail de l'évaluation des vulnérabilités

Vous pouvez suivre la liste des actifs impactés pour les nouveaux logiciels en exportant les éléments de configuration (CI) associés à un enregistrement d'évaluation de l'exposition vers une feuille Excel. Cette feuille peut être utilisée pour partager les détails et les propriétaires

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

des actifs afin de créer des incidents avec les actifs impactés connus pour les vulnérabilités zero-day.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par logiciel**.
2. Sélectionnez le modèle de détection pour l'enregistrement dont vous souhaitez exporter les CI.
   L'onglet Installations de logiciel contient les CI actifs associés à l'enregistrement de logiciel. Ces CI sont stockés dans la colonne **Installé le** .
3. Sélectionnez l'option **Exporter** .
4. Dans la boîte de dialogue Exporter, sélectionnez le **type de fichier** et le **type de livraison** pour exporter les CI associés.
5. Sélectionnez l'option **Exporter** .

Exploration de l'évaluation des vulnérabilités

L'espace de travail d'évaluation de la vulnérabilité est conçu pour que le gestionnaire d'événements de vulnérabilité crée un événement de vulnérabilité et effectue une évaluation de la vulnérabilité, en particulier pendant l'analyse de vulnérabilité zero-day.

Vous pouvez utiliser l'espace de travail d'évaluation de la vulnérabilité pour gérer les vulnérabilités critiques, telles que :

- Vulnérabilités zero-day de gravité critique ou élevée
- Nouveaux renseignements sur les menaces identifiés pour une vulnérabilité
- Exploitation rapide d'une vulnérabilité de gravité critique ou élevée.

Espace de travail d'évaluation de vulnérabilité et Gestion de crise de vulnérabilité

En tant que gestionnaire d'événements de vulnérabilité, identifiez et créez un enregistrement d'événement de vulnérabilité pour les vulnérabilités d'intérêt. Une fois que vous avez créé l'événement vulnérable, vous pouvez effectuer une évaluation des risques, mettre à jour manuellement les attributs de risque et calculer automatiquement le score de risque. À l'aide de l'espace de travail d'évaluation de la vulnérabilité, vous pouvez effectuer les actions suivantes pour gérer les événements de crise de vulnérabilité de la conception à la résolution.

- Créer un enregistrement d'évaluation de vulnérabilité
- Modifier l'enregistrement de l'évaluation de vulnérabilité
- Effectuer une évaluation de la vulnérabilité
- Passer en revue les détails de l'évaluation
- Affecter une priorité et un niveau d'exposition à l'enregistrement de l'évaluation des vulnérabilités
- Ajouter les CI affectés à l'enregistrement de l'évaluation

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Créer des éléments vulnérables pour le CI affecté ou le composant logiciel affecté
- Lier l'enregistrement de l'évaluation des vulnérabilités à un incident de sécurité majeur dans Gestion des incidents de sécurité majeurs

Prérequis pour l'évaluation de la vulnérabilité

Versions disponibles

Application	Version
Module d'extension Vulnerability Crisis Management	1.0
Réponse aux vulnérabilités	20.0
Réponse aux vulnérabilités avec NVD **Remarque :** Pour plus d'informations, consultez Présentation des intégrations NVD.	1.4.2
Intégration de Réponse aux vulnérabilités à CISA	1.2
Modèle de données pour SBOM	1.1.2
Nomenclature logicielle Core	2.0.2
Gestion des actifs logiciels	Module d'extension Software Asset Management Foundation ou Gestion des actifs logiciels - Professional module d'extension
Gestion des incidents de sécurité majeurs	2.2.5

Travaux planifiés

Voici les travaux planifiés.

Nom de la tâche planifiée	Description
Évaluation de la vulnérabilité	Met à jour la table des éléments de configuration affectés et la source du CI si des éléments vulnérables (VIT ou AVIT) sont créés après l'évaluation. **Remarque :** Cette tâche planifiée s'exécute quotidiennement. Elle s'exécute pendant une période plus longue que les autres travaux planifiés.

Information associée

Gestion de crise de vulnérabilité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un enregistrement d'évaluation de vulnérabilité

Créez des enregistrements d'évaluation pour les vulnérabilités d'intérêt. Après avoir créé l'évaluation, vous pouvez lancer l'évaluation initiale des risques, mettre à jour manuellement l'enregistrement et calculer automatiquement le score de risque.

Avant de commencer

Vous devez faire partie du groupe d'affectation du gestionnaire d'événements d'évaluation de vulnérabilité du système de base pour pouvoir effectuer les tâches associées à l'évaluation de vulnérabilité. Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche

Vous pouvez créer un enregistrement d'évaluation de la vulnérabilité pour les vulnérabilités d'intérêt en associant l'enregistrement d'événement à une CVE principale ou à un produit affecté.

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez l'icône **Évaluation de la vulnérabilité** .
3. Sélectionnez **Nouveau**.
4. Saisissez un titre approprié dans le champ **Titre** .
5. Facultatif : Sélectionnez un CVE primaire à associer au nouvel enregistrement d'évaluation dans le champ **CVE primaire** .

   Remarque : Tous les détails préliminaires de l'enregistrement d'évaluation sont renseignés en fonction du produit que vous sélectionnez ou créez ou du CVE principal que vous associez à l'enregistrement.

6. Sélectionnez **Soumettre**.
   L'enregistrement d'évaluation de vulnérabilité avec le titre que vous avez saisi est créé et s'affiche dans un nouvel onglet d'évaluation de vulnérabilité. Par défaut, l'enregistrement de l'évaluation de vulnérabilité s'affiche dans l'onglet **Détails** .

   Remarque : Par défaut, les détails du CVE primaire associé/mappé sont affichés.

   - Si aucun CVE primaire n'est sélectionné lors de la création de l'enregistrement de l'événement d'évaluation de la vulnérabilité, un enregistrement par défaut est créé.
   - Si le CVE principal a des CVE associés, les CVE connexes sont renseignés dans l'onglet **Entrées de vulnérabilité** . Vous pouvez ajouter d'autres CVE associées à partir de l'onglet **Entrées de vulnérabilité** .

7. Accédez à l'onglet **Produits affectés** .

   a. Sélectionnez **Nouveau**.

   b. Renseignez les champs du formulaire.

Champ	Description
Éditeur	Éditeur du logiciel.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Il s'agit d'un champ obligatoire.
Produit	Nom du produit du logiciel. Il s'agit d'un champ obligatoire.
Version	Version du produit logiciel.
Édition	Édition du logiciel.

Remarque : Si vous essayez d'ajouter une vulnérabilité pour un logiciel qui existe dans la table avec l'état « faux », un enregistrement en double n'est pas créé. L'état du logiciel existant est mis à jour sur « vrai ».

c. Sélectionnez **OK**.

8. Sélectionnez **Enregistrer**.

Mettre à jour l'enregistrement de vidage automatique de l'évaluation de vulnérabilité

Mettre à jour l'enregistrement de vidage automatique de l'évaluation de vulnérabilité.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche
Dans le système de base, la période de conservation des enregistrements d'évaluation de vulnérabilité est fixée à 6 mois. Si un état d'enregistrement d'évaluation de vulnérabilité est fermé, les enregistrements d'évaluation de vulnérabilité sont conservés uniquement jusqu'à la période de conservation définie et les enregistrements connexes de cette évaluation sont supprimés après 6 mois de toutes les tables connexes.

Procédure

1. Accédez à la **Tout** > **Purges automatiques**.
2. Ouvrez l'enregistrement avec la table, sn_vul_analyst_vulnerability_assessment.
3. Cochez la case **Actif** pour activer l'option de vidage automatique pour l'enregistrement d'évaluation de vulnérabilité.
4. Cliquez sur **Mettre à jour**.

Modifier l'enregistrement de l'évaluation de vulnérabilité

Mettez à jour l'enregistrement de l'évaluation des vulnérabilités, publiez sa création. En fonction des valeurs du champ, vous pouvez calculer le score de risque.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche
Une fois les CVE primaires ajoutés à l'évaluation des vulnérabilités, l'enregistrement passe à l'état En attente d'évaluation. Vous pouvez ajouter d'autres CVE connexes dans l'onglet **Entrées de vulnérabilité**ou ajouter les produits affectés par cette vulnérabilité à partir de l'onglet **Produits affectés** . Vous pouvez apporter d'autres modifications aux champs **d'évaluation des risques** et le **score de risque** de l'enregistrement d'évaluation est automatiquement mis à jour en conséquence.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de la vulnérabilité**.
2. Dans l'onglet **Détails** , mettez à jour les champs.

Champ	Description
Titre	Titre décrivant l'enregistrement de l'événement de vulnérabilité.
CVE primaire	CVE principal que vous avez associé à l'enregistrement d'événement.
État	État actuel de l'enregistrement d'événement.
Priorité	Priorité de l'enregistrement de l'événement sur une échelle de 1 à 5.
Sources d'alerte	Source de l'événement de vulnérabilité potentiel.
Score du risque	Score de risque calculé automatiquement. Non modifiable par défaut.
Niveau d'exposition	Niveau d'exposition de l'événement de vulnérabilité sur une échelle de 1 à 5.
Groupe d'affectation	Groupe d'affectation auquel l'enregistrement d'événement est affecté.
Affecté à	Utilisateur auquel l'enregistrement d'événement est affecté.
Description	Description détaillée de l'enregistrement d'événement.

3. Accédez à l'onglet **Entrées de vulnérabilité** pour ajouter des CVE associés ou connexes.
   a. Sélectionnez **Nouveau**.
   b. Recherchez l'enregistrement dans le champ **Entrée de vulnérabilité** .
   c. Sélectionnez l'enregistrement de vulnérabilité que vous souhaitez associer à l'enregistrement d'évaluation.
   d. Facultatif : Sélectionnez **Parcourir** pour parcourir et joindre un fichier.
   e. Sélectionnez **Enregistrer**.
   Les enregistrements de vulnérabilité que vous avez sélectionnés sont ajoutés à l'enregistrement d'évaluation et s'affichent dans l'onglet **Entrées de vulnérabilité.**
4. Facultatif : Ajouter les produits affectés.
5. Ajouter un lien connexe à l'enregistrement de l'évaluation.
6. **Modifiez les attributs de risque** pour les CVE primaires associées à l'enregistrement d'événement d'évaluation de vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Corruption de la mémoire	Indique si cet enregistrement d'événement peut corrompre la mémoire.
Exécutable de code distant	Indique si l'exécution de code à distance est possible.
Escalade de privilèges locaux	Indique s'il existe une vulnérabilité d'élévation de privilèges locaux.
Accès non autorisé	Indique s'il existe une vulnérabilité d'accès non autorisé.
DDOS	Indique si l'événement potentiel pourrait impliquer un déni de service distribué.
Complexité d'attaque	Indique la complexité de la pièce jointe. Les options sont faible, moyenne ou élevée.
Vecteur d'attaque	Indique la voie ou la méthode d'attaque potentielle. Les options sont les suivantes : Réseau, Réseau adjacent, Local, Physique, Aucun.
Privilèges requis	Indique le niveau de privilèges requis par un attaquant pour exploiter la vulnérabilité. Les options sont Aucun, Faible ou Élevé.
Interaction de l'utilisateur	Indique si une interaction de l'utilisateur est nécessaire pour exploiter la vulnérabilité.
Impact de la confidentialité	Indique la mesure de l'impact potentiel sur la confidentialité de la vulnérabilité. Les options sont Aucun, Faible ou Élevé
Changement du périmètre	Indique si le périmètre a changé.
Impact sur la disponibilité	Indique l'impact potentiel sur la disponibilité d'une vulnérabilité d'utilisation abusive exploitée avec succès. La disponibilité fait référence à l'accessibilité des ressources d'information. Les options sont Aucun, Faible ou Élevé
Impact sur l'intégrité	Indique l'impact potentiel sur l'intégrité d'une vulnérabilité d'utilisation abusive exploitée avec succès. L'intégrité fait référence à la fiabilité et à la véracité garantie de l'information. Les options sont Aucun, Faible ou Élevé
Niveau de rattrapage	Indique l'état ou la disponibilité d'un rattrapage pour la vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Les options sont les suivantes : Correctif officiel, Correctif temporaire, Solution de contournement, Non disponible, Non défini.
Maturité du code d'exploitation	Indique la probabilité d'exploitation de la vulnérabilité en fonction de l'état actuel des techniques d'exploitation et de la disponibilité du code. Les options sont les suivantes : Non prouvé, Preuve de concept, Fonctionnel, Élevée et Non défini.
Fiabilité du rapport	Indique votre niveau de certitude quant à l'existence de la vulnérabilité.

7. Saisissez les commentaires pertinents dans le champ **Composer** .
   - Saisissez vos notes de travail dans le champ **Notes de travail (privées).**
   - Saisissez vos commentaires (visibles par tous) dans le champ **Commentaires** .
8. **Enregistrez** l'enregistrement de l'évaluation.
   En fonction des mises à jour que vous avez apportées aux champs **d'attribut de risque** pour la CVE principale ou le produit affecté associé à l'enregistrement d'évaluation, le champ de **score de risque** est automatiquement mis à jour.

   Remarque : Pour modifier les règles ou les critères du calculateur de score de risque du système de base, accédez à **Tout** > **Calculateurs de l'évaluation de la vulnérabilité** > **Calculateur du risque de l'évaluation de la vulnérabilité** > **Règle de risque pour l'évaluation de la vulnérabilité**. Vous pouvez ajouter des critères et modifier la pondération au niveau du champ en fonction des critères existants, si nécessaire.

Que faire ensuite
Effectuez une évaluation initiale de l'enregistrement de l'événement.

Supprimer les CVE associés ou les produits affectés de l'enregistrement d'évaluation des vulnérabilités

Supprimez un enregistrement d'événement de vulnérabilité s'il n'est plus nécessaire.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche
Vous pouvez supprimer les CVE ou les produits affectés associés à l'enregistrement d'évaluation de vulnérabilité. Vous ne pouvez supprimer des entrées de vulnérabilité/CVE associées ou des produits affectés que s'ils sont dans l'état **Nouvelle** évaluation ou **En attente d'évaluation** .

Procédure
1. Accédez à la **Tout** > **Espaces de travail** > **Évaluation de la vulnérabilité**.
2. Sélectionnez l'enregistrement de l'évaluation de vulnérabilité.
3. Sélectionnez l'onglet **Entrées de vulnérabilité** ou l'onglet **Produits affectés** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez le CVE associé ou l'enregistrement du produit affecté.
5. Sélectionnez **Supprimer**.

> **Remarque :** Le bouton **Supprimer** s'affiche uniquement pour un enregistrement d'évaluation dont l'état est **Nouveau** ou **En attente d'évaluation** .

Ajouter un lien connexe à l'enregistrement de l'évaluation

Ajouter des liens et des informations supplémentaires relatifs à l'enregistrement de l'évaluation.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Procédure
1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez l'entrée d'enregistrement de l'évaluation.
3. Sélectionnez l'onglet **Liens connexes** .
4. Entrez une description pertinente dans le champ **Description** .
5. Entrez l'URL dans le champ **Lien** .
6. Sélectionnez **OK**.
   Le lien connexe est ajouté et répertorié dans l'onglet Liens connexes.

Effectuer une évaluation

Après avoir créé l'enregistrement d'évaluation de vulnérabilité et mis à jour les champs d'attribut de risque, exécutez une évaluation de l'enregistrement d'événement.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche
Effectuez une évaluation initiale après la création d'un événement pour une vulnérabilité d'intérêt et déterminé comme présentant un risque pour les systèmes et les données. L'objectif de cette activité est d'analyser plus en détail la menace en mettant à jour l'évaluation des risques avec une évaluation approfondie de l'exposition.

Procédure
1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de la vulnérabilité**.
2. Sélectionnez l'enregistrement approprié dans la liste des enregistrements d'événements d'évaluation de vulnérabilité.
3. Sélectionnez **Évaluer** pour exécuter l'évaluation de vulnérabilité.
   La tâche en arrière-plan Réponse aux vulnérabilités - Traiter l'événement d'évaluation de la vulnérabilité est lancée et une notification pertinente s'affiche.
4. Sélectionnez **Afficher l'état** dans la notification pour afficher l'état de la tâche en cours d'exécution.
5. Sélectionnez **Enregistrer**.

   L'onglet **Évaluations affiche les détails de l'évaluation** . Lorsque l'évaluation est traitée, les VIT ou AVIT associés aux entrées vulnérables ou aux CVE s'affichent dans l'onglet **Éléments vulnérables** ou **Éléments vulnérables de l'application** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

- Les éléments vulnérables ou les TPE associés aux CVE associées sont récupérés pendant l'évaluation. Les CI associés aux éléments vulnérables sont également identifiés et s'affichent dans la table Éléments de configuration affectés.
- Si les CI associés n'existent pas dans la table de CI affectée, les CI identifiés sont ajoutés à la table et la valeur du champ **A un élément vulnérable** est définie sur **Vrai** et la valeur du champ **Source** est définie sur Scanner.
- Si le CI existe déjà dans la table de CI affectée, seule la valeur du champ **A un élément vulnérable** est définie sur **vrai** et la valeur **Champs sources** pour le CI reste la même qu'au moment de la création de l'enregistrement d'évaluation.
- Si des éléments vulnérables sont créés après l'évaluation, une tâche planifiée d'évaluation de vulnérabilité est exécutée pour mettre à jour la table des CI affectés et la source du CI.

Que faire ensuite

- Affecter une priorité et un niveau d'exposition à l'enregistrement de l'évaluation des vulnérabilités
- Ajouter les CI affectés à l'enregistrement de l'évaluation
- Créer des éléments vulnérables pour le CI affecté ou le composant logiciel affecté
- Ajouter un lien connexe à l'enregistrement de l'évaluation

Information associée

Onglet Évaluation

Onglet Vue d'ensemble

Onglet Évaluation

Examinez les résultats de l'évaluation dans l'onglet Évaluation. Une fois que vous avez effectué une évaluation de l'événement de vulnérabilité, l'enregistrement est corrélé aux données de et de Nomenclature logicielle et Gestion des actifs logiciels affiché avec des visualisations.

L'onglet Évaluation renseigne les données (le cas échéant) en fonction de l'enregistrement d'évaluation que vous créez et met en corrélation les détails avec les évaluations de la CMDB et Nomenclature logicielle les données des Gestion des actifs logiciels composants.

Mode de fonctionnement de l'évaluation

En cliquant sur le bouton **Évaluer** , une évaluation de toutes les CVE associées et des produits affectés utilisant les deux Gestion des actifs logicielsSBOM et les données est lancée. Une tâche en arrière-plan est déclenchée et, lorsque l'évaluation est traitée, les VIT ou AVIT associés aux entrées vulnérables ou aux CVE s'affichent dans les **onglets Éléments vulnérables** et **Éléments vulnérables de l'application** .

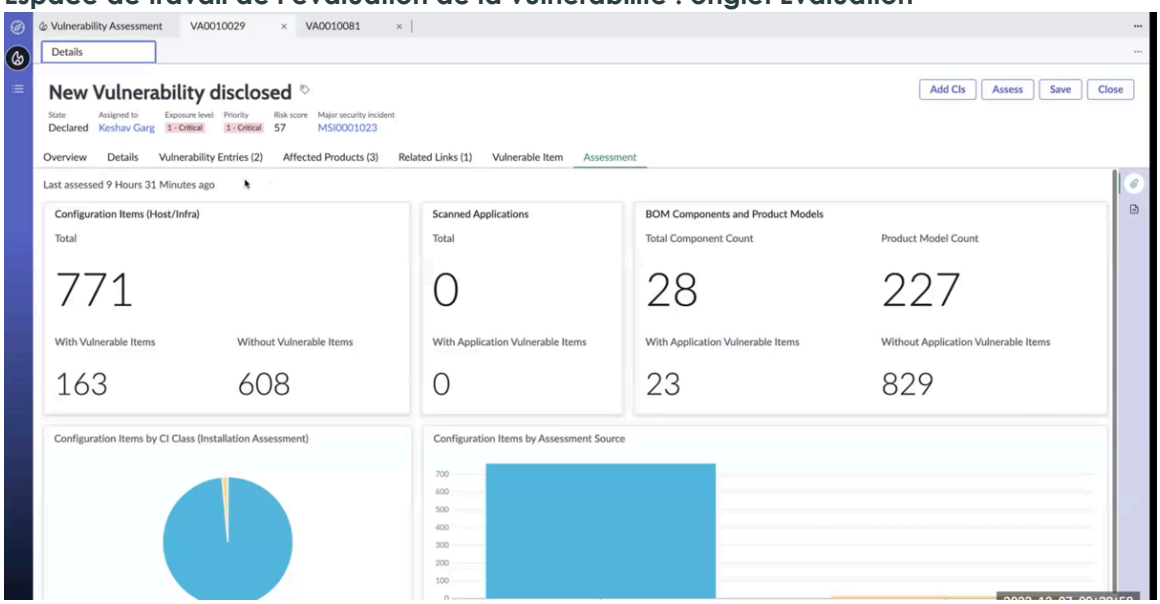
- Tous les éléments vulnérables ou TPE liés aux CVE sont identifiés.
- Les éléments de configuration (CI) associés aux éléments vulnérables sont également identifiés et s'affichent dans la table Éléments de configuration affectés.
- Si les CI ne figurent pas dans la table de CI affectés, les CI identifiés sont ajoutés à la table, le marqueur **A un élément vulnérable** prend la valeur vrai et la valeur du champ **Source** est définie sur Scanner.
- Si le CI existe déjà dans la table des éléments de configuration affectés, seul le marqueur **A un élément vulnérable** est défini sur vrai et la **source** reste inchangée depuis la création de l'enregistrement d'évaluation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si des éléments vulnérables sont créés après l'évaluation, une tâche planifiée d'évaluation de vulnérabilité est exécutée pour mettre à jour la table des CI affectés et la source du CI.
- Dans l'espace de travail Évaluation, vous pouvez afficher les horodatages pour voir la dernière évaluation des événements. L'onglet **Évaluation** n'est visible que lorsque les nouvelles évaluations sont créées. Si l'état de l'évaluation est En cours, le dernier état de la dernière évaluation s'affiche car l'évaluation est en cours. Pour afficher l'état de l'évaluation mis à jour, vous devez actualiser la page. Une fois l'évaluation terminée, l'utilisateur pourra voir tous les onglets associés à cette évaluation.

Espace de travail de l'évaluation de la vulnérabilité : onglet Évaluation



Les détails de l'évaluation s'affichent pour les widgets suivants.

- Éléments de configuration (Hôte/Infra)
- Applications numérisées
- Composants de nomenclature et modèles de produits
- Éléments de configuration par classe CI (évaluation de l'installation)
- Éléments de configuration par source d'évaluation : affiche la liste des éléments de configuration affectés.

Visualisations des données

Nom	Type	Description
Éléments de configuration (Hôte/Infra)	Score unique	Affiche le nombre de CI avec et sans VI. Le widget Éléments de configuration affiche le nombre total de CI associés à l'enregistrement d'évaluation. Le widget affiche en outre les éléments de configuration avec des

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
		éléments vulnérables et sans éléments vulnérables.
Applications numérisées	Nombre	Nombre total d'applications analysées avec AVIT. **Remarque :** Vous pouvez afficher le nombre d'applications analysées pour les CVE primaires et secondaires.
Composants de nomenclature et modèles de produits	Score unique	Nombre total de composants, nombre de modèles de produits, avec éléments vulnérables de l'application, sans nombre d'éléments vulnérables de l'application.
Éléments de configuration par source d'évaluation	Barre empilée	Éléments de configuration affectés empilés par la source d'évaluation.
Éléments de configuration par classe CI (évaluation de l'installation)	Graphique circulaire	Éléments de configuration empilés par classe CI.

Onglet Vue d'ensemble

La vue d'ensemble des détails de l'évaluation s'affiche dans l'onglet Vue d'ensemble. Une fois l'évaluation initiale effectuée, l'enregistrement est corrélé aux données de et Gestion des actifs logiciels et Nomenclature logicielle affiché avec des visualisations.

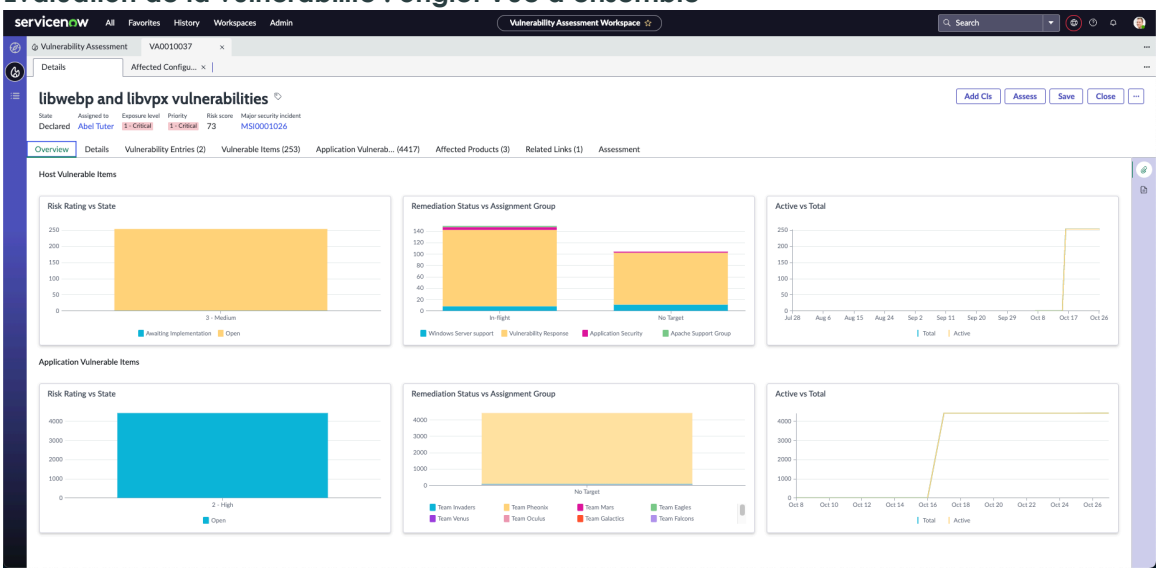
Onglet Vue d'ensemble

L'onglet Vue d'ensemble renseigne les données (le cas échéant) en fonction de l'enregistrement d'évaluation que vous créez et met en corrélation les détails avec les évaluations et Nomenclature logicielle les données de Gestion des actifs logiciels la CMDB. Le champ

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluation de la vulnérabilité : onglet Vue d'ensemble



Les détails de l'évaluation s'affichent pour les widgets suivants.

- Éléments vulnérables de l'hôte (Hôte/Infra)
  - Cote de risque par rapport à l'état
  - État du rattrapage par rapport au groupe d'affectation
  - Actif par rapport à total
- Éléments vulnérables de l'application
  - Cote de risque par rapport à l'état
  - État du rattrapage par rapport au groupe d'affectation
  - Actif par rapport à total

Visualisations des données

Éléments vulnérables d'hôte

Nom	Type	Description
Cote de risque par rapport à l'état	Barre empilée	État des éléments vulnérables empilés par leur cote de risque.
État du rattrapage par rapport au groupe d'affectation	Barre empilée	État du rattrapage de l'élément vulnérable empilé par son groupe d'affectation.
Actif par rapport à total	Liste et ligne	Nombre total d'éléments vulnérables associés à cette entrée par rapport aux éléments vulnérables actifs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Éléments vulnérables de l'application

Nom	Type	Description
Cote de risque par rapport à l'état	Barre empilée	État des éléments vulnérables de l'application empilés par leur cote de risque.
État du rattrapage par rapport au groupe d'affectation	Barre empilée	État du rattrapage de l'élément vulnérable de l'application empilé par son groupe d'affectation.
Actif par rapport à total	Liste et ligne	Nombre total d'éléments vulnérables de l'application associés à cette entrée par rapport aux éléments vulnérables actifs.

Affecter une priorité et un niveau d'exposition à l'enregistrement de l'évaluation des vulnérabilités

Affectez manuellement une priorité et un niveau d'exposition à l'enregistrement d'évaluation de vulnérabilité.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez un enregistrement d'évaluation de vulnérabilité.
3. Accédez aux **attributs de risque** dans l'onglet **Détails** .
4. Sélectionnez une **priorité** dans la liste des options.
5. Sélectionnez un **niveau d'exposition** dans la liste des options.
6. Sélectionnez **Enregistrer**.

Ajouter les CI affectés à l'enregistrement de l'évaluation

Ajoutez manuellement dans votre organisation les CI qui, selon vous, devraient être associés à l'enregistrement de l'évaluation de vulnérabilité, mais qui ne s'affichent pas dans les CI affectés après l'évaluation initiale .

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche
Ajoutez des CI dont vous savez qu'ils peuvent avoir été affectés, mais qui ne s'affichent pas une fois l'évaluation terminée. Vous ne pouvez ajouter des CI que lorsque l'enregistrement de l'évaluation est à l'état **Déclaré** ou **En attente d'évaluation** .

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez l'enregistrement d'évaluation requis dans la liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez **Ajouter des CI**.
4. Sélectionnez les éléments de configuration dans la boîte de dialogue Éléments de configuration.
5. Sélectionnez **Ajouter des CI**.
   La tâche en arrière-plan Réponse aux vulnérabilités - Ajouter des éléments de configuration à l'événement est lancée et une notification pertinente s'affiche.
6. Sélectionnez **Afficher l'état** dans la notification pour afficher l'état de la tâche en cours d'exécution.

Résultats
Les enregistrements sont ajoutés à la table Éléments de configuration affectés avec **Source** comme *Manuel*.

Que faire ensuite
Accédez à l'onglet **Évaluation** et actualisez le widget **Éléments de configuration (Hôte/Infra)** pour afficher les CI que vous avez ajoutés.

Créer des éléments vulnérables pour le CI affecté ou le composant logiciel affecté

Créez des éléments vulnérables (VI) ou des éléments vulnérables de l'application (AVIT) à partir de l'espace de travail d'évaluation de la vulnérabilité. Les analystes de vulnérabilité analysent la liste des éléments vulnérables et recommandent des solutions et des correctifs qui aident l'équipe informatique à corriger ces vulnérabilités.

Le gestionnaire des événements de vulnérabilité doit être en mesure de sélectionner un, plusieurs ou tous les résultats de recherche d'exposition pour créer des éléments de vulnérabilité.

- Élément vulnérable de l'application pour les résultats d'évaluation de nomenclature logicielle qui n'ont pas d'AVIT associés
- Éléments vulnérables pour les éléments de configuration qui n'ont pas de VIT associés
- Associez les CVE primaires aux éléments de vulnérabilité.

Créer des VI pour les éléments de configuration sans éléments vulnérables associés

Créez des VIT d'éléments vulnérables pour les éléments de configuration identifiés via l'évaluation de vulnérabilité, mais qui n'ont pas de VIT associés à l'enregistrement.

Avant de commencer
Rôle requis : administrateur

Procédure
1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluations**.
2. Sélectionnez l'enregistrement d'évaluation pour lequel vous devez créer le VIT.
3. Sélectionnez l'onglet **Évaluation** .
4. Sélectionnez **Sans nombre d'éléments de configuration** à partir du widget **Éléments de configuration (Infra hôte).**
5. Sélectionnez les éléments de configuration pour lesquels vous souhaitez créer des VIT dans la liste **Éléments de configuration affectés** .
6. Sélectionnez **Créer un élément vulnérable**.
   Le travail en arrière-plan Vulnerability Response - Create Manual VIT Assessment Vul Assessment est lancé et une notification pertinente s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Sélectionnez **Afficher l'état** dans la notification pour afficher l'état de la tâche en cours d'exécution.
   Les éléments vulnérables pour les éléments de configuration affectés que vous avez sélectionnés sont créés.

   Le widget **Éléments de configuration (Infra hôte)** affiche désormais le même CI dans le nombre **Avec éléments vulnérables** .

Créer des éléments vulnérables de l'application (AVIT) pour les produits, modèles ou composants affectés sans éléments vulnérables de l'application associés

Créez des éléments vulnérables de l'application (AVIT) pour les produits ou composants affectés, éléments identifiés via l'évaluation de vulnérabilité, mais n'ayant pas d'AVIT associés à l'enregistrement.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluations**.
2. Sélectionnez l'enregistrement d'évaluation pour lequel vous devez créer le VIT.
3. Sélectionnez l'onglet **Évaluation** .
4. Sélectionnez **Nombre d'éléments vulnérables d'application sans** dans le widget **Composants de nomenclature et Modèles de produits** .
5. Sélectionnez les modèles de produits affectés pour lesquels vous souhaitez créer des AVIT dans la liste **Modèles de produits affectés** .
6. Sélectionnez **Créer un élément vulnérable de l'application**.
   Le travail en arrière-plan Vulnerability Response - Create Manual VIT Assessment Vul Assessment est lancé et une notification pertinente s'affiche.
7. Sélectionnez **Afficher l'état** dans la notification pour afficher l'état de la tâche en cours d'exécution.
   Les éléments vulnérables de l'application pour les modèles de produits affectés que vous avez sélectionnés sont créés. pour les CVE primaires associées à l'enregistrement.

   Les widgets **Composants de nomenclature et Modèles de produits** affichent désormais le même modèle de produit ou le même composant dans le décompte **Avec éléments vulnérables de l'application** .

Lier l'enregistrement de l'évaluation des vulnérabilités à un incident de sécurité majeur dans Gestion des incidents de sécurité majeurs

Vous pouvez lier, proposer ou promouvoir l'enregistrement de l'évaluation à condition d'avoir Incident de sécurité majeur accès à l'application Gestion des incidents de sécurité majeurs .

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager, sn_si.analyst, sn_msi.workspace_admin

Pourquoi et quand exécuter cette tâche
Vous pouvez déplacer l'enregistrement d'évaluation pour qu'il soit associé à un incident de sécurité majeur existant, créer un nouveau MSI à partir de l'enregistrement d'évaluation ou promouvoir l'enregistrement de l'évaluation des vulnérabilités en incident de sécurité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

majeur. Exploitez les fonctionnalités telles que les Gestion des incidents de sécurité majeurs intégrations avec Microsoft Teams et Microsoft SharePoint.

Vous pouvez également afficher le lien vers les incidents de sécurité majeurs sur l'espace de travail du gestionnaire de vulnérabilité pour les éléments vulnérables. Le MSIM lien sera associé à l'évaluation de vulnérabilité qui s'affichera sur les éléments de vulnérabilité ainsi que sur les autres espaces de travail de Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez l'enregistrement d'évaluation que vous souhaitez associer à un incident de sécurité majeur.
3. Sélectionnez l'icône **Actions supplémentaires** , dans l'onglet **Détails** .
4. Sélectionnez l'une des options suivantes :

Option	Description
Lier à l'incident de sécurité majeur	Sélectionnez l'enregistrement MSI existant dans la liste des incidents de sécurité majeurs. L'enregistrement de l'évaluation des vulnérabilités est lié à l'incident de sécurité majeur existant.
Proposer comme incident de sécurité majeur	Entrez les détails suivants et sélectionnez **Proposer**. ◦ Date de détection ◦ Justification ◦ Impact potentiel
Promouvoir comme incident de sécurité majeur	Renseignez les données suivantes et sélectionnez **Promouvoir**. ◦ Date de détection ◦ Date de résolution estimée ◦ Justification ◦ Impact potentiel

5. Sélectionnez **Enregistrer**.

Que faire ensuite

Sélectionnez l'enregistrement MSI pour ouvrir l'enregistrement dans la Gestion des incidents de sécurité majeurs vue.

Information associée

Lier à Incident de sécurité majeur

Proposer en tant que Incident de sécurité majeur

Promouvoir à Incident de sécurité majeur

Traduction automatique

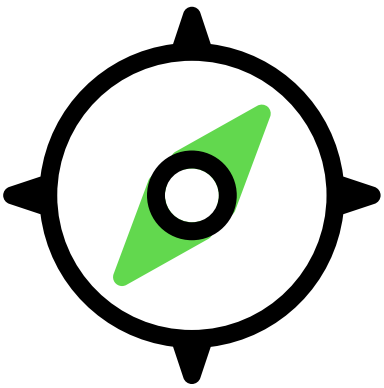
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nomenclature logicielle

Consultez la liste des composants logiciels open source et tiers que vous utilisez dans le développement de votre application. Obtenez un aperçu des licences logicielles, des informations de version et des vulnérabilités connues de vos composants dans les Nomenclature logicielle fichiers (SBOM) que vous chargez dans votre instance.

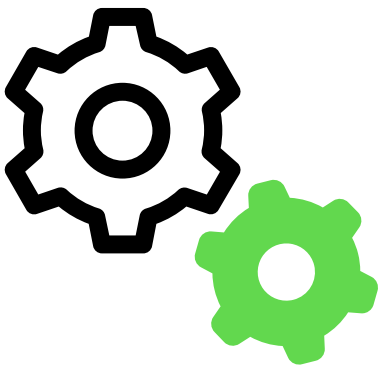
Premiers pas

Explorer



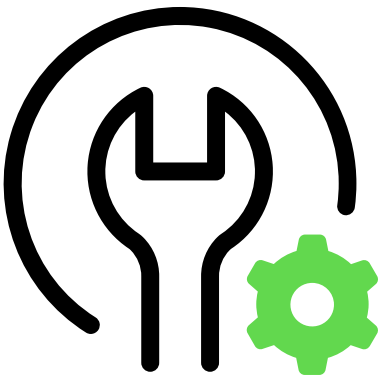
En savoir plus sur SBOM les concepts et les fonctionnalités.

Configurer



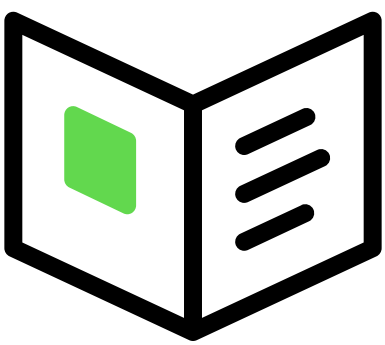
Configurer SBOM les applications.

Utiliser



Découvrez comment importer SBOM des composants et afficher des données dans l'espace de travail.

Référence



Obtenez des détails sur SBOM les formulaires, les champs, les tables et les propriétés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage et demande d'aide

- Communauté Security Operations
- CycloneDX - Nomenclature logicielle (SBOM).
- SPDX .
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues .
- Contact Service et assistance client.

Explorer Nomenclature logicielle

Identifiez les composants utilisés dans les applications de votre organisation à partir des Nomenclature logicielle fichiers (SBOM) que vous chargez dans votre instance. Comprenez tous les risques associés à l'utilisation de logiciels open source pour vous aider à déterminer votre exposition potentielle et à corriger les vulnérabilités.

Versions disponibles Nomenclature logicielle

Version	Notes de publication
Modèle de données pour SBOM v 2.0, v1.4, v1.3, v1.1, v1.0	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production Notes de publication Réponse aux vulnérabilités des applications
SBOM Core v4.0, v3.0, v2.1, v2.0, v1.0	
SBOM Réponse v4.0, v3.2, v3.1, v3.0, v2.0	

Cas d'utilisation d'SBOM

À partir des versions répertoriées dans la table, les cas d'utilisation des opérations de développement logiciel (DevOps) pour le SBOM chargement de fichiers à partir de pipelines d'intégration continue et de livraison/déploiement en continu (CI/CD) sont pris en charge. Consultez Chargement des Nomenclature logicielle fichiers DevOps SBOM pour plus d'informations.

Version	Application
v1.4 et versions ultérieures	Modèle de données pour SBOM
v3.0 et versions ultérieures	SBOM Core
v4.0 et versions ultérieures	SBOM Réponse

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les composants tiers et open source vous offrent de nombreux avantages pour la création et la publication rapides de vos projets logiciels. Toutefois, dans certains cas, l'utilisation de composants accessibles au public présente des risques, tels que les suivants :

- Manque de visibilité sur l'intégrité des composants
- Vulnérabilités dans le logiciel open-source
- Package Intelligence pour les logiciels open source

Trois Nomenclature logicielle applications vous permettent de visualiser un inventaire précis de vos composants logiciels et des risques associés :

- Modèle de données pour SBOM
- SBOM Core
- SBOM Réponse

Vous pouvez télécharger vos fichiers de nomenclature logicielle via une API ou manuellement. Affichez les fichiers que vous importez en tant qu'entités, qui sont des inventaires des bibliothèques de composants tiers utilisées dans votre logiciel, y compris les dépendances transitives.

Pour plus d'informations sur ce qui est inclus dans les inventaires logiciels dans les SBOM CycloneDX et SPDX, consultez CycloneDX - Nomenclature logicielle (SBOM) et SPDX .

Modèle de données pour SBOM

Cette application fournit les tables utilisées pour stocker les données SBOM.

SBOM Core

À partir de la version 3.0 de SBOM Core, chargez, analysez et traitez vos fichiers de nomenclature logicielle dans les normes CycloneDX et SPDX. Reportez-vous au tableau suivant pour connaître les formats de fichiers et les versions pris en charge pour ces produits. Affichez les entités de nomenclature (BOM) et un inventaire de vos composants logiciels. Une entité BOM est le composant de niveau racine d'un SBOM fichier. Par exemple, pour une nomenclature logicielle CycloneDX, le composant répertorié dans les métadonnées est considéré comme l'entité BOM.

Version de SBOM Core	Versions prises en charge de CycloneDx et SPDX
v4.0	XML et JSON dans CycloneDx (versions 1.0 - 1.6) JSON dans SPDX (versions 2.2-2.3)
v3.0	XML et JSON dans CycloneDX (jusqu'à la version 1.4 incluse) XML dans SPDX (jusqu'à la version 2.3 incluse)

Reportez-vous à la section intitulée Utilisation de l'API REST dans Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API pour plus d'informations sur les améliorations apportées à la prise en charge du format CycloneDX.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de la version 4.0 de SBOM Core, vous pouvez télécharger SBOM des fichiers dans vos Now Platform®GitHub référentiels.

Déterminez si SBOM les fichiers générés dans vos pipelines CI/CD (intégration continue et livraison/déploiement continus) ont été correctement mis en file d'attente dans votre Now Platform® instance.

- Protégez vos environnements contre les composants potentiellement dangereux pendant les cycles de développement logiciel avec GitHub les actions que vous lancez à partir de votre GitHub environnement.
- Obtenez toutes les actions requises GitHub pour SBOM le chargement dans GitHub Marketplace.

SBOM Réponse

Affichez l'inventaire de vos composants et évaluez votre exposition aux risques dans l'espace de travail SBOM. Vous pouvez identifier si des vulnérabilités connues sont associées aux composants logiciels et afficher les informations de gestion des licences et de version, ainsi que d'autres détails.

Consultez le tableau suivant pour plus d'informations sur chaque ServiceNow® application SBOM.

Applications requises pour SBOM

Application ServiceNow	**Description**
Modèle de données pour SBOM	Cette application est requise. Il comprend les tables, les ACL et les rôles requis pour lire SBOM les données.
SBOM **Noyau**	Cette application est requise. Il comprend l'API requise pour charger SBOM les documents et la logique métier requise pour analyser et importer les données de ces documents dans votre instance. À partir de la version 2.1, vous pouvez afficher un inventaire de vos composants logiciels dans SBOM Workspace.
SBOM **Réponse**	À partir de la version 4.0 de Response, vous pouvez afficher les composants identifiés comme périmés ou abandonnés comme « non conformes » dans l'interface Policy as Code Engine (PaCE) disponible dans l'espaceSBOM de SBOM travail. • Déterminez si les composants sont périmés ou abandonnés avec la tâche planifiée Exécuter les stratégies PaCE pour la réponse SBOM. La tâche planifiée est désactivée par défaut. • Affichez les composants identifiés comme périmés ou abandonnés comme non conformes dans l'interface PaCE disponible dans l'espace de travail SBOM. SBOM La réponse nécessite l'application Réponse aux vulnérabilités . Installez l'application Réponse aux vulnérabilités avant d'installer SBOM la réponse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications requises pour SBOM (suite)

Application ServiceNow	**Description**
	Affichez l'inventaire de vos composants et évaluez votre exposition au risque dans l'espace SBOM de travail. Configurez des règles pour créer automatiquement des éléments vulnérables de l'application (AVIT) et corrigez-les avec le workflow Application Vulnerability Response. Les intégrations OSV.dev et Deps.dev sont incluses lors de l'installation SBOM de Response. • OSV.dev est une API open source qui fournit des informations de renseignements sur la vulnérabilité pour une version donnée d'un package ou d'une bibliothèque. • Deps.dev est une API open source qui fournit une liste de versions pour un package ou une bibliothèque donnée.

L'installation de l'intelligence de vulnérabilité tierce prise en charge et d'autres intégrations vous permet d'afficher le nombre de composants considérés comme périmés et abandonnés, ainsi que des informations indiquant si vous pouvez corriger les vulnérabilités associées aux composants. Les ServiceNow® applications et intégrations tierces répertoriées dans le tableau suivant sont prises en charge par l'application SBOM . Ces applications vous fournissent des données de vulnérabilité enrichies, des renseignements sur les vulnérabilités et d'autres informations clés qui peuvent vous aider à afficher et à hiérarchiser les vulnérabilités associées aux SBOM fichiers. Toutes ces applications et intégrations sont disponibles à partir du ServiceNow Storefichier .

Applications tierces prises en charge pour SBOM

Application	**Description**
Réponse aux vulnérabilités	Requis si vous installez l'application SBOM Response. Réponse aux vulnérabilités des applications Les fonctionnalités sont installées avec Réponse aux vulnérabilités. Ces fonctionnalités permettent d'accéder à l'espace de travail du gestionnaire de vulnérabilités dans l'application Réponse aux vulnérabilités et au workflow de vulnérabilité pour vous aider à corriger les éléments vulnérables de l'application (AVIT).
Intégration de Vulnerability Response avec NVD	Affichez des données améliorées sur la vulnérabilité et la gravité NVD. Si vous avez installé SBOM Response, vous pouvez afficher les données importées à partir des intégrations NVD et CWE pour enrichir toutes les données de vulnérabilité que vous pourriez trouver dans vos SBOM données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications tierces prises en charge pour SBOM (suite)

Application	Description
	Consultez Importation de données avec les intégrations NVD et CWE et gestion des bibliothèques tierces pour plus d'informations.
Veracode Vulnerability Integration	La version 4.3 de la Veracode Vulnerability Integration inclut les améliorations suivantes avec Veracode SBOM les fichiers : • Si vous avez installé SBOM Response, vous avez la possibilité d'inclure les vulnérabilités trouvées par Veracode pour les fichiers SBOM que vous téléchargez. • Veracode est mappé au champ **Source** des enregistrements de la table Nomenclature [sn_sbom_doc] pour les Veracode fichiers SBOM que vous chargez. Importez des fichiers de nomenclature logicielle avec le Veracode Vulnerability Integrationfichier . Si cette intégration est déjà installée, vous pouvez également télécharger les données importées Veracode SBOM aux formats CycloneDX (JSON et XML) et SPDX (XML) à partir de la version v3.0 de SBOM Core.

Installer les applications prises en charge pour Nomenclature logicielle

Téléchargez et activez les applications requises pour l'application (SBOM) avant de Nomenclature logicielle charger les fichiers.

Avant de commencer

Rôles requis : administrateur pour le téléchargement, l'installation et l'activation de toutes les applications et affectations de rôles dans votre instance.

Pourquoi et quand exécuter cette tâche

Procédure

1. Téléchargez les applications requises SBOM à partir de dans ServiceNow Store votre ServiceNow instance.

   Ces applications vous permettent de charger et d'importer SBOM des fichiers dans votre instance. Vous pouvez afficher les données de composant dans l'espace de travail à partir de la SBOM version 2.1 de SBOM Core.

   - Modèle de données pour SBOM
   - SBOM Core

   Pour en savoir plus sur le téléchargement et l'activation des applications, consultez les rubriques suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Security Operations et ServiceNow Store
-

2. Facultatif : Si vous souhaitez afficher vos SBOM données dans l'espace SBOM de travail, afficher les informations sur les vulnérabilités tierces importées, évaluer votre exposition aux risques et corriger les vulnérabilités à l'aide des workflows Application Vulnerability Response et Vulnerability Response, téléchargez les applications suivantes :
   - Réponse aux vulnérabilités et ses dépendances
   - Intégration de Vulnerability Response avec NVD
   - SBOM Réponse

   Pour en savoir plus sur ces applications et sur d'autres applications prises en charge SBOM , reportez-vous à la section Explorer Nomenclature logicielle.

3. Une fois les applications téléchargées, accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
4. Localisez les SBOM applications que vous avez téléchargées et sélectionnez **Installer** pour les activer ainsi que leurs dépendances.

   Un message s'affiche lorsqu'une application est activée avec succès. Activez les applications dans l'ordre suivant :

   - Réponse aux vulnérabilités et ses dépendances
   - Intégration de Vulnerability Response avec NVD
   - Modèle de données pour SBOM
   - SBOM Core
   - SBOM Réponse, qui inclut les intégrations OSV.dev et Deps.dev

   Pour Configuration des intégrations Deps.dev et OSV.dev pour Nomenclature logicielle plus d'informations sur la configuration de ces applications d'intégration après l'installation SBOM de Response, reportez-vous à la section .

5. Facultatif : Activez les intégrations en accédant à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout** et en sélectionnant **Installer**.

   (Optional) Pour en savoir plus sur ces intégrations et les options qu'elles offrent, reportez-vous à la section Explorer Nomenclature logicielle.

   - Intégration de Vulnerability Response avec Veracode. Consultez Installer l'intégration de ServiceNow Vulnerability Response avec Veracode pour plus d'informations.
   - Vulnerability Response Integration with NVD, qui est nécessaire si vous souhaitez afficher les données améliorées pour les vulnérabilités associées aux composants chargés. Consultez Présentation des intégrations NVD pour plus d'informations.
   - Intégration complète de CWE 2000. Reportez-vous à la rubrique Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE pour en savoir plus sur l'activation de cette tâche planifiée.

   Un message s'affiche lorsqu'une application est activée avec succès.

6. Affectez les rôles suivants aux utilisateurs.
   - sn_sbom_dm.app_créer
   - sn_sbom_dm.app_read

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_sbom_dm.app_écriture
- sn_sbom_core.sbom_ingest
- sn_sbom_core.admin
- sn_sbom_resp.sbom_analyst
- sn_sbom_resp.manage_avi_rule

7. Facultatif : Affectez des utilisateurs au groupe App-Sec Manager si vous créez des éléments vulnérables de l'application pour des vulnérabilités dans vos données importées SBOM .

   (Optional) Les utilisateurs affectés au groupe App-Sec Manager priorisent et gèrent les éléments vulnérables de l'application. Les utilisateurs de ce groupe héritent d'un grand nombre des rôles nécessaires à la lecture et à la modification des enregistrements, ainsi qu'à la configuration des applications prises en charge par l'application Réponse aux vulnérabilités des applications et ses workflows de rattrapage.

Que faire ensuite

Chargez vos SBOM fichiers. Voir Charger Nomenclature logicielle des fichiers manuellement et Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API pour plus d'informations.

Configuration des intégrations Deps.dev et OSV.dev pour Nomenclature logicielle

Vous pouvez modifier certains paramètres pour les intégrations Deps.dev et OSV.dev. Il existe deux intégrations de déclencheur de code qui sont utilisées uniquement pour les flux de travail internes.

Intégrations de déclencheurs de code pour les workflows internes

À partir de la version 3.2 de Response, les améliorations de performances comprenaient l'ajout de SBOM deux intégrations pour OSV.dev et Deps.dev :

- Intégration OSV (déclencheur de code à la demande)
- Intégration Deps.dev (déclencheur de code sur demande)

Ces intégrations sont initiées automatiquement par des workflows internes et ne sont destinées qu'à un usage interne. Vous ne devez pas lancer ces intégrations à la demande avec le bouton **Exécuter maintenant** sur leurs enregistrements d'intégration.

Configuration du calendrier d'exécution pour Deps.dev

Si elle est installée, l'intégration Deps.dev est activée par défaut (case Actif sélectionnée sur l'enregistrement d'intégration) et son exécution est planifiée chaque semaine. Vous pouvez modifier le calendrier et lancer la tâche planifiée sur demande à partir de l'enregistrement d'intégration. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Intégrations** > **Intégration Deps.dev**. Le rôle sn_vul.app_configure_integrations est requis pour modifier le calendrier de cette intégration.

L'intégration Deps.dev est utilisée pour identifier les composants qui sont dans **les états périmés** et **abandonnés** . La version d'un composant périmé a plus de deux versions majeures de retard sur la dernière version et deux ans de retard sur la dernière version. Un composant abandonné n'a pas été mis à jour depuis plus de deux ans. Les seuils de deux ans et de deux versions peuvent être modifiés avec les propriétés système. Pour modifier ces paramètres, accédez à **Tout** > **Propriétés système** > **Toutes les propriétés** et localisez les enregistrements suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_sbom_resp.pkg_abandoned_threshold
- sn_sbom_resp.pkg_stale_threshold
- sn_sbom_resp.pkg_stale_version_threshold

Les valeurs de seuil pour Abandonné et Périmé sont en mois. La valeur de seuil pour la version est numérique.

Configurer OSV.dev

Si elle est installée, l'intégration OSV.dev est activée (case Actif sélectionnée sur l'enregistrement d'intégration) par défaut, mais vous devez la lancer sur demande à partir de l'enregistrement d'intégration. Accédez à la **Tout** > **Réponse aux vulnérabilités** > **Intégrations** > **Intégration OSV.dev : complète**. Le rôle sn_vul.app_configure_integrations est requis pour modifier le calendrier de cette intégration.

Remarque : Vous pouvez configurer le paramètre d'intégration OSV.dev au niveau de l'intégration des vulnérabilités *batchSize* Open Source. La valeur par défaut est de 75 Purls par appel d'API.

Vous préférerez peut-être conserver cette valeur dans son paramètre par défaut. La modification de la valeur peut avoir un impact sur les performances.

Utilisation de l'espace de Nomenclature logicielle travail

Les SBOM applications vous permettent de charger des fichiers et d'afficher les détails des entités et des inventaires de composants dans l'espace Nomenclature logicielle de travail (SBOM).

Les SBOM applications vous permettent d'effectuer les tâches suivantes :

1. Téléchargez des fichiers avec une API ou manuellement.

   Voir Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API et Charger Nomenclature logicielle des fichiers manuellement, et Chargement des Nomenclature logicielle fichiers DevOps SBOM pour plus d'informations.

2. Passez en revue les composants BOM chargés dans l'espace de travail. La façon dont vous vérifiez les composants dépend des applications que vous avez installées.

   Consultez Afficher les rapports et les tableaux de bord dans l'espace de Nomenclature logicielle travail pour plus d'informations.

3. Évaluez votre exposition au risque et créez des éléments vulnérables de l'application pour les composants qui présentent des vulnérabilités associées.
   - Identifiez si des vulnérabilités connues sont associées aux composants logiciels.
   - Passez en revue les détails des renseignements sur les vulnérabilités améliorés tels que les informations sur les versions, la disponibilité des versions corrigées et les informations sur la gestion des licences pour vous aider à résoudre les éléments vulnérables.

   Voir Afficher les rapports et les tableaux de bord dans l'espace de Nomenclature logicielle travail et Création de règles pour les éléments vulnérables de l'application dans l'espace Nomenclature logicielle de travail pour plus d'informations.

Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API

Vérifiez les informations suivantes avant de Nomenclature logicielle charger des fichiers à l'aide d'une API.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation de REST API

Pour charger un fichier SBOM avec une API, le rôle sn_sbom_core.sbom_ingest est requis.

Charger l'API.

Cette API est utilisée pour charger et ingérer un fichier SBOM (CycloneDX/SPDX) dans votre instance.

La version 4.0 de SBOM Core prend en charge :

- XML et JSON dans CycloneDx (versions 1.0 - 1.6).
- JSON dans SPDX (versions 2.2-2.3)

- **Remarque :** Les fichiers de plus de 32 Mo peuvent ne pas se charger correctement.

Méthode HTTP : (POST)

URL de *l'API : <host_name>/api/sbom/core/upload*

Remarque : *<host_name> s'agit* de votre ServiceNow nom d'instance.

Tous les paramètres de demande ci-dessous sont facultatifs ; le corps de la demande est le contenu du fichier SBOM. Si vous utilisez DevOps dans le cadre de votre processus de développement, la valeur de « requestedBy » doit être « devops ». Pour plus d'informations générales sur DevOps, consultez la rubrique Chargement des Nomenclature logicielle fichiers DevOps SBOM Si la valeur de « requestedby » est « devops » (opérations de développement), les paramètres suivants sont obligatoires :

- ID de construction
- lifecycleStage

En outre, si « requestedBy » est « devops », les données pour fetchVulenrabilityInfo et fetchPackageInfo sont incluses.

- buildId : chaîne que vous envoyez
- lifecycleStage : deux valeurs, production ou pre_production
- fetchVulenrabilityInfo- t/f
- fetchPackageInfo-t/f

Paramètres de demande	Valeurs possibles	Description
ID modèle produit	ID système	ID système du modèle de produit à mapper avec l'application racine de la nomenclature logicielle donnée.
ID d'application commerciale	ID système	ID système de l'application d'entreprise à mapper avec l'application racine de la nomenclature logicielle donnée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de demande	Valeurs possibles	Description
businessApplicationName (en anglais seulement)	Nom de votre application d'entreprise	Nom de l'application d'entreprise à mapper avec l'application racine de la nomenclature logicielle donnée.
sbomSource (en anglais seulement)	Un produit tel que Vericode, par exemple	La source de votre fichier SBOM.
requestedBy	Un outil, ou le nom d'une méthodologie, Jenkins. Si vous utilisez « devops », buildId et lifecycleStage sont obligatoires.	Chargement demandé par
ID de construction	Une chaîne envoyée par le demandeur.	ID de build de la build SBOM.
lifecycleStage	Production ou pre_production	Étape du cycle de vie de l'entité.
fetchVulenrabilityInfo	T/F	Si vrai, déclenche l'intégration de l'intelligence des vulnérabilités.
informations sur le package fetchPackage	T/F	Si vrai, déclenche l'intégration de l'intelligence du package.

Réponse API de chargement : réussite/échec « état » inclus, « message » (chaîne), « bomRecordId » (il s'agit de l'ID système de la nomenclature logicielle qui est renvoyé via l'API de chargement pour un chargement de nomenclature logicielle réussi.

```
{

"result": {

"status": "success",

"message": "Queued for processing.",

"bomRecordId": "f207059b4393c290629aa597cbb8f247"

}

}
```

API d'état

Cette API obtient l'état et le résumé d'une nomenclature logicielle mise en file d'attente pour l'ingestion.

- URL de l'API : `/api/sbom/core/upload/status`
- Méthode HTTP (GET)

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de demande	Valeurs possibles	Description
BomRecordId (en anglais seulement)	ID système	ID d'enregistrement SBOM renvoyé via l'API de chargement pour un chargement SBOM réussi.

Exemple de réponse par défaut de l'API d'état.

```
{
   "result": {
      "bomRecordId": "0407c0fea3e70a505df340f5251e617e",
      "uploadStatus": "processed",
      "additionalInfoStatus": "not_requested",
      "uploadSummary": {
         "components": {
            "added": 0,
            "removed": 0,
            "total": 70
         }
       }
    }
}
```

Réponse API d'état avec exemple de paramètres supplémentaires. Si vous avez demandé fetchVulenrabilityInfo pour ce SBOM, vous obtenez la répartition des vulnérabilités dans le cadre de la réponse.

```
{
 "result": {

  "bomRecordId": "93af349b4393c290629aa597cbb8f258",

  "uploadStatus": "processed",

  "additionalInfoStatus": "complete",

  "uploadSummary": {

    "components": {

     "added": 0,

     "removed": 0,

     "total": 3

   },

   "vulnerabilityInfo": {

    "critical": 0,

    "high": 0,
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    "medium": 0,
    "low": 0,
    "none": 0
   }
  },
  "buildId": "1"
 }
}
```


Si vous avez demandé fetchPackageInfo pour cette nomenclature logicielle, vous obtenez les nombres périmés et abandonnés dans le cadre de la réponse.

Une fois qu'un SBOM processus est traité avec succès, l'emplacement d'affichage des enregistrements chargés dépend des applications que vous utilisez.

- Si vous utilisez SBOM la réponse, l'enregistrement de l'entité BOM s'affiche dans la liste État d'ingestion SBOM du module File d'attente BOM de l'espace SBOM de travail.
- Si vous utilisez SBOM Core, accédez à **SBOM principal** > **État de l'ingestion BOM**.

Améliorations apportées aux normes prises en charge SBOM et aux informations générales sur l'utilisation

La version 4.0 de SBOM Core prend en charge :

- XML et JSON dans CycloneDx (versions 1.0 - 1.6).
- JSON dans SPDX (versions 2.2-2.3)

- **Remarque :** Les fichiers de plus de 32 Mo peuvent ne pas se charger correctement.

À partir de la version 4.0 de SBOM Core, les améliorations suivantes ont été apportées pour prendre en charge les normes CycloneDx pour les versions 1.0 à 1.6 :

- Importez des informations supplémentaires dans les fichiers SBOM CycloneDX avec la propriété (sn_sbom_core.collect_properties). Cette propriété est désactivée par défaut. Activez la propriété pour importer des informations qui ne sont généralement pas prises en charge. Toutes les informations importées à partir de ces propriétés sont téléchargées dans la table Propriété du composant SBOM [sn_sbom_comp_property] pour ce qui suit :
  - Fichiers SBOM chargés
  - Métadonnées
  - Vulnérabilités individuelles
  - Composants
- Affichez les données de composants importés pour les licences déclarées et conclues pour les fichiers SBOM dans les versions 1.4 et ultérieures de CycloneDX dans deux nouveaux champs de licence :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Déclaré**
- **Conclu**

- La prise en charge de l'analyse SBOM est étendue aux types de composants CycloneDX suivants :
  - Version 1.5 : plateforme, données, pilote d'appareil, modèle d'apprentissage automatique
  - Version 1.6 : Cryptographique

La version 3.0 de SBOM Core prend en charge :

- XML et JSON dans CycloneDx (jusqu'à la version 1.4 incluse).
- JSON dans SPDX (jusqu'à la version 2.3 incluse).

Si l'utilisateur appelant est authentifié avec succès et qu'il dispose du rôle sn_sbom_core.sbom_ingest dans votre ServiceNow instance, vous pouvez accéder à l'API depuis l'extérieur de votre instance pour charger les SBOM données.

Une fois les données chargées, elles sont analysées. Avant l'analyse des données, les exigences suivantes sont vérifiées :

- On vérifie que les données entrantes sont valides au format JSON ou XML.
- Le format BOM est pris en charge. À partir de la version 2.1 de SBOM Core, les formats CycloneDX (JSON et XML) et SPDX (XML) sont pris en charge.
- Le nombre minimum de champs est disponible afin que les données puissent être analysées.

Une fois ces vérifications vérifiées, une entrée est effectuée dans la table Nomenclature [sn_sbom_doc] avec les données entrantes SBOM en pièce jointe.

La *`Process BOM file`* règle métier est déclenchée automatiquement à la suite de l'insertion de l'enregistrement et de l'analyse des données.

Remarque : Cette règle métier est activée par défaut lors de l'installation de SBOM Core.

Tous les composants répertoriés dans un SBOM ont un `type` défini.

- Les composants pour lesquels SBOM les fichiers ont été chargés sont considérés comme des entités BOM.
- Les composants répertoriés comme `type=library` sont considérés comme des composants tiers.

Information associée

Affichage de l'état du chargement des Nomenclature logicielle fichiers

Afficher les rapports et les tableaux de bord dans l'espace de Nomenclature logicielle travail

Charger Nomenclature logicielle des fichiers manuellement

Chargez Nomenclature logicielleSBOM() des fichiers manuellement.

Avant de commencer

Rôle requis : sn_sbom_core.sbom_ingest

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Téléchargez des fichiers manuellement.

La méthode que vous utilisez pour charger vos fichiers varie selon que vous avez installé l'application Core ou SBOM l'application SBOM Response.

À partir de la version 4.1 de Core, les formats de SBOM fichiers SBOM suivants sont pris en charge :

- XML et JSON dans CycloneDX (versions 1.0 à 1.6).
- JSON dans SPDX (versions 2.2 - 2.3).

Option	Description
Si vous avez installé SBOM Core	**a.** Accédez à la **SBOM principal** > **État de l'ingestion BOM**. **b.** Dans la liste Nomenclature, sélectionnez **Nouveau**. **c.** Cliquez sur le lien **Cliquer pour ajouter** . Vous ne pouvez charger qu'un seul SBOM fichier à la fois. **d.** Sélectionnez **Choisir un fichier** et localisez le fichier souhaité. Le nom du fichier s'affiche sur la page Choisir un fichier de pièce jointe. **e.** Sélectionnez **OK**.
Si vous avez installé SBOM Response	**a.** Accédez à la **Tout** > **Espaces de travail** > **Espace de travail SBOM** > **File d'attente BOM**. **b.** Sélectionnez **Charger BOM**. **c.** Sélectionnez **Parcourir** et recherchez le fichier souhaité. Vous ne pouvez charger qu'un seul SBOM fichier à la fois. **d.** Sélectionnez **Charger**. Le fichier s'affiche dans la boîte de dialogue Télécharger SBOM un fichier. **e.** Sélectionnez **Charger** à nouveau.

2. Facultatif : Chargez SBOM des fichiers importés par le Veracode Vulnerability Integrationfichier .

Remarque : Vous pouvez télécharger Veracode des fichiers aux formats CycloneDX (JSON et XML) et SPDX (XML) uniquement si vous avez installé et activé l'intégration Veracode avec Réponse aux vulnérabilités des applications. Voir le pour plus d'informations Veracode Vulnerability Integration .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Une fois qu'un est traité avec succès, l'emplacement SBOM d'affichage de l'état du chargement dépend des applications que vous utilisez.

- Si vous utilisez SBOM la réponse, l'enregistrement de l'entité BOM s'affiche dans la liste État d'ingestion SBOM du module File d'attente BOM de l'espace SBOM de travail.
- Si vous utilisez SBOM Core, accédez à **SBOM principal** > **État de l'ingestion BOM**.

Information associée

Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API

Chargement des Nomenclature logicielle fichiers DevOps SBOM

Générez et téléchargez Nomenclature logicielle SBOM des fichiers pour les logiciels tout au long de leurs cycles de développement d'intégration et de déploiement continus.

SBOM et opérations de développement logiciel

SBOM Les fichiers peuvent être générés à plusieurs étapes tout au long du cycle de développement de l'intégration continue et du déploiement continu du logiciel (CI/CD). La plupart des opérations de développement logiciel (DevOps) dans les organisations utilisent un certain type de processus CI/CD pour les aider à identifier et à prévenir les bogues coûteux qui pourraient apparaître après la publication. Tout au long du pipeline CI/CD, DevOps peut générer des fichiers SBOM et vérifier de manière proactive les vulnérabilités et les composants à risque. Ces vérifications peuvent aider les organisations à obtenir une meilleure qualité logicielle et à éviter une maintenance coûteuse par la suite. La génération de SBOM fichiers est essentielle pour implémenter et automatiser avec succès des évaluations de version précises pendant le développement CI/CD.

Le chargement des fichiers SBOM à partir des pipelines de développement est pris en charge à partir des versions suivantes des SBOM applications.

Versions prises en charge

Application	Versions prises en charge
Modèle de données pour SBOM	v2.0, v1.4
SBOM Core	v4.0 et 3.0
SBOM Réponse	v3.2, 3.1

Cas d'utilisation

La génération SBOM de fichiers et leur envoi via l'API de chargement SBOM dans le cadre du pipeline de version DevOps peuvent fournir des nombres pour les éléments suivants afin de déterminer si le pipeline doit réussir ou échouer :

- Composants ajoutés
- Composants supprimés
- Informations sur les vulnérabilités
- Informations sur le package (composants abandonnés/périmés)

Les politiques et règles DevOps pour la réussite ou l'échec d'un pipeline peuvent être définies par les nombres de vulnérabilités et les seuils de nombre de composants périmés et abandonnés reçus de l'API d'état SBOM .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour un pipeline défaillant, les utilisateurs DevOps peuvent accéder aux informations sur la version échouée dans leur ServiceNow® instance pour les aider à mieux comprendre la cause première et l'origine des vulnérabilités.

Pour plus d'informations sur les paramètres (POST) et (GET) et les URL des API Upload et Status, consultez la section Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API pour en savoir plus sur les paramètres (POST) et (GET) et les URL des API Upload et Status.

Séparation en domaines

Toutes les tables des applications SBOM sont séparées par domaine.

Afficher les rapports et les tableaux de bord dans l'espace de Nomenclature logicielle travail

Les analystes de vulnérabilité consultent les fichiers de nomenclature logicielle chargés dans des enregistrements, des visualisations de données, ainsi que des informations de vulnérabilité améliorées dans l'espace Nomenclature logicielle de travail (SBOM).

Exigences relatives à l'affichage des données

SBOM principal

À partir de la version 2.1 de l'application SBOM Core, vous pouvez afficher les entités BOM et une liste des composants que vous avez téléchargés sur la page d'accueil (de destination) et dans le module Composants de l'espace SBOM de travail. Avant la version 2.1, accédez à **SBOM principal** > **État de l'ingestion BOM** pour afficher les composants.

Réponse SBOM

L'application SBOM Response vous fournit des visualisations de données avec des informations détaillées sur les entités BOM, les entités présentant des vulnérabilités et les éléments vulnérables de l'application actifs sur la page de destination de l'écran d'accueil de l'espace SBOM de travail. L'espace de travail avec SBOM Response comprend les modules suivants :

- Page d'accueil : visualisations de données et détails améliorés sur les vulnérabilités.
- Composants : informations sur les versions et les correctifs des composants.
- AVIT (élément vulnérable de l'application) Règles de création : conditions déterminant quand les éléments vulnérables de l'application (AVIT) sont créés.
- File d'attente BOM : état et historique du chargement des fichiers.
- Liste : enregistrements AVIT pour vos composants et bibliothèques vulnérables (NVD, CWE et vulnérabilités d'applications).

Les rubriques suivantes fournissent plus d'informations sur la façon de localiser les détails de vos composants dans l'espace Nomenclature logicielle de travail.

- #unique_854
- Examen du module Composants dans l'espace Nomenclature logicielle de travail
- Affichage de l'état du chargement des Nomenclature logicielle fichiers
- Vérification des vulnérabilités d'une Nomenclature logicielle entité

Examen du module Composants dans l'espace Nomenclature logicielle de travail

Le module Composants de l'espace Nomenclature logicielle de travail (SBOM) affiche des informations actualisées sur les combinaisons vulnérables, périmées, abandonnées et à haut risque pour les composants que vous importez.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage du module Composants

Rôles requis :

- À partir de la v2.1 de SBOM Core : sn_sbom_resp.sbom_analyst
- Avant la v2.1 de SBOM Core : sn_sbom_resp.admin

Accédez à la **Espaces de travail** > **Espace de travail SBOM** > **Composants**.

Ce que vous pouvez voir dans le module dépend des applications que vous avez installées.

À partir de la version 3.2 de SBOM Response, les données importées ne sont pas calculées et sont renseignées par des requêtes actives. Les scores des pages d'accueil et des composants sont mis à jour une fois par jour avec des améliorations des performances pour la génération de rapports. Cette amélioration peut vous permettre d'accélérer les temps de chargement des tableaux de résultats sur les modules Accueil et Composants de l'espace SBOM de travail.

Ces améliorations n'ont aucun impact sur la manière dont les données sont stockées ni sur leur emplacement.

Application installée	Description
Si vous avez installé SBOM Core	À partir de la version 2.1, un inventaire de tous les composants chargés qui inclut les informations suivantes : • Nom • Description • Version • Nombre d'entités BOM
Si vous avez installé SBOM Response	À partir de la version 3.1 de SBOM la réponse, sélectionnez un graphique ou un nombre sur le graphique pour afficher une liste des enregistrements associés. Tous les composants La liste des composants **périmés** et **abandonnés** , ainsi que ceux qui ont au moins une vulnérabilité dans votre nombre total de composants. Ces nombres peuvent vous aider à identifier les composants qui requièrent votre attention. Ces sous-ensembles de composants peuvent ne pas correspondre à votre nombre total de composants, car tous vos composants peuvent ne pas correspondre à ces catégories. • La version d'un composant périmé a plus de deux versions majeures de retard

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application installée	Description
	sur la dernière version et deux ans de retard sur la dernière version. • Un composant abandonné n'a pas été mis à jour depuis plus de deux ans. • Les composants vulnérables sont des composants qui présentent des vulnérabilités d'une gravité **élevée** ou supérieure. Combinaisons à haut risque Les composants à haut risque peuvent nécessiter votre attention immédiate. L'intégration Deps.dev, qui est installée lorsque vous installez l'application SBOM Response, fournit l'intelligence des packages pour les composants à l'état **Périmé** et **Abandonné** . Les combinaisons importées à haut risque sont composées de composants périmés et abandonnés présentant au moins une vulnérabilité grave (**critique** ou **élevée**) que vous pouvez corriger par des mises à jour, un remplacement ou un autre type de réparation. L'état **Entièrement réparable** signifie qu'un composant dispose d'une version disponible qui peut le corriger. Le pourcentage du nombre total de composants à haut risque ayant des versions réparables est indiqué. Composants vulnérables et réparables Totaux et répartitions des composants présentant des vulnérabilités **critiques**, **élevées**, **moyennes** et **faibles** , et si certaines ou toutes leurs vulnérabilités peuvent être corrigées. Si un composant comporte plusieurs vulnérabilités, la vulnérabilité la plus critique prévaut. L'état de réparabilité :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application installée	Description
	• Terminé : il existe des versions de correctifs pour toutes les vulnérabilités associées à la version actuelle du composant. • Partiel : il existe une version de correctif pour au moins une des vulnérabilités associées à la version actuelle du composant, mais pas pour toutes. Composants par licence Totaux et répartitions des composants par licences. La liste des composants sous les visualisations vous permet de voir le nom, la description, la version et les nombres d'entités. Dans le panneau de droite, vous pouvez afficher un historique des versions. La version actuelle est mise en surbrillance dans l'historique des versions. Les colonnes Vulnérabilités et exposition communes (**CVE)** et **Réparabilité** sont également affichées.

Évaluation de vos risques à l'aide de la connaissance des vulnérabilités

Consultez Vérification des vulnérabilités d'une Nomenclature logicielle entité pour en savoir plus sur la façon d'examiner les données d'intelligence de vulnérabilité dans l'espace de travail.

Création de règles pour les éléments vulnérables de l'application dans l'espace Nomenclature logicielle de travail

Avant de pouvoir voir les éléments vulnérables de l'application (AVIT) dans l'espace deSBOM travail de la nomenclature logicielle, vous devez configurer les conditions dans lesquelles les AVIT sont créés.

AVIT dans l'espace de SBOM travail

Si vous avez installé et activé l'application SBOM Response, des AVIT sont créés pour SBOM les fichiers si l'une des données importées correspond aux conditions de vos règles de création AVIT existantes.

La SBOM réponse et Réponse aux vulnérabilités les applications sont tenues de configurer des règles pour créer automatiquement des éléments vulnérables de l'application (AVIT) et les corriger avec le Réponse aux vulnérabilités des applications workflow. Consultez Explorer Nomenclature logicielle pour plus d'informations.

Vous devez ajouter des règles de création d'AVIT dans l'espace SBOM de travail avant de pouvoir créer des AVIT pour les vulnérabilités détectées dans vos données ingérées SBOM . Les AVIT vous permettent d'évaluer l'intégrité des composants tiers dans vos applications. Un

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

AVIT est créé dans votre instance lorsqu'une application est mise en correspondance avec un composant présentant une vulnérabilité associée.

Dans l'espace SBOM de travail, vous ne pouvez afficher que les AVIT SBOM. Toutefois, vous pouvez afficher SBOM les AVIT ainsi que d'autres types d'éléments vulnérables dans Vulnerability Manager Workspace dans Réponse aux vulnérabilités. Vous pouvez afficher tous les AVIT qui ont été créés dans l'espace de travail SBOM dans le module Liste. Le module de liste comprend également toutes les entrées NVD et CWE ainsi que les vulnérabilités d'application.

Vous pouvez également affecter des AVIT pour le rattrapage en fonction des recommandations des listes de vulnérabilités connues telles que la Base de données de vulnérabilité nationale (NVD). Un travail planifié est déclenché, et si les conditions de vos règles de création correspondent aux données ingérées, des AVIT sont créés.

Vous pouvez suivre et corriger les AVIT en configurant des règles personnalisées.

Reportez-vous à la rubrique Créer une règle d'élément vulnérable d'application dans l'espace Nomenclature logicielle de travail pour en savoir plus sur la création d'une règle.

SBOM AVIT dans Espace de travail du gestionnaire de vulnérabilités dans Réponse aux vulnérabilités

Vous pouvez afficher tous les SBOM AVIT créés dans l'espace SBOM de travail si Espace de travail du gestionnaire de vulnérabilités vous y avez accès.

Remarque : Pour afficher uniquement SBOM les AVIT de la liste des éléments vulnérables de l'application dans le Espace de travail du gestionnaire de vulnérabilités plutôt que dans tous les AVIT, définissez la condition **[Source] [est] [SBOM] ET [Type d'analyse] [est] [SBOM-SCA]** dans la table Éléments vulnérables de l'application [sn_vul_app_vulnerable_item]. Pour afficher la table, accédez à **Tout** dans votre instance et saisissez **sn_vul_app_vulnerable_item.list** dans le navigateur de filtre.

Pour plus d'informations sur l'espace de travail du gestionnaire de vulnérabilité, sur l'affichage des rubriques de surveillance, sur les efforts de rattrapage des applications et sur les règles de tâche de rattrapage des applications pour les AVIT configurées à partir de l'application Réponse aux vulnérabilités dans le , reportez-vous Espace de travail du gestionnaire de vulnérabilitésà la section Utiliser des rubriques de visualisation dans Espace de travail du gestionnaire de vulnérabilités.

Les tâches de rattrapage (AVUL) sont créées à partir des AVIT et affectées automatiquement à des groupes de tâches de rattrapage en fonction de vos règles d'affectation. Pour en savoir plus sur la création de ces règles, consultez les rubriques suivantes :

- Créer ou modifier des Réponse aux vulnérabilités règles d'affectation
- Créer ou modifier Réponse aux vulnérabilités des règles de tâche de rattrapage et Créer un effort de rattrapage dans Vulnerability Manager Workspace.

Affichage de l'état du chargement des Nomenclature logicielle fichiers

Vérifiez l'état du chargement des fichiers de nomenclature logicielle (SBOM) que vous chargez dans le module File d'attente BOM de l'espace Nomenclature logicielle de travail (SBOM). Suivez les fichiers que vous chargez avec succès, votre historique de chargement et les erreurs.

Rôle requis :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- À partir de la v2.1 de SBOM Core : sn_sbom_resp.sbom_analyst
- Avant la v2.1 de SBOM Core : sn_sbom_resp.admin

1. Afficher l'état de votre chargement.

   La méthode que vous utilisez pour afficher l'état de votre chargement dépend des applications que vous avez installées.

Option	Description
SBOM Core	**a.** Accédez à la **Tout** > **SBOM principal** > **État de l'ingestion BOM**. **b.** Dans la liste Nomenclature, examinez les colonnes telles que les colonnes **État**, **Temps de génération de la nomenclature** et **Créé** pour plus de détails.
SBOM Réponse	**a.** Accédez à la **Tout** > **Espace de travail SBOM** > **File d'attente BOM**. **b.** Sélectionnez une carte de visualisation pour examiner les détails suivants relatifs aux catégories de vos fichiers chargés : ▪ Mises à jour de nomenclature au cours des 30 derniers jours : nombre total d'entités BOM téléchargées et analysées avec succès au cours des 30 derniers jours. ▪ Source du chargement : total des fichiers chargés SBOM avec succès et répartition des méthodes utilisées pour les ingérer (API ou manuel). ▪ Erreurs de chargement par catégorie : cinq principales catégories d'erreurs de chargement. Si aucune donnée n'apparaît sur cette visualisation, tous vos SBOM fichiers ont été chargés avec succès.

Les informations d'état de la table de nomenclature [sn_sbom_doc_list] et du module File d'attente de nomenclature comprennent tous deux les formats de nomenclature, l'état d'ingestion et le délai de génération de la nomenclature. La colonne État de l'ingestion BOM comprend les états suivants :

- Mis en file d'attente : SBOM les données ont été chargées.
- Traitement : les données du composant sont en cours de traitement dans le cadre de l'importation.
- Traité : l'ingestion de données a été effectuée avec succès.
- Erreur : une erreur s'est produite pendant le traitement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En plus de l'état de vos fichiers chargés, vous pouvez afficher des listes de composants que vous avez ingérés en sélectionnant un enregistrement d'entité BOM.

2. Accédez à plus d'informations sur les erreurs et l'état du chargement en sélectionnant l'icône d'engrenage et en ajoutant des champs tels que **Catégorie d'erreur** et **Détail de l'erreur**.

Vérification des vulnérabilités d'une Nomenclature logicielle entité

Déterminez si des vulnérabilités sont associées aux composants d'un fichier chargé Nomenclature logicielle (SBOM).

Les applications suivantes doivent être installées et activées avant de pouvoir afficher les vulnérabilités et les données de vulnérabilité améliorées :

- SBOM Réponse
- Intégration de Vulnerability Response avec les tâches NVD et CWE
- Réponse aux vulnérabilités

Consultez Explorer Nomenclature logicielle pour plus d'informations.

Rôle requis :

- À partir de la v2.1 de SBOM Core : sn_sbom_resp.sbom_analyst
- Avant la v2.1 de SBOM Core : sn_sbom_resp.admin

1. Accédez à la **Tout** > **Espace de travail SBOM** > **Composants**.
2. Avant la version 3.1 de SBOM Response, affichez les informations relatives à la vulnérabilité via une visualisation ou un enregistrement de composant.

Méthode	Actions
Entités BOM avec visualisation des vulnérabilités	Sélectionnez le graphique de visualisation des **entités BOM avec vulnérabilités** . ◦ Si des vulnérabilités sont associées à ce composant, les totaux sont affichés dans les colonnes CVE et CWE de la liste. Un composant peut avoir plusieurs vulnérabilités. Le cas échéant, vous pouvez consulter la colonne Réparabilité de cette liste pour les entrées. ◦ Si aucune vulnérabilité n'est associée à ce composant, ces colonnes affichent 0 ou aucune valeur pour le composant. Si les colonnes CVE, CWE et Réparabilité ne sont pas affichées, vous pouvez les ajouter à la page en sélectionnant l'icône d'engrenage en haut à droite de la page et les **colonnes Modifier**. Sélectionnez-les dans la liste de colonnes Disponible et sélectionnez **OK**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Méthode	Actions
Enregistrement du composant	**a.** Sélectionnez un enregistrement dans la liste située sous les visualisations. **b.** Sélectionnez l'onglet **Vulnérabilités** sur l'enregistrement. **i.** Si aucune donnée n'est affichée, aucune vulnérabilité signalée n'est associée à l'enregistrement. **ii.** Si des données sont affichées, consultez Examen du module Composants dans l'espace Nomenclature logicielle de travail et suivez les étapes du workflow de rattrapage pour Réponse aux vulnérabilités des applications remédier à la vulnérabilité. Pour plus d'informations, consultez Rattrapage des Réponse aux vulnérabilités des applications vulnérabilités.

Évaluation de vos risques à l'aide de la connaissance des vulnérabilités

À partir de la version 3.1 de Response, affichez davantage de données de vulnérabilité améliorées avec SBOM Response sur les enregistrements de SBOM composants. Les SBOM travaux planifiés de l'application Response, de la réponse aux vulnérabilités, de l'intégration de la base de données de vulnérabilité nationale (NVD) et de l'énumération des faiblesses courantes (CWE) décrits dans Applications prises en charge doivent être installés et activés.

1. Sélectionnez la visualisation **Tous les composants** pour afficher la liste des enregistrements associés.
2. Sélectionnez un lien dans la colonne **Nom** pour ouvrir un enregistrement.

   Les états (**États), Périmé**, **Abandonné** et **Vulnérable** sont affichés sous le nom du composant. Un composant peut avoir n'importe quelle combinaison de ces états. Si aucun état n'est affiché, le composant n'est ni périmé, ni abandonné, ni vulnérable.

   Passez en revue la version actuelle et la dernière version publiée. Dans le panneau de droite, vous pouvez afficher un historique des versions. La version actuelle est mise en évidence dans l'historique des versions et son emplacement dans la liste peut vous donner un aperçu des raisons pour lesquelles un composant est **périmé**, **abandonné** et **vulnérable**. Par exemple, vous utilisez peut-être une version antérieure d'un composant.

3. Sélectionnez les onglets **connexes Vue d'ensemble**, **Hachages**, **Entités BOM**, **Vulnérabilités** et **AVI** de l'enregistrement.
   - Vue d'ensemble : un résumé des détails du composant.
   - Entités BOM : liste des entités associées à ce composant.
   - Hachages : s'ils sont importés, les hachages sont affichés.
   - Vulnérabilités : informations sur les vulnérabilités connues associées à ce composant. Si cette liste est vide, il n'y a aucune vulnérabilité connue.

     Si la liste est renseignée, sélectionnez l'onglet pour afficher les ID de vulnérabilité, les résumés et d'autres informations sur les vulnérabilités pour les données CVE (Common

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vulnerabilities and Exposures) et CWE (Common Weakness Enumeration) associées à cet enregistrement. Les CVE sont ventilés par gravité, les CWE sont ventilés en fonction de la probabilité que le composant puisse être exploité. Vous pouvez afficher les enregistrements de vulnérabilité améliorés dans les applications ou Réponse aux vulnérabilitésRéponse aux vulnérabilités des applications en sélectionnant le lien de l'ID de vulnérabilité.

- AVI (AVIT) : éléments vulnérables de l'application associés à ce composant si vous avez créé des règles de création AVIT qui associent le composant à une vulnérabilité connue. L'application Application Vulnerability Response (AVR) associe une vulnérabilité à une application pour créer un enregistrement AVI. Pour plus d'informations, consultez Création de règles pour les éléments vulnérables de l'application dans l'espace Nomenclature logicielle de travail.

Composants installés avec Nomenclature logicielle les applications

Plusieurs types de composants sont installés avec l'activation des applications, y compris les tables, les rôles d'utilisateur et les Nomenclature logicielle travaux planifiés.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
SBOM write [sn_sbom_dm.app_write], SBOM create [sn_sbom_dm.app_create], SBOM read [sbom_dm.app_read]	Ces rôles sont installés avec le modèle de données pour SBOM l'application. Ils vous permettent de lire, de créer et de modifier des enregistrements dans SBOM des tables.	Aucun
SBOM Corees ingère [sn_sbom_core.sbom_ingest] et SBOM Core admin [sn_sbom_core.admin]	Ces rôles sont installés avec l'application SBOM Core. Le rôle sn_sbom_core.sbom_ingest vous permet de charger des SBOM manuellement et via l'API REST. Le rôle sn_sbom_core.admin vous permet de créer, lire, modifier des données et charger des SBOM. Ce rôle vous donne également accès aux SBOM modules Core de votre instance. Elle hérite des rôles du modèle de données pour SBOM l'application.	• sn_sbom_dm.app_écriture • sn_sbom_dm.app_créer • sn_ sbom_dm.app_read

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
Analyste SBOM [sn_sbom_resp.sbom_analyst]	Ce rôle est installé avec l'application SBOM Response. Il hérite du rôle sn_sbom_core.admin et vous permet d'accéder à l'espace SBOM de travail.	• sn_sbom_core.admin • sn_sbom_dm.app_écriture • sn_sbom_dm.app_créer • sn_ sbom_dm.app_read • sn_sbom_resp.manage_avi_rule • sn_sbom_config_rule table

Tables installées avec les SBOM applications

Les tables répertoriées dans la table suivante sont installées avec le modèle de données pour SBOM l'application.

Modèle de données pour SBOM les tables

Table	Description
Document SBOM [sn_sbom_doc]	Contient les entités BOM que vous avez chargées.
SBOM composant [sn_sbom_component]	Contient des composants, des classifieurs et des versions importés SBOM qui sont inclus dans le composant parent.
SBOM Relation de composant [sn_sbom_comp_relationship]	Contient des composants et leurs dépendances.
SBOM Composant BOM M2M [sn_sbom_m2m_bom_comp]	Contient les mappages des composants BOM.
Licence SBOM [sn_sbom_license]	Contient les ID de licence open source utilisés pour les composants.
SBOM fournisseur [sn_sbom_supplier]	Contient l'organisation qui a fourni le composant, qui peut être un fabricant, un distributeur ou un reconditionneur.
SBOM ID de composant [sn_sbom_comp_id]	Contient les identificateurs de composants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modèle de données pour SBOM les tables (suite)

Table	Description
SBOM Propriétés des composants [sn_sbom_comp_property]	Contient les propriétés nom-valeur du composant.
SBOM hachis [sn_sbom_hash]	Contient des algorithmes de hachage de composants.
SBOM contact [sn_sbom_contact]	Contient les coordonnées du fournisseur.
SBOM Références externes [sn_sbom_comp_external_ref]	Contient des composants, des types de composants et des URL externes qui documentent des systèmes, des sites et des informations qui peuvent être pertinents, mais qui ne sont pas inclus dans le SBOMfichier .
SBOM Groupe de packages [sn_sbom_pkg_group]	Contient les informations du groupe de packages pour chaque composant. Plusieurs versions de bibliothèques peuvent être utilisées dans les applications. Les versions des mêmes composants sont regroupées et ajoutées à cette table pour éviter d'extraire les mêmes données plusieurs fois.

Les tables répertoriées dans la table suivante sont installées avec l'application SBOM Response

SBOM Tables de réponses

Table	Description
SBOM Configuration de la règle de création [sn_sbom_config_rule]	Contient les règles de création AVIT utilisées dans l'espace de SBOM travail.
SBOM Vulnérabilités des composants M2M [sn_sbom_m2m_comp_vuln]	Contient les composants et les vulnérabilités associées.
Informations sur le correctif de vulnérabilité du composant [sn_sbom_comp_vuln_fix_info]	Contient les versions de correctifs pour chaque vulnérabilité tierce associée à une version du composant.
Aperçus du rapport sur les composants [sn_sbom_comp_report_insight]	Contient des aperçus sur les données périmées, abandonnées et réparables pour les composants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

SBOM Tables de réponses (suite)

Table	Description
Importations d'intégration Deps [sn_sbom_deps_integration_import]	Contient des informations sur la liste des versions importées pour un package ou une bibliothèque donnée.
Importations d'intégration OSV [sn_sbom_osv_integration_import]	Contient des informations de Vulnerability Intelligence pour une version donnée d'un package ou d'une bibliothèque.
Listes de versions de composants [sn_sbom_st_version_list]	Contient des informations sur les versions et les dates de publication des composants.

Travaux planifiés

Tâche	Description
Calculer la réparabilité et la vulnérabilité du composant	Calcule les informations sur la façon de corriger les composants présentant des vulnérabilités et la probabilité que vous puissiez corriger les composants.
Nouveaux composants d'intégration OSV	Récupère toutes les vulnérabilités connues du public associées aux packages (bibliothèques) qui ont été importés après la dernière exécution de l'intégration.
Intégration complète d'OSV	Récupère toutes les vulnérabilités connues du public associées à tous les packages qui ont été importés.
Intégration Deps.dev	Récupère toutes les versions connues du public pour les packages et les permet d'identifier les composants dans **les états périmés** et **abandonnés** .
Mettre à jour les vuln_based_criticality sur les composants BOM	Met à jour la criticité pour les composants présentant des vulnérabilités.

Créer une règle d'élément vulnérable d'application dans l'espace Nomenclature logicielle de travail

Configurez les conditions dans lesquelles les éléments vulnérables de l'application (AVIT) sont créés automatiquement dans le module Règles de création AVI de l'espace Nomenclature logicielle de travail (SBOM).

Avant de commencer

L'application SBOM Réponse est requise si vous souhaitez créer des éléments vulnérables de l'application. Consultez Explorer Nomenclature logicielle pour plus d'informations.

Rôle requis : sn_sbom_resp.manage_avi_rule.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espace de travail SBOM** > **Règles de création AVI**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs.

Champ	Description
Nom	Nom de la règle.
Actif	Indique si la règle de création est activée.
Ordre d'exécution	Ordre dans lequel les règles sont évaluées. La règle dont la valeur numérique est la plus faible s'exécute en premier. Par exemple, vous pouvez créer des règles de priorité plus élevées pour les éléments qui nécessitent une gestion spéciale ou pour lesquels le risque est critique, de sorte qu'elles soient exécutées en premier. Ensuite, créez des règles générales pour les éléments qui ne nécessitent aucune manipulation spéciale. Enfin, créez une règle par défaut pour intercepter tous les composants présentant des vulnérabilités.
Description	Description de la règle pour vous aider à la distinguer des autres règles.
Conditions	Créez les conditions dans lesquelles les éléments vulnérables de l'application (AVI) sont créés. Par exemple, vous pouvez sélectionner **[Vulnérabilité > gravité][est][1-Critique]** pour créer des AVIT pour les composants qui présentent des vulnérabilités à haut risque et susceptibles de vous affecter gravement. Notez que vous pouvez ajouter plus de conditions.

4. Sélectionnez **Enregistrer**.
   Votre règle de création s'exécute automatiquement après le prochain chargement et crée des AVI pour les composants qui correspondent à vos conditions. Vous pouvez également exécuter la règle à la demande à partir du module Règles de création AVI en sélectionnant **Exécuter maintenant**.

Résultats

Une fois qu'ils ont été créés, vous pouvez vérifier qu'un AVIT a été créé spécifiquement pour SBOM les données en vérifiant les valeurs dans les champs **Source** et **Type d'analyse** d'un enregistrement AVI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Source	SBOM
Type d'analyse	SBOM-SCA

Applications de gestion des tickets de sécurité d'entreprise

Les applications de gestion des tickets de sécurité d'entreprise incluent Réponse aux incidents de sécurité, une solution d'orchestration et d'automatisation de la sécurité (SOAR) qui vous aide à répondre rapidement à l'évolution des menaces tout en optimisant et en orchestrant les opérations de sécurité de l'entreprise. Il élimine les erreurs et les frictions inhérentes aux transferts manuels entre les systèmes, les équipes et les responsabilités.

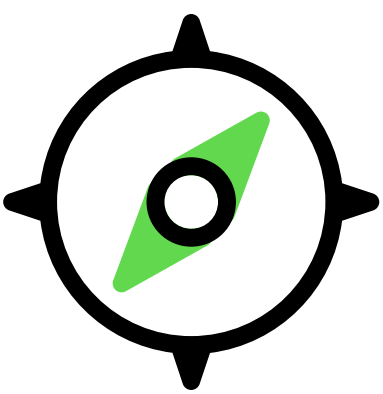
Vue d'ensemble

<Video to be added.>

Premiers pas

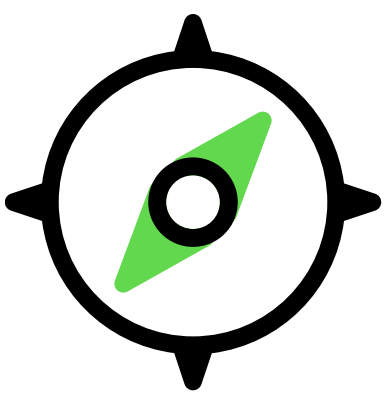
Les applications suivantes Réponse aux incidents de sécurité sont disponibles avec des abonnements distincts à partir du ServiceNow® Store. Consultez pour plus d'informations sur la façon de localiser, d'obtenir une autorisation et de télécharger des applications sur votre instance.

Réponse aux incidents de sécurité



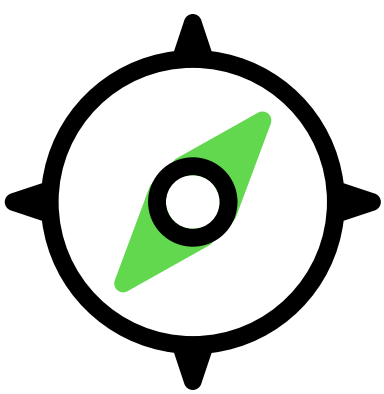
En savoir plus sur l'application Security Incident Response

Gestion des incidents de sécurité majeurs



En savoir plus sur l'application Major Security Incident Management

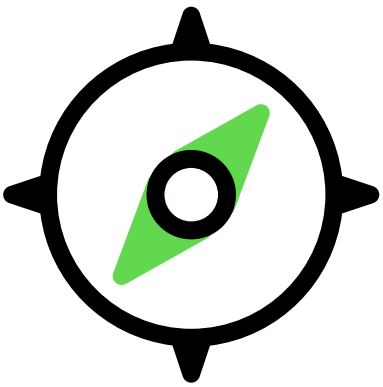
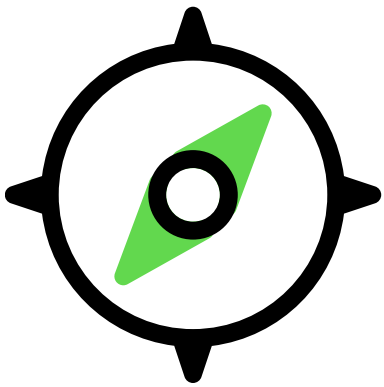
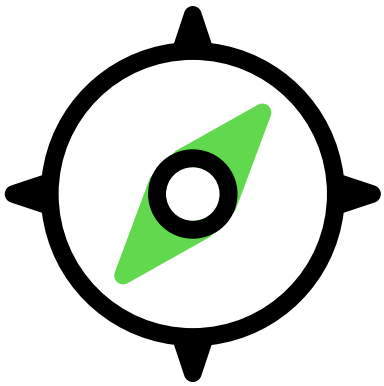
Renseignements sur les menaces



En savoir plus sur l'application Threat Intelligence

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Threat Intelligence Security Center	Data Loss Prevention Incident Response	Fonctionnalités partagées des applications Security Incident Response
		
En savoir plus sur l'application Centre de sécurité Threat Intelligence	En savoir plus sur l'application de prévention des pertes de données	En savoir plus sur les fonctionnalités partagées entre les applications Security Incident Response

Dépannage et demande d'aide

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

Réponse aux incidents de sécurité

L'application ServiceNow® Réponse aux incidents de sécurité suit la progression des incidents de sécurité depuis leur détection et leur analyse initiale, en passant par le confinement, l'éradication et la récupération, jusqu'à l'examen final après incident, la création d'articles de la base de connaissances et la fermeture.

Demander des applications dans l'App Store

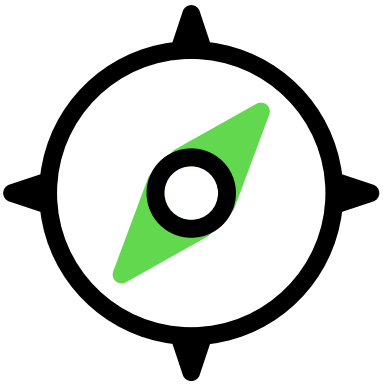
Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

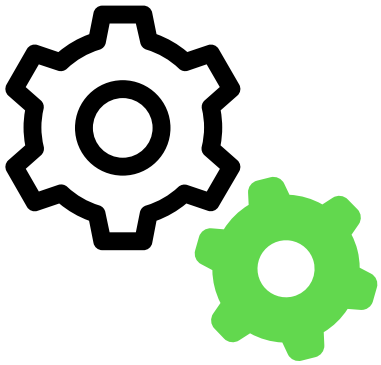
Réponse aux incidents de sécurité

Explorer



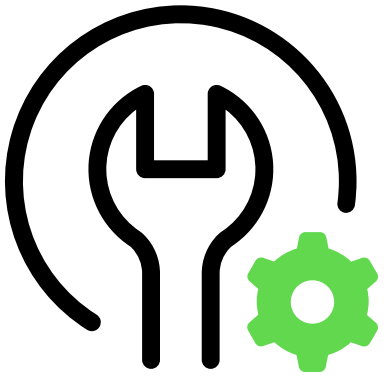
Découvrir les fonctionnalités de Security Incident Response

Installation et configuration



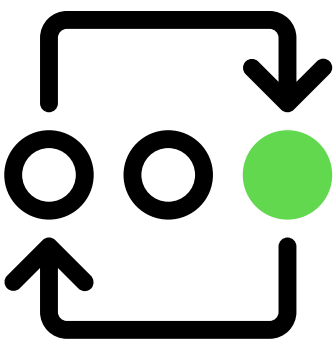
Installez et configurez votre application Réponse aux incidents de sécurité

Administrer



Gérer et personnaliser vos incidents de sécurité

Intégrer



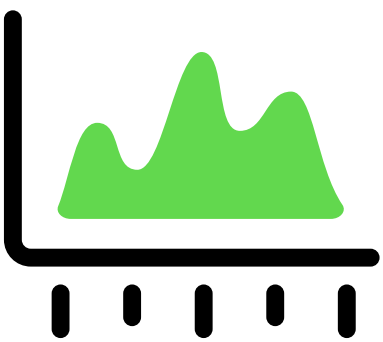
Étendre Security Incident Response en l'intégrant à d'autres applications

Utiliser l'espace de travail Security Incident Response



Apprenez à utiliser les espaces de travail Réponse aux incidents de sécurité et Rattrapage informatique

Analyse et génération de rapports



Surveiller la progression du rattrapage

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Obtenir des informations supplémentaires sur Security Incident Response

Demander une application Opérations de sécurité dans l'App Store

Si vous êtes un nouveau client Opérations de sécurité du correctif London 6 ou ultérieur, visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique.

Présentation de Réponse aux incidents de sécurité

Avec Réponse aux incidents de sécurité (SIR), gérez le cycle de vie de vos incidents de sécurité, de l'analyse initiale à l'émancipation, à l'éradication et à la récupération. Security Incident Response vous permet d'obtenir une compréhension complète des procédures de réponse aux incidents exécutées par vos analystes, et de comprendre les tendances et les goulots d'étranglement de ces procédures grâce à des tableaux de bord et des rapports basés sur l'analyse.

Une introduction à Security Incident Response, montrant comment commencer à utiliser l'application.

Regardez cette vidéo de neuf minutes pour en savoir plus sur le processus SIR, son utilisation Réponse aux incidents de sécurité pour contrecarrer les attaques et l'affichage de l'activité de sécurité dans l'Explorateur Réponse aux incidents de sécurité .

Les intégrations intégrées avec des solutions de cybersécurité tierces et les intégrations développées par des partenaires à partir de la ServiceNow boutique permettent l'automatisation et l'orchestration de la sécurité pour une réponse efficace et précise aux incidents.

Pour protéger vos enquêtes et préserver la confidentialité des incidents de sécurité, Réponse aux incidents de sécurité fournit les moyens de restreindre l'accès au système à des rôles et des ACL spécifiques liés à la sécurité. L'accès aux personnes qui ne sont pas des administrateurs de sécurité peut être restreint, sauf si vous leur autorisez expressément l'accès.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les administrateurs de système informatique [admin] peuvent emprunter l'identité d'utilisateurs ServiceNow. Toutefois, lorsque vous empruntez l'identité d'un utilisateur disposant du rôle d'administrateur d'application pour Réponse aux incidents de sécurité, un administrateur ne peut pas accéder aux fonctionnalités accordées par ce rôle, y compris les incidents de sécurité et les informations de profil. L'accès aux modules et aux applications dans la barre de navigation est également restreint. En outre, l'administrateur ne peut pas modifier le mot de passe d'un utilisateur ayant un rôle d'administrateur d'application pour Security Incident Response.

Flux d'informations de Security Incident Response

Security Incident Response utilise le flux d'informations suivant, de l'intégration à l'enquête, puis à la résolution et à l'examen.

Remarque : Il s'agit d'une infographie interactive, vous pouvez donc essayer de cliquer sur l'une des icônes ou étapes de l'image pour en savoir plus sur ce processus ou cette tâche.



1. Cliquez sur cette image pour en savoir plus sur les intégrations SIR
2. Cliquez sur cette image pour en savoir plus sur la création d'incidents de sécurité
3. Cliquez sur cette image pour en savoir plus sur Threat Intelligence
4. Cliquez sur cette image pour en savoir plus sur l'espace de travail SIR
5. Cliquez sur cette image pour en savoir plus sur les fonctionnalités d'attaque MITRE
6. Cliquez sur cette image pour en savoir plus sur les activités de revue post-incident

Découverte

Les incidents de sécurité peuvent être journalisés ou créés de la manière suivante.

- À partir du formulaire d'incident de sécurité
- À partir d'événements générés en interne, ou créés par des systèmes externes de surveillance ou de suivi des vulnérabilités via des règles d'alerte, ou manuellement
- À partir de systèmes externes de surveillance ou de suivi
- À partir du catalogue de services

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Analyse

En fonction de la vue sélectionnée que vous utilisez (par défaut, sécurité non informatique, ITIL de sécurité, etc.), le formulaire d'incident de sécurité peut afficher n'importe quelle combinaison de vulnérabilités, d'incidents, de changements, de problèmes, de tâches sur le CI affecté et les groupes de CI affectés. Le système peut identifier les programmes malveillants, les virus et d'autres zones de vulnérabilité en croisant la base de données du National Institute of Standards and Technology (NIST) ou un autre logiciel de détection tiers. Au fur et à mesure que les incidents de sécurité sont résolus, vous pouvez utiliser n'importe quel incident pour créer un article de la base de connaissances de sécurité pour référence ultérieure.

Effectuez une analyse plus approfondie à l'aide d'une carte des services aux entreprises pour localiser les autres systèmes ou services aux entreprises affectés qui peuvent être infectés.

Confinement, éradication et reprise

Tout en surveillant et en analysant les vulnérabilités, vous pouvez créer et affecter des tâches à d'autres départements. Vous pouvez utiliser une carte des services aux entreprises pour créer des tâches, des problèmes ou des changements pour tous les systèmes affectés, les documents, les activités, les messages SMS, les appels de pont, etc.

Revue

Une fois l'incident résolu, d'autres étapes peuvent avoir lieu avant la fermeture. Vous pouvez effectuer une révision post-incident. La création d'articles de la base de connaissances peut aider à résoudre de futurs incidents similaires. Les incidents importants peuvent nécessiter un examen de résolution post-incident. Cet examen peut prendre plusieurs formes. Par exemple :

- Organisez une réunion pour discuter de l'incident et recueillir des réponses.
- Rédigez et distribuez aux équipes qui ont travaillé sur un incident une liste de questions d'examen de résolution conçues pour chaque catégorie ou priorité d'incident.
- Les gestionnaires d'incidents peuvent rédiger le rapport et recueillir des informations par eux-mêmes.

Un rapport d'examen de la résolution des incidents peut être généré automatiquement et comprend :

1. un résumé de ce qui a été fait ;

2. la chronologie

3. Type d'incident de sécurité rencontré

4. tous les incidents, changements, problèmes, tâches, groupes de CI associés

5. Les détails de la résolution

De plus, un système automatisé d'enquête d'examen de la résolution des incidents de sécurité est disponible. Il rassemble les noms de tous les utilisateurs affectés à un incident de sécurité et envoie une enquête personnalisée pour recueillir des données sur la gestion de l'incident. Ces données peuvent ensuite être mises à disposition dans un rapport d'examen d'incident de sécurité généré, que vous pouvez modifier dans une version finale. Des données similaires peuvent être ajoutées à un article de la base de connaissances pour contenir les enseignements tirés et les étapes à suivre pour résoudre des problèmes similaires à l'avenir.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Terminologie de Security Incident Response

Les termes suivants sont utilisés dans Réponse aux incidents de sécurité.

Terme	Définition
Actif	Tout incident de sécurité dont l'état n'est pas fermé ou annulé.
Verrouillage de l'administrateur	La possibilité de restreindre Réponse aux incidents de sécurité l'accès au personnel ayant des rôles et des ACL liés à la sécurité.
Demandes de sécurité entrantes	Demandes soumises pour des demandes de sécurité à faible impact, telles que la demande d'un nouveau badge électronique.
Gérer les activités post-incident	Examen des origines et du traitement d'un incident de sécurité Le produit final est un rapport post-incident, qui documente toutes les actions effectuées et les raisons pour lesquelles elles sont effectuées.
Tâches de réponse	Tâches affectées à un incident de sécurité pour le suivi des actions en réponse à la menace.
Comprendre les calculateurs d'incidents de sécurité	Les calculateurs sont utilisés pour mettre à jour les valeurs d'enregistrement lorsque les conditions préconfigurées sont remplies.
Arborescences des incidents de sécurité	Type de graphique qui affiche hiérarchiquement les données d'incident de sécurité sous la forme de rectangles imbriqués.
Recherche de menace	Demande soumise à partir du catalogue des incidents de sécurité pour l'analyse des fichiers, des URL et des adresses IP à la recherche de programmes malveillants.
Analyse de vulnérabilité	Demande lancée à partir du formulaire d'incident de sécurité pour l'analyse des ressources affectées (serveurs, ordinateurs et autres éléments de configuration) à la recherche de vulnérabilités.

Séparation de domaine et Réponse aux incidents de sécurité

L'application Séparation de domaine est prise en charge dans Réponse aux incidents de sécurité. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveau de prise en charge : Standard

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Vue d'ensemble

Dans l'application Réponse aux incidents de sécurité , Séparation de domaine permet aux fournisseurs de services (SP) de standardiser les procédures SOC (Security Operations Center) et Security Incident Response (SIR) dans l'ensemble de la base de clients qu'ils servent, avec des coûts d'exploitation réduits et une meilleure qualité de service. Des espaces de travail client distincts pour les workflows, les tableaux de bord, les rapports, etc., garantissent que les données client sont séparées et ne sont jamais exposées à d'autres clients.

Prise en charge de Domain Separation dans Security Incident Response par versions

Version	Niveau de prise en charge	Notes
Genève, Helsinki	Aucune prise en charge	Initiation de Séparation de domaine au niveau des données
Istanbul	Données uniquement	
Jakarta	Niveau 2 (données, demandeur, prestataire)	**Nouvelles fonctionnalités** : prise en charge des intégrations tierces avec séparation de domaine de niveau 2 sous une seule instance d'intégration, y compris les intégrations Threat Intelligence
Kingston	Niveau 2 (données, demandeur, prestataire)	**Nouvelles fonctionnalités** : l'intégration de la recherche de perception pour SIR est activée avec plusieurs instances, mais toutes les instances sont toujours sous un seul domaine. Exemple : si deux instances d'une intégration Splunk sont configurées (SplunkCLOUD et SplunkCORP), elles sont toujours exploitées

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prise en charge de Domain Separation dans Security Incident Response par versions (suite)

Version	Niveau de prise en charge	Notes
		pour les activités de réponse aux incidents dans un seul domaine, où l'implémentation a été configurée à l'origine.
Londres	Niveau 2 (données, demandeur, prestataire)	**Nouvelles fonctionnalités** : toutes les intégrations résident dans plusieurs domaines
Madrid	Niveau 2 (données, demandeur, prestataire)	Toutes les intégrations peuvent désormais résider dans plusieurs domaines. Dans l'exemple ci-dessus, SplunkCloud peut être domain1 et SplunkCORP domain2.
New York	Niveau 2 (données, demandeur, prestataire)	Toutes les intégrations résident dans plusieurs domaines.
Orlando	Standard	Toutes les intégrations résident dans plusieurs domaines.
Paris	Standard	Toutes les intégrations résident dans plusieurs domaines.

Séparation de domaine pour l'application Réponse aux incidents de sécurité couvre les fonctionnalités du produit suivantes :

- Les alertes de sécurité sont dirigées vers le domaine approprié de l'utilisateur dont l'ID/ les informations d'identification/le périmètre génère l'incident et est enregistré comme incident de sécurité.
- Les alertes génèrent des « observables », qui représentent des propriétés d'état ou des événements mesurables : Les workflows de sécurité dans le domaine de l'incident de sécurité sont utilisés pour orchestrer la réponse.
- Les intégrations sont configurées dans le domaine de l'incident de sécurité pour l'automatisation des réponses.
- Les options sont configurées dans le domaine de l'incident de sécurité pour l'automatisation de la réponse. Ces fonctionnalités (à partir de la version Kingston) sont les suivantes :
  - Recherche de menace
  - Enrichir les observables
  - Enrichir l'élément de configuration
  - Obtenir les processus d'exécution
  - Obtenir les statistiques réseau

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

  - Demande de bloc
  - Isoler l'hôte
  - Recherche de perception
  - Recherche et suppression d'e-mail
  - Publier dans la liste de surveillance
- Les résultats de l'automatisation des réponses (comme la recherche de menace ou la recherche de perception) sont stockés dans le domaine de l'incident de sécurité.
- D'autres incidents de sécurité sont référencés dans le même domaine de l'incident de sécurité en fonction d'un ensemble partagé d'observables.
- D'autres utilisateurs sont référencés dans le domaine de l'incident de sécurité.
- Les éléments de configuration sont référencés dans le même domaine que l'incident de sécurité.
- Les tâches de réponse manuelle sont ajoutées au domaine de l'incident de sécurité.
- Les articles de la base de connaissances et les livres d'exécution sont référencés dans le domaine de l'incident de sécurité.
- Les mesures de Security Incident Response pertinentes pour les incidents dans le domaine sont affichées sur les tableaux de bord ainsi que dans la génération de rapports.

Remarque : Dans les cas précédents, les principes généraux de visibilité dans des domaines distincts de la NOW Platform s'appliquent. Comme toujours, un incident dans le domaine parent peut faire référence à des artefacts dans le domaine enfant, mais pas l'inverse.

Fonctionnement de Séparation de domaine dans Security Incident Response

L'application Réponse aux incidents de sécurité gère le cycle de vie d'un incident de sécurité de bout en bout. Les cas d'utilisation suivants prennent en charge la séparation par domaine :

- **Ingestion d'événements et d'alertes** pour créer des incidents de sécurité afin que l'analyste du SOC client ou le MSP y réponde :
  - Analyseurs d'e-mails (basés sur la plateforme, hameçonnage signalé par les utilisateurs, personnalisés)
  - Événements/alertes de déduplication avant la création de l'incident
  - Extraction automatique des observables
  - Applications dans un magasin SIEM tiers
- **Enrichissement** des artefacts impliqués dans les incidents (adresses IP, URL, domaines, hachages de fichiers) :
  - Enrichissement des actifs (CMDB)
  - Utilisateurs (plateforme)
  - Automatisation : enrichissement des observables (ex : Whols)
- **Enquêter sur** les incidents à l'aide des artefacts et de leur réputation ou de leur association avec des menaces connues
  - Orchestrer : playbooks et articles de la base de connaissances
  - Automatisation : recherche de menace (ex : VirusTotal), recherche de perception (ex : Splunk), obtention des processus en cours d'exécution (ex : Carbon Black)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Éradiquer** les artefacts liés à la menace impliqués dans l'incident en fonction de l'enquête effectuée
  - Orchestrer : playbooks et articles de la base de connaissances
  - Automatisation : recherche et suppression d'e-mails (ex : Microsoft Exchange), blocage d'IP (ex : pare-feu Palo Alto)
- **Mesurer** l'efficacité des opérations de réponse aux incidents
  - Tableaux de bord Performance Analytics : productivité et tendances d'incidents
  - Reconstruction des étapes d'enquête sur l'incident à partir des notes de travail
  - Examen post-incident

Configuration de Domain Separation

La configuration de Séparation de domaine pour Réponse aux incidents de sécurité ne nécessite aucune étape supplémentaire. Toutes les Réponse aux incidents de sécurité tables acquièrent la colonne Domaine une fois que l'instance est séparée par domaine.

Données séparées par domaine

Les données peuvent être séparées par domaine, ce qui signifie :

- Les incidents de sécurité d'un domaine ne peuvent pas être affichés à partir d'autres domaines.
- Les observables extraits de l'incident de sécurité sont placés dans le même domaine et ne peuvent pas être affichés à partir d'autres domaines.
- Jusqu'à la version Kingston, des intégrations tierces configurées existent dans le domaine global et sont accessibles à tous les autres domaines de l'instance.
- Dans la version Madrid, les intégrations tierces peuvent être configurées et activées pour chaque domaine. Cela signifie que l'intégration activée et configurée dans un domaine ne peut pas être exploitée dans un autre domaine.
- Les automatisations qui s'exécutent sur les observables à l'aide d'intégrations tierces (pour l'investigation, l'endiguement ou l'éradication des menaces) placent leurs résultats dans le domaine de l'incident de sécurité et ne peuvent pas être consultés à partir d'un autre domaine.
- Les workflows Orchestration créés dans un domaine ne sont pas visibles dans un autre domaine.
- Les options (telles que définies dans la liste des fonctions d'aptitudes de prédication) qui sont invoquées restent génériques dans tous les domaines avec une implémentation spécifique au domaine de l'option appelée. Par exemple, une recherche d'observation sur une adresse IP peut invoquer une implémentation Splunk dans un domaine et une implémentation QRadar dans un autre.

Configuration

Tous les aspects de la configuration du produit sont autonomes dans un environnement séparé par domaine. La configuration peut être adaptée à des domaines individuels.

Remarque : La logique métier et les processus de #2-5 ci-dessous peuvent être administrés dans le domaine du locataire.

Les tâches suivantes doivent être configurées :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Administration système
   - Affecter des rôles aux utilisateurs et aux groupes d'utilisateurs : rôles d'utilisateur installés avec Réponse aux incidents de sécurité
   - Installez un ou plusieurs modules d'extension d'intégration tiers à utiliser Réponse aux incidents de sécuritéavec : Intégrations de Réponse aux incidents de sécurité
2. Administration du Réponse aux incidents de sécurité
   - Ajouter ou passer en revue les rôles : Composants installés avec Réponse aux incidents de sécurité
   - Configurez les groupes et les utilisateurs : Créer un groupe d'incidents de sécurité
   - Configurer les escalades d'incidents : Escalader un incident de sécurité
   - Configurez les calculateurs de score de risque des incidents de sécurité : Comprendre les calculateurs d'incidents de sécurité
   - Configurer des accords sur les niveaux de service : Créer un Réponse aux incidents de sécurité SLA
   - Configurez les définitions de processus d'incident de sécurité : Comprendre la définition du processus de Security Incident Response
   - Mettez en place des processus d'examen post-incident : Gérer les activités post-incident
3. Paramètres d'e-mail d'incident de sécurité
   - Définissez la boîte de réception d'analyse des e-mails : Opérations de sécurité Analyse des e-mails
   - Configurer des analyseurs d'e-mails pour l'ingestion d'alertes : Créer des analyseurs d'e-mails dans Security Operations
   - Définissez des règles de correspondance des e-mails pour le hameçonnage signalé par les utilisateurs : Créer des règles pour valider les attaques de hameçonnage signalées par les utilisateurs
   - Configurer des actions sur e-mail entrant :actions sur e-mail entrant
4. Paramètres du Playbook d'incident de sécurité
   - Examinez et configurez les documents du Runbook : Créer un Runbook Security Incident Response
   - Configurer des workflows d'incident de sécurité : Opérations de sécurité Fonctionnalité commune
5. Configurations d'option
   - Bloquer la demande : Security Operations Integration - Aptitude de demande de bloc
   - Recherche et suppression d'e-mail : Security Operations Integration - Aptitude de recherche et de suppression d'e-mails
   - Enrichir l'élément de configuration : Security Operations Integration - Enrichir la capacité CI
   - Enrichir les observables : Intégration de Security Operations : aptitude d'enrichissement des observables
   - Obtenir les statistiques réseau : Security Operations Integration - Aptitude Obtenir les statistiques réseau
   - Obtenir les processus en cours d'exécution : Security Operations Integration - Obtenir l'aptitude Processus en cours d'exécution
   - Isoler l'hôte : Intégration de Security Operations : capacité Isoler l'hôte

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Publier dans la liste de surveillance : Intégration de Security Operations : aptitude Publier dans la liste de surveillance
- Recherche de perception : Intégration de Security Operations : fonctionnalité de recherche de perceptions
- Recherche de menaces : Security Operations Integration - Aptitude Recherche de menace

Comment les domaines de locataire gèrent-ils leurs propres données d'application ?

- Les propriétaires de domaines locataires créent leurs propres règles d'analyse des e-mails pour ingérer des incidents de sécurité.
- Les propriétaires de domaines locataires peuvent configurer des intégrations spécifiques exclusivement pour une utilisation au sein du domaine.
- Les propriétaires de domaines locataires peuvent créer leurs propres workflows de réponse aux incidents.
- Les propriétaires de domaines locataires peuvent créer leurs propres catégories d'incidents, articles de base de connaissances sur la réponse aux incidents et runbooks à associer aux workflows de réponse aux incidents.
- Les utilisateurs de domaine de locataire créent et ferment leurs propres incidents de sécurité.

Logique métier et processus qui peuvent être séparés par domaine par propriétaire de l'instance

- Réponse aux incidents de sécurité Utilisateurs et groupes
- Réponse aux incidents de sécurité intégrations (à partir de la version Madrid)
- Règles d'analyse des e-mails pour la création d'incidents
- Règles métier pour consolider plusieurs événements ou alertes dans un incident de sécurité
- Workflows pour l'orchestration de la réponse aux incidents
- Calculateurs de score de risque d'incident de sécurité
- Chemin d'escalade des incidents de sécurité
- SLA d'incidents de sécurité
- Définitions de processus d'incidents de sécurité
- Processus d'examen post-incident de sécurité

Information associée

Séparation de domaine pour les fournisseurs de services

Configurer Réponse aux incidents de sécurité

La configuration implique Réponse aux incidents de sécurité des étapes obligatoires et plusieurs étapes facultatives, en fonction de vos besoins spécifiques. Une fois que ServiceNow Store vous l'avez téléchargé Réponse aux incidents de sécurité et installé, vous pouvez exécuter l'assistant de configuration pour effectuer la configuration de base des Réponse aux incidents de sécurité intégrations tierces.

Traduction automatique

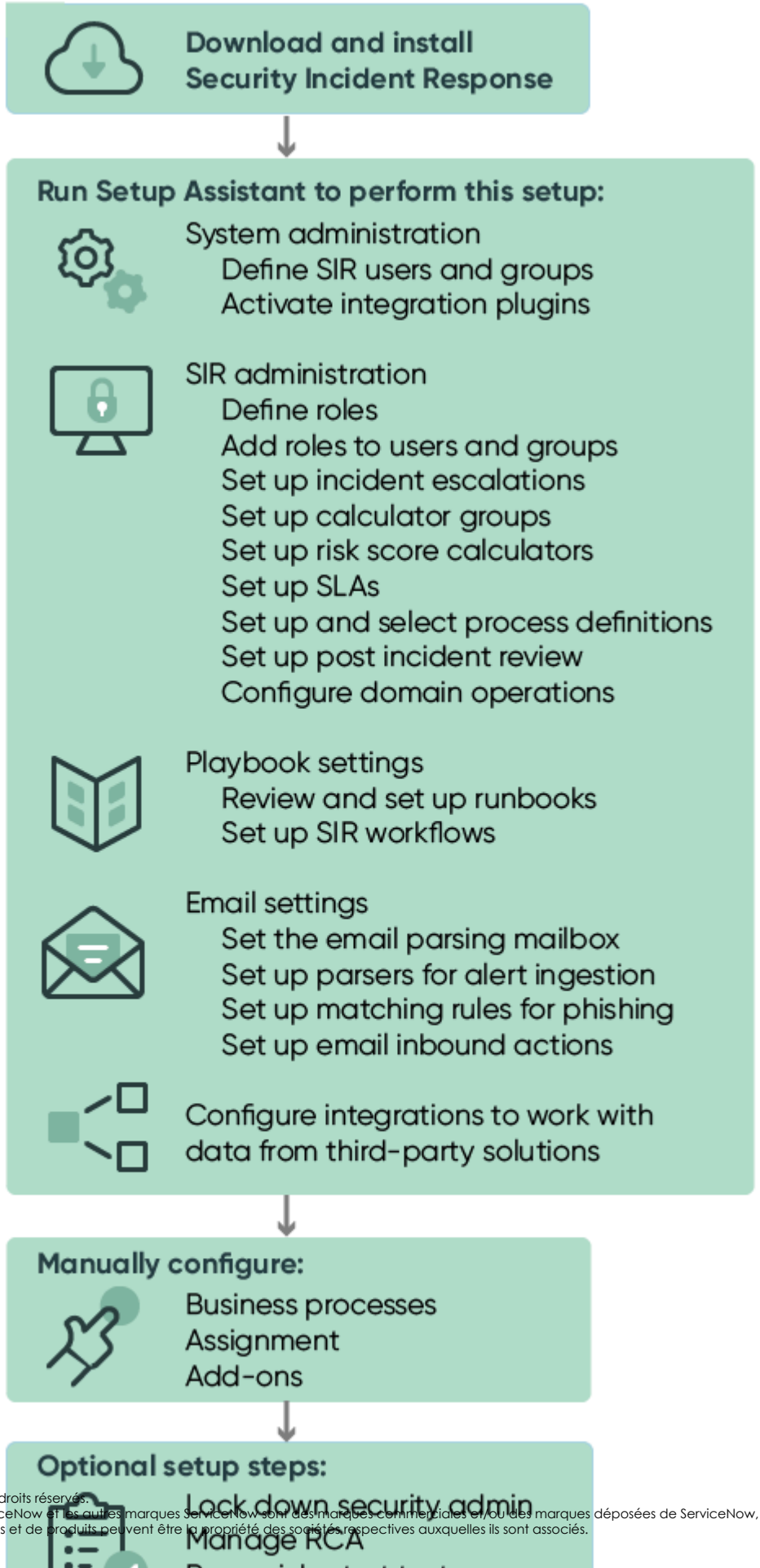
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Processus Réponse aux incidents de sécurité de configuration

Le diagramme suivant illustre le processus de configuration. Il est séparé en deux sous-processus, le téléchargement et la configuration de l'application Réponse aux incidents de sécurité .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La première étape de configuration consiste à Télécharger le Réponse aux incidents de sécurité application à partir de la ServiceNow Store. Une fois le téléchargement terminé, plusieurs applications dépendantes, y compris l'assistant de configuration, sont chargées et prêtes à l'emploi pour configurer Réponse aux incidents de sécurité.

Assistant de configuration

L'assistant Réponse aux incidents de sécurité de configuration est une application de type assistant qui vous guide, étape par étape, dans la configuration de votre instance de base Réponse aux incidents de sécurité .



Les étapes de configuration sont assez explicites ; Toutefois, si vous avez besoin d'explications supplémentaires, vous pouvez trouver de l'aide supplémentaire dans la référence de l'assistant de configuration. Une fois que vous avez terminé la configuration à l'aide de l'Assistant de configuration, vous pouvez effectuer d'autres procédures de configuration facultatives, si nécessaire. Ces procédures comprennent des options pour :

- Configurer le cycle de vie de la demande
- Création de catalogues et de demandes
- Configuration des notifications
- Configuration de l'affectation manuelle et automatique
- Activation de la base de connaissances, des documents gérés et des activités de tâches

Un nouvel espace de travail amélioré de Réponse aux incidents de sécurité est disponible. Pour plus d'informations, consultez Espace de travail de la Réponse aux incidents de sécurité.

Installer et configurer Réponse aux incidents de sécurité

Avant de l'exécuter Réponse aux incidents de sécurité dans votre instance, vous devez le télécharger à partir de et d'effectuer ServiceNow Store les étapes de configuration.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

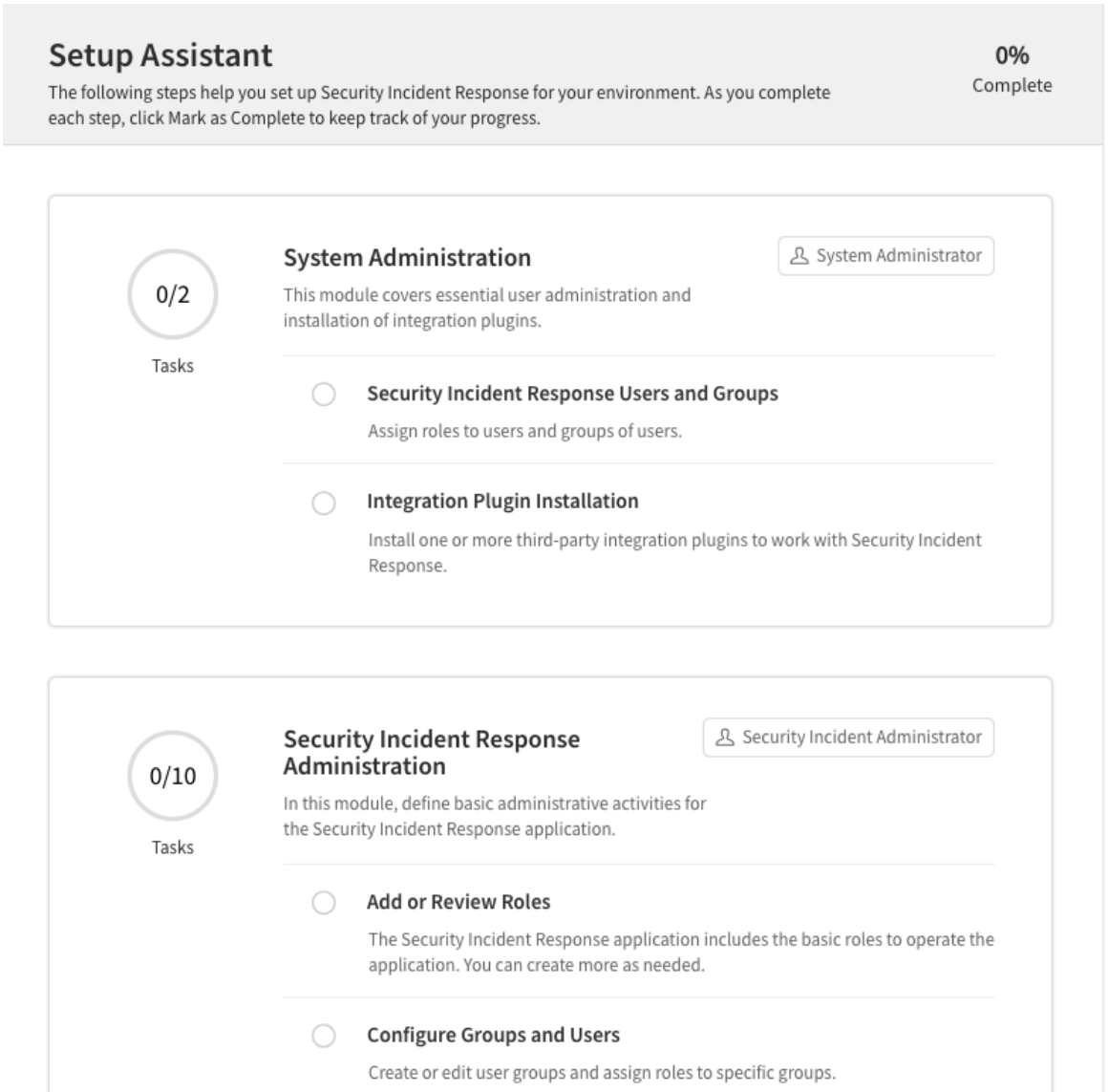
- L'installation de la Réponse aux incidents de sécurité version 13.4.5 ou ultérieure à partir de installe ServiceNow Store automatiquement la version 1.5.1 ou ultérieure Espace de travail de la Réponse aux incidents de sécurité (sn_si_aw) par défaut. Pour plus d'informations sur les applications dépendantes, reportez-vous à la SIR Workspace Modules d'extension et rôles section.
- Veuillez noter que les versions 1.5.1 et supérieures de l'espace de travail Security Incident Response ne peuvent être installées/mises à niveau que via une installation/mise à niveau de Security Incident Response et ne peuvent pas être installées indépendamment.
- Les dernières fonctionnalités de sont Réponse aux incidents de sécurité exclusivement disponibles dans le Espace de travail de la Réponse aux incidents de sécurité. Veuillez installer ou mettre à niveau vers la dernière Réponse aux incidents de sécurité version pour Espace de travail de la Réponse aux incidents de sécurité accéder et exploiter des fonctionnalités telles que Transfert d'équipe, Calculateur de score de risque, etc.

Procédure

1. Suivez les instructions pour le téléchargement d'une application à partir de ServiceNow Store.
2. Une fois que vous avez téléchargé l'application Réponse aux incidents de sécurité et toutes ses applications dépendantes, accédez à **Incident de sécurité** > **Configuration d'Analyst Workspace** > **Assistant de configuration**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Suivez les instructions sur les formulaires pour configurer le système de Réponse aux incidents de sécurité base.
   Pour plus d'informations sur certaines des tâches de configuration les plus complexes, reportez-vous à la section Référence de l'assistant de configuration, au besoin.

Télécharger et installer Security Analyst Workspace

Avant d'exécuter la Réponse aux incidents de sécurité nouvelle interface utilisateur dans votre instance, vous devez la télécharger ServiceNow® Store et l'installer.

Avant de commencer

Pour garantir une installation fluide, vérifiez que vous disposez des rôles requis ServiceNow pour votre instance. Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus :

- Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte le rôle d'administrateur de Réponse aux incidents de sécurité [sn_si.admin].
- L'administrateur de Réponse aux incidents de sécurité [sn_si.admin] supervise la configuration et vérifie les résultats attendus.

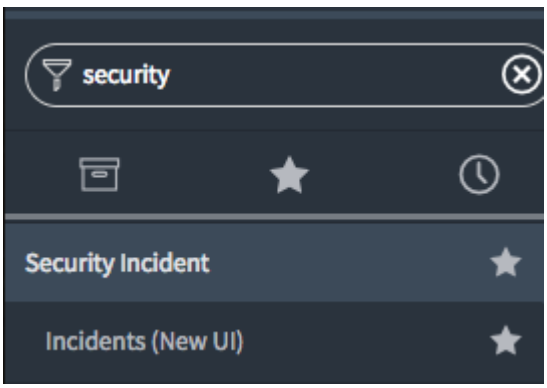
Rôle requis : administrateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Suivez les instructions pour le téléchargement d'une application à partir de ServiceNow Store et installez l'application **Security Incident Response UI** .
2. Une fois l'installation terminée, vous pouvez ouvrir Security Analyst Workspace en accédant à **Incident de sécurité** > **Incidents (nouvelle UI)**



Composants installés avec Réponse aux incidents de sécurité

Plusieurs types de composants sont installés lorsque vous téléchargez et activez l'application, notamment les rôles d'utilisateur, les tables, les propriétés et les Réponse aux incidents de sécurité travaux planifiés.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

Propriétés installées

Les utilisateurs disposant du rôle d'administrateur système [admin] peuvent afficher les propriétés. Les utilisateurs disposant du rôle d'administrateur de sécurité [sn_si.admin] peuvent les modifier.

Propriété	Utilisation
L'heure de début par défaut pour tous les agents quand aucune planification n'est définie, au format suivant : 08:00 sn_si.default.start.time	• **Type** : chaîne • **Valeur par défaut** : 08:00 • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Heure de fin par défaut pour tous les agents quand aucun calendrier n'est défini, au format suivant : 17:00 sn_si.default.end.time	• **Type** : chaîne • **Valeur par défaut** : 17:00 • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Inclure les observables de type Destination ainsi que d'autres observables de type contexte dans les relations entre	Détermine si un incident de sécurité observable avec le type de contexte Destination s'affiche sous les **onglets Éléments de configuration** ou

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
l'utilisateur de l'incident de sécurité et le CI sn_si.link_dest_ip	**Utilisateurs affectés** . Par défaut, les observables avec un type de contexte de destination sont exclus. Pour inclure les observables, choisissez Oui.
Autoriser la personnalisation lors de la création d'un problème ou d'une demande de changement à partir d'un incident de sécurité sn_si.fenêtre contextuelle	Lorsqu'un problème ou un changement est créé, cette propriété ouvre une fenêtre contextuelle pour modifier la demande. Si ces propriétés sont définies sur **faux**, le problème ou la demande de changement a la même priorité, la même description courte et la même description que l'incident de sécurité sans la possibilité d'ajouter ou de modifier ces champs. • **Type** : vrai | faux • **Valeur par défaut** : true • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Associez les résultats de recherche de perceptions aux CI dans la CMDB. sn_si.associate_ci_with_sighting_search	Lorsqu'ils sont définis sur vrai, les résultats de la recherche de perceptions incluent les éléments de configuration associés qui se trouvent dans votre CMDB. • **Type** : vrai | faux • **Valeur par défaut** : true • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Le score de risque dans la plage est en surbrillance verte, au format 0-49 sn_si.risk.score.green	Dans la liste des incidents de sécurité, les incidents de sécurité avec un score de risque compris entre 0 et 49 sont marqués d'un point vert.
Le score de risque dans la plage est en surbrillance orange, au format 50-79 sn_si.risk.score.orange	Dans la liste des incidents de sécurité, les incidents de sécurité avec un score de risque compris entre 50 et 79 sont signalés par un point orange.
Le score de risque dans la plage est en surbrillance rouge, au format 80-100 sn_si.risk.score.red	Dans la liste des incidents de sécurité, les incidents de sécurité avec un score de risque compris entre 80 et 100 sont marqués d'un point rouge.
Ce paramètre active ou désactive les configurations de recherche de perceptions qui ont implémenté cette fonctionnalité.	Lorsqu'elle est définie sur vrai, les recherches de perceptions peuvent être effectuées sur les intégrations activées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
sn_si.enable_sighting_search	• **Type** : vrai | faux • **Valeur par défaut** : true • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Nombre de lignes de données brutes enregistrées lors de l'exécution d'une recherche d'observations. Plage 0-100 sn_si.sighting_search_raw_data_rows	Cette propriété est définie par défaut sur 50 lignes de données brutes. La moitié des lignes de résultats sont signalées à partir du début de l'intervalle de temps de recherche et l'autre moitié à partir de la fin de l'intervalle de temps de recherche. Ainsi, si vous sélectionnez 50 lignes, 25 proviennent du début de l'intervalle de temps de recherche et 25 de la fin de l'intervalle de temps de recherche.
Faire passer automatiquement l'état de l'incident à Maîtriser lorsqu'une tâche de réponse passe à Travail en cours sn_si.rollup_task_state	Lors de l'utilisation de flux ou de workflows, pensez à définir cette propriété sur **faux**. Cela vous permet de contrôler l'état de l'incident à partir de flux ou de workflows. Cela permet également d'éviter tout conflit potentiel lors de la transition d'un état d'incident à un autre. • **Type** : vrai | faux • **Valeur par défaut** : true • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Propriétés de l'affectation pour Réponse aux incidents de sécurité	
Poids de l'emplacement sn_si.Emplacement.Poids	Une note utilisée lors du calcul des critères à utiliser pour l'affectation automatique d'un analyste de sécurité. Si, par exemple, l'emplacement est pris en compte pour une tâche, la valeur de poids de l'emplacement est ajoutée à l'évaluation de l'analyste de sécurité. • **Type** : nombre entier • **Valeur par défaut** : 10 • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Poids des compétences sn_si.compétences.poids	Une note utilisée lors du calcul des critères à utiliser pour l'affectation automatique d'un analyste de sécurité. Si, par exemple, des compétences sont prises en compte pour une tâche, la valeur de poids des compétences est ajoutée à la note d'analyste de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
	• **Type** : nombre entier • **Valeur par défaut** : 10 • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Définir le nombre maximal d'analystes de sécurité à traiter par affectation automatique à un moment donné sn_si.max.agents.traités	Le système a une limite absolue de 300 analystes de sécurité. Si vous spécifiez plus de 300, cette valeur est définie sur ce niveau. Le système ne peut pas répartir automatiquement une tâche pour un groupe de répartition qui contient plus d'analystes de sécurité que la valeur configurée. • **Type** : nombre entier • **Valeur par défaut** : 100 • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Poids du fuseau horaire sn_si.fuseau.horaire.poids	Une note utilisée lors du calcul des critères à utiliser pour l'affectation automatique d'un analyste de sécurité. Si, par exemple, le fuseau horaire de l'analyste de sécurité est pris en compte pour une tâche, la valeur de pondération du fuseau horaire est ajoutée à l'évaluation de l'analyste de sécurité. • **Type** : nombre entier • **Valeur par défaut** : 10 • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Durée (en minutes) à ajouter entre la fin d'une tâche et le début du déplacement pour la suivante. sn_si.espacement.travail.espacement	Un exemple d'une valeur de temps valide est 10. • **Type** : nombre entier • **Valeur par défaut** : 0 • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Champs de journal spécifiés contenant des balises `de code` qui restituent le contenu au format HTML. sn_si.journal_field.html_enabled	• **Type** : chaîne • **Valeur par défaut** : work_notes, commentaires • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Calculez les services impactés en arrière-plan.	La liste connexe des services affectés et des CI impactés est générée par le biais d'événements. Lorsqu'elle est activée,

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
sn_si.refresh_impacted.event	l'actualisation est exécutée en arrière-plan et des balises de sécurité sont ajoutées à l'incident. Définissez la valeur sur **vrai** pour effectuer l'opération en arrière-plan. • **Type** : vrai | faux • **Valeur par défaut** : faux • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**
Récupérez le service critique à partir de données précalculées. sn_si.critical_service.calculator.use_cache	Permet au calculateur de services critiques d'utiliser les données précalculées des éléments de configuration. Définir la valeur sur **vrai** pour effectuer une recherche à partir de données précalculées • **Type** : vrai | faux • **Valeur par défaut** : faux • **Localisation** : **Incident de sécurité** > **Administration** > **Propriétés**

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
Administrateur d'incident de sécurité [sn_si.admin]	Contrôle total de toutes les Réponse aux incidents de sécurité données. Administre également les territoires et les compétences, selon les besoins.	• assessment_admin • catalog_admin • decision_table_admin • decision_table_reader • filter_admin • flow_designer • pd_author • pd_content_author

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	Remarque : Dans le système de base, l'administrateur a également accès à sn_si.admin. Réponse aux incidents de sécurité Peut être restreint par l'administrateur tant qu'au moins un autre utilisateur se voit affecter le rôle d'administrateur de sécurité.	• pd_operator • skill_admin • skill_model_admin • sn_si.analyst • sn_si.knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_access_manager • sn_si.special_access_read_manager • sn_si.special_access_write_manager • sn_ti.malicious_attachment_access • sn_ti.observable.admin • tags_admin • template_admin • territory_admin • treemap_admin • user_admin
Analyste des incidents de sécurité [sn_si.analyste]	Gérer les incidents de sécurité. Rôle sous-jacent pour l'accès de sécurité de base. Les utilisateurs disposant de ce rôle peuvent créer et mettre à jour des incidents de sécurité, des demandes et des tâches, ainsi que des problèmes, des changements et des pannes liés à leurs incidents.	• pd_operator • snc_platform_rest_api_access • sn_msi.promoteur • sn_msi.proposant • sn_si.basic • sn_ti.malicious_attachment_access
Incident de sécurité - Base [sn_si.basic]	Rôle sous-jacent pour l'accès de sécurité de base. Les utilisateurs disposant de ce rôle peuvent créer et mettre à jour des incidents de sécurité, des demandes et des tâches, ainsi que des problèmes, des changements et des	• canvas_user • document_management_user • email_composer • flow_operator • inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.write

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	pannes liés à leurs incidents.	• sn_si.read • sn_ti.observable.read • sn_ti.observable.write • sn_ti.read • task_activity_writer • task_editor • treemap_user
Directeur de la sécurité de l'information (CISO) [sn_si.ciso]	Afficher et manipuler le tableau de bord CISO. En outre, si le module d'extension est activé, les Réponse aux vulnérabilités utilisateurs ayant ce rôle peuvent ajouter des arborescences de définition de l'importance de la vulnérabilité au tableau de bord. Vous pouvez également faire la même chose avec Réponse aux incidents de sécurité le plugin.	• pa_viewer • sn_si.basic • sn_si.read
Incident de sécurité externe [sn_si.externe]	Afficher tous les incidents de sécurité qui appartiennent à son groupe particulier.	service_fulfiller

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	Remarque : Les deux règles suivantes s'appliquent partout ServiceNow , quel que soit l'administrateur du champ d'application ou l'application du champ d'application. • Lorsque vous ajoutez un utilisateur à un groupe, vous affectez également des rôles à ce groupe. De même, lorsque vous supprimez un utilisateur d'un groupe, les rôles hérités sont également supprimés. • Chaque rôle peut être affecté par un rôle de priorité supérieur.	
Utilisateur d'intégration d'incident de sécurité [sn_si.integration_user]	Les outils externes peuvent fournir de nouveaux enregistrements d'incidents de sécurité et mettre à jour les enregistrements d'incidents de sécurité.	import_transformer
Administrateur de la base de connaissances sur les incidents de sécurité [sn_si.knowledge_admin]	Gérez, mettez à jour et supprimez les informations de la base de connaissances des incidents de sécurité.	• knowledge_admin • sn_si.read

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
Gestionnaire d'incident de sécurité [sn_si.manager]	Même accès que les analystes de sécurité.	• pd_author • pd_operator • sn_si.basic
Lecture de l'incident de sécurité [sn_si.read]	Lire les incidents de sécurité.	• canvas_user • sn_sec_cmn.read • sn_templated_snip.template_snippet_read • sn_ti.observable.read • workspace_user
Gestionnaire d'accès restreint à la sécurité [sn_si.restriction_access_manager]	Permet aux utilisateurs ou aux groupes d'appliquer des restrictions sur les incidents de sécurité. Cela ne s'applique qu'au changement de champ.	N/A
Accès spécial à l'incident de sécurité sn_si.accès_speciale	Permet d'accéder à des incidents de sécurité spécifiques à des utilisateurs extérieurs à l'organisation des opérations de sécurité.	N/A
Activateur d'accès spécial à la sécurité [sn_si.special_access_enabler]	Fournit un rôle d'accès spécial à un utilisateur extérieur à l'organisation des opérations de sécurité à des incidents de sécurité spécifiques.	N/A
Gestionnaire de lecture d'accès spécial aux incidents de sécurité [sn_si.special_access_read_manager]	Gérez le rôle Accès spécial aux incidents de sécurité [sn_si.special_access]. Utilisez ce rôle pour modifier le champ **Accès en lecture** dans le formulaire d'incident de sécurité. Ce rôle peut être affecté par sn_si.admin.	sn_si.special_access_enabler

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
Gestionnaire des rédacteurs d'accès spécial aux incidents de sécurité [sn_si.special_access_write_manager]	Gérez le rôle Accès spécial aux incidents de sécurité [sn_si.special_access]. Utilisez ce rôle pour modifier le champ **Accès privilégié** dans le formulaire d'incident de sécurité. Ce rôle peut être affecté par sn_si.admin.	sn_si.special_access_enabler

Travaux planifiés installés

Tâche planifiée	Description
Rechercher des observables d'incident de sécurité	Effectue une recherche d'observables selon un calendrier défini par l'utilisateur.

Tables installées

Table	Description
Configuration du flux d'actualités [sn_si_feed_configuration]	Enregistrements de configuration utilisés pour définir le contenu affiché dans le flux d'actualités de l'incident de sécurité.
Règle d'affectation de revue post-incident [sn_si_pir_condition]	Automatise la sélection des participants d'une enquête de revue post-incident lorsqu'un incident de sécurité est fermé.
Incident de sécurité [sn_si_incident]	Stocke un incident de sécurité, les réponses à l'incident, toutes les tâches liées, les changements, les problèmes et les incidents liés à cet incident de sécurité.
Vecteurs d'attaque des incidents de sécurité [sn_si_attack_vector]	Options de vecteur d'attaque.
Journal d'audit des incidents de sécurité [sn_si_audit_log]	Stocke les journaux d'audit d'enrichissement des incidents de sécurité.
Calculateur d'incidents de sécurité [sn_si_calculator]	Un calculateur pour définir certains champs d'incident de sécurité lorsque certaines conditions sont remplies.
Groupe de calculateurs d'incidents de sécurité [sn_si_calculator_group]	Un regroupement de calculateurs d'incident de sécurité L'ordre du groupe de calculateurs détermine quel groupe est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	évalué en premier, et dans chaque groupe, un calculateur au maximum est utilisé.
Pare-feu d'enrichissement des incidents de sécurité [sn_si_enrichment_firewall]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques à Palo Alto Networks Firewall.
Enrichissement des incidents de sécurité Résultats concernant les programmes malveillants [sn_si_enrichment_malware]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques aux programmes malveillants.
Enrichissement des incidents de sécurité Statistiques réseau [sn_si_enrichment_network_statistics]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques aux statistiques réseau.
Processus en cours d'enrichissement des incidents de sécurité [sn_si_enrichment_running _processes]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques aux processus en cours d'exécution.
Services d'exécution d'enrichissement des incidents de sécurité [sn_si_enrichment_running_service]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques aux services d'exécution.
Recherche d'e-mails d'incidents de sécurité [sn_si_m2m_incident_email_search]	Mappe les enregistrements de recherche d'e-mails aux incidents de sécurité.
Importation des incidents de sécurité [sn_si_incident_import]	Table à importer pour les incidents de sécurité. Utilisée pour créer des incidents de sécurité à partir de systèmes externes.
Définition de processus d'incident de sécurité [sn_si_process_definition]	Stocke la configuration des flux de processus des incidents de sécurité.
Sélecteur de définitions de processus d'incidents de sécurité [sn_si_process_definition_selector]	Stocke la définition du processus d'incident de sécurité à utiliser pour les incidents de sécurité.
Incident de sécurité associé au ticket du service clientèle [sn_si_m2m_incident_customerservice_case]	Mappe les tickets du service clientèle et les incidents de sécurité
Données d'enrichissement associées aux incidents de sécurité	Mappe les incidents de sécurité et les enregistrements de données d'enrichissement associés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_si_m2m_incident_enrichment]	
Tâche Réponse aux incidents de sécurité [sn_si_task]	Gère les sous-tâches liées à la gestion d'un incident de sécurité. Ces tâches peuvent être affectées au personnel de sécurité, ou à des personnes d'autres départements, pour gérer la communication entre les départements et le suivi des tâches.
Modèle de tâche Réponse aux incidents de sécurité [sn_si_task_template]	Utilisé pour créer une Réponse aux incidents de sécurité tâche. Ces modèles sont souvent utilisés dans les entrées de catalogue, afin de créer automatiquement un ensemble de sous-tâches appropriées pour un type particulier d'incident de sécurité.
Document Runbook d'incident de sécurité [sn_si_runbook_document]	Associe les conditions ou les filtres d'incident de sécurité à un article de la base de connaissances. Utilisé pour spécifier des procédures de runbook pour la résolution des incidents de sécurité.
Modèle d'incident de sécurité [sn_si_incident_template]	Utilisée pour créer un incident de sécurité. Ces modèles sont souvent utilisés dans les entrées de catalogue pour créer un incident de sécurité prédéfini.
Demande de sécurité [sn_si_request]	Une demande liée à la sécurité à l'équipe de sécurité.
Demande d'analyse de sécurité [sn_si_scan_request]	Une demande de recherche de menace.
Calculateur de gravité sn_si_severity_calculator	Définit les valeurs de gravité, d'impact, de risque et de criticité d'un incident de sécurité.
Tâche Utilisateur concerné [sn_si_m2m_task_affected_user]	Table plusieurs-à-plusieurs associant des incidents de sécurité à des utilisateurs affectés.
Évaluateur de résultats de l'activité du workflow de modèle [sn_si_wf_activity_outcome_evaluator]	Mappe une aptitude avec un script d'évaluation. Un nouveau flux secondaire peut être ajouté à un workflow de modèle pour définir un résultat de tâche de réponse plutôt que d'être défini manuellement par un analyste.

Autres tâches de configuration supplémentaires Réponse aux incidents de sécurité

Si vous êtes un administrateur du domaine global, vous configurez la manière dont Réponse aux incidents de sécurité il gère les opérations quotidiennes.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Ces options sont standard à de nombreuses applications de gestion des services et, à ce titre, elles utilisent la terminologie de gestion des services. Par exemple, la demande est utilisée pour la tâche principale (c'est-à-dire l'incident de sécurité) et la tâche est utilisée pour les sous-tâches ou les tâches de réponse.

Si vous êtes un administrateur d'un domaine inférieur au domaine global, vous pouvez afficher l'écran Configurations, mais vous ne pouvez pas modifier les paramètres.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Administration** > **Configuration**.
   Les options de configuration des applications sont organisées sous ces onglets :
   - L'onglet **Processus de gestion** contient des options pour configurer le cycle de vie de la demande, créer des catalogues et des demandes et configurer des notifications.
   - L'onglet **Affectation** contient des options pour configurer l'affectation manuelle et automatique.
   - L'onglet **Compléments** contient des options pour l'activation de la base de connaissances, des documents gérés et des activités de tâches.
2. Renseignez les champs de l'onglet **Processus business** .

Écran Configuration — Onglet Processus de gestion

Champ	Description
Cycle de vie.	
Des notes de travail sont requises pour fermer ou annuler une demande ou une tâche	Activez cette option pour exiger de l'utilisateur qu'il saisisse des notes de travail avant qu'un incident de sécurité ou une tâche de réponse puisse être fermé ou annulé.
Copier les notes de travail de la tâche dans la demande	Activez cette option pour synchroniser les notes de travail de tâche de réponse avec les notes de travail sur l'incident de sécurité. Ainsi, lorsque des notes de travail sont ajoutées à la tâche, les mêmes notes de travail s'affichent dans l'incident de sécurité parent.
Catalogue et création de demande	
Créer ou mettre à jour les demandes par e-mail entrant	Activez cette option pour créer ou mettre à jour des incidents de sécurité à partir d'e-mails entrants.
Les demandes sont créées avec	Sélectionnez le **catalogue ou le formulaire standard** pour activer le catalogue et activer la publication automatique des modèles d'incidents de sécurité dans le catalogue. Sélectionnez le **formulaire classique uniquement** pour désactiver le catalogue et désactiver la publication automatique des modèles d'incidents de sécurité dans le catalogue.
Les modèles créent un élément de catalogue dédié	Activez cette option pour activer la publication automatique des éléments de catalogue pour l'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Notifications	
Pour une demande ou une tâche, lorsque le champ sélectionné change, envoyer une notification aux destinataires	Vous pouvez configurer des notifications à envoyer à des destinataires spécifiques lorsque les champs sélectionnés dans les incidents de sécurité et les tâches de réponse changent. **a.** Dans **Table**, sélectionnez **Demande (incident de sécurité**) ou **Tâche (tâche de réponse)**. **b.** Dans **Champ**, sélectionnez le champ à utiliser pour générer des notifications. Lorsqu'une modification est apportée au champ sélectionné, une notification est envoyée aux destinataires identifiés. **c.** Dans **Destinataires**, sélectionnez un ou plusieurs destinataires. **d.** Si vous sélectionnez **un utilisateur spécifique** ou **un groupe spécifique**, vous êtes invité à sélectionner un utilisateur ou un groupe. **e.** Pour définir d'autres notifications à l'aide d'autres champs ou destinataires, répétez les étapes précédentes pour l'ensemble suivant de paramètres de notification. **f.** Pour supprimer une notification, cliquez sur l'icône du ⊖ située à droite de la notification.

3. Cliquez sur l'onglet **Affectation** et remplissez les champs.

Écran de configuration : onglet Affectation

Champ	Description
Méthode d'affectation des demandes	Sélectionnez la méthode d'affectation des incidents de sécurité : ◦ **Utilisation de l'affectation automatique** : les incidents de sécurité sont automatiquement affectés. ◦ **Utilisation d'un workflow** : les incidents de sécurité sont affectés par le workflow sélectionné. ◦ **manuellement** : les incidents de sécurité sont affectés manuellement.
Utilisez ce workflow pour affecter des demandes	Sélectionnez le workflow pour la répartition des incidents de sécurité. Ce champ **s'affiche lorsque vous utilisez un workflow** sélectionné dans la liste **Méthode d'affectation pour les demandes** .
Méthode d'affectation des tâches	Sélectionnez la méthode d'affectation des tâches de réponse : ◦ **à l'aide de l'affectation automatique** : les tâches de réponse sont automatiquement affectées. ◦ **Utilisation d'un workflow** : les tâches de réponse sont affectées par le workflow sélectionné. ◦ **Manuellement** : les tâches de réponse sont affectées manuellement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utilisez ce workflow pour affecter des tâches	Sélectionnez le workflow pour l'affectation des tâches de réponse. Ce champ **s'affiche lorsqu'un workflow** est sélectionné dans la liste **Méthode d'affectation des tâches** .
Affectez les demandes ou les tâches en fonction des zones de couverture des groupes d'affectation	Activez cette option pour limiter l'affectation des incidents de sécurité et des tâches de réponse aux groupes qui couvrent l'emplacement de la tâche.
Ordonnancement	
La sélection automatique d'agents tient compte du fuseau horaire pour les tâches	Activez cette option pour tenir compte du fuseau horaire de l'agent lors de l'affectation d'une tâche. Ce champ s'affiche lorsque l'affectation automatique est sélectionnée pour les incidents de sécurité ou les tâches de réponse.
Facteurs supplémentaires	
La sélection automatique d'agents tient compte de leur localisation	Activez cette option pour donner la préférence aux agents qui sont plus proches de l'emplacement de la tâche, lors de l'affectation de tâches. Ce champ s'affiche lorsque l'affectation automatique est sélectionnée pour les incidents de sécurité ou les tâches de réponse.
La sélection automatique d'agents pour des tâches requiert qu'ils aient des compétences	Sélectionnez le degré auquel les compétences de l'agent doivent être adaptées à une tâche lors de la détermination de l'affectation automatique. ◦ Sélectionnez **Tout** pour exiger qu'un agent affecté possède toutes les compétences nécessaires pour exécuter la tâche. Un agent qui n'a pas ne serait-ce qu'une seule compétence est éliminé. ◦ **Sélectionnez-en quelques-uns** si vous voulez des agents qui possèdent la plupart des compétences requises pour effectuer la tâche. ◦ Sélectionnez **Aucun** si vous souhaitez affecter automatiquement des agents sans tenir compte des compétences. Ce champ s'affiche lorsque l'affectation automatique est sélectionnée pour les incidents de sécurité ou les tâches de réponse.
La sélection automatique tente d'affecter le même agent à toutes les tâches d'une demande	Activez cette option pour affecter automatiquement toutes les tâches de réponse d'un incident de sécurité au même agent.

4. Cliquez sur l'onglet **Compléments** et remplissez les champs.

Écran de configuration : onglet Compléments

Champ	Description
Documentation	

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Activer une base de connaissances dédiée	Activez cette option pour activer la base de connaissances pour Réponse aux incidents de sécurité.
Activer les documents gérés	Activez cette option pour ajouter une liste connexe aux documents gérés.
Activer les activités de la tâche	Activez cette option pour consigner les interactions et les communications de tâche, telles que les appels téléphoniques et les messages électroniques.

5. Cliquez sur **Enregistrer**.

Verrouiller l'administration de la sécurité

Pour protéger les enquêtes et préserver la confidentialité des incidents de sécurité, vous pouvez restreindre Réponse aux incidents de sécurité l'accès aux rôles et aux ACL spécifiques à la sécurité. L'accès aux personnes qui ne sont pas des administrateurs de sécurité peut être restreint, sauf si vous leur autorisez expressément l'accès.

Avant de commencer

Lorsque l'application est activée, l'utilisateur Réponse aux incidents de sécurité administrateur système se voit accorder le rôle sn_si.admin par défaut. L'administrateur système est le seul administrateur qui peut configurer des groupes et des utilisateurs de sécurité.

Un rôle de sécurité est requis pour avoir accès aux fonctionnalités et aux Réponse aux incidents de sécurité enregistrements.

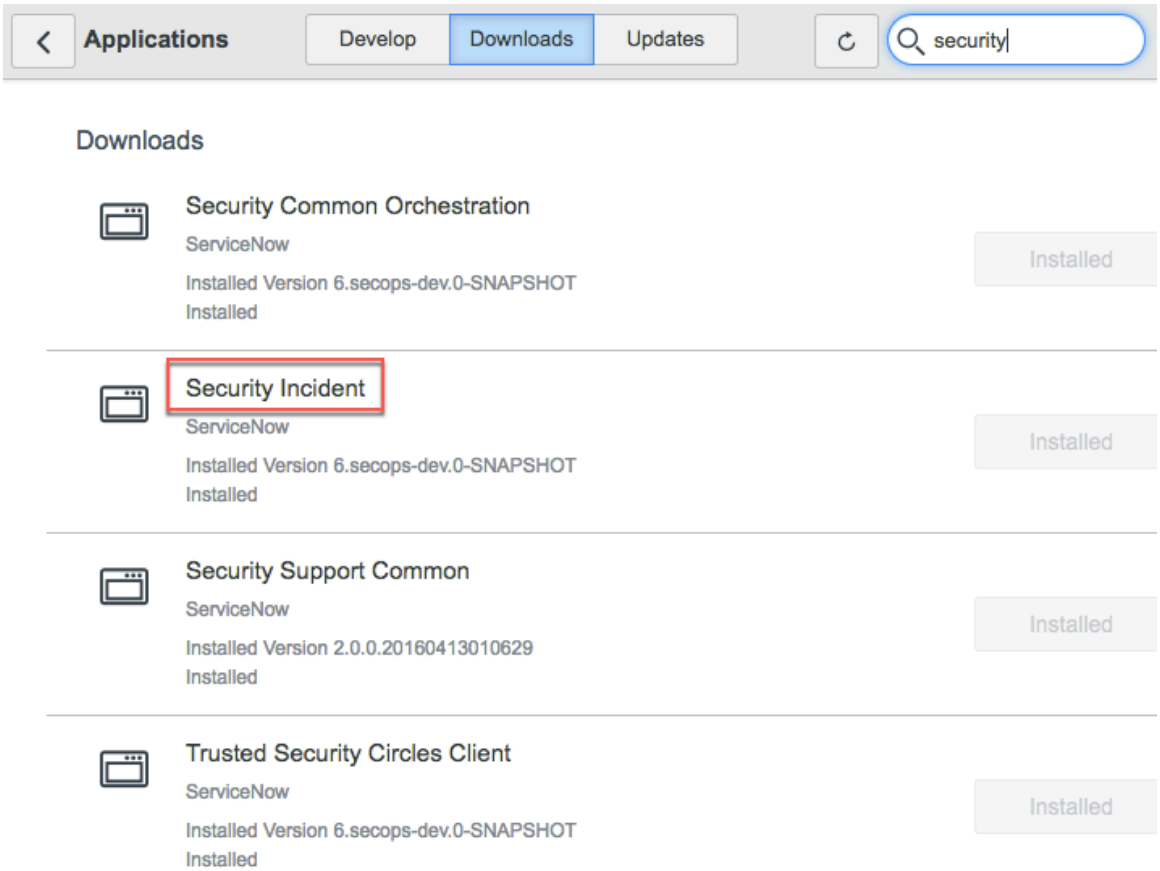
Rôle requis : sn_si.admin

Procédure

1. Une fois le Réponse aux incidents de sécurité module d'extension activé, un utilisateur ayant le rôle admin affecte le rôle Administrateur inclus dans le périmètre (sn_si.admin) à au moins un utilisateur.
2. L'utilisateur ayant le rôle administrateur passe au champ d'application de l'incident de sécurité.
3. Accédez à la **Applications système** > **Applications**.
4. Cliquez sur **Téléchargements**.
5. Saisissez **sécurité** dans le champ **Rechercher des applications** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Incident de sécurité**.
7. Faites défiler l'écran vers le bas jusqu'aux **liens connexes** et cliquez sur **Supprimer du rôle contenu par l'administrateur**.
8. Déconnectez-vous, puis reconnectez-vous.
   L'utilisateur administrateur ne peut pas accéder à l'application Réponse aux incidents de sécurité .

Information associée

Administration d'application

Gérer l'accès restreint de l'appelant

La fonctionnalité d'accès restreint pour l'appelant (RCA) permet à l'administrateur de définir un accès entre périmètres à une application ou à une ressource d'application et d'autoriser ou de refuser les demandes d'accès. Cette fonctionnalité est activée par défaut afin Réponse aux incidents de sécurité que les analystes de sécurité puissent protéger les informations sensibles liées à la sécurité.

Un champ appelé **Accès pour l'appelant** a été ajouté à l'ensemble des tables et des includes de script dans Réponse aux incidents de sécurité, et le champ est défini par défaut sur **Suivi de l'appelant**. Ce paramètre signifie que les périmètres de l'application sont autorisés à accéder aux tables et aux includes de Réponse aux incidents de sécurité script. Toutefois, un enregistrement de suivi est créé pour chaque enregistrement et stocké dans la table Privilège d'accès restreint pour l'appelant [sys_restricted_caller_access].

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Soyez prudent lorsque vous modifiez les enregistrements de **Suivi de l'appelant** à **Restreint pour l'appelant**. Les enregistrements avec cet état ne sont pas accessibles tant qu'un administrateur n'en autorise pas l'accès manuellement. L'administrateur doit accéder à **Applications système** > **Accès restreint à l'application pour l'appelant**, localisez la table ou l'include de script pour lequel l'accès a été demandé et faites passer le champ **État** de **Demandé** à **Autorisé**.

Information associée

Paramètres de privilège d'accès restreint pour l'appelant

Définir le périmètre de l'application, la ressource de l'application et l'accès aux événements

Exécuter des tests de démarrage rapide pour Réponse aux incidents de sécurité

Valider que Réponse aux incidents de sécurité cela fonctionne toujours après avoir apporté des changements de configuration, tels que l'application d'une mise à niveau ou le développement d'une application. Copiez et personnalisez ces tests de démarrage rapide à effectuer lorsque vous utilisez des données spécifiques à votre instance.

Les tests de démarrage rapide pour Réponse aux incidents de sécurité nécessitent l'activation du module d'extension Réponse aux incidents de sécurité (com.snc.security_incident) et le chargement des données de démonstration.

Tests Réponse aux incidents de sécurité

Test	Description	Version
SIR : créer un incident de sécurité	Déterminez si un utilisateur peut créer un incident de sécurité depuis le formulaire d'incident de sécurité.	Xanadu
SIR : créer un incident de sécurité via le catalogue d'incidents de sécurité	Déterminez si un utilisateur peut créer un incident de sécurité depuis le catalogue.	Xanadu
SIR : cycle de vie des incidents de sécurité	Validez les tâches de réponse du workflow de violation de la politique.	Xanadu
SIR : rechercher des menaces	Validez la capacité de recherche des menaces.	Xanadu
SIR : configuration prête à l'emploi des évaluations PIR	Utilisez ce test pour valider les évaluations PIR et les configurations du système de base.	Xanadu
SIR : configuration conditionnelle des évaluations PIR	Vérifiez que les incidents de sécurité correspondant à la règle conditionnelle obligatoire ne sont pas fermés avant que l'évaluation post-incident ne soit terminée. Vérifiez que les incidents de sécurité correspondant	Xanadu

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests Réponse aux incidents de sécurité (suite)

Test	Description	Version
	à la règle conditionnelle facultative peuvent être fermés avant que l'évaluation post-incident ne soit terminée. Vérifiez que les évaluations ne sont pas générées pour les incidents de sécurité qui ne correspondent à aucune règle.	
SIR : vérification de l'heure d'exécution PIR	Vérifiez que les rapports PIR sont configurés et joints aux incidents de sécurité selon la nouvelle conception.	Xanadu
SIR : vérification de la configuration de l'heure de conception PIR	Vérifiez que l'incident de sécurité est mappé au modèle de rapport en fonction de la configuration de l'administrateur.	Xanadu
SIR : lier l'incident de sécurité à un incident de sécurité majeur	Liez un incident de sécurité à un incident de sécurité majeur existant et validez les données de l'incident de sécurité repris sur l'incident de sécurité majeur.	Xanadu
SIR : promouvoir l'incident de sécurité comme incident de sécurité majeur	Promouvoir un incident de sécurité en tant qu'incident de sécurité majeur et valider les données de l'incident de sécurité déployé jusqu'à l'incident de sécurité majeur.	Xanadu
SIR : proposer un incident de sécurité comme incident de sécurité majeur	Proposez un incident de sécurité en tant qu'incident de sécurité majeur et validez les données de l'incident de sécurité déployé jusqu'à l'incident de sécurité majeur.	Xanadu
Vérifier que seuls les membres autorisés peuvent accéder à l'incident de sécurité une fois que l'option Appliquer la restriction est activée	Vérifiez que seuls les membres autorisés peuvent accéder à l'incident de sécurité une fois que l'option Appliquer la restriction est activée.	Xanadu
Vérifier que seuls les groupes autorisés peuvent accéder à l'incident de sécurité une	Vérifiez que seuls les groupes autorisés peuvent accéder à l'incident de sécurité une	Xanadu

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests Réponse aux incidents de sécurité (suite)

Test	Description	Version
fois que l'option Appliquer la restriction est activée	fois que l'option Appliquer la restriction est activée.	
Valider l'accès en lecture	Validez l'accès à l'affichage.	Xanadu
Valider l'accès en écriture	Validez l'accès en modification.	Xanadu

Information associée

Tests de démarrage rapide

Référence de l'assistant de configuration

L'assistant de configuration vous guide tout au long des étapes que vous devez effectuer pour configurer le système de Réponse aux incidents de sécurité base. Cette section fournit des informations supplémentaires sur les étapes compliquées pour lesquelles vous pourriez avoir besoin de plus d'explications.

Création d'une définition de Réponse aux incidents de sécurité processus

Vous pouvez créer une définition de processus pour définir la manière dont les incidents de sécurité passent d'un état à l'autre. Les définitions de processus permettent aux centres de services et aux utilisateurs finaux de suivre le problème tout au long de son cycle de vie.

Avant de commencer

Rôle requis : sn.si_admin

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Administration** > **Définition de processus**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs comme il convient.

Création de définitions de processus

Champ	Description
Nom	Nom de l'enregistrement qui décrit le processus codé dans le fichier d'include de script. Le nom est affiché en tant que choix dans la liste **Sélecteur de définition de processus** .
Include de script	Nom (y compris le préfixe `sn_si.`) de l'include de script contenant la définition du processus. Le script doit se trouver dans le périmètre de l'application Incident de sécurité (`sn_si`). Consultez Créer un include de script de définition de processus personnalisé Réponse aux incidents de sécurité pour plus d'informations. Si ce champ ne contient pas de nom d'include de script valide, la définition de ProcessDefinition_NIST_Stateful par défaut est utilisée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Informations utiles sur le script include.
Ordre	Détermine la position dans la liste de définition du processus.
Actif	Lorsque cette option est cochée, cette définition de processus peut être sélectionnée à partir de la page **Sélecteur de définition de processus** .

4. Cliquez sur **Envoyer**.

Information associée

Sélection du processus de réponse aux incidents de sécurité

Comprendre la définition du processus de Security Incident Response

Comprendre la définition du processus de Security Incident Response

Réponse aux incidents de sécurité Définition du processus Remplace les flux d'états et fournit aux utilisateurs finaux et aux centres de services l'état d'un problème. Une définition de processus permet de suivre le problème tout au long de son cycle de vie. Réponse aux incidents de sécurité est une application de Gestion des services (SM) qui possède son propre ensemble d'états. Les états non valides sont signalés dans le cadre de Sélection du processus.

Définition de processus de réponse aux incidents de sécurité

La définition de processus par défaut (état NIST) définit les états d'incident suivants :

Remarque : Les états disponibles varient en fonction de l'état actuel de l'incident.

États des définitions de processus d'incidents de sécurité

État	Description
Brouillon	L'initiateur de la demande ajoute des informations sur l'incident de sécurité, mais il n'est pas encore prêt à être traité.
Analyse	L'incident a été affecté et le problème est en cours d'analyse.
Contenir	Le problème a été identifié et le personnel de sécurité s'efforce de le contenir et de limiter les dégâts. Ces actions peuvent inclure la mise hors ligne des serveurs, la déconnexion de l'équipement d'Internet et la vérification de l'existence des sauvegardes.
Éradiquer	Le problème a été maîtrisé et le personnel de sécurité prend des mesures pour le résoudre.
Récupérer	Le problème est résolu et l'état de préparation opérationnelle des systèmes concernés est en cours de vérification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des définitions de processus d'incidents de sécurité (suite)

État	Description
Revue	L'incident de sécurité est terminé et tous les systèmes ont repris un fonctionnement normal, mais un examen post-incident est encore nécessaire.
Fermé	L'incident est terminé. Toutefois, avant de pouvoir fermer un incident de sécurité, vous devez renseigner les informations de l'onglet Informations sur la **fermeture** .

Définitions de processus de tâche d'incident de sécurité

Les définitions de processus suivantes sont utilisées pour les tâches d'incident de sécurité.

États des définitions des processus de tâches

État	Description
Prêt	La tâche est prête à être traitée après avoir été affectée à un agent.
Affecté	La tâche est affectée à un agent.
En cours de résolution	L'agent affecté travaille actuellement sur la tâche.
Terminé	La tâche est terminée.
Annulé	La tâche a été annulée.

NIST prend en charge les deux modèles suivants :

- **NIST Stateful**

  Cette définition de processus permet aux analystes de passer d'un état à un autre dans un ordre séquentiel sans ignorer aucune étape. Par exemple, si l'analyste commence avec l'état **Brouillon** , l'ordre séquentiel de cette définition de processus est **Brouillon**>**Analyse**>**Contain**>**Eradicate**>**Recover**. Ainsi, la définition du processus avec état NIST est unidirectionnelle et permet aux analystes de progresser uniquement vers les états prospectifs.

  Autre exemple, si l'analyste commence par l'état Analyse, l'ordre séquentiel de cette définition de processus est **Analyse**>**Contenir**>**Éradiquer**>**Récupérer**.

- **NIST Open**

  Cette définition de processus permet aux analystes de passer d'un état à un autre, en avant ou en arrière. Par exemple, si l'analyste commence par l'état **Analyse** , l'ordre de la définition du processus peut être **Analyse**>**Contenir**>**Éradiquer**>**Récupérer** ou **Analyse**>**Brouillon**. Ainsi, la définition du processus NIST Open est bidirectionnelle et permet aux analystes de passer aux états en avant ou en arrière en fonction de leurs besoins.

Sélection du processus de réponse aux incidents de sécurité

Réponse aux incidents de sécurité La sélection de processus répertorie les processus avec des états non valides pour les incidents de sécurité et les tâches de réponse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un administrateur peut corriger l'incident ou la tâche à des états valides manuellement ou à l'aide d'un script. Une liste connexe vide (aucun incident ; aucune tâche) indique que chaque tâche active se trouve dans un état valide. Les états disponibles varient en fonction de l'état actuel de l'incident. Pour plus d'informations, consultez Corriger un état d'incident ou de tâche de sécurité non valide avec la définition du processus.

Sélectionner une définition de Réponse aux incidents de sécurité processus

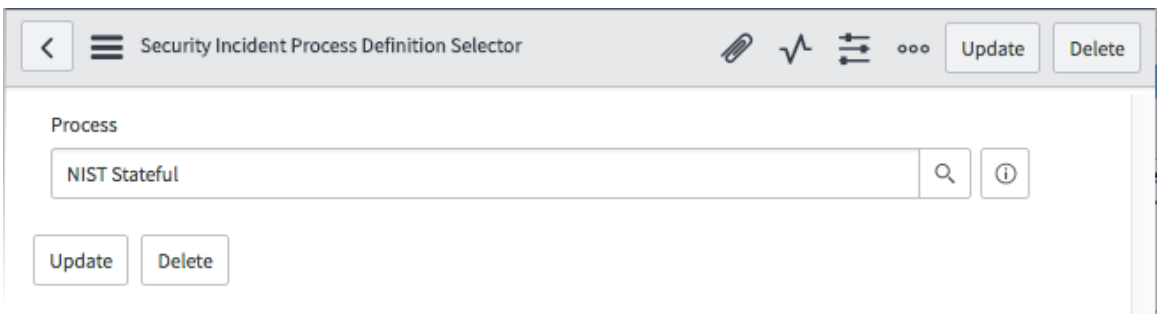
Vous pouvez sélectionner la définition de processus à utiliser pour les états appropriés pour les incidents de sécurité et les tâches de réponse de votre entreprise.

Avant de commencer
Rôle requis : admin et sn_si.admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tout** > **Réponse aux incidents de sécurité** > **Administration** > **Sélection du processus**.
2. Cliquez sur l'icône de recherche pour répertorier les définitions de processus disponibles.



3. Sélectionnez une définition de processus.
4. Cliquez sur **Mettre à jour**.

Créer un include de script de définition de processus personnalisé Réponse aux incidents de sécurité

Créez un script de définition de processus personnalisé pour les états appropriés aux incidents de sécurité et aux tâches de réponse de votre entreprise.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Le sn_si. Le script principal ProcessDefinition contrôle les définitions de processus. **La définition de processus** détermine quelle définition est utilisée (à l'aide **de la sélection de processus**). Il appelle le fichier d'include de script approprié pour déterminer les états initiaux et les transitions pour les incidents de sécurité et les tâches de réponse.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Includes de script**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs comme il convient.

Traduction automatique

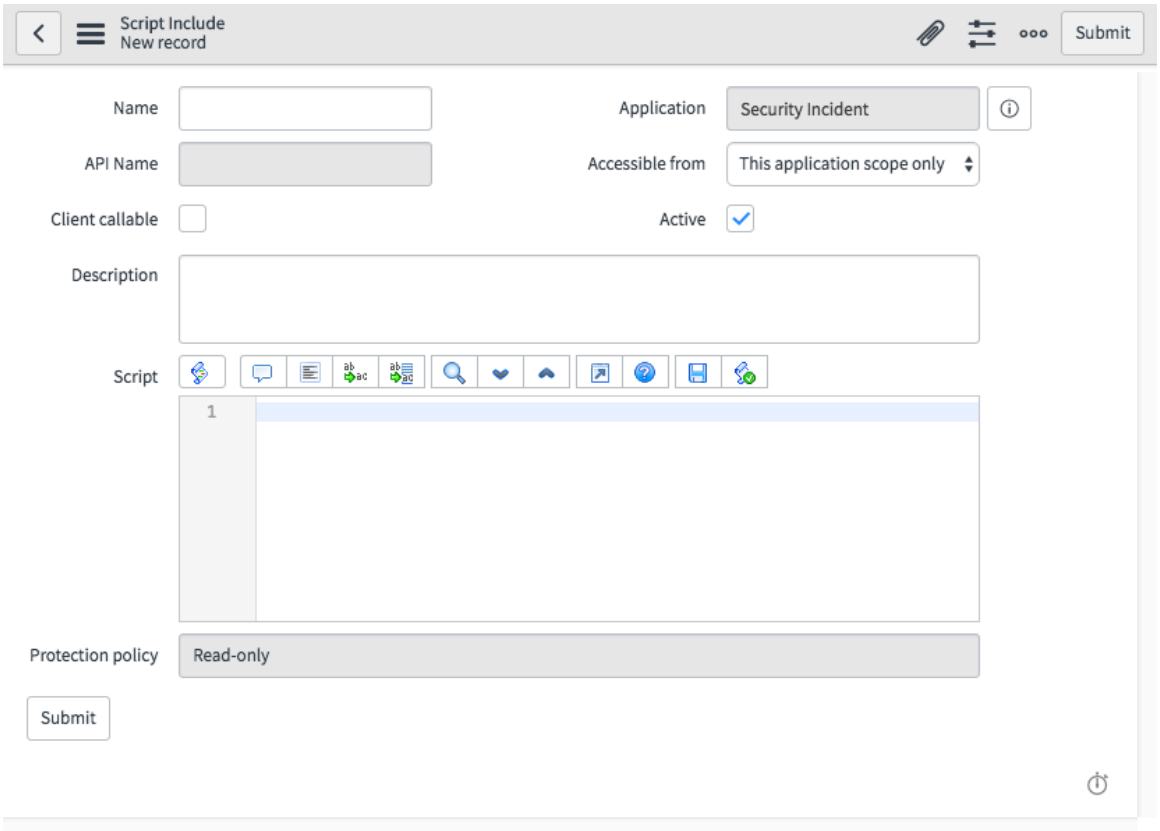
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Création de définitions de processus

Champ	Description
Nom	Nom de cet include de script.
Nom d'API	Créé sur la base du nom de l'include de script.
Client joignable	Met l'include de script à la disposition des scripts clients, des filtres de liste et de rapport, des qualificatifs de référence ou, si spécifié, dans le cadre de l'URL.
Application	Incident de sécurité
Accessible depuis	Choisissez **Ce périmètre de l'application uniquement** .
Actif	Lorsque cette option est cochée, cet include de script peut être sélectionné à partir de la page **Définition du processus** .
Description	Informations utiles sur le script include.
Script	Définit le script côté serveur à exécuter lorsqu'il est appelé à partir d'autres scripts. Le script doit définir une seule classe JavaScript ou une fonction globale. Le nom de la classe ou de la fonction doit correspondre au champ Nom. Pour en savoir plus sur le contenu des scripts, reportez-vous à la section Script include de définition de processus.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Envoyer**.

Information associée

Script include de définition de processus

Script include de définition de processus

Le script include de définition de processus fournit des méthodes pour définir une définition de processus.

Implémentez les constantes, les attributs, les tableaux et les appels de méthode décrits ici pour personnaliser un include de script de définition de processus.

Où l'utiliser ?

Utilisez cet include de script pour créer une définition de processus.

Corps d'include de script

Le corps du script include est composé de trois sections :

- Constantes : définitions de l'état initial
- Incident de sécurité et tâche de réponse : tableaux de définitions de processus
- Appels de méthode : Récupération d'informations

Constantes

Les constantes sont utilisées pour définir les états initiaux des incidents de sécurité et des tâches de réponse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'utilisation de constantes est facultative mais encouragée pour la lisibilité. Par exemple :

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Qui sont ensuite utilisés par les méthodes suivantes :

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

L'ensemble de constantes suivant définit les états des incidents de sécurité et des tâches de réponse.

Chaque tableau contient également la définition des états disponibles lorsque l'incident ou la tâche se trouve dans un état spécifique.

Par exemple :

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

L'exemple est un tableau d'objets. Chaque objet définit un état et des états de transition possibles.

L'ordre de l'objet de l'état détermine l'ordre souhaité pour le flux.

Lorsque la tâche est à l'état « Brouillon » (valeur 1), les états possibles sont : 1 (Brouillon, qui n'est pas un changement) et 10 (Prêt, l'étape suivante du processus).

Il n'y a pas de limite au nombre de transitions en dehors d'un état. Les états « Fermé terminé » et « Annulé » sont des états finaux et n'ont donc aucune transition d'état possible.

L'ordre des attributs dans l'objet n'a pas d'importance. Si cela rend la définition plus claire, mettez l'étiquette en premier.

Attributs

Les attributs requis dans un objet de définition d'état sont les suivants :

- state : valeur numérique de l'état
- Étiquette : texte lisible par l'homme associé à l'état
- Choix : tableau de valeurs d'état vers lesquelles l'état peut effectuer la transition (détermine le contenu de la liste déroulante d'état)

Les attributs facultatifs sont les suivants :

- obligatoire : liste des ID de champs qui deviennent obligatoires dans cet état
- readonly : liste des ID de champs qui passent en lecture seule dans cet état

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- visible : liste des ID de champs qui deviennent visibles dans cet état
- notmandatory : liste des ID de champs qui deviennent non obligatoires dans cet état
- notvisible : liste des ID de champs qui ne seraient plus visibles dans cet état

Remarque :

Si des attributs facultatifs sont utilisés, il est de la responsabilité de l'auteur de s'assurer que les champs sont rendus visibles/invisibles, obligatoires/non obligatoires, visibles/masqués ou en lecture seule de manière appropriée entre les états.

Par exemple, le masquage d'un champ dans un état ne le rend pas visible dans un autre état ultérieurement, sauf si l'attribut « visible » est utilisé.

Tableaux de définitions de flux de processus

Pour définir les informations affichées dans le formateur de flux de processus (la barre en haut des formulaires Incident de sécurité et Tâche de réponse), le système a besoin d'informations sur ce qu'il faut afficher pour chaque état.

Par exemple :

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ",
 description:"<p>Security Incident Response Task is in draft</p>"},
 {label:"Ready", condition:"state=10^EQ", description:"<p>Security
 Incident Response Task is ready to be assigned</p>"},
 {label:"Assigned", condition:"state=16^EQ", description:"<p>Security
 Incident Response Task is assigned</p>"},
 {label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work
 has started on this Security Incident Response Task</p>"},
 {label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ",
 description:"<p>Security Incident Response Task is complete</p>"},
],
```

Le tableau TASK_PF est une collection d'étiquettes, de conditions et de descriptions utilisées pour déterminer le texte affiché dans la barre du formateur de processus (y compris l'ordre et l'activité).

Dans l'exemple, le texte « Prêt » est le deuxième élément affiché. Il est mis en surbrillance lorsque la tâche satisfait à la condition 'state=10^EQ'.

Lorsque le pointeur pointe sur le texte, la description « La tâche Réponse aux incidents de sécurité est prête à être affectée » s'affiche.

Remarque :

Les états peuvent être combinés en un seul état du formateur.

Dans l'exemple, les états « Fermé terminé » et « Annulé » s'affichent tous deux comme « Fermé » dans la barre supérieure.

Appels de méthode

Les méthodes suivantes doivent être présentes dans l'include de script, car elles sont utilisées par sn_si. Définition du processus :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type de retour	Résumé de la méthode	Description
Chaîne	getInitialIncidentState : function()	renvoyer la valeur numérique de l'état d'incident initial
Chaîne	getInitialTaskState : fonction() :	renvoyer la valeur numérique de l'état de la tâche initiale
Tableau de chaîne	getIncidentStates : function() :	renvoyer le tableau de l'état de l'incident
Tableau de chaîne	getTaskStates : fonction() :	renvoyer le tableau de l'état de la tâche
Tableau d'objets	getIncidentProcessFlows : function() :	Renvoyer le tableau de définition de flux de processus d'incident
Tableau d'objets	getTaskProcessFlows : function() :	Renvoyer le tableau de définition du flux de processus de tâche

L'ensemble suivant de méthodes est appelé chaque fois qu'un incident ou une tâche est mis à jour et permet d'entreprendre des actions sur des transitions de changement spécifiques.

Type de retour	Résumé de la méthode	Description
nul	performIncidentStateChange : fonction (actuelle, précédente)	Dans les exemples, cette méthode est utilisée pour définir des valeurs liées à SM et s'assurer qu'un incident sort de l'état « Brouillon » une fois qu'une personne lui est affectée.
nul	performTaskStateChange : fonction (actuelle, précédente)	Dans l'exemple, cette méthode est utilisée pour mettre à jour les horodatages (lors de l'affectation et de la fermeture) et faire passer la tâche de « Prêt » à « Affecté » une fois le champ assigned_to renseigné.

Les mêmes actions effectuées par ces deux méthodes peuvent être accomplies à l'aide d'une règle métier. En les définissant dans l'include de script, il est plus facile de changer les définitions de processus.

Corriger un état d'incident ou de tâche de sécurité non valide avec la définition du processus

Un administrateur peut corriger l'incident ou la tâche de sécurité sur des états valides, manuellement ou à l'aide d'un script. Les états disponibles varient en fonction de l'état actuel de l'incident.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Une fois que vous avez changé de définition de processus, il est possible que la nouvelle définition ne prenne pas en charge certains des anciens états. Pour corriger les états orphelins de l'incident ou de la tâche, vous pouvez modifier votre définition de processus, modifier votre script include ou ouvrir manuellement chaque incident ou tâche pour mettre à jour l'état. Généralement, la mise à jour de l'état (qui peut être effectuée en masse) est la solution la plus simple.

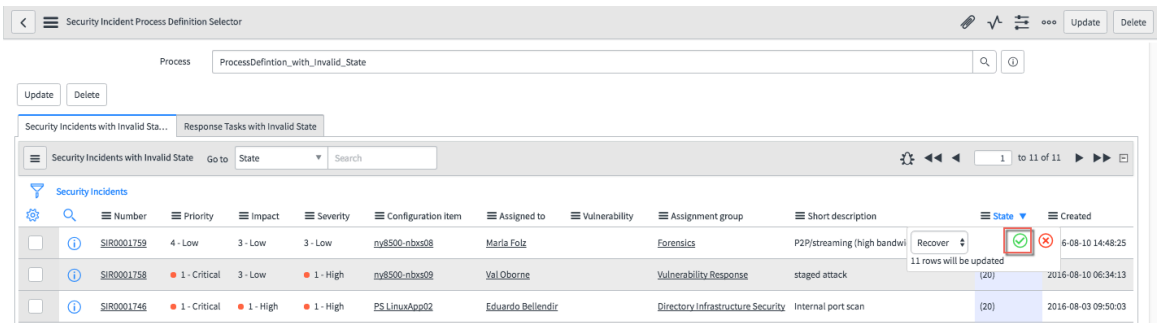
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour modifier les états en bloc, procédez comme suit :

Procédure

1. Accédez à la **Tout** > **Sélection du processus**.
2. Mettez en surbrillance le champ **État** des incidents ou des tâches que vous souhaitez modifier.
3. Double-cliquez sur le champ **État** dans le premier enregistrement, sélectionnez le nouvel **état**, puis cliquez sur la coche verte ( ) pour terminer la modification.



4. Cliquez sur **Mettre à jour**.

Créer un groupe d'incidents de sécurité

Définissez un groupe d'incidents de sécurité et affectez-lui les rôles et les utilisateurs appropriés.

Avant de commencer

Rôles requis :

- Si vous disposez du rôle user_admin, vous pouvez créer des groupes d'affectation d'incident de sécurité.
- Si vous disposez du rôle sn_si.admin, vous pouvez créer et modifier des groupes d'affectation d'incident de sécurité.

Pourquoi et quand exécuter cette tâche

Les utilisateurs d'un groupe héritent les rôles du groupe. Il n'est donc pas nécessaire d'affecter les rôles à chaque utilisateur séparément.
Il est judicieux de créer autant de groupes que nécessaire dans votre organisation. Il est également recommandé de créer un groupe pour les administrateurs et de n'affecter le rôle administrateur qu'à ce groupe.

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Groupes** ou **Incident de sécurité** > **Configuration** > **Groupes**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Remarque :

Pour plus d'informations, consultez Créer un groupe d'utilisateurs .

4. Assurez-vous de sélectionner le type **d'incident de sécurité** pour ce groupe.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Si le champ **Type** n'est pas visible, configurez le formulaire pour l'ajouter.

b. Cliquez sur l'icône de verrouillage à côté du champ **Type**.

c. Cliquez sur l'icône de recherche de référence ()

d. Recherchez et sélectionnez le type **d'incident de sécurité** .

5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
6. Dans la liste connexe **Rôles** , ajoutez les rôles que chaque membre de ce groupe reçoit. Par exemple, si vous créez un groupe pour Réponse aux incidents de sécurité les membres de l'équipe, ajoutez sn_si.analyst. Si vous créez un groupe pour Réponse aux incidents de sécurité les administrateurs, ajoutez sn_si.admin.
7. Dans la liste connexe **Membres du groupe** , ajoutez des utilisateurs à ce groupe.
8. Cliquez sur **Mettre à jour**.

Créer un groupe de calculateurs d'incident de sécurité

Les groupes de calculateurs d'incident de sécurité sont utilisés pour regrouper les calculateurs.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Configuration** > **Groupes de calculateurs d'incidents de sécurité**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom du calculateur d'incident de sécurité.
Application	L'application qui contient l'enregistrement.
Ordre	Ordre dans lequel le calculateur d'incident de sécurité est exécuté Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Description	Description de ce groupe de calculateurs.
Créé par	Entrer le nom de l'utilisateur qui a créé

4. Cliquez sur **Envoyer**.

Créer un calculateur d'incident de sécurité

Les calculateurs d'incident de sécurité vous permettent de calculer la gravité d'un incident de sécurité en fonction de formules prédéfinies. Vous pouvez définir vos propres calculateurs d'incident de sécurité, selon les besoins.

Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Configuration** > **Groupes de calculateurs d'incidents de sécurité**.
2. Cliquez sur le nom du groupe pour lequel vous souhaitez créer un calculateur, ou vous pouvez créer un groupe de calculateurs.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom du calculateur d'incident de sécurité.
Groupe de calculateurs	Nom du groupe auquel ce calculateur appartient. **Remarque :** La création ou la modification du groupe de calculateurs devient disponible une fois que vous avez entré un **nom** et une **table**.
Table	Sélectionnez la table à utiliser pour ce calculateur. Lorsque vous ajoutez des calculateurs à des tables autres que Vulnérabilité [sn_vul_vulnerability] et Élément vulnérable [sn_vul_vulnerable_item], vous devez ajouter des règles métier et des actions d'interface utilisateur à ces tables. Pour voir des exemples : ◦ Accédez à la **Définition du système** > **Règles métier**et localisez la règle métier **Calculer la gravité** dans la table Élément vulnérable [sn_vul_vulnerable_item]. ◦ Accédez à la **Interface utilisateur du système** > **Actions d'interface utilisateur**et localisez l'action d'interface utilisateur **Calculer la gravité** dans la table Élément vulnérable [sn_vul_vulnerable_item]. En outre, le rôle d'administrateur de vulnérabilité doit disposer de toutes les options de lecture, d'écriture (ou save_as_template) sur n'importe quelle table utilisée par un calculateur pour voir correctement les valeurs à appliquer au modèle.
Application	Application incluse dans le périmètre à laquelle le calculateur appartient.
Ordre	Ordre dans lequel le calculateur d'incident de sécurité est exécuté. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Actif	Allumez ou éteignez la calculatrice.
Description	Description de ce calculateur.

5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**. Les onglets **Conditions** et **Valeurs à appliquer s'affichent** .
6. Renseignez les champs de l'onglet **Conditions** comme il convient.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utiliser un groupe de filtres	Cochez cette case pour utiliser un groupe de filtres prédéfini ou créez un nouveau groupe de filtres pour définir les critères du calculateur.
Groupe de filtres	Sélectionnez le groupe de filtres à utiliser pour définir un calculateur. Ce champ s'affiche uniquement si vous avez coché la case **Utiliser des groupes de filtres** .
Utiliser une condition avancée	Cochez cette case pour indiquer qu'une condition de script est utilisée pour déterminer quand ce calculateur est appliqué. Lorsque vous cochez la case, un champ de scripting de **condition avancée** s'affiche. Si vous avez coché la case **Utiliser un groupe de filtres** , ce champ est masqué. **Remarque :** Avant de définir des conditions avancées et d'écrire des scripts pour déterminer quand les calculateurs d'incident de sécurité sont appliqués, revenez à la liste des calculateurs d'incident de sécurité. Explorez les enregistrements de calculateur fournis avec le système de base.
Condition	Définit les conditions de filtre de base pour déterminer si le calculateur est utilisé. Si vous avez coché les cases **Utiliser le groupe de filtres** ou Utiliser des **conditions avancées** , ce champ est masqué.

7. Cliquez sur **l'onglet Valeurs à appliquer** et renseignez les champs du formulaire comme il convient.
   Vous avez le choix de créer un script pour définir les valeurs à appliquer au calcul ou de définir un modèle basé sur les champs de la table sélectionnée.

Champ	Description
Utiliser des valeurs de script	Cochez cette case pour définir des valeurs de champ avec un script.
Valeurs de script	Définit les valeurs auxquelles appliquer les calculs. Ce champ s'affiche uniquement si vous avez coché la case **Utiliser les valeurs de script.**
Modèle	Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**. Sélectionnez les champs et les valeurs que vous souhaitez utiliser pour le calculateur.

8. Lorsque vous avez rempli toutes les entrées, cliquez sur **Soumettre**.

Comprendre les calculateurs d'incidents de sécurité

Les calculateurs d'incident de sécurité sont utilisés pour mettre à jour les valeurs d'enregistrement lorsque les conditions prédéfinies sont remplies. Les calculateurs sont

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

regroupés en fonction des critères utilisés pour déterminer comment les enregistrements sont mis à jour.

Le Réponse aux incidents de sécurité système de base inclut les groupes de calculateurs d'incident de sécurité et les calculateurs suivants. Au sein de chaque groupe, c'est le premier calculateur qui correspond aux conditions qui est exécuté.

Calculateurs d'incident de sécurité dans le système de base

Nom du groupe du calculateur d'incident de sécurité	Calculatrices incluses dans le groupe	Description
Impact sur l'entreprise	Regrouper à partir des calculateurs de gravité	Ce calculateur délègue au calculateur de criticité de sécurité qui détermine la criticité en pondérant les valeurs d'autres champs.
Gravité	Impact sur l'entreprise	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un créateur de conditions simple.
	Service critique affecté	Ce calculateur de gravité définit ses critères de sélection à l'aide d'une condition avancée. Si l'élément de configuration de l'incident de sécurité est associé à un service aux entreprises hautement critique, les champs **Score de risque**, **Impact sur l'entreprise** et **Priorité** sont élevés comme défini par le calculateur.
	Changements de services critiques	Ce calculateur de gravité définit ses critères de sélection à l'aide d'une condition avancée. Si l'incident de sécurité répond aux conditions, un script s'exécute pour définir les niveaux auxquels les champs sont élevés. Si l'élément de configuration de l'incident de sécurité est associé à un service aux entreprises très critique ou quelque peu critique, les champs **Score de risque**, **Impact sur l'entreprise** et **Priorité** sont élevés tels que définis par le calculateur.
	Vecteurs d'attaques multiples	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un créateur de conditions simple. Si l'élément de configuration de l'incident de sécurité est associé

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculateurs d'incident de sécurité dans le système de base (suite)

Nom du groupe du calculateur d'incident de sécurité	Calculatrices incluses dans le groupe	Description
		à des vecteurs d'attaque par le Web, la messagerie électronique et l'emprunt d'identité, les champs **Score de risque**, **Impact sur l'entreprise** et **Priorité** sont élevés comme défini par le calculateur.
	Définir la priorité avec la catégorie et les services	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un générateur de conditions avancé. La priorité de l'incident de sécurité est définie sur **1 - Critique** lorsque les conditions suivantes sont remplies : • L'incident de sécurité a des services affectés associés et l'un d'entre eux est critique. • La catégorie d'incident de sécurité est l'une des suivantes : ◦ Déni de service ◦ Harponnage ◦ Activité du code malveillant **Remarque :** Ce calculateur est disponible dans le système de base avec le niveau tarifaire Opération de sécurité de démarrage.
	Définir la priorité avec les observables	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un générateur de conditions avancé. La priorité de l'incident de sécurité est définie sur**1 - Critique** lorsque les conditions suivantes sont remplies : • L'incident de sécurité a des services affectés associés et l'un d'entre eux est critique. • La catégorie d'incident de sécurité est l'une des suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculateurs d'incident de sécurité dans le système de base (suite)

Nom du groupe du calculateur d'incident de sécurité	Calculatrices incluses dans le groupe	Description
		◦ Déni de service ◦ Harponnage ◦ Activité du code malveillant • L'un des observables ou indicateurs associés a un nombre de perceptions qui dépasse deux observations avec des indicateurs actifs (c'est-à-dire que les observables ou les indicateurs sont confirmés comme étant mauvais à partir de plusieurs sources). **Remarque :** Ce calculateur est disponible dans le système de base lorsque vous disposez du niveau tarifaire Opération de sécurité avancée et que vous activez le module d'extension Flux de menaces.
Criticité de l'utilisateur	Obtenir la criticité de l'utilisateur	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un créateur de conditions simple. Ce calculateur de gravité entraîne le passage de la criticité opérationnelle de l'utilisateur à **1 - Critique** lorsque le champ **Département** est remplacé par **Finances**.
	Obtenir la criticité du groupe d'utilisateurs	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un générateur de conditions avancé. Ce calculateur de gravité fournit un exemple de calculateur qui s'exécute sur les données d'une liste connexe.

Calculateurs de gravité

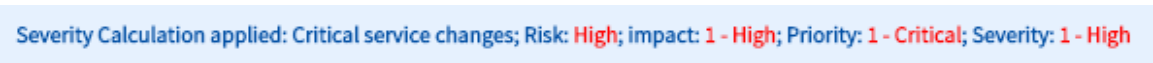
Lorsque vous créez un incident de sécurité, les champs **Score de risque**, **Impact sur l'entreprise** et **Priorité** contiennent des valeurs par défaut. Lorsque vous enregistrez l'incident, une règle métier valide automatiquement les informations contenues dans l'incident de sécurité par rapport aux conditions définies dans chacun de vos calculateurs de gravité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

actifs. Ils sont validés un calculateur de sécurité à la fois, dans l'ordre défini par le champ **Ordre** de chaque calculateur. Si les informations de l'incident de sécurité correspondent aux conditions définies dans l'un des calculateurs, les valeurs des champs de gravité sont mises à jour en conséquence des règles définies dans le calculateur.

Par exemple, supposons que vous créez un incident de sécurité pour un CI affecté et que le CI est hautement critique. Lorsque l'incident de sécurité est enregistré, les informations de CI sont comparées aux conditions définies dans les calculateurs de gravité. Lorsque l'incident de sécurité est validé par rapport au calculateur de gravité **affectée par le service critique** , les champs de gravité sont automatiquement mis à jour et un message similaire au suivant apparaît en haut de l'incident de sécurité.



Vous pouvez utiliser ces calculateurs de gravité tels quels ou vous pouvez les modifier pour mieux répondre aux besoins de votre entreprise. Par exemple, si vous souhaitez identifier les menaces Web et e-mail spécifiques à la business unit Finance, vous pouvez modifier les conditions du calculateur de **vecteurs d'attaques multiples** :

- [Vecteur d'attaque] [contient] [Web]
- [Vecteur d'attaque] [contient] [Courriel]
- [Unité business] [contient] [Finances]

Vous pouvez également mettre à jour les valeurs de gravité d'un incident de sécurité existant à tout moment en ouvrant l'enregistrement et en cliquant sur le lien connexe **Calculer la gravité** .

Calculateurs de score de risque d'incident de sécurité

Les calculateurs **Définir la priorité avec la catégorie et les services** et **Définir la priorité avec les observables** sont utilisés pour calculer un score de risque pour un incident de sécurité.

Calculateurs de criticité de l'utilisateur

Les deux calculateurs du groupe de **criticité de l'utilisateur** (**Obtenir la criticité de l'utilisateur** et **Obtenir la criticité du groupe d'utilisateurs**) fournissent des exemples de la façon dont vous pouvez piloter la criticité en fonction de critères définis dans un enregistrement utilisateur ou en fonction du groupe auquel un utilisateur appartient.

Ils peuvent être modifiés selon les besoins, ou de nouveaux calculateurs de criticité utilisateur peuvent être créés.

Le calculateur **Obtenir la criticité de l'utilisateur** entraîne le passage de la criticité opérationnelle de l'utilisateur à **1 - Critique** lorsque le champ **Département** est remplacé par **Finances**.

Le calculateur de **criticité Obtenir un groupe d'utilisateurs** entraîne le passage de la criticité opérationnelle de l'utilisateur à **1 - Critique** lorsque l'utilisateur est ajouté au groupe **de base de données** .

Remarque : Obtenir la criticité du groupe d'utilisateurs est un exemple de calculateur qui s'exécute sur les données d'une liste connexe. Si vous souhaitez ajouter d'autres groupes pour initier un changement de criticité, ajoutez une liste de sys_ids de groupe séparés par des virgules dans la première ligne du script. Exemple : `var CRITICAL_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id].`

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculs du score de risque d'incident de sécurité

Le score de risque est calculé comme une moyenne arithmétique qui représente le risque en fonction de la priorité d'un incident de sécurité, du type d'incident de sécurité (déni de service, harponnage ou activité de code malveillant) et du nombre de sources qui ont déclenché un score d'échec de réputation sur un indicateur.

Le score de risque permet aux analystes de hiérarchiser le travail lié aux incidents de sécurité.

Important : Si vous souhaitez utiliser le nouveau calculateur de score de risque, reportez-vous à Définir les nouvelles règles du calculateur de score de risque.

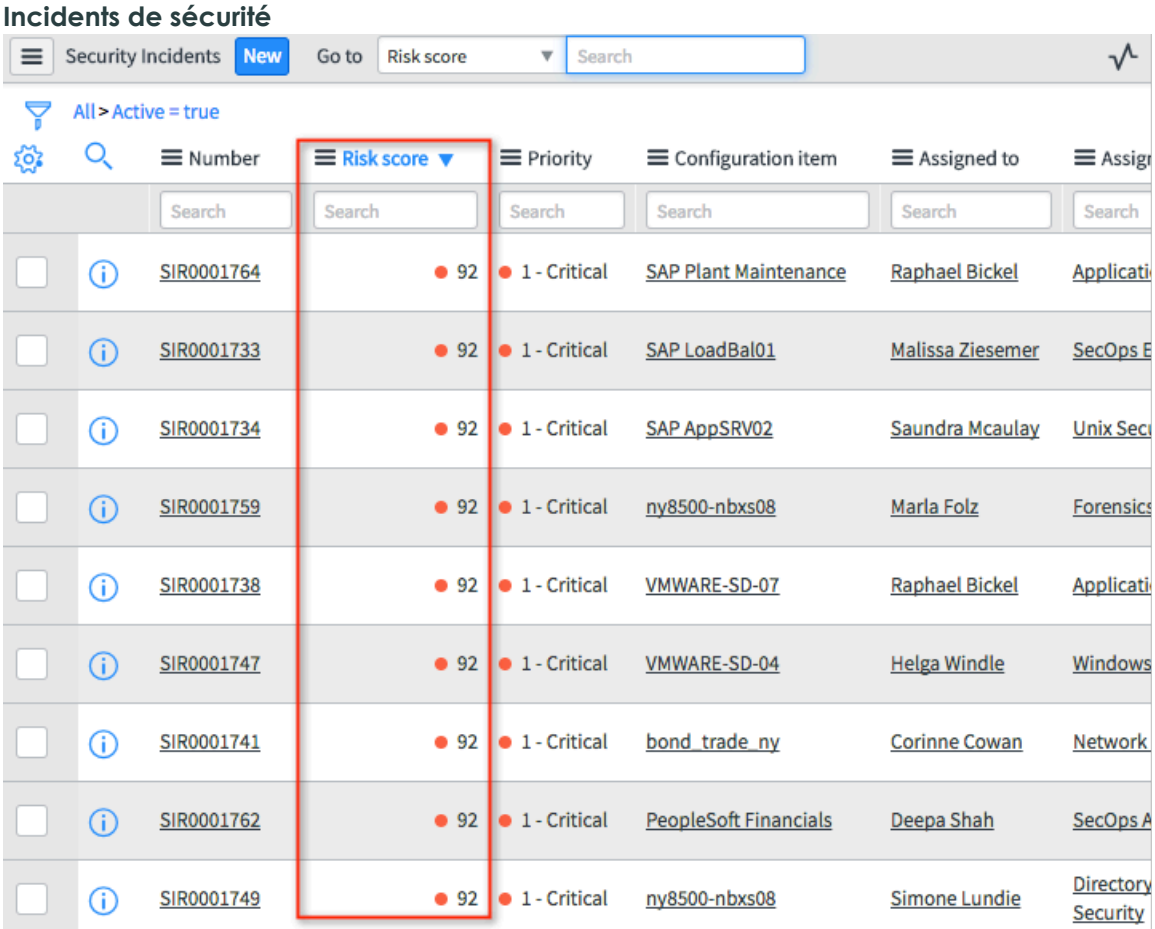
Les calculateurs d'incident de sécurité**Définir la priorité avec la catégorie et les services** et **Définir la priorité avec les observables** sont utilisés pour calculer le score de risque d'un incident de sécurité. En outre, les règles métier suivantes déclenchent le calcul automatique des scores de risque :

- Calculer la gravité
- Mettre à jour le score de risque
- Mettre à jour le score de risque SI

Remarque : Le calculateur de risque disponible dans le système de base dépend de votre niveau tarifaire Security Operations.

Lorsque vous examinez une liste d'incidents de sécurité dans le système de base, remarquez la colonne **Score de risque** .

Incidents de sécurité

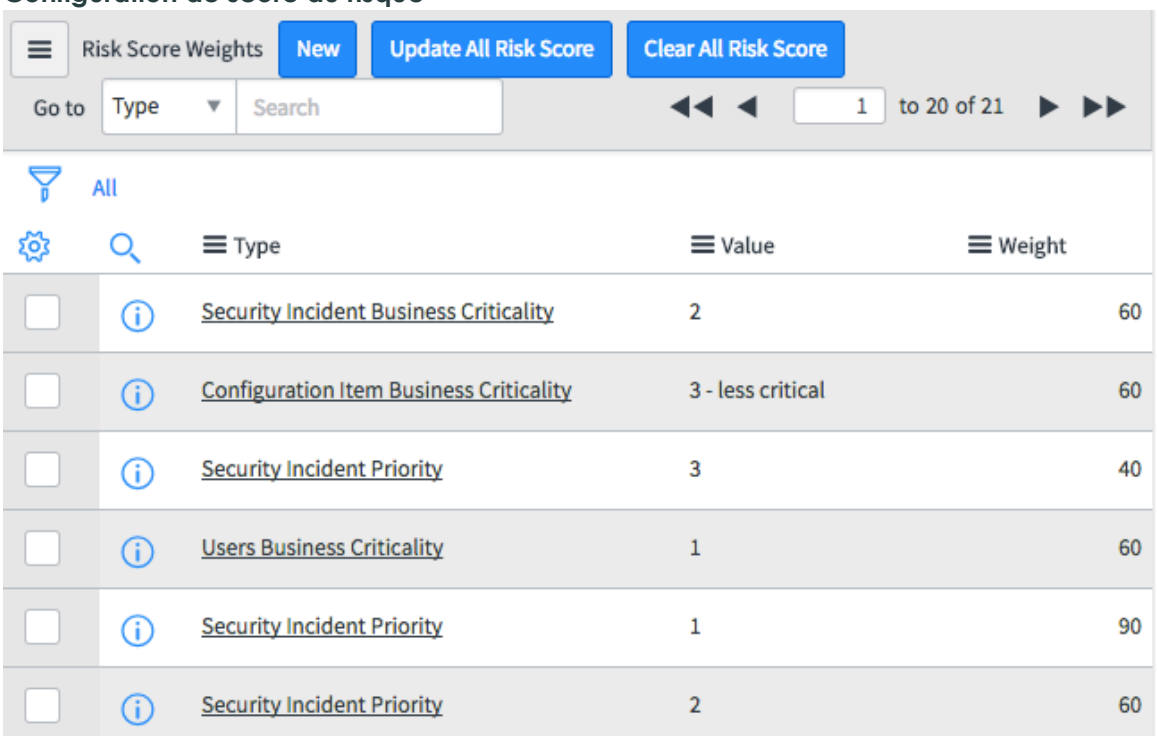


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le score de risque est calculé à l'aide des pondérations définies dans la **configuration du score de risque**.

Configuration de score du risque



Par exemple, si **l'impact sur l'entreprise** d'un incident de sécurité est défini sur **2-Élevé** et la **priorité** sur **3-Modérée**, les pondérations respectives de la table des poids de score de risque sont recherchées et calculées comme suit :

Impact opérationnel d'un incident de sécurité avec une valeur de 2 = une pondération de 60.

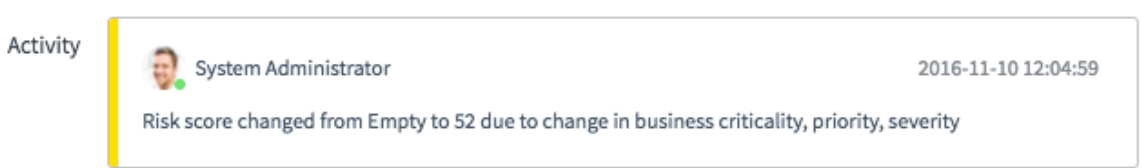
Priorité de l'incident de sécurité avec une valeur de 3 = un poids de 40.

(60 + 40)/2 = un score de risque de 50.

La position de l'incident de sécurité dans la liste des incidents de sécurité est ensuite réorganisée en fonction de son score de risque mis à jour.

Si, dans l'exemple ci-dessus, **l'impact sur l'entreprise** ou la **priorité** de l'incident de sécurité sont modifiés, le score de risque est recalculé et les modifications sont reflétées dans les notes de travail.

Notes de travail



Les notes de travail sont mises à jour lorsque les champs suivants sont modifiés (ce qui entraîne la mise à jour du score de risque) :

- **Impact sur l'activité** du formulaire d'incident de sécurité
- **Priorité** sur le formulaire d'incident de sécurité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Gravité** sur le formulaire d'incident de sécurité (masqué par défaut)
- **Impact sur l'entreprise** sur la liste connexe **Utilisateurs affectés**
- **Impact sur l'activité** sur la liste connexe **Services affectés**
- **Impact sur l'entreprise** sur les vulnérabilités de la liste connexe **des éléments vulnérables**

En outre, les notes de travail sont mises à jour dans les situations suivantes :

- Lorsqu'une association entre les utilisateurs affectés et un incident de sécurité est créée ou modifiée
- Lorsqu'une association entre les services affectés et un incident de sécurité est créée ou modifiée
- Lorsqu'une association entre des éléments vulnérables et un incident de sécurité est créée ou modifiée

Les notes de travail sont également mises à jour chaque fois que vous cliquez sur **Mettre à jour tous les scores de risque** et **Effacer tous les scores de risque** sur le formulaire de pondération des scores de risque .

Gérer les pondérations du score de risque

Les poids de score de risque utilisés pour calculer les scores de risque dans les incidents de sécurité peuvent être supprimés ou mis à jour individuellement. Ils peuvent également être supprimés ou mis à jour pour tous les incidents de sécurité. La possibilité de les supprimer des incidents de sécurité est utile lors du changement des valeurs de poids.

Avant de commencer

Rôle requis : sn_sec_cmn.admin

Remarque : Les utilisateurs disposant du rôle sn_si.read peuvent afficher la configuration du score de risque dans Réponse aux incidents de sécurité.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Configuration** > **Configuration du score du risque**.

   Remarque : Les utilisateurs disposant du rôle sn_si.read peuvent afficher la configuration du score de risque en accédant à **Incident de sécurité** > **Alertes et événements** > **Configuration du score des risques**.

2. Pour ajouter un nouveau poids de score de risque, cliquez sur **Nouveau** et entrez des informations dans les champs.

Champ	Description
Type	Sélectionnez le type de score de risque que vous définissez.
Valeur	Spécifiez la valeur associée au type sélectionné. Si plusieurs valeurs sont disponibles pour le type, vous pouvez définir plusieurs enregistrements de poids de score de risque. Exemple : priorité de l'incident de sécurité avec une valeur de 1, priorité de l'incident de sécurité avec une valeur de 2, etc.
Poids	Poids associé à la paire type/valeur sélectionnée. Les entrées valides sont comprises entre 0 et 100, 0 étant le poids le plus bas et 100 le poids le plus élevé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Envoyer**.
4. Effectuez l'une de ces étapes, au besoin.
   - Pour effacer un enregistrement de poids de score de risque, ouvrez-le à partir de la liste et cliquez sur **Supprimer**.
   - Pour effacer tous les enregistrements de poids de score de risque, cliquez sur **Effacer tous les scores de risque**.
   - Pour mettre à jour tous les enregistrements de poids de score de risque, cliquez sur **Mettre à jour tous les scores de risque**.

Créer un Réponse aux incidents de sécurité SLA

Vous pouvez définir un accord sur les niveaux de service (SLA) pour Réponse aux incidents de sécurité.

Avant de commencer
Rôle requis : sn_si.admin

Procédure
1. Accédez à la **Tout** > **Incident de sécurité** > **Configuration** > **SLA**.
2. Cliquez sur **Nouveau**.
   Pour obtenir une description des champs et des instructions détaillées, reportez-vous à la section Créer une définition de SLA .

Réparer les SLA d'incidents de sécurité

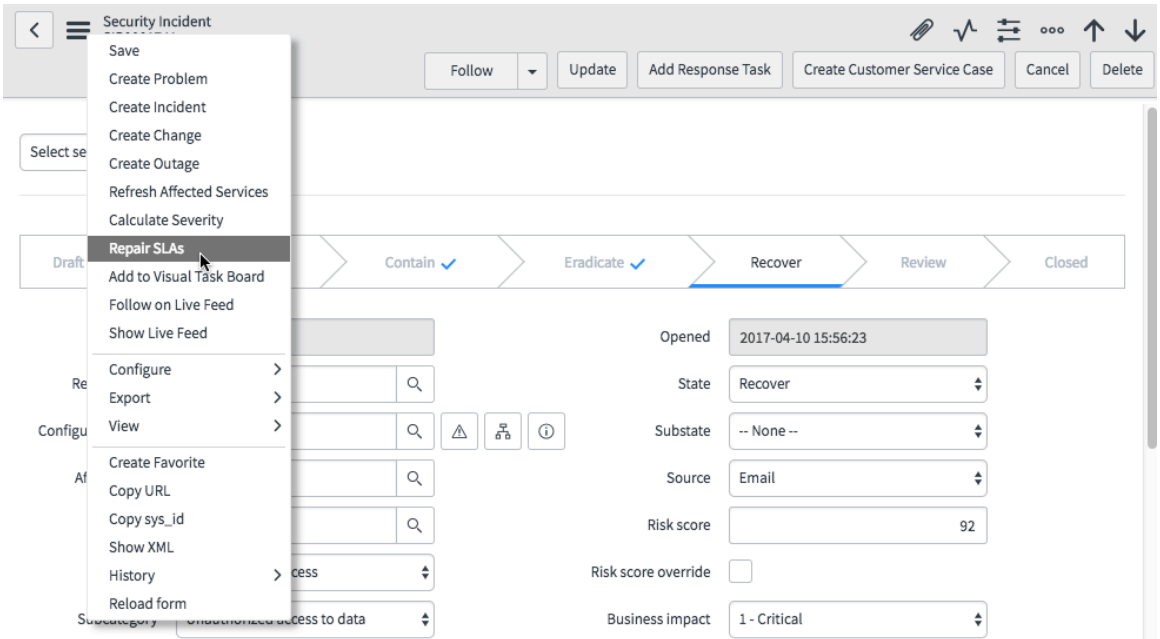
Vous pouvez réparer les enregistrements SLA pour vous assurer que les informations de calendrier et de durée des SLA sont exactes.

Avant de commencer
Rôle requis : sn_si.basic

Procédure
1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez réparer les SLA.
2. Cliquez sur le menu contextuel de l'en-tête du formulaire et sélectionnez **Réparer les SLA** :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur **OK** dans la zone de confirmation d'avertissement.
   Pour plus d'informations, consultez Réparer les SLA .

Créer un Runbook Security Incident Response

Un runbook est une association entre un article de la base de connaissances publié et une tâche spécifique. Pendant que vous effectuez la tâche, un article de la base de connaissances dans le Runbook s'ouvre automatiquement, fournissant des informations pertinentes pour la tâche.

Avant de commencer

La base de Réponse aux incidents de sécurité connaissances Runbook doit comporter des articles existants. Lorsque vous créez un article de la base de connaissances sur un incident de sécurité, assurez-vous de sélectionner **Runbook de réponse aux incidents de sécurité** dans le champ **de la base de connaissances** . Une fois l'article publié, vous pouvez cliquer sur le bouton **Créer un Runbook** .

Rôle requis : sn.si.knowledge_admin

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser des runbooks pendant les processus de création d'incidents de sécurité ou de tâches de réponse, ou associer les articles de la base de connaissances dans un runbook avec des tâches du playbook.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Runbook manuel** > **Créer un nouveau Runbook**.
2. Renseignez les champs comme il convient.

Champ	Description
Article de la base de connaissances	Sélectionnez un article de la base de connaissances à inclure dans le runbook.
Actif	Cochez la case pour rendre le runbook disponible à partir du **navigateur de filtre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utiliser un groupe de filtres	Cochez cette case pour utiliser un groupe de filtres prédéfini ou créez un nouveau groupe de filtres pour définir les critères du runbook.
Groupe de filtres	Sélectionnez le groupe de filtres à utiliser pour définir un runbook. Ce champ s'affiche uniquement si la case **Utiliser des groupes de filtres** est cochée.
Table	Sélectionnez Incident de sécurité [sn_si_incident] ou Réponse aux incidents de sécurité Tâche [sn_si_task]. Si vous avez coché la case **Utiliser un groupe de filtres** et sélectionné un groupe de filtres, ce champ est par défaut la table associée au groupe de filtres sélectionné.
Condition	Définissez les conditions qui connectent ce runbook à l'incident ou à la tâche. Si vous avez coché la case **Utiliser un groupe de filtres** et sélectionné un groupe de filtres, les champs **Condition** ne s'affichent pas.

3. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**. L'onglet Détails de l'article de la base de connaissances et une série de boutons apparaissent.
4. Pour afficher les détails du runbook, cliquez sur l'onglet Détails de la **base de connaissances** .
5. Pour afficher l'article de la base de connaissances tel qu'il apparaît à l'utilisateur, cliquez sur **Afficher l'article**.
6. À Pour modifier les détails de l'article de la base de connaissances , cliquez sur **Modifier l'article**.

Créer des règles pour valider les attaques de hameçonnage signalées par les utilisateurs

Lorsque vos employés reçoivent des e-mails qui semblent être des attaques d'hameçonnage, ils peuvent vous les signaler à l'aide d'une adresse e-mail d'hameçonnage. L'e-mail suspect est validé à l'aide de règles définies par votre organisation.

Avant de commencer

Avant que les règles de correspondance des e-mails puissent être utilisées pour identifier les attaques de hameçonnage potentielles, définissez une adresse e-mail vers laquelle les e-mails transférés par vos employés seront envoyés pour traitement. Vous disposez des options suivantes pour définir cette adresse e-mail (en supposant que le domaine de messagerie de votre entreprise est acme.com) :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Définissez une adresse e-mail telle que **acme+phishing@service-now.com**. La balise **+hameçonnage** est prise en charge par SMTP pour activer le filtrage et votre instance peut recevoir les e-mails qui lui sont envoyés.
- Définissez une adresse e-mail, telle que **phishing@acme.com** (votre boîte aux lettres Exchange), qui à son tour la transfère à **acme+phishing@service-now.com** (votre boîte aux lettres d'instance définie par une règle de transfert de messagerie).

Rôle requis : sn_sec_cmn.write

Pourquoi et quand exécuter cette tâche

Lorsqu'un employé rencontre un e-mail suspect, il doit le transférer en pièce jointe à votre adresse e-mail d'hameçonnage. Si l'e-mail joint correspond à une règle définissant une menace, un incident de sécurité est créé.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Traitement des e-mails** > **Hameçonnage signalé par un utilisateur**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs nécessaires.

Formulaire Règles de correspondance d'e-mail

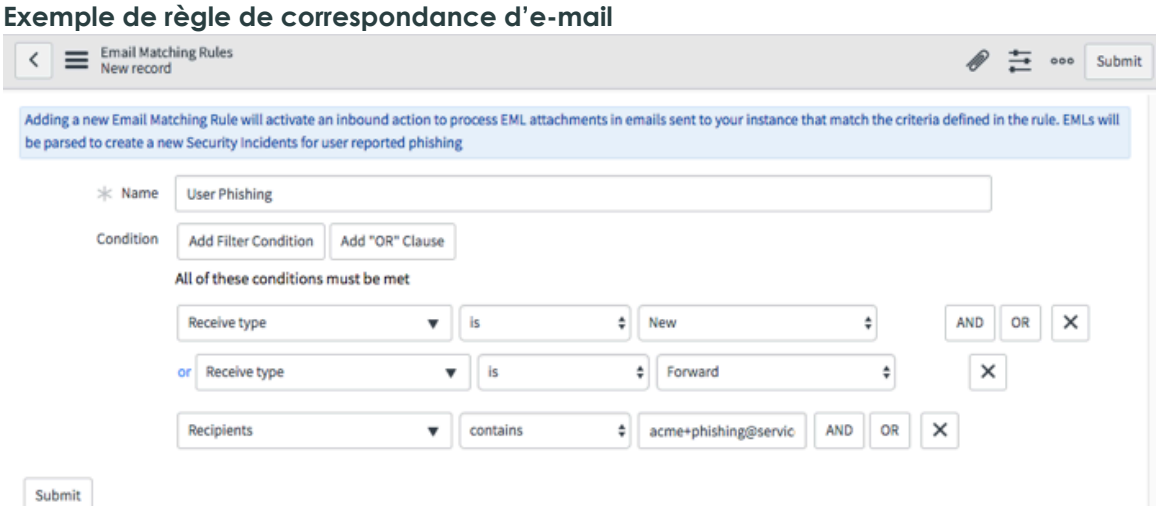
Champ	Description
Nom	Nom de cette règle de correspondance d'e-mail. Par exemple, Hameçonnage signalé par un utilisateur.
Conditions	Utiliser le Générateur de conditions permettant de valider si un e-mail envoyé à l'adresse e-mail d'hameçonnage de votre entreprise est une attaque d'hameçonnage. Reportez-vous à l'exemple suivant.

4. Cliquez sur **Envoyer**.

Example:

Cet exemple montre une règle de correspondance pour le traitement du hameçonnage signalé par les utilisateurs.

Exemple de règle de correspondance d'e-mail



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurez la Security Analyst Workspace.

Configurez l'interface utilisateur de l'enregistrement d'incident dans le Security Analyst Workspace pour spécifier les champs que vous souhaitez afficher.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Spécifiez les champs à afficher dans votre enregistrement d'incident et l'ordre dans lequel les champs doivent apparaître sur le formulaire d'incident de sécurité et le formulaire de tâche de réponse. Vous pouvez également définir une limite sur le nombre de champs que vous souhaitez afficher.

Remarque : Vous pouvez créer des règles pour déterminer quelle vue doit être utilisée pour un formulaire spécifique. Plusieurs vues sont incluses dans le système de base, y compris les vues par défaut et SIR Nouvelle interface utilisateur. Plusieurs règles de vue sont également fournies avec le système de base, y compris la règle de la tâche de réponse Tous les autres. Cette règle applique la vue par défaut sur le formulaire Tâche de réponse lorsque la condition spécifiée dans la règle de vue est remplie. Le Security Analyst Workspace utilise la nouvelle vue d'interface utilisateur SIR. Si les champs de formulaire affichés dans le Security Analyst Workspace ne correspondent pas aux champs de formulaire de l'environnement classique, une règle d'affichage est très probablement appliquée. Pour utiliser la **nouvelle vue d'interface utilisateur SIR** pour le formulaire, vous devez désactiver la règle de vue. Pour plus d'informations, reportez-vous à la section Contrôle lorsque le système affiche une vue .

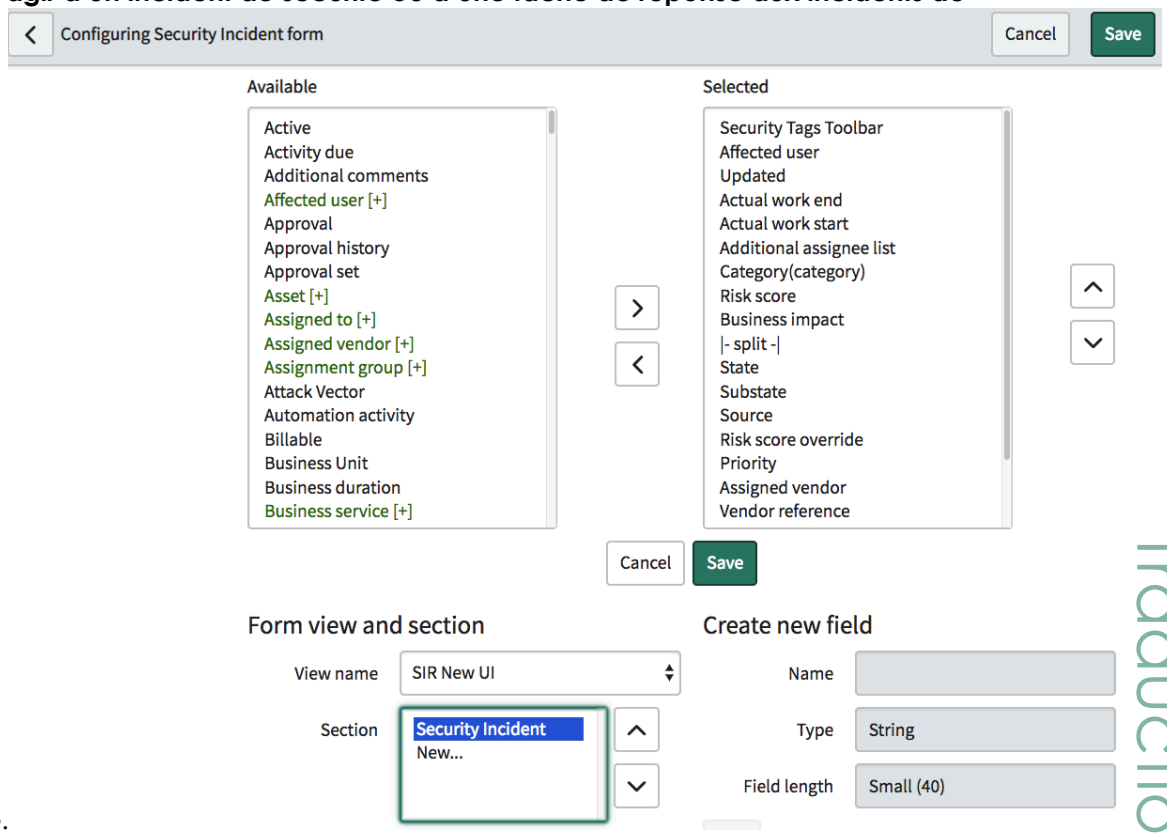
Procédure

1. Accédez à n'importe quelle liste d'incidents de sécurité (par exemple, **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**).
2. Pour ouvrir l'enregistrement d'incident de sécurité, cliquez sur le lien d'un incident de sécurité.
3. Pour accéder à la page du formulaire de configuration de l'incident de sécurité, cliquez sur l'icône du et sélectionnez **Configurer** > **Mise en page**.
4. Dans la liste **Nom de vue**, sélectionnez **Nouvelle interface utilisateur SIR.**
5. Dans le champ **Section** , sélectionnez la section appropriée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il peut **s'agir d'un incident de sécurité** ou **d'une tâche de réponse aux incidents de sécurité**.



6. Sélectionnez les champs et l'ordre dans lequel vous souhaitez qu'ils apparaissent dans la bannière d'incident dans la nouvelle interface utilisateur.
7. Cliquez sur **Enregistrer**.

Remarque :

- Certains champs sont masqués par défaut dans les bannières Incident et Tâche de réponse. Modifiez les champs masqués ou affichés en modifiant les propriétés `sn_app_secops_ui.form.excluded_fields.incident` et `sn_app_secops_ui.form.excluded_fields.response_task`, comme décrit à la rubrique Propriétés de Security Analyst Workspace.
- Spécifiez le nombre de champs qui peuvent être affichés dans les bannières d'incident et de tâche de réponse et sur la première ligne de la bannière d'incident en définissant les propriétés suivantes :
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_app_secops_ui.task_summary.single_summary.limit.response_task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

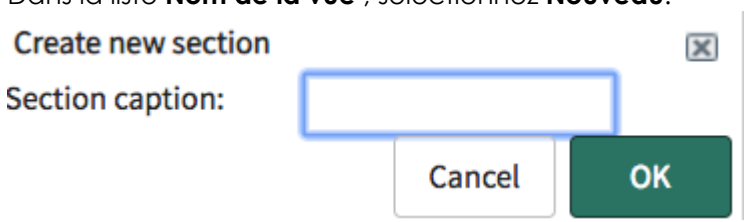
8. Pour configurer les styles des cercles en pointillés qui apparaissent à côté d'une valeur de champ dans l'enregistrement d'incident, par exemple, , accédez à **Interface utilisateur du système** > **Styles de champ** et modifiez ou créez un nouvel enregistrement de style pour le nom de table et de champ spécifique.
   La couleur d'arrière-plan de la propriété dans le champ Style de l'enregistrement de style détermine la couleur du cercle en pointillés.
9. Pour afficher la bannière d'incident mise à jour, cliquez sur **Incidents de sécurité** > **Incidents (nouvelle UI)** pour accéder à l'enregistrement d'incident dans et Security Analyst Workspace actualisez la page pour afficher la bannière d'incident mise à jour.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Pour configurer la bannière Tâche de réponse dans l'enregistrement d'incident, accédez à **Incidents de sécurité** > **Tâches de réponse** > **Afficher toutes les tâches** et répétez les étapes.
11. Si vous créez une table de tâches étendant à partir de la table de base de Tâche de réponse aux incidents de sécurité, vous devez également ajouter la nouvelle vue d'interface utilisateur SIR à la table.

    a. Dans la liste **Nom de la vue** , sélectionnez **Nouveau**.



    b. **Entrez Nouvelle interface utilisateur SIR** (sensible à la casse) dans la fenêtre Créer une nouvelle vue, puis cliquez sur **OK**.

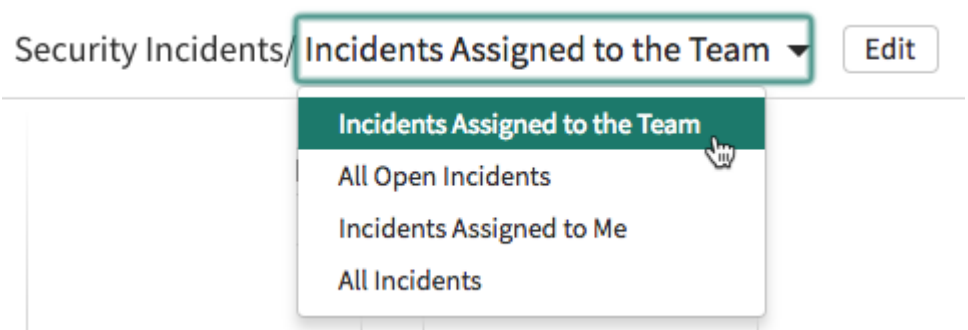
Résultats
Les bannières d'incident de sécurité et de tâche de réponse sont mises à jour dans le Security Analyst Workspace (Gérer les menaces de sécurité à l'aide de l' Security Analyst Workspace).

Configurer des filtres primaires et secondaires pour Security Analyst Workspace

Le Security Analyst Workspace système de base comprend un ensemble de filtres primaires destinés à réduire la liste des incidents de sécurité pour l'analyse (pour les incidents de sécurité qui vous sont affectés, tous les incidents ouverts, entre autres) et un ensemble de filtres rapides (ou secondaires) permettant de réduire encore plus la liste (par nouveaux incidents, incidents ouverts, incidents critiques uniquement, et ainsi de suite).

Avant de commencer
Vous pouvez utiliser l'environnement classique pour définir des filtres primaires et secondaires supplémentaires.

Lorsque vous définissez les filtres à utiliser dans le Security Analyst Workspace, vous pouvez affecter des balises pour indiquer si elles peuvent être utilisées comme filtres primaires ou secondaires. Les filtres primaires sont affichés en haut de la liste des incidents de sécurité.



Cliquez sur **Modifier** à côté de l'option Filtres rapides pour sélectionner des filtres secondaires (ou rapides).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Rôle requis : admin ou sn_sec_cmn.write

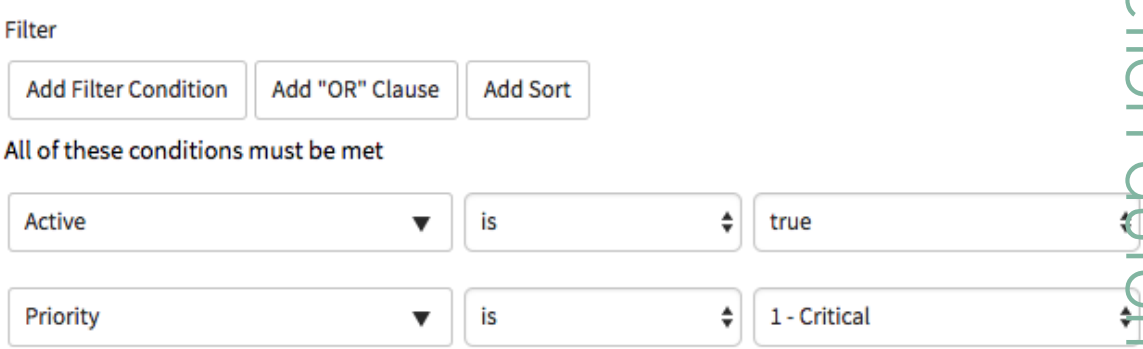
Procédure

1. Accédez à la **Tout** > **Définition du système** > **Filtres**.
2. Cliquez sur **Nouveau** et procédez comme suit.

   a. Saisissez un **titre**.

   b. Sélectionnez **Incident de sécurité [sn_si_incident]** dans la liste de choix **Table** .

   c. Ajoutez vos conditions de filtre.
   Par exemple, le filtre **Incidents ouverts avec priorité = critique** utilise les conditions suivantes.



   d. Cliquez sur **Envoyer**.

3. Si la colonne **Balises** n'est pas visible dans la liste de filtre, cliquez sur l'icône en forme d'engrenage et personnalisez la vue pour l'ajouter.
4. Localisez le filtre que vous avez créé et ajoutez l'une des balises suivantes pour indiquer comment le filtre doit apparaître dans le Security Analyst Workspacefichier .
   - **SN_SI_Primary** : si cette balise est sélectionnée, le filtre peut être sélectionné à partir de la zone de sélection du filtre primaire dans le Security Analyst Workspace.
   - **SN_SI_Primary_OOB** : Si cette balise est sélectionnée, le filtre apparaît par défaut dans la partie **Sélectionné** de la zone de sélection du filtre principal.
   - **SN_SI_Secondary** : Si cette balise est sélectionnée, le filtre peut être sélectionné à partir de la zone de sélection du filtre secondaire (rapide).
   - **SN_SI_Secondary_OOB** : si cette balise est sélectionnée, le filtre apparaît par défaut dans la partie **Sélectionné** de la zone de sélection du filtre principal.

Information associée

Créer et modifier des filtres

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace

Ces propriétés système sont utilisées pour configurer Security Analyst Workspace.

Il existe deux types de propriétés :

- Propriétés qui ne sont généralement pas modifiées, comme les clés de sys_ids et de produit.
- Propriétés qui sont modifiées selon les besoins, telles que les longs intervalles d'interrogation et les configurations de l'interface utilisateur.

Remarque : Les propriétés de l'espace de travail de l'analyste de la sécurité se trouvent à l'emplacement suivant : **Incident de sécurité** > **Configuration d'Analyst Workspace** > **Propriétés d'Analyst Workspace**.

Propriétés de Security Analyst Workspace

Nom de la propriété	Description
Champs qui sont masqués par défaut dans la bannière de tâche de réponse. sn_app_secops_ui.form.excluded_fields.response_task	• **Type** : chaîne • **Valeur par défaut** : ◦ Numéro ◦ Description brève ◦ commentaires ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity
Champs qui sont masqués par défaut dans la bannière d'incident. sn_app_secops_ui.form.excluded_fields.incident	• **Type** : chaîne • **Valeur par défaut** : ◦ Numéro ◦ Description brève ◦ commentaires ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity ◦ security_tags
Le style de couleur d'arrière-plan est appliqué aux champs répertoriés ici. sn_app_secops_ui.form.color_coded_fields	• **Type** : chaîne • **Valeur par défaut** : ◦ Criticité opérationnelle ◦ impact ◦ Priorité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
	◦ risk_score ◦ severity
Si vrai, les tables étendues à partir de la table de tâche de réponse de base sn_si_task auront également accès aux modèles d'e-mails créés pour la table de tâche de réponse de base. sn_app_secops_ui.extend.base.response_task.email_templates	• **Type** : vrai | faux • **Valeur par défaut** : true
Définit la largeur de chaque champ de résumé dans chaque bannière de tâche de réponse. sn_app_secops_ui.task_summary.single_summary.width.response_task	• **Type** : nombre entier • **Valeur par défaut** : 10
Définit la largeur de chaque champ de résumé dans chaque bannière d'incident. sn_app_secops_ui.task_summary.single_summary.width.incident	• **Type** : nombre entier • **Valeur par défaut** : 15
Définit une limite du nombre de champs de synthèse autorisés dans la bannière d'incident. sn_app_secops_ui.task_summary.single_summary.limit.incident	• **Type** : nombre entier • **Valeur par défaut** : 12
Définit une limite du nombre de champs de synthèse autorisés dans la bannière de tâche de réponse. sn_app_secops_ui.task_summary.single_summary.limit.response_task	• **Type** : nombre entier • **Valeur par défaut** : 12
Définit une limite au nombre de champs de synthèse autorisés dans la première ligne de la bannière d'incident. sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• **Type** : nombre entier • **Valeur par défaut** : 3
Liste de champs séparés par des virgules qui peuvent avoir des photos d'utilisateurs. sn_app_secops_ui.form.user_fields	• **Type** : chaîne • **Valeur par défaut** : ◦ affected_user ◦ appelant ◦ sys_updated_by

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
	◦ sys_created_by ◦ opened_by ◦ closed_by ◦ submitted_by
Définit la largeur de chaque champ de résumé dans chaque mode d'aperçu d'incident. sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• **Type** : nombre entier • **Valeur par défaut** : 13,5
Liste de champs séparés par des virgules qui affichent l'heure. sn_app_secops_ui.form.time_fields	• **Type** : chaîne • **Valeur par défaut** : ◦ opened_at ◦ sys_created_on ◦ sys_updated_on
Contrôle la fréquence (en millisecondes) à laquelle les résultats de la recherche de perception sont actualisés. sn_app_secops_ui.interval_poller.search_action	• **Type** : nombre entier • **Valeur par défaut** : 30 000 **Minimum** : 15000
Contrôle la fréquence (en millisecondes) à laquelle les données de compte ou de requête sont actualisées. sn_app_secops_ui.poller_interval.related_list	• **Type** : nombre entier • **Valeur par défaut** : 30 000 **Minimum** : 15000
Contrôle la fréquence (en millisecondes) à laquelle les données de résultat sont actualisées (pour le playbook). sn_app_secops_ui.poller_interval.playbook_tasks	• **Type** : nombre entier • **Valeur par défaut** : 30 000 **Minimum** : 15000
ID pour le workflow Intégration des opérations de sécurité - Isoler l'hôte. sn_app_secops_ui.workflow.id.isolate_host	• **Type** : chaîne • **Valeur par défaut** : d72041f1ff203200c68c84648e94fa5e

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
ID du workflow Security Operations Integration - Liste de surveillance. sn_app_secops_ui.workflow.id.publish_to_watchlist	• **Type** : chaîne • **Valeur par défaut** : 35800c0eff343200c68c84648e94fa85
ID pour le workflow Security Operations Integration - Block Request. sn_app_secops_ui.workflow.id.block_request	• **Type** : chaîne • **Valeur par défaut** : 11a6a5270b9032008f9108e3c5673a24
ID du rôle d'utilisateur sn_si_analyst. sn_app_secops_ui.roles.id.sn_si.write	• **Type** : chaîne • **Valeur par défaut** : 66878663ff123100158bfffffffff8d
ID du rôle d'utilisateur sn_si_read. sn_app_secops_ui.roles.id.sn_si.read	• **Type** : chaîne • **Valeur par défaut** : ae878663ff123100158bfffffffff8e
ID du rôle d'utilisateur sn_si_admin. sn_app_secops_ui.roles.id.sn_si.admin	• **Type** : chaîne • **Valeur par défaut** : 22878663ff123100158bfffffffff8d
ID pour le workflow Microsoft Exchange - Effectuer une recherche et une suppression d'e-mail. sn_app_secops_ui.email.phishing.manual.workflow	• **Type** : chaîne • **Valeur par défaut** : ed9f289cc310220031fbdccdf3d3aeb4
ID de l'action personnalisée Ajouter à la liste de refus sous l'onglet Explorer du Security Analyst Workspace. sn_app_secops_ui.explore.action.direct.id.deny_list	• **Type** : chaîne • **Valeur par défaut** : DENY_e9bd0ac50b632200263a089b37673a0b
ID de l'action personnalisée Ajouter à la liste d'autorisation sous l'onglet Explorer de Security Analyst Workspace sn_app_secops_ui.explore.action.direct.id.allow_list	• **Type** : chaîne • **Valeur par défaut** : ALLOWLIST_e9bd0ac50b632200263a089b37673a0b
ID de l'action d'interface utilisateur Exécuter la recherche de menace. sn_app_secops_ui.explore.action.id.run_threat_lookup	• **Type** : chaîne • **Valeur par défaut** : da5ff4420b540300263a089b37673ae7

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
ID de l'option d'intégration Recherche de menace. sn_app_secops_ui.explore.capability.id.threat_lookup	• **Type** : chaîne • **Valeur par défaut** : 39344d4f0b273200263a089b37673ab1
ID de l'action personnalisée d'enrichissement des observables sous l'onglet Explorer du Security Analyst Workspace. sn_app_secops_ui.explore.action.id.observable_enrichment	• **Type** : chaîne • **Valeur par défaut** : OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673a1e
ID de l'option d'intégration Enrichir les observables. sn_app_secops_ui.explore.capability.id.observable_enrichment	• **Type** : chaîne • **Valeur par défaut** : 9ad183640b1003009f66e94685673af4
ID de l'action d'interface utilisateur Publier dans la liste de surveillance. sn_app_secops_ui.explore.action.id.publish_to_watchlist	• **Type** : chaîne • **Valeur par défaut** : 8ee94002ff743200c68c84648e94faf9
ID de l'action d'interface utilisateur Demande de blocage. sn_app_secops_ui.explore.action.id.block_request	• **Type** : chaîne • **Valeur par défaut** : 7158f6e40b2032008f9108e3c5673adf
ID de l'action d'interface utilisateur Exécuter la recherche de perceptions. sn_app_secops_ui.explore.action.id.sightings_search	• **Type** : chaîne • **Valeur par défaut** : 43f91a6f0b032200b97c67d985673a2c
ID de l'action d'interface utilisateur Créer un incident de sécurité enfant. sn_app_secops_ui.explore.action.id.create_child_incident	• **Type** : chaîne • **Valeur par défaut** : 5a6882645363530099d5ddeeff7b1272
ID de l'action d'interface utilisateur Ajouter une annotation de sécurité. sn_app_secops_ui.explore.action.id.add_security_annotation	• **Type** : chaîne • **Valeur par défaut** : 1e3a3e723b5332005a9149a4d2efc4eb
ID de l'action personnalisée d'enrichissement de CI sous l'onglet Explorer du Security Analyst Workspace. sn_app_secops_ui.explore.action.id.ci_enrichment	• **Type** : chaîne • **Valeur par défaut** : CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1e

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
ID de l'action d'interface utilisateur Isoler l'hôte. sn_app_secops_ui.explore.action.id.isolate_host	• **Type** : chaîne • **Valeur par défaut** : d6244e0aff203200c68c84648e94fad3
ID de l'action d'interface utilisateur Ajouter plusieurs observables. sn_app_secops_ui.explore.action.id.multiple_observable	• **Type** : chaîne • **Valeur par défaut** :138de478d78322007a6de294de6103aa
Clé de produit pour ag-Grid-Enterprise. sn_app_secops_ui.ag-grid-license	• **Type** : chaîne • **Valeur par défaut** :ServiceNow_ServiceNow_5Devs2_August_2018__MT

Configuration supplémentaire de l'espace de travail de l'analyste de la sécurité

Configurez et définissez les filtres, les actions d'interface Security Analyst Workspace utilisateur et les listes connexes.

- Configuration du filtre de la page de destination
- Activer les actions d'interface utilisateur
- Actions d'interface utilisateur du formulaire
- Configuration de la liste connexe
- Actions d'interface utilisateur de la liste connexe
- Propriétés système de configuration de formulaire
- Activer les playbooks pour la sélection d'analystes

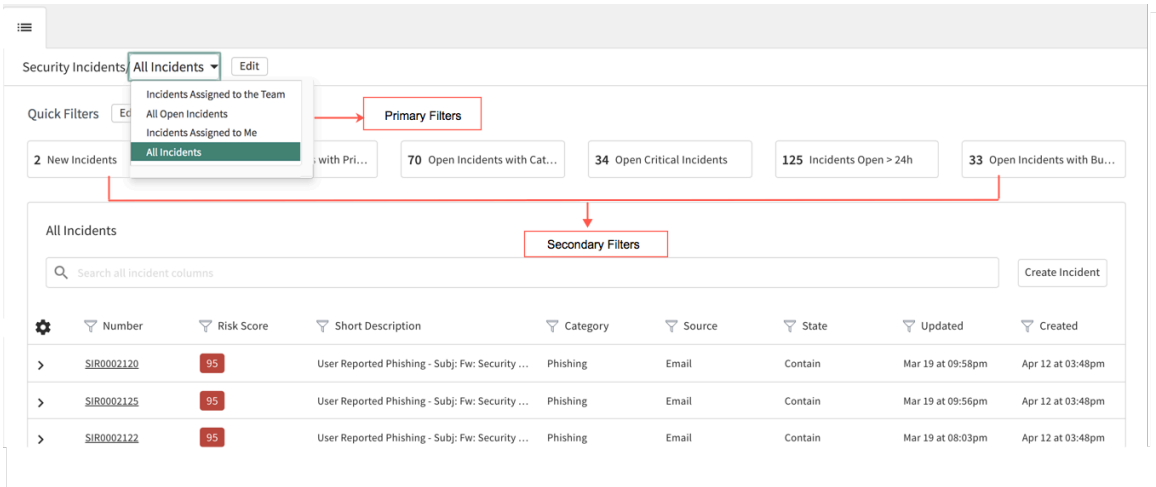
Configuration du filtre de la page de destination

Vous pouvez ajouter de nouveaux filtres ou modifier les filtres existants qui apparaissent dans le Security Analyst Workspacefichier .

Le Security Analyst Workspace dispose de filtres primaires et secondaires qui vous permettent de filtrer la liste des incidents de sécurité afin de trouver rapidement les incidents de sécurité que vous souhaitez analyser. Pour plus d'informations, reportez-vous à la section Gérer les menaces de sécurité à l'aide de l' Security Analyst Workspace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Créer un nouveau filtre

1. Accédez à la **Incidents de sécurité** > **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Configuration du filtre de la page de destination**.
2. Cliquez sur **Nouveau**.
3. Saisissez un titre pour le filtre, spécifiez la condition de filtre et cliquez sur **Soumettre** pour revenir à la page précédente.

   Vous verrez le filtre nouvellement ajouté répertorié sur la page.
4. Ajoutez une balise pour ce filtre afin d'indiquer s'il s'agit d'un filtre primaire ou secondaire. Les balises suivantes sont disponibles :
   - SN_SI_Primary
   - SN_SI_Secondary

Modifier les filtres existants

Vous pouvez également effectuer les opérations suivantes :

- Modifier les filtres existants : cliquez sur le titre d'un filtre existant. Modifiez le titre et la condition de filtre, puis cliquez sur **Mettre à jour**.
- Modifier les balises : sélectionnez un filtre et cliquez sur la colonne Balise dans la configuration du filtre de la page de destination. Vous pouvez supprimer la balise existante ou ajouter une nouvelle balise pour le filtre.

Activer les actions d'interface utilisateur

Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles soient disponibles à la configuration dans le Security Analyst Workspace.

Remarque : Pour modifier les actions d'interface utilisateur, connectez-vous en tant qu'utilisateur avec les rôles suivants :

- ui_action_admin
- ui_page_admin
- web_service_admin

Il existe deux types d'actions d'interface utilisateur qui peuvent être configurés pour :Security Analyst Workspace

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Action d'interface utilisateur basée sur la boîte de dialogue
- Action d'interface utilisateur côté serveur

Action d'interface utilisateur basée sur la boîte de dialogue

Pour activer les actions d'interface utilisateur basées sur des boîtes de dialogue dans le Security Analyst Workspace, apportez les modifications suivantes aux pages d'interface utilisateur associées aux actions d'interface utilisateur standard respectives.

1. **Section HTML** : modifiez la section HTML pour inclure la balise d'entrée *react* . La valeur de la balise d'entrée *react* est utilisée dans la section du script client pour identifier si la page d'interface utilisateur a été lancée à partir du Security Analyst Workspace. Un exemple est présenté ci-dessous :

   ```
   <input id="react" name="react" type="hidden"
   value="${JS,HTML:sysparm_react}" />
   ```

2. **Script client** : une logique supplémentaire doit être écrite dans le script client lorsque l'indicateur *react* est vrai. Cela est nécessaire pour gérer les événements des boutons **Soumettre** et **Annuler** affichés dans le cadre de la boîte de dialogue.
   a. Le gestionnaire d'événements onCancel () doit répartir l'événement « SIR_WORKBENCH_POPUP_CANCEL » à partir de Security Analyst Workspace
   b. Le gestionnaire d'événements onSubmit () doit répartir l'événement « SIR_WORKBENCH_POPUP_SUBMIT » à partir du Security Analyst Workspace
3. L'exécution du script de traitement est ignorée du Security Analyst Workspace contexte, car l'action « onSubmit » a été modifiée pour renvoyer la valeur « faux » lorsque la valeur de la balise d'entrée *react* est vrai. La logique du script de traitement doit être gérée soit via un script client pouvant être appelé (invoqué via l'API GlideAjax), soit via un point de terminaison de ressource REST.

Pour plus d'informations, reportez-vous aux exemples de pages d'interface utilisateur suivants :

- Exemple d'action d'interface utilisateur de liste connexe : publier dans la liste de surveillance (nom de la page de l'interface utilisateur : publish_to_watchlist)
- Exemple d'action d'interface utilisateur du formulaire : Créer un problème (nom de la page de l'interface utilisateur : create_prb_change_inc)

Action d'interface utilisateur côté serveur

Pour activer les actions d'interface utilisateur côté serveur, procédez comme suit :

La logique du script d'action d'interface utilisateur standard doit être traitée dans le cadre d'une ressource REST scriptée.

Pour plus d'informations, consultez les exemples d'actions d'interface utilisateur de formulaire suivants :

- Créer une panne
- Annuler

Actions d'interface utilisateur du formulaire

Vous pouvez configurer les actions d'interface utilisateur qui s'affichent dans le Security Analyst Workspacefichier .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions préalables:

Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles puissent être configurées dans le Security Analyst Workspace. Consultez Activer les actions d'interface utilisateur pour en savoir plus.

Pour configurer une action d'interface utilisateur de formulaire pour le Security Analyst Workspace, procédez comme suit :

1. Accédez à la **Incidents de sécurité** > **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Actions d'interface utilisateur du formulaire**.
2. Renseignez les champs suivants :

Nom de champ	Description
Action	Sélectionnez une action d'interface utilisateur dans la liste de choix.
Type	Sélectionnez le type d'action. Il peut s'agir de : ◦ Action basée sur la boîte de dialogue : ce type d'action est utilisé lorsque l'interaction ou les entrées de l'utilisateur sont requises pour exécuter une logique métier spécifique. ◦ Action côté serveur : cette action exécute la logique métier requise sans aucune entrée supplémentaire de l'utilisateur. **Remarque :** Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles puissent être configurées dans le Security Analyst Workspace. Consultez Activer les actions d'interface utilisateur pour en savoir plus.
Application	Le nom du périmètre de l'application (Security Incident Response UI) dans lequel l'action d'interface utilisateur est ajoutée s'affiche ici.
Action basée sur la boîte de dialogue Si vous sélectionnez Action basée sur la boîte de dialogue dans le champ Type, entrez les détails suivants :	
Page de l'IU	Sélectionnez la page d'interface utilisateur associée à l'action.
Titre de la boîte de dialogue	Saisissez un titre pour l'action de boîte de dialogue.
Largeur et hauteur de la boîte de dialogue	Entrez la hauteur et la largeur de la boîte de dialogue en pixels.
Script	Pour la page d'interface utilisateur sélectionnée, vous pouvez spécifier des paramètres de requête supplémentaires ici. Le modèle fourni avec le système de base construit et renvoie `sysparm_sys_id` paramètre uniquement. Vous pouvez remplacer cela en spécifiant différents paramètres ici.
Action côté serveur Si vous sélectionnez Action côté serveur dans le champ Type, saisissez les détails suivants :	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

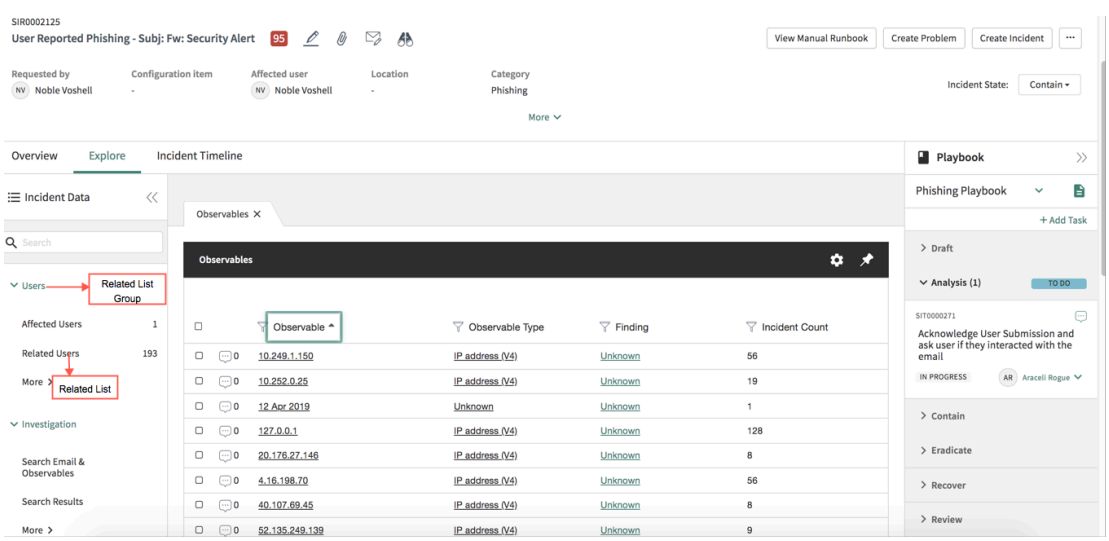
Nom de champ	Description
Ressource REST scriptée	Sélectionnez la ressource REST scriptée qui définit l'action. **Remarque :** L'ACL **D'ANALYSTE D'INTERFACE UTILISATEUR SIR** doit être ajoutée à la ressource Rest.

3. Cliquez sur **Envoyer**.
4. Accédez à la **Incidents de sécurité** > **Incidents (nouvelle UI)** la page.
5. Cliquez sur un numéro d'incident de sécurité pour afficher l'enregistrement de l'incident de sécurité. Vous pouvez voir la nouvelle action d'interface utilisateur en haut de la page.

Pour modifier une action d'interface utilisateur de formulaire existante, cliquez sur le nom de l'action pour accéder à la page Actions d'interface utilisateur de formulaire. Vous pouvez modifier le nom de l'action, le type et le reste des champs en fonction du type sélectionné.

Configuration de la liste connexe

Vous pouvez ajouter de nouvelles listes connexes ou de nouveaux groupes de listes connexes, et modifier les groupes ou listes connexes existants qui apparaissent dans le Security Analyst Workspacefichier .



Ajouter un groupe de listes connexes

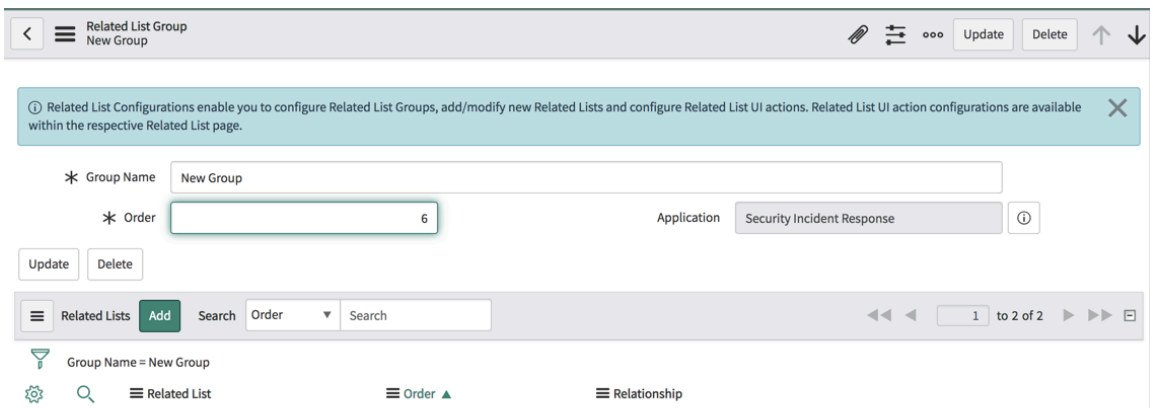
Pour ajouter un groupe de listes connexes, procédez comme suit :

1. Accédez à la **Incidents de sécurité** > **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Configurations de Liste connexe**.
2. Cliquez sur **Nouveau** pour ajouter un nouveau groupe de listes connexes. Entrez le nom du groupe et l'ordre dans lequel il doit apparaître sur la page Incidents (nouvelle interface utilisateur).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Envoyer**. Le groupe nouvellement ajouté apparaît dans la page Groupes de listes connexes.



Ajouter une liste connexe

Pour ajouter une nouvelle liste connexe, procédez comme suit :

1. Cliquez sur le lien d'un groupe de listes connexes.
2. Dans la section Listes connexes, cliquez sur **Ajouter** pour ajouter une nouvelle liste connexe.

   Si vous ne voyez pas le bouton **Ajouter** , vérifiez si vous êtes dans le même périmètre de l'application que le groupe de listes connexes.

3. Sélectionnez la liste connexe à inclure dans le groupe.

   Remarque : Si vous ne voyez pas de liste connexe spécifique, procédez comme suit :

   a. Accédez à la **Interface utilisateur du système** > **Listes connexes** et recherchez les listes connexes présentes dans la table *sn_si_incident* .

   b. Cliquez sur la table *sn_si_incident* associée à la **nouvelle vue d'interface utilisateur SIR**.

   c. Dans la section Entrées de liste connexe, cliquez sur **Nouveau** pour ajouter la liste connexe à la nouvelle vue **d'interface utilisateur SIR** .

4. Spécifiez l'ordre dans lequel il doit apparaître, puis cliquez sur **Soumettre**.

   La liste connexe que vous avez ajoutée s'affichera dans le Security Analyst Workspacefichier .

Pour modifier un groupe de listes connexes existant, cliquez sur le nom du groupe pour accéder à la page du groupe de listes connexes. Vous pouvez modifier le nom et l'ordre du groupe, et ajouter ou supprimer des listes connexes du groupe.

Actions d'interface utilisateur de la liste connexe

Vous pouvez ajouter de nouvelles actions d'interface utilisateur aux listes connexes qui apparaissent dans le Security Analyst Workspace.

Conditions préalables:

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles puissent être configurées dans le Security Analyst Workspace. Consultez Activer les actions d'interface utilisateur pour en savoir plus.

Pour ajouter une nouvelle action d'interface utilisateur de liste connexe, procédez comme suit :

1. Accédez à la **Incidents de sécurité** > **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Configurations de Liste connexe**.
2. Cliquez sur le nom du groupe. La page de configuration du groupe de listes connexes s'affiche.
3. Cliquez sur la liste connexe pour laquelle vous souhaitez ajouter une action d'interface utilisateur.
4. Cliquez sur **Ajouter** dans la section Actions d'interface utilisateur de la liste connexe.
5. Renseignez les champs suivants :

Nom de champ	Description
Action	Sélectionnez une action d'interface utilisateur dans la liste de choix.
Type	Sélectionnez le type d'action. Il peut s'agir de : ◦ Action basée sur la boîte de dialogue : ce type d'action est utilisé lorsque l'interaction ou les entrées de l'utilisateur sont requises pour exécuter une logique métier spécifique. ◦ Action côté serveur : cette action exécute la logique métier requise sans aucune entrée supplémentaire de l'utilisateur. **Remarque :** Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles puissent être configurées dans le Security Analyst Workspace. Consultez Activer les actions d'interface utilisateur pour en savoir plus.
Application	Le nom du périmètre de l'application (Security Incident Response UI) dans lequel l'action d'interface utilisateur est ajoutée s'affiche ici.
Action basée sur la boîte de dialogue Si vous sélectionnez Action basée sur la boîte de dialogue dans le champ Type, entrez les détails suivants :	
Page de l'IU	Sélectionnez la page d'interface utilisateur associée à l'action.
Titre de la boîte de dialogue	Saisissez un titre pour l'action de boîte de dialogue.
Largeur et hauteur de la boîte de dialogue	Entrez la hauteur et la largeur de la boîte de dialogue en pixels.
Script	Pour la page d'interface utilisateur sélectionnée, vous pouvez spécifier des paramètres de requête supplémentaires ici. Le modèle fourni avec le système de base construit et renvoie uniquement `les paramètres sysparm_incident_id`,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description
	`sysparm_record_table` et `sysparm_related_sys_ids`. Vous pouvez les remplacer en spécifiant différents paramètres ici.
Action côté serveur Si vous sélectionnez Action côté serveur dans le champ Type, spécifiez les éléments suivants :	
Ressource REST scriptée	Sélectionnez la ressource REST scriptée qui définit l'action. **Remarque :** L'ACL **D'ANALYSTE D'INTERFACE UTILISATEUR SIR** doit être ajoutée à la ressource Rest.

6. Cliquez sur **Envoyer**.
7. Accédez à la **Incidents de sécurité** > **Incidents (nouvelle UI)** la page.
8. Cliquez sur un numéro d'incident de sécurité pour afficher l'enregistrement de l'incident de sécurité. Lancez la liste connexe respective pour afficher la nouvelle action d'interface utilisateur.

Propriétés système de configuration de formulaire

Ces propriétés système définissent les intervalles d'actualisation du formulaire pour les tâches du playbook.

Pour configurer ces propriétés, accédez à **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Propriétés d'Analyst Workspace**.

Propriété	Valeur par défaut	Description
sn_app_secops_ui.poller_interval.playbook_tasks	10000 millisecondes	Intervalle de temps utilisé par le composant de playbook pour actualiser ses tâches de réponse pour chaque intervalle de temps configuré.
sn_app_secops_ui.poller_interval_count.playbook_tasks	3 fois	Nombre de fois que le composant du playbook interroge les tâches de réponse.
sn_app_secops_ui.poller_interval.related_list	30000 millisecondes	Cet intervalle de temps est utilisé par le composant Explore pour actualiser ses décomptes de listes connexes pour chaque intervalle de temps configuré.

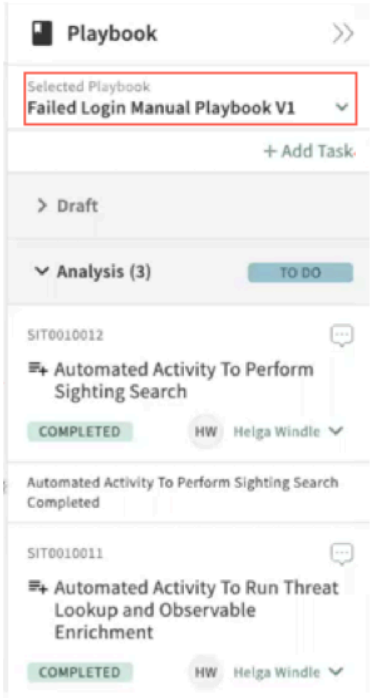
Activer les playbooks pour la sélection d'analystes

Ajoutez de nouveaux playbooks à la liste de sélection des playbooks.

Vous pouvez sélectionner un playbook approprié pour enquêter sur les incidents de sécurité dans le Security Analyst Workspace (Gérer les menaces de sécurité à l'aide de l' Security Analyst Workspace). L'option de sélection de playbook ne prend en charge que les playbooks conçus à l'aide de Flow Designer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois que vous avez créé un playbook à l'aide de Concepteur de flux, procédez comme suit pour l'inclure dans la liste de choix de Playbooks sélectionnés :

1. Accédez à *sys_hub_flow* table.
2. Recherchez le nouveau playbook que vous avez créé à l'aide de Flow Designer.
3. Ajoutez la balise **sir_playbook** aux Playbooks que vous souhaitez inclure dans la liste de choix de Playbooks sélectionnés.

Remarque : Si vous avez d'anciens playbooks qui n'ont pas été migrés des workflows vers Flow Designer, ils n'apparaîtront pas dans la liste. Toutefois, si un playbook créé à l'aide de workflows est affecté à un incident de sécurité soit par une condition de déclenchement, soit par sélection manuelle (à l'aide de l'option **Exécuter l'orchestration** dans l'environnement classique), ce playbook est lancé lorsque vous ouvrez l'incident de sécurité dans le Security Analyst Workspace.

Dépannage de Security Incident Response

Cette section couvre des conseils de dépannage importants et des questions fréquemment posées liées à Security Incident Response.

Problèmes liés aux règles de contrôle d'accès

Les règles de contrôle d'accès autorisent l'accès à la ressource spécifiée si les trois conditions suivantes sont remplies :

- L'utilisateur a l'un des rôles spécifiés dans la liste **de rôles** , ou la liste est vide.
- Les conditions du champ **Condition** sont vraies, ou les conditions sont vides.
- Le script dans le champ **Script** (avancé) donne la valeur vrai, ou définit la **réponse** de variable comme vrai, ou est vide.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les règles de contrôle d'accès, voir Exploration des listes de contrôle d'accès

Important : Si l'option **Remplacements** administrateur n'est pas cochée pour une table d'incidents de sécurité et si l'administrateur est en mesure d'accéder à la table d'incidents de sécurité, consultez KB1444673

Réponse aux incidents de sécurité Solutions Analyse de la plateforme et Reporting

Solutions Analyse de la plateforme et Reporting contiennent des tableaux de bord préconfigurés. Les tableaux de bord présentent des mesures importantes pour analyser votre Réponse aux incidents de sécurité processus, telles que les nouveaux incidents de sécurité ou l'âge moyen des incidents de sécurité ouverts.

Les visualisations de données Platform Analytics utilisent des données d'indicateurs Analyse des performances pour vous montrer des données au fil du temps, ce qui vous aide à analyser vos processus business et à identifier des domaines d'amélioration. Avec Solutions Analyse de la plateforme et Reporting, vous pouvez optimiser votre application avec Analyse des performances sans configuration minimale. Vous pouvez aussi toujours créer vos propres objets.

Important : Configurez et testez les Solutions Analyse de la plateforme et Reporting sur une instance de non-production avant de les activer dans une instance de production.

La Réponse aux incidents de sécurité Analyse des performances solution est disponible à partir du ServiceNow Storefichier . Pour en savoir plus sur le téléchargement et l'installation de cette application, reportez-vous à la rubrique Security Operations et ServiceNow Store.

Remarque : Pour évaluer les fonctionnalités, vous pouvez activer les solutions Analyse des performances et les analyses en formulaire sur des instances qui n'ont pas de licence Analyse des performances. Cependant, vous serez sujet aux limitations suivantes :

- Vous ne pouvez pas créer de nouveaux indicateurs.
- Vous ne pouvez pas collecter de données datant de plus de 180 jours.

Pour une fonctionnalité complète, achetez une licence Analyse des performances. Pour plus d'informations, consultez Activer votre abonnement Analyse des performances .

Important : Par défaut, la limite de collecte de données pour la propriété *(com.snc.pa.dc.max_records)* dans Analyse des performances est fixée à 5 000 enregistrements. Toutefois, vous pouvez augmenter cette limite en fonction de vos besoins, par exemple 50 000 enregistrements. Toutefois, l'augmentation de cette limite peut avoir un impact sur les performances lors de la collecte de données ou lors de l'exécution d'opérations sur la table Instantané. Pour en savoir plus sur les propriétés d'Analyse des performances, reportez-vous à Propriétés du Analyse des performances .

Information associée

Solutions Analyse de la plateforme et Reporting

Activer votre abonnement Analyse des performances

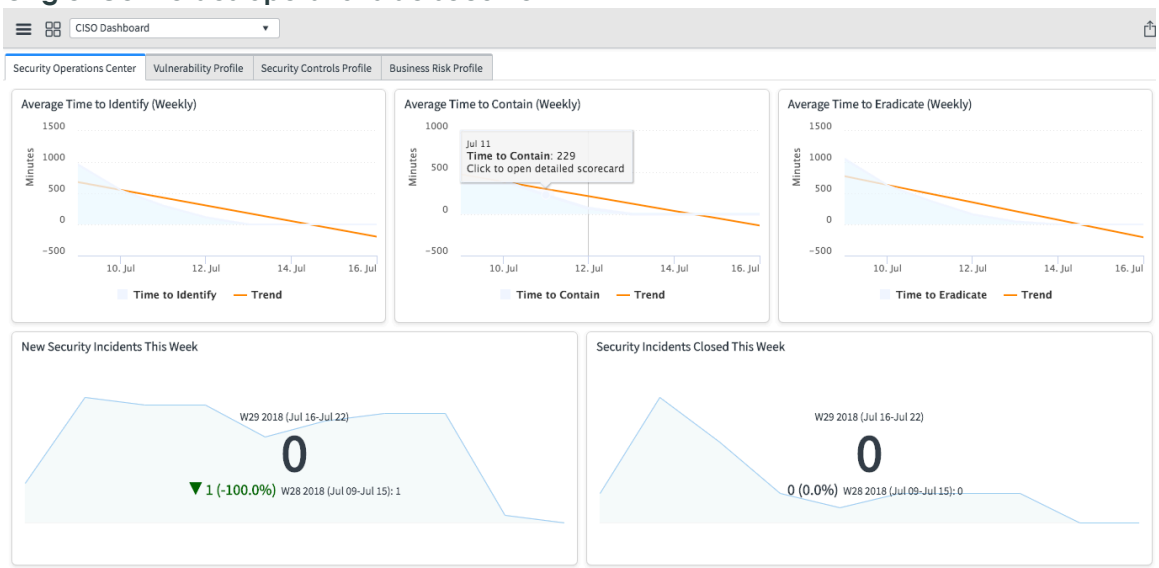
Tableau de bord des CISO

Ce tableau de bord révèle la posture de sécurité globale de votre organisation, y compris les vulnérabilités et incidents de sécurité.

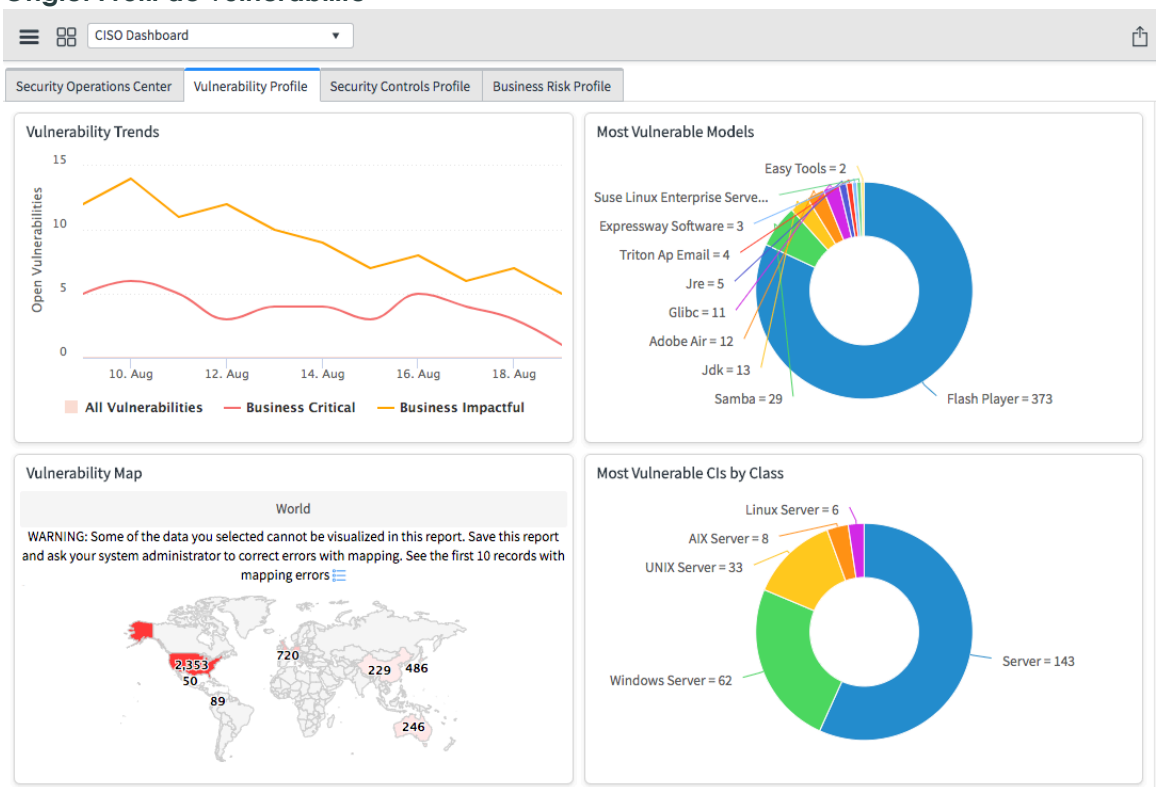
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Centre des opérations de sécurité



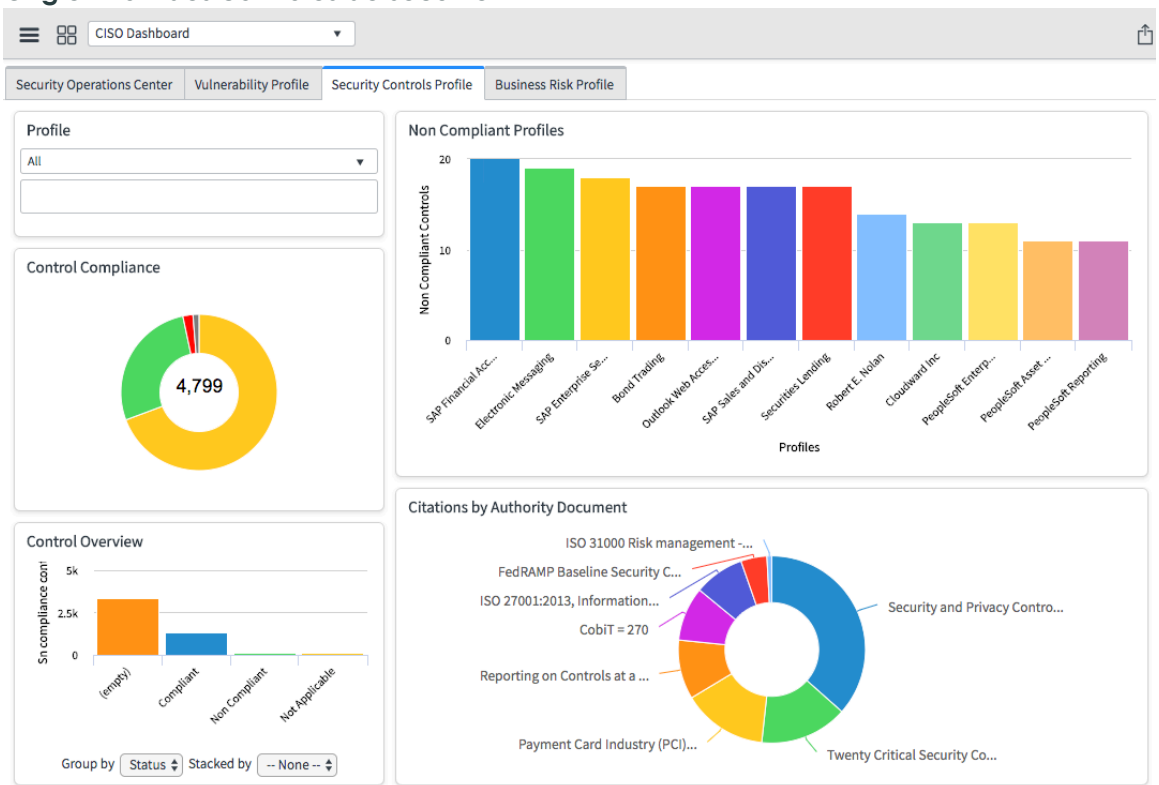
Onglet Profil de vulnérabilité



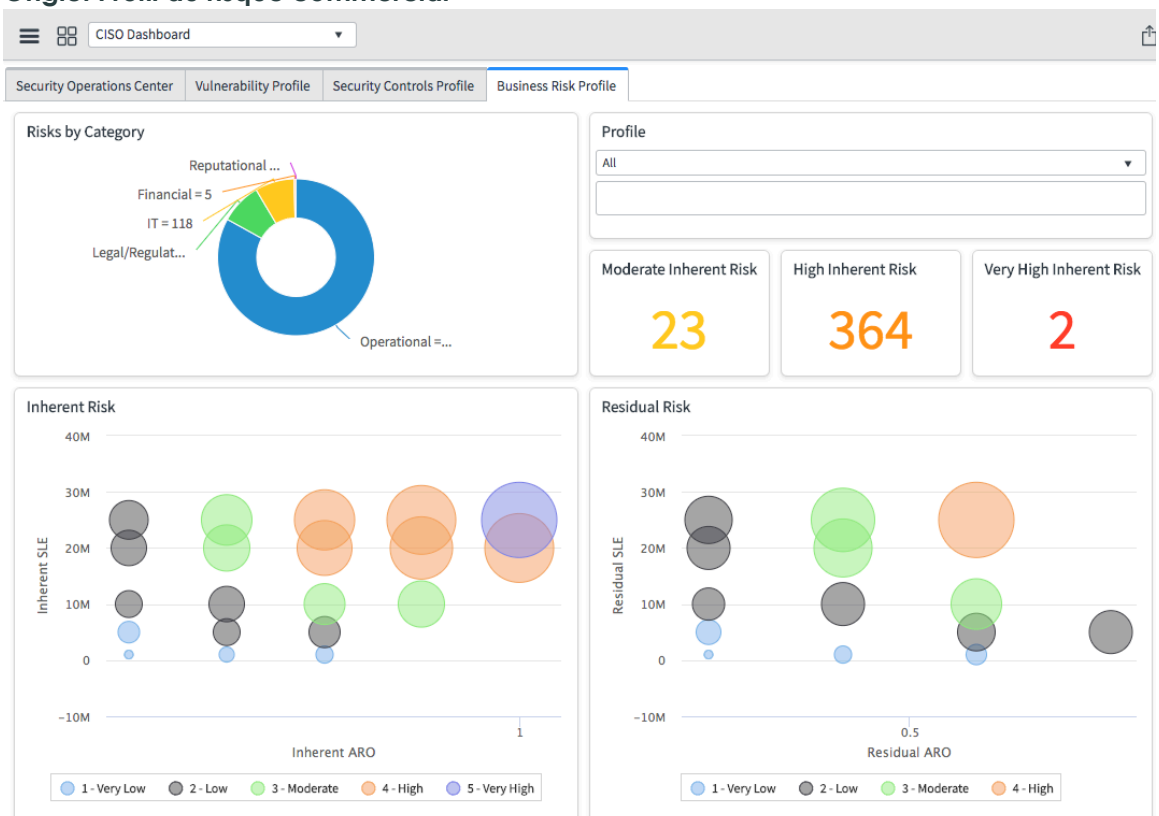
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Profil des contrôles de sécurité



Onglet Profil du risque commercial



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs finaux et rôles

Utilisateur final et objectif	Rôle requis
CISO : a besoin d'une visibilité claire sur la posture de sécurité actuelle de l'organisation globale	sn_si.ciso

Indicateurs du tableau de bord des CISO

Le tableau de bord CISO présente les indicateurs clés de performance suivants :

SI : délai moyen d'identification

Moyenne sur 7 jours du temps, en minutes, nécessaire pour identifier un incident de sécurité, calculée quotidiennement.

Délai moyen pour contenir

Moyenne sur 7 jours du temps, en minutes, nécessaire pour contenir un incident de sécurité, calculée quotidiennement.

Délai moyen pour éradiquer

Moyenne sur 7 jours du temps, en minutes, nécessaire pour supprimer un incident de sécurité, calculée quotidiennement. Le temps moyen pour contenir et le temps moyen pour éradiquer sont basés sur l'indicateur SI : durée moyenne répartie par état d'incident de sécurité.

Nouveaux incidents de sécurité de cette semaine

La somme hebdomadaire du score de l'indicateur quotidien Nombre de nouveaux incidents de sécurité.

Incidents de sécurité clôturés (hebdomadaire)

Somme cumulée sur 7 jours de l'indicateur quotidien Nombre d'incidents de sécurité fermés.

Nouveaux incidents de sécurité, par priorité

Répartition quotidienne de l'indicateur Nombre de nouveaux incidents de sécurité par priorité.

Volume d'incidents de sécurité nouveaux par rapport à fermés (hebdomadaire)

Série chronologique de la somme cumulée sur 7 jours de l'indicateur Nombre de nouveaux incidents présentée graphiquement par rapport à la série chronologique cumulée sur 7 jours de l'indicateur Nombre d'incidents fermés.

Carte thermique des incidents de sécurité

Carte mondiale montrant le nombre d'incidents de sécurité ouverts dans chaque pays.

Arborescence de l'incident de sécurité

Une arborescence interactive dans laquelle vous pouvez choisir de voir :

- Incidents de sécurité par service d'entreprise, répartis par criticité opérationnelle
- Incidents de sécurité ventilés par catégorie ou sous-catégorie d'incident
- Incidents de sécurité par groupe d'affectation ou par délégataire
- « Statistiques de victimes » d'incidents de sécurité par ressource ou utilisateur affecté

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Répartitions

Les répartitions suivantes s'appliquent aux indicateurs du tableau de bord :

- Criticité pour l'entreprise
- Groupe de sécurité
- Âge de l'incident de sécurité
- Catégorie d'incident de sécurité
- Code de fermeture de l'incident de sécurité
- Priorité de l'incident de sécurité
- État de l'incident de sécurité
- IS : service d'entreprise
- Vulnérabilité

Visualisations des données

Le tableau de bord comprend les visualisations suivantes :

Titre	Type	Description
Incidents de sécurité ouverts depuis plus de 30 jours par groupe d'affectation et par état	Carte thermique	Affiche les modèles avec les éléments les plus vulnérables.
Risques par catégorie	Anneau	Répertorie l'âge des éléments vulnérables rouverts.
Contenu des documents de référence par document de référence	Anneau	Nombre de vulnérabilités actives
Incidents de sécurité avec un délégataire qui n'est pas actif	Carte thermique	Affiche le nombre d'éléments vulnérables ouverts associés à des vulnérabilités (enregistrements Common Vulnerability Enumeration (CVE)), du plus au moins élevé.
Incidents de sécurité non mis à jour depuis plus de 30 jours par groupe d'affectation et par état	Carte thermique	Affiche les éditeurs ayant les éléments les plus vulnérables.
Carte de vulnérabilité	Carte	Une carte du monde montrant les vulnérabilités par emplacement
Modèles les plus vulnérables	Anneau	Les applications qui contiennent le plus de vulnérabilités
CI les plus vulnérables par classe	Anneau	CI par type de serveur
Services avec des vulnérabilités d'importance critique	Liste	

Traduction automatique

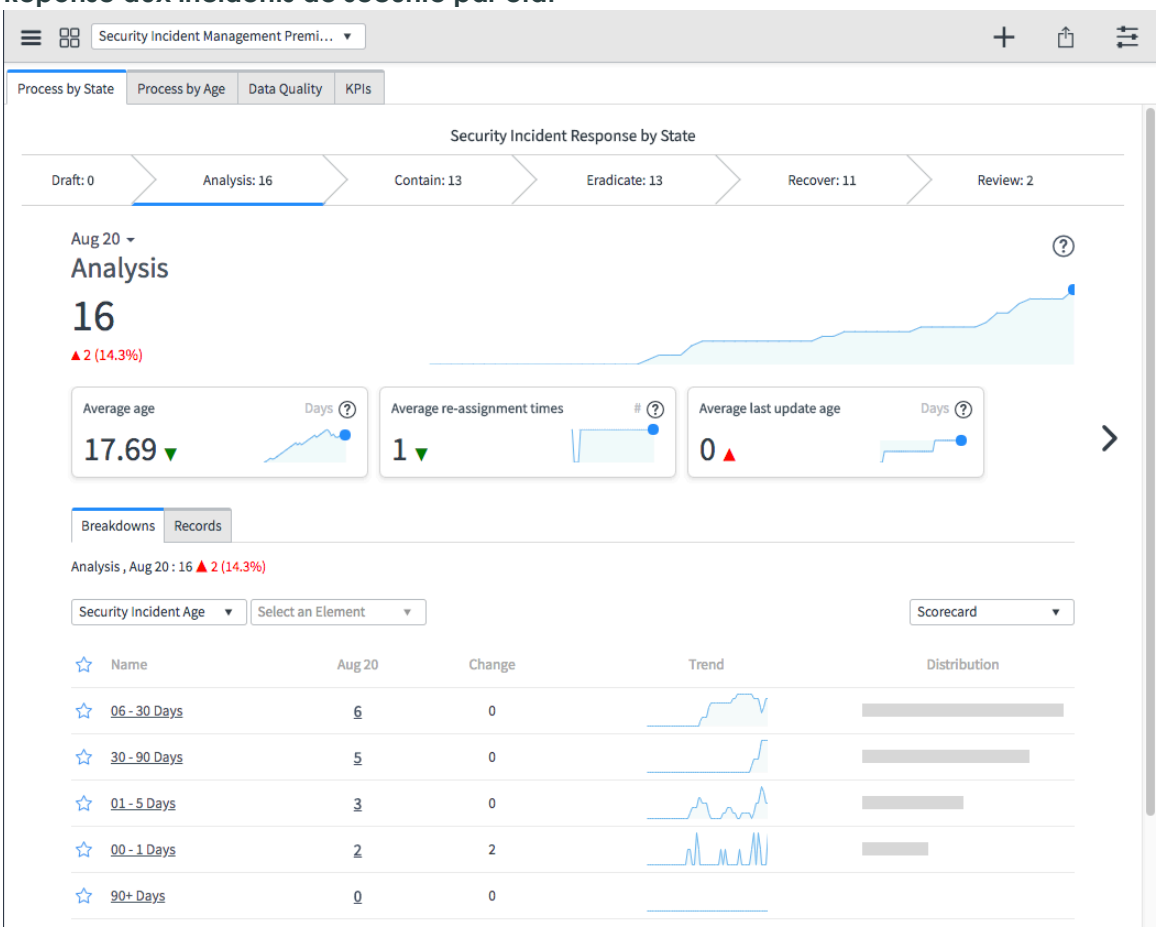
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre	Type	Description
Profils non-conformes	Barre	Contrôles non conformes par profil
Vue d'ensemble des contrôles	Barre	Nombre de contrôles conformes et non conformes
Exceptions de politique	Liste	Exceptions de politique avec priorité, propriétaire et description brève
Risques par catégorie	Anneau	Nombre de risques dans chaque catégorie de risque
Risque inhérent	Bulle	SLE inhérente par rapport à ARO inhérent
Risque résiduel	Bulle	SLE résiduelle par rapport à ARO résiduel
Risques modérés, élevés et très élevés	Icône Score	Nombre de risques modérés, élevés et très élevés, respectivement
Risque par profil	Barre empilée	Décompte des risques dans lequel vous pouvez sélectionner les éléments à regrouper et les éléments à empiler

Tableau de bord de Gestion des incidents de sécurité Premium

Ce tableau de bord utilise des visualisations avancées Platform Analytics pour aider les gestionnaires de sécurité à suivre le volume, les performances et la progression des incidents de sécurité, de l'analyse/détection initiale au confinement, à l'éradication et à la récupération. La version sous licence de Analyse des performances est donc requise.

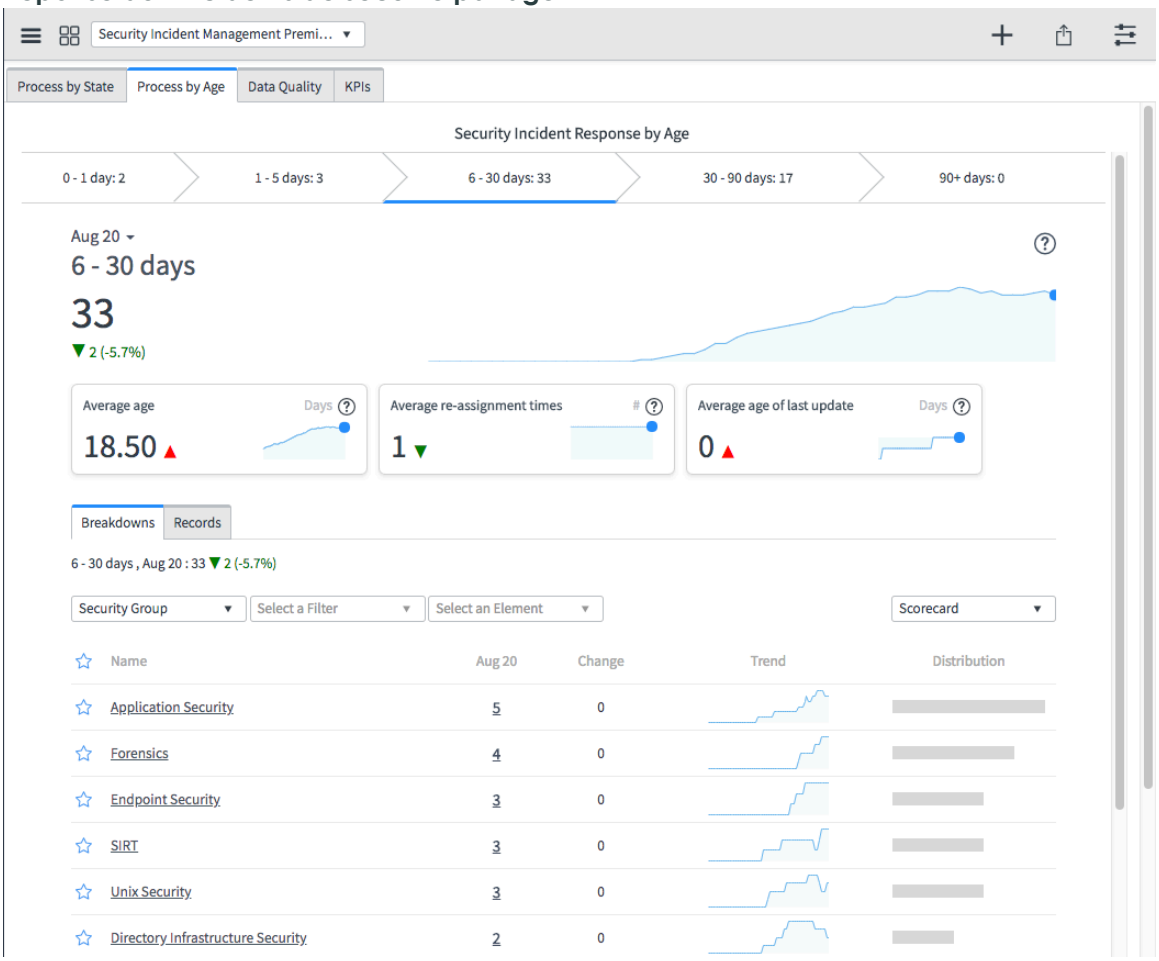
Réponse aux incidents de sécurité par état



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux incidents de sécurité par âge



Utilisateurs finaux et rôles

Utilisateur final et objectif	Rôle requis	Avantages
Security Response Manager : a besoin d'une visibilité claire sur l'état global et le volume des incidents de sécurité associés aux applications et aux services.	sn_si.manager	Peut examiner la posture de sécurité globale avec la possibilité d'ajuster les membres des groupes d'affectation.
Administrateur Security Response : doit identifier rapidement les zones de préoccupation et avoir un contrôle total sur toutes les données de Security Incident Response tout en administrant les territoires et les compétences, selon les besoins.	sn_si.admin	Peut ajuster les paramètres de calcul des risques pour s'assurer que les éléments vulnérables les plus pertinents pour l'organisation sont traités en premier.
Analystes Security Response : ils doivent rapidement hiérarchiser les vulnérabilités sur lesquelles se concentrer	sn_si.analyst	Les analystes de sécurité de niveau 1 et 2 travaillent sur les incidents de sécurité. Ils peuvent créer et mettre

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur final et objectif	Rôle requis	Avantages
en fonction de la criticité pour l'organisation.		à jour des incidents de sécurité, des demandes et des tâches, ainsi que des problèmes, des changements et des pannes liés à leurs incidents.

Indicateurs de sécurité Gestion des incidents Premium

Les onglets Processus par état et Processus par âge contiennent des widgets de console avec les indicateurs suivants :

Âge moyen

L'indicateur Âge moyen des incidents de sécurité ouverts utilise la formule `[[Âge cumulé des incidents de sécurité ouverts]] / [[Nombre d'incidents de sécurité ouverts]] / 24` pour donner un résultat en jours.

Délais de réaffectation moyens

L'indicateur Réaffectation moyenne des incidents de sécurité ouverts utilise la formule `Réaffectation cumulée des incidents de sécurité ouverts / Nombre d'incidents de sécurité ouverts`.

Âge moyen de la dernière mise à jour

L'indicateur Âge moyen de la dernière mise à jour des incidents de sécurité ouverts utilise la formule `Âge cumulé de la dernière mise à jour des incidents de sécurité ouverts / Nombre d'incidents de sécurité ouverts / 24` pour donner un résultat en jours.

% non mis à jour au cours des 5 derniers jours

L'indicateur % d'incidents de sécurité ouverts non mis à jour au cours des 5 derniers jours utilise la formule `([[nombre d'incidents de sécurité ouverts non mis à jour au cours des 5 derniers jours]] / [[nombre d'incidents de sécurité ouverts]]) * 100`.

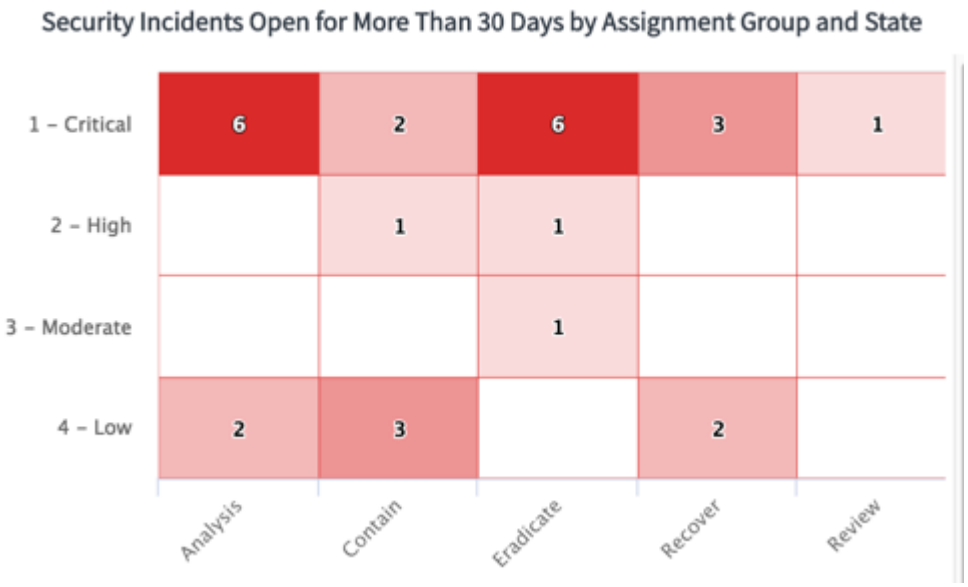
L'onglet Qualité des données comporte des filtres interactifs pour la catégorie de l'incident de sécurité et les niveaux de risque, de priorité et de gravité. Ces filtres sont appliqués simultanément aux indicateurs suivants :

Incidents de sécurité ouverts depuis plus de 30 jours par groupe d'affectation et par état

Nombre d'incidents de sécurité ouverts filtrés pour une période d'âge de 30 jours et répartis par groupe d'affectation et état.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Incidents de sécurité avec un délégataire qui n'est pas actif

Nombre d'incidents de sécurité ouverts sans délégataire ou avec un délégataire inactif.

Incidents de sécurité ouverts depuis plus de 30 jours par groupe d'affectation et par état

L'indicateur Nombre d'incidents de sécurité ouverts non mis à jour au cours des 30 derniers jours, répartis par groupe d'affectation et par état.

L'onglet KPI comporte les indicateurs supplémentaires suivants :

- % de nouveaux incidents de sécurité critiques
- Âge moyen des incidents de sécurité ouverts
- Délai moyen de clôture des incidents de sécurité
- % d'incidents de sécurité qui ont été réaffectés
- % d'incidents de sécurité clôturés lors de leur première affectation
- % d'incidents de sécurité clôturés par libre-service
- % d'incidents de sécurité non résolus
- Délai moyen de clôture des tâches d'incident de sécurité

Répartitions

Les répartitions suivantes s'appliquent aux indicateurs du tableau de bord :

- Groupe de sécurité
- Âge de l'incident de sécurité
- Catégorie d'incident de sécurité
- Priorité de l'incident de sécurité
- État de l'incident de sécurité

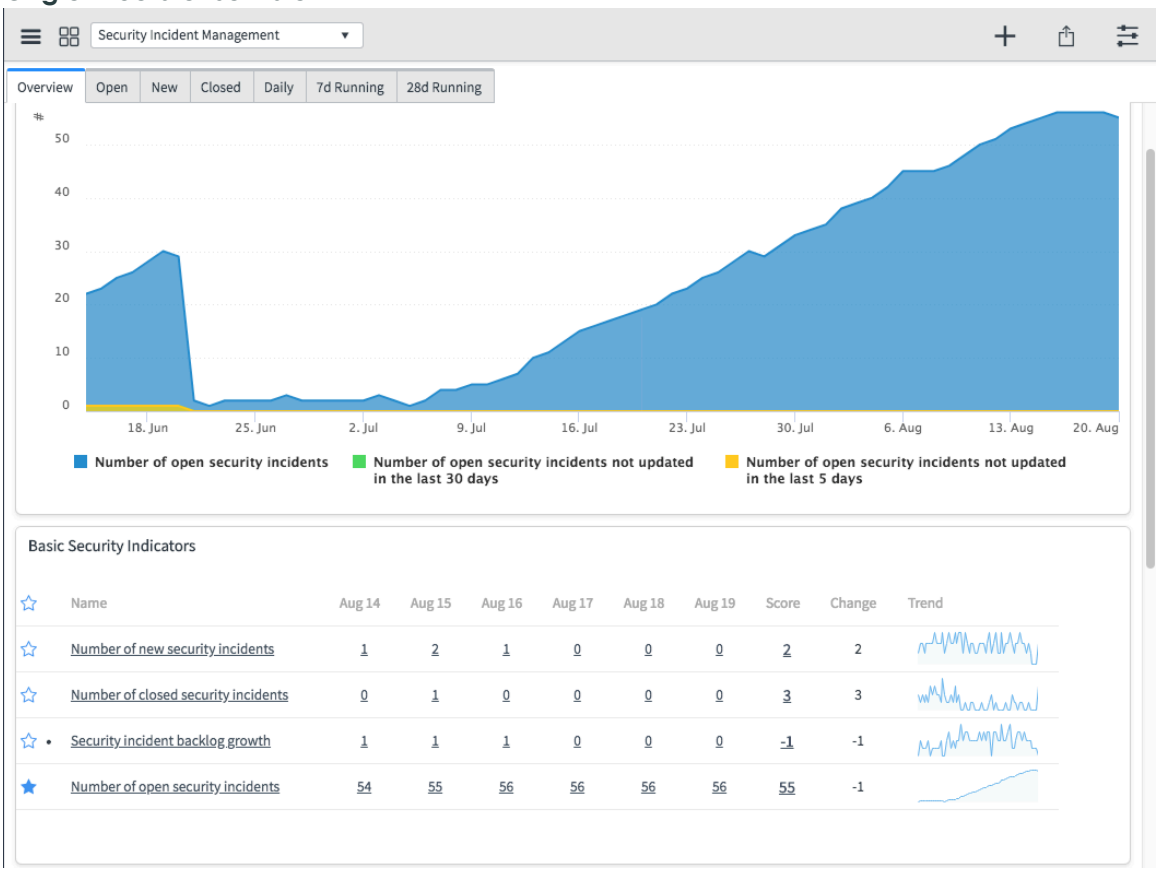
Tableau de bord Security Incident Management

Grâce à ce tableau de bord, les responsables de la sécurité peuvent facilement suivre le volume, les performances et la progression des incidents de sécurité, de l'analyse/détection initiale au confinement, à l'éradication et à la récupération.

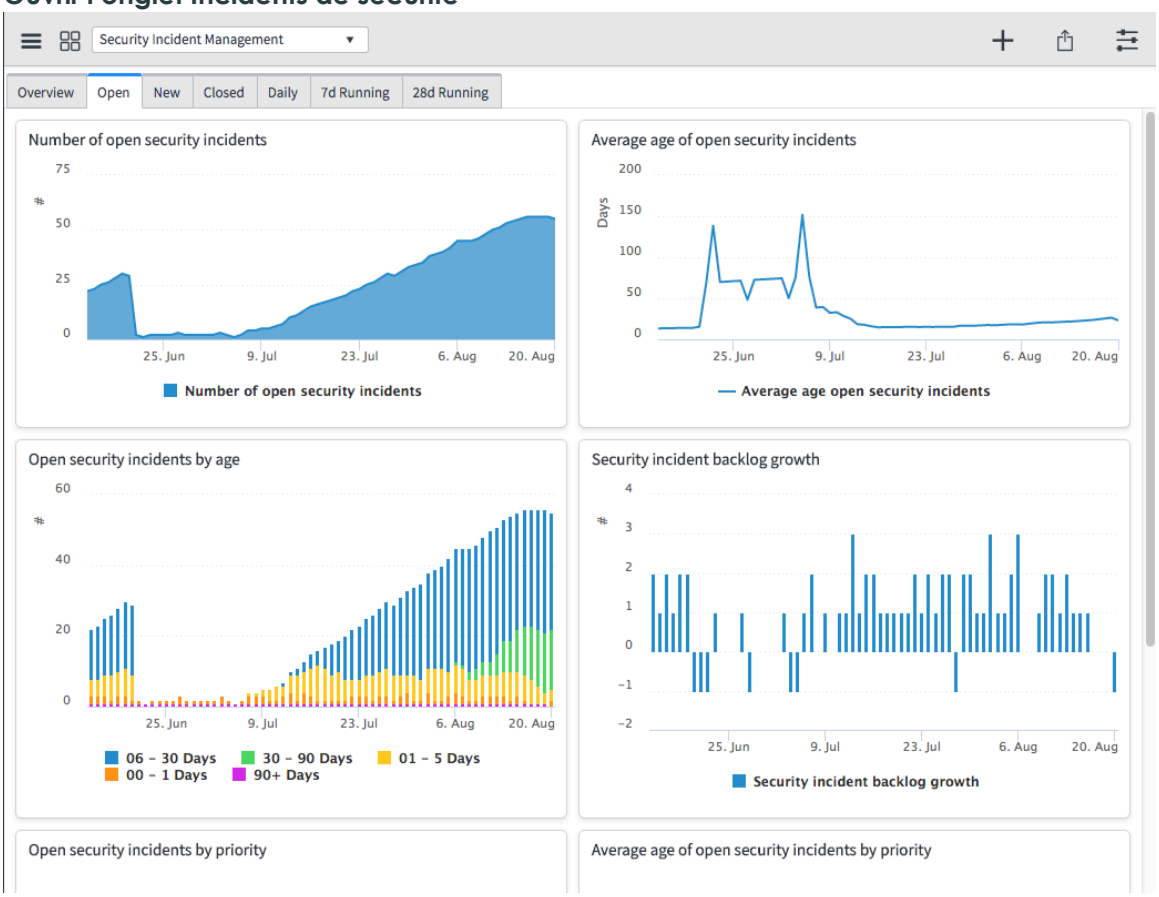
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble



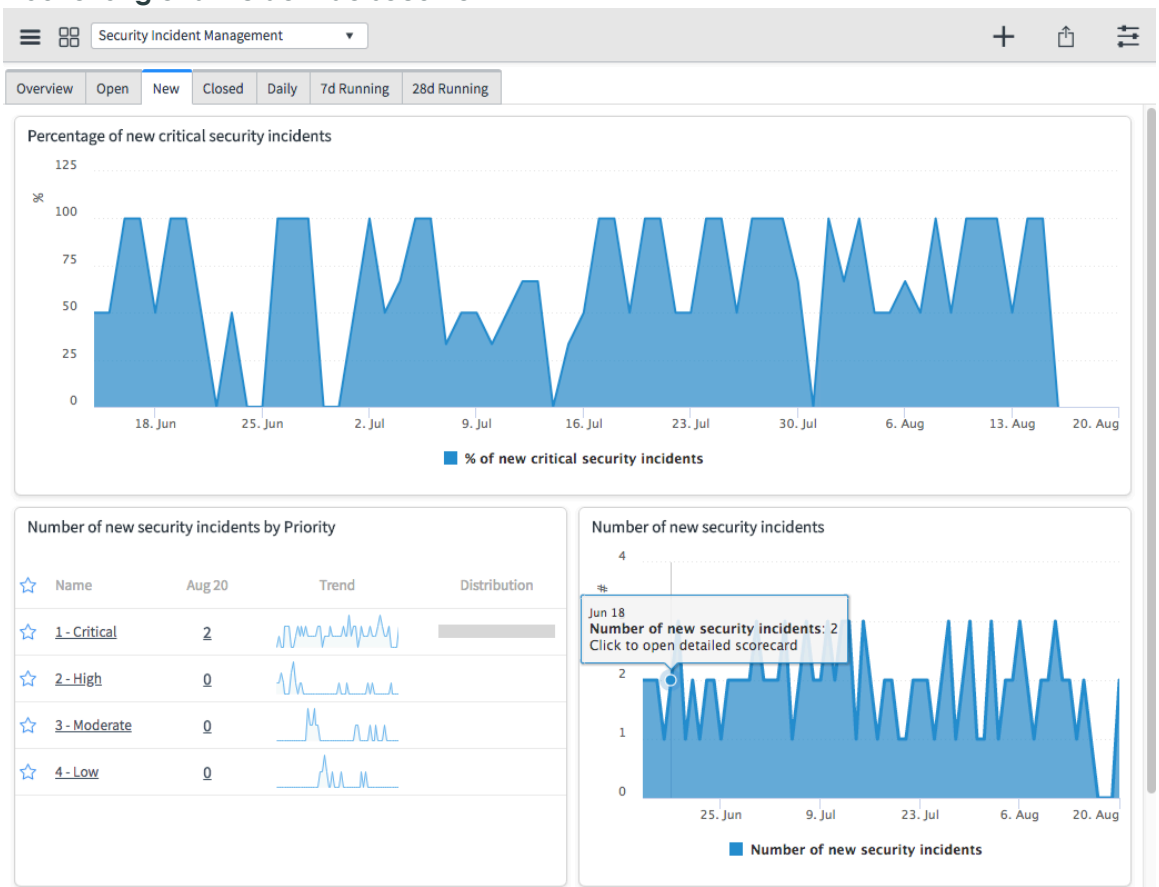
Ouvrir l'onglet Incidents de sécurité



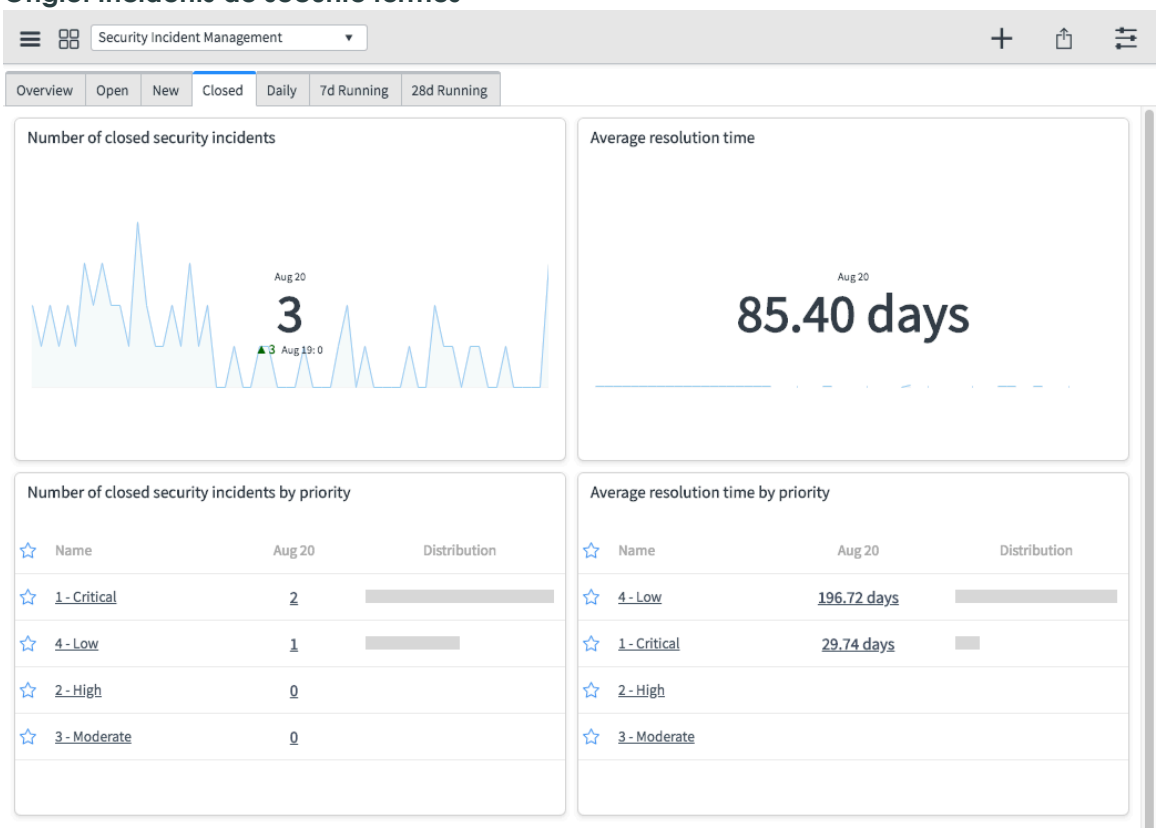
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nouvel onglet d'incident de sécurité



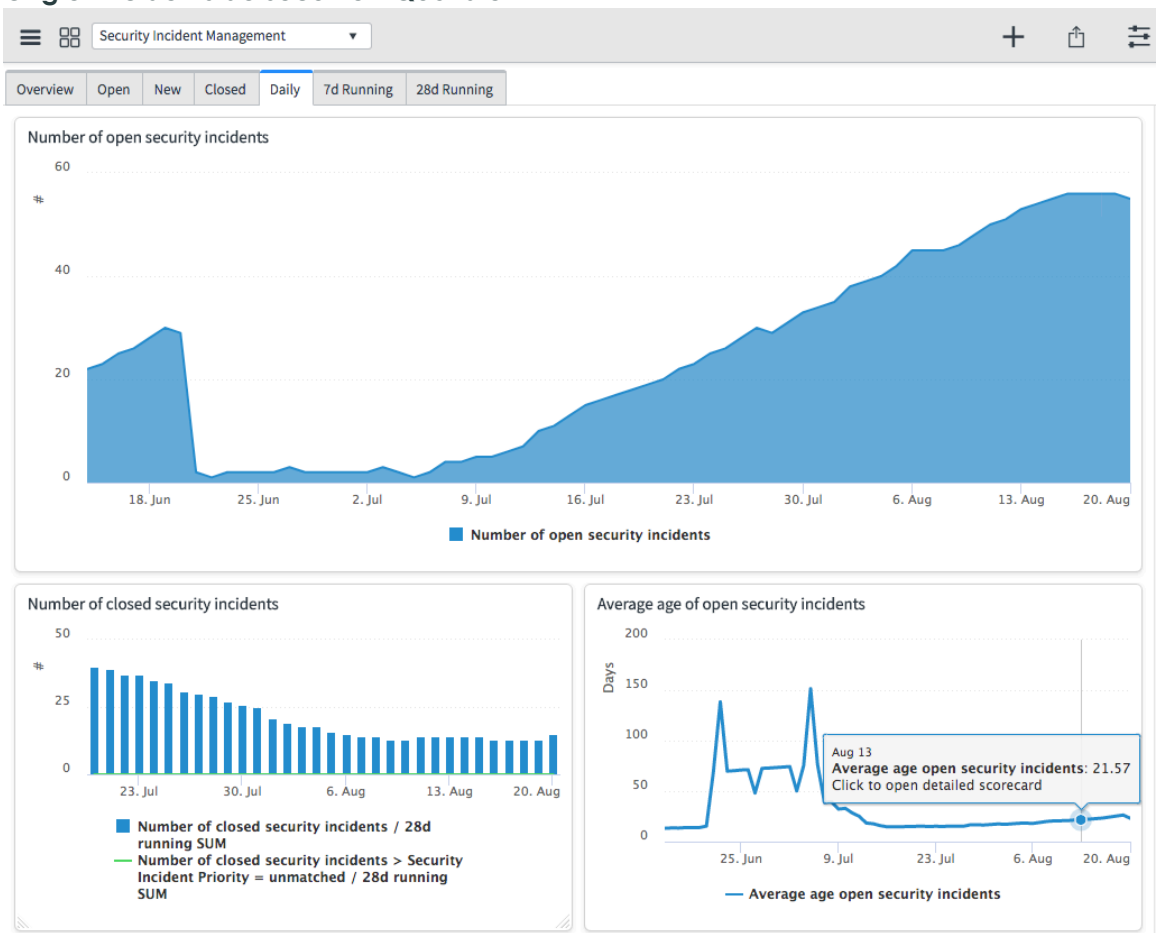
Onglet Incidents de sécurité fermés



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Incidents de sécurité - Quotidien



Les onglets **7 jours consécutifs** et **28 jours consécutifs** suivent le format de l'onglet **Quotidien** .

Utilisateurs finaux et rôles

Utilisateur final et objectif	Rôle requis	Avantages
Security Response Manager : a besoin d'une visibilité claire sur l'état global et le volume des incidents de sécurité associés aux applications et aux services.	sn_si.manager	Peut examiner la posture de sécurité globale avec la possibilité d'ajuster les membres des groupes d'affectation.
Administrateur Security Response : doit identifier rapidement les zones de préoccupation et avoir un contrôle total sur toutes les données de Security Incident Response tout en administrant les territoires et les compétences, selon les besoins.	sn_si.admin	Peut ajuster les paramètres de calcul des risques pour s'assurer que les éléments vulnérables les plus pertinents pour l'organisation sont traités en premier.
Analystes Security Response : ils doivent rapidement hiérarchiser les vulnérabilités	sn_si.analyst	Les analystes de sécurité de niveau 1 et 2 travaillent sur les incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur final et objectif	Rôle requis	Avantages
sur lesquelles se concentrer en fonction de la criticité pour l'organisation.		Ils peuvent créer et mettre à jour des incidents de sécurité, des demandes et des tâches, ainsi que des problèmes, des changements et des pannes liés à leurs incidents.

Indicateurs de Gestion des incidents de sécurité

Le tableau de bord Security Incident Management présente les indicateurs clés de performance suivants :

Nouveaux incidents de sécurité

Graphique du nombre de nouveaux incidents de sécurité.

Incidents de sécurité ouverts

Graphique dans lequel vous pouvez comparer le nombre d'incidents de sécurité ouverts, le nombre d'incidents de sécurité ouverts non mis à jour au cours des 30 derniers jours et le nombre d'incidents de sécurité ouverts non mis à jour au cours des 5 derniers jours.

Indicateurs de sécurité de base

Les scores des 6 derniers jours des indicateurs du nombre de nouveaux incidents de sécurité, du nombre d'incidents de sécurité fermés, de la croissance du backlog des incidents de sécurité et du nombre d'incidents de sécurité ouverts.

Nouveaux incidents de sécurité, par priorité

Nombre de nouveaux incidents de sécurité répartis par priorité.

Répartitions

Les répartitions suivantes s'appliquent aux indicateurs du tableau de bord :

- Groupe de sécurité
- Âge de l'incident de sécurité
- Catégorie d'incident de sécurité
- Priorité de l'incident de sécurité
- État de l'incident de sécurité

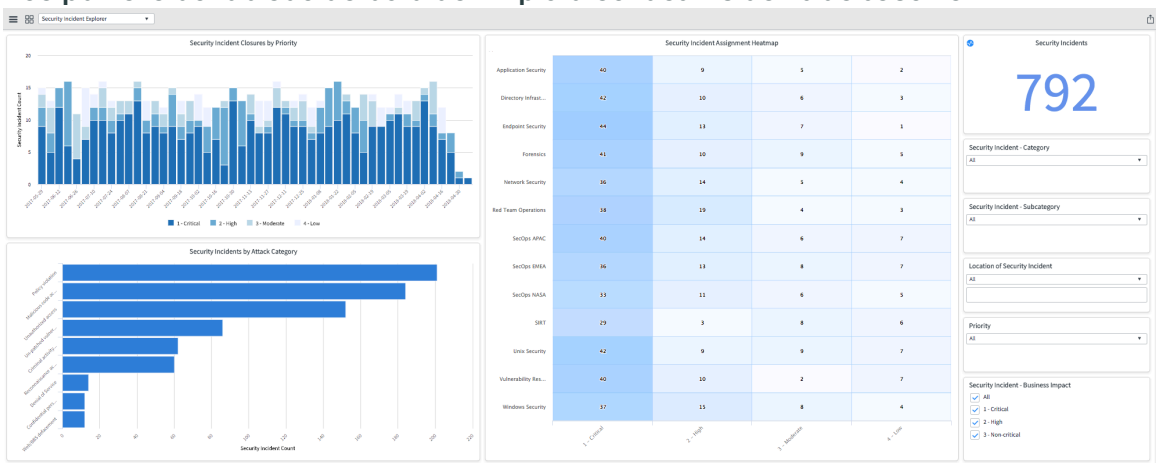
Tableau de bord de l'explorateur des incidents de sécurité

Grâce à ce tableau de bord, les gestionnaires de sécurité peuvent visualiser les incidents de sécurité résumés et regroupés par catégorie, sous-catégorie, emplacement, priorité et impact sur l'entreprise. Ces vues permettent aux gestionnaires d'avoir un aperçu rapide de la fréquence à laquelle les attaques se produisent et des services aux entreprises qui sont affectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue partielle du tableau de bord de l'Explorateur des incidents de sécurité



Utilisateurs finaux et rôles

Utilisateur final et objectif	Rôle requis	Avantages
Security Response Manager : a besoin d'une visibilité claire sur l'état global et le volume des incidents de sécurité associés aux applications et aux services.	sn_si.manager	Peut examiner la posture de sécurité globale avec la possibilité d'ajuster les membres des groupes d'affectation.
Administrateur Security Response : doit identifier rapidement les zones de préoccupation et avoir un contrôle total sur toutes les données de Security Incident Response tout en administrant les territoires et les compétences, selon les besoins.	sn_si.admin	Peut ajuster les paramètres de calcul des risques pour s'assurer que les éléments vulnérables les plus pertinents pour l'organisation sont traités en premier.
Les analystes Security Response doivent hiérarchiser rapidement les vulnérabilités sur lesquelles se concentrer en fonction de leur criticité pour l'organisation.	sn_si.analyst	Les analystes de sécurité de niveau 1 et 2 travaillent sur les incidents de sécurité. Ils peuvent créer et mettre à jour des incidents de sécurité, des demandes et des tâches, ainsi que des problèmes, des changements et des pannes liés à leurs incidents.

Indicateurs de l'Explorateur des incidents de sécurité

Le tableau de bord de l'Explorateur des incidents de sécurité présente les indicateurs clés de performance suivants :

Incidents de sécurité

Volume total d'incidents de sécurité ouverts et en attente.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fermetures d'incidents de sécurité par priorité

Nombre d'incidents de sécurité fermés répartis par priorité.

Incidents de sécurité par catégorie d'attaque

Nombre d'incidents de sécurité ouverts, répartis par catégorie.

Carte thermique d'affectation des incidents de sécurité

Répartition à deux niveaux du nombre d'incidents de sécurité ouverts, par groupe d'affectation et par priorité.

Carte thermique des incidents de sécurité

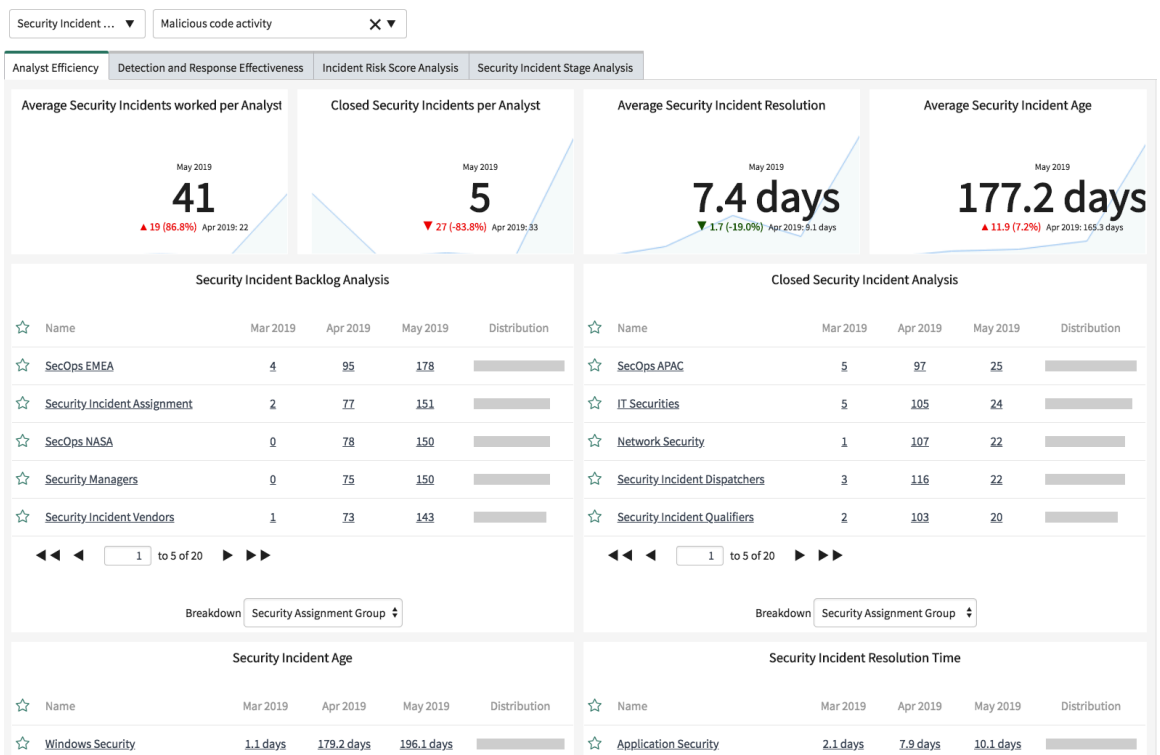
Carte mondiale montrant le nombre d'incidents de sécurité ouverts dans chaque pays.

Tableau de bord Security Operations Efficiency

Les responsables des centres des opérations de sécurité (SOC) peuvent consulter les mesures d'efficacité globales et mesurer les performances individuelles des membres de l'équipe SOC au sein de l'organisation.

Le responsable SOC peut utiliser le tableau de bord Analyse des performances pour améliorer l'efficacité et développer une image des performances du SOC dans des domaines généraux et spécifiques au fil du temps.

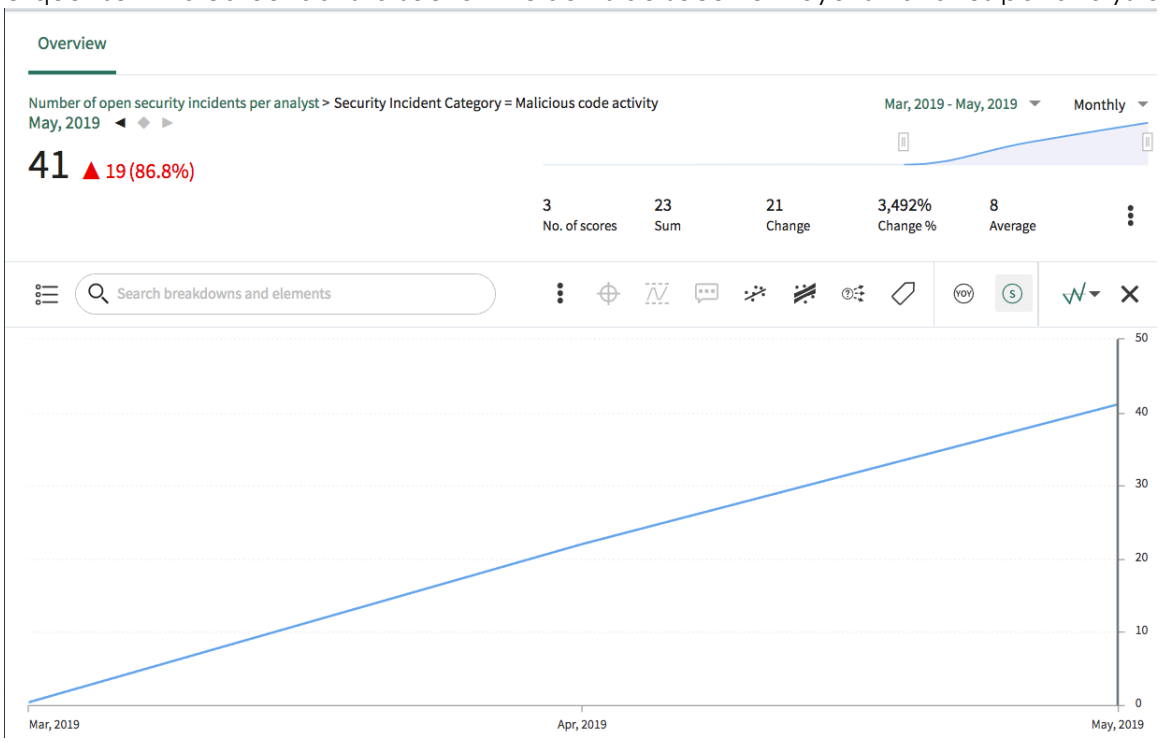
Onglet Efficacité de l'analyste



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cliquez sur l'un des indicateurs pour l'explorer et obtenir plus de détails. Par exemple, cliquez sur l'indicateur dans la section Incidents de sécurité moyens travaillés par analyste.



Le graphique montre que le nombre d'incidents de sécurité ouverts est passé de 0 en mars à plus de 40 en mai. Notez les données affichées dans l'en-tête :

- Indicateur de tendance : affiche la variation du nombre d'incidents ouverts au cours de la dernière période pour laquelle les données ont été collectées. Ce graphique montre les données pour la période de mars 2019 à mai 2019 et le nombre d'incidents ouverts a augmenté de 19 au cours du mois de mai. L'efficacité des analystes est meilleure si le nombre d'incidents ouverts a diminué au fil du temps.
- Non. des scores : La période pour laquelle les données ont été collectées (mars à mai 2019).
- Somme : nombre de nouveaux incidents ouverts pour la période comprise entre mars et mai.
- Changement : nombre de nouveaux incidents ouverts entre mars et avril.
- Moyenne : nombre moyen d'incidents ouverts par analyste pour la période sélectionnée.

Onglet Efficacité de l'analyste

Indicateur	Description
Nombre moyen d'incidents de sécurité travaillés par analyste	Nombre moyen d'incidents de sécurité ouverts par analyste pour la période spécifiée. La formule utilisée est `la suivante : [[nombre d'incidents de sécurité ouverts / MOY par mois +]] / [[nombre d'agents de sécurité]]`
Incidents de sécurité fermés par analyste	Nombre total d'incidents fermés par chaque analyste dans la catégorie sélectionnée au cours de la période spécifiée. La formule utilisée est `la suivante : [Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité = <category_name> / SOMME par mois +]] / [[Nombre d'agents de sécurité / MOY par mois +]]`

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Efficacité de l'analyste (suite)

Indicateur	Description
Résolution moyenne des incidents de sécurité	Délai moyen nécessaire à chaque analyste pour fermer les incidents de sécurité au cours de la période spécifiée. La formule utilisée pour afficher le résultat en jours est `la suivante : [[durée cumulée des incidents de sécurité fermés > catégorie d'incident de sécurité = <category_name> / MOY par mois +]] / [[nombre d'incidents de sécurité fermés > catégorie d'incident de sécurité = <category_name> / MOY par mois +]]) / 24`
Âge moyen de l'incident de sécurité	Nombre moyen de jours pendant lesquels les incidents de sécurité restent ouverts pour chaque analyste. La formule utilisée pour afficher le résultat en jours est `la suivante : [[Âge cumulé des incidents de sécurité ouverts > catégorie d'incident de sécurité = <category_name> / MOY par mois +]] / [[Nombre d'incidents de sécurité ouverts > catégorie d'incident de sécurité = <category_name> / MOY par mois +]]) / 24`
Analyse en backlog d'incidents de sécurité	Nombre total d'incidents de sécurité ouverts au cours de la période spécifiée. Sélectionnez une option dans la liste Répartition pour afficher les backlogs pour chaque analyste, groupe de sécurité, priorité, etc. Vous pouvez également comparer le nombre d'incidents de sécurité ouverts entre deux mois sélectionnés.
Analyse des incidents de sécurité fermés	Nombre total d'incidents de sécurité qui sont fermés au cours de la période spécifiée. Sélectionnez une option dans la liste Répartition pour afficher le nombre de chaque analyste, groupe de sécurité, priorité, etc. Vous pouvez également comparer le nombre d'incidents de sécurité qui ont été fermés entre deux mois sélectionnés.
Âge de l'incident de sécurité	Nombre moyen de jours pendant lesquels les incidents de sécurité restent ouverts au cours de la période spécifiée. Sélectionnez une option dans la liste Répartition pour afficher l'âge de l'incident de sécurité pour chaque analyste, groupe de sécurité, priorité, et ainsi de suite. La formule utilisée pour afficher le résultat en jours est `la suivante : [[âge cumulé des incidents de sécurité ouverts > catégorie d'incident de sécurité = <category_name> > groupe d'affectation de sécurité = <group_name> / MOY par mois +]] / [[nombre d'incidents de sécurité ouverts > catégorie d'incident de sécurité = <category_name> > groupe d'affectation de sécurité = <group_name> / MOY par mois +]]) / 24`
Délai de résolution des incidents de sécurité	Nombre moyen de jours consacrés à la résolution des incidents de sécurité au cours de la période spécifiée. Sélectionnez une option dans la liste Répartition pour afficher le délai de résolution des incidents de sécurité pour chaque analyste, groupe de sécurité, priorité, etc. La formule utilisée pour afficher le résultat en jours est `la suivante : [[Durée cumulée des incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité affectée à = John Ashby / MOY par mois +]] / [[Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité`

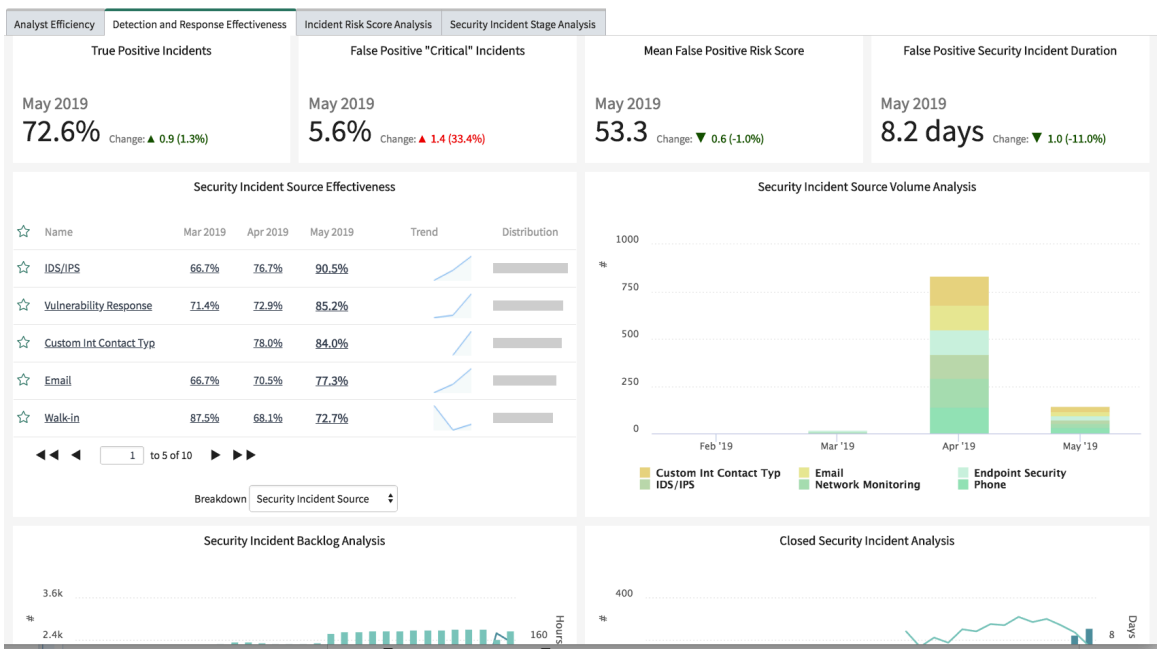
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Efficacité de l'analyste (suite)

Indicateur	Description
	= Activité du code malveillant > Sécurité affectée à = John Ashby / MOY par mois +]]) / 24

Onglet Efficacité de la détection et de la réponse



Onglet Efficacité de la détection et de la réponse

Indicateur	Description
Incidents vrais positifs	Pourcentage d'incidents de sécurité vrais positifs dans la catégorie sélectionnée pour la période spécifiée. La formule utilisée est la suivante : (1-([[Nombre d'incidents de sécurité signalés comme faux positifs > Catégorie d'incident de sécurité = Activité du code malveillant / SOMME par mois +]] / [[Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant / SOMME par mois +]])) * 100
Incidents critiques signalés comme faux positifs	Pourcentage d'incidents de sécurité critiques signalés comme faux positifs dans la catégorie sélectionnée pour la période spécifiée. La formule utilisée est la suivante : ([[Nombre d'incidents de sécurité signalés comme faux positifs > Score de risque d'incident de sécurité = Risque critique > Catégorie d'incident

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Efficacité de la détection et de la réponse (suite)

Indicateur	Description
	`de sécurité = Activité du code malveillant / SOMME par mois +]] / [[Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant / SOMME par mois +]]) * 100` **Remarque :** Tout incident de sécurité dans lequel le `code Fermé = Vulnérabilité non valide ou Faux positif` est traité comme un incident de faux positif
Score moyen de risque faux positif	Score de risque mensuel moyen des incidents de sécurité clôturés qui ont été identifiés comme des incidents de faux positif. Un score de risque plus faible indique que les analystes de sécurité ont passé moins de temps à analyser les incidents de faux positif. La formule utilisée est `la suivante : ([[Nombre d'incidents de sécurité signalés comme faux positifs > Score de risque d'incident de sécurité = Risque critique > Catégorie d'incident de sécurité = Activité du code malveillant / SOMME par mois +]] / [[Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant / SOMME par mois +]]) * 100`
Durée de l'incident de sécurité signalé comme faux positif	Nombre moyen de jours que les analystes de sécurité ont consacrés à l'enquête sur les incidents de faux positif. La formule utilisée est `([[durée cumulée des incidents de sécurité faux positifs]] / [[nombre d'incidents de sécurité signalés comme faux positifs]]) / 24`
Efficacité des sources d'incidents de sécurité	Pourcentage d'incidents de sécurité vrais positifs identifiés par une source spécifique pour la période spécifiée. La source peut être l'e-mail, l'activité réseau, le support client, etc. Ces données permettent de mesurer l'efficacité de la source d'incident de sécurité. La formule utilisée est `la suivante : (1-([[Nombre d'incidents de sécurité signalés comme faux positifs > Catégorie d'incident de sécurité = Activité du code`

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

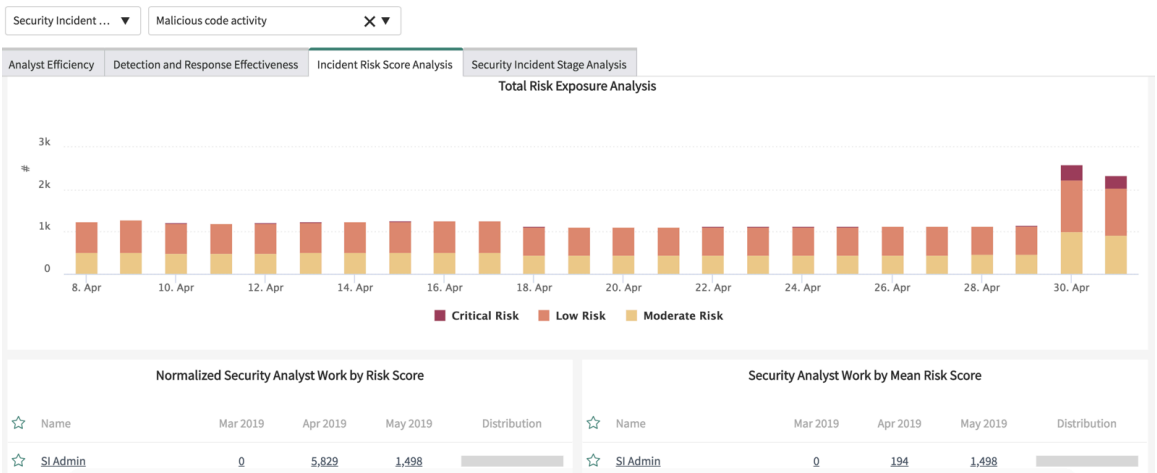
Onglet Efficacité de la détection et de la réponse (suite)

Indicateur	Description
	`malveillant > Source d'incident de sécurité = IDS/IPS / SOMME par mois +]] / [[Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant > Source d'incident de sécurité = IDS/IPS / SOMME par mois +]])) * 100`
Analyse du volume source des incidents de sécurité	Nombre d'incidents de sécurité fermés pour le mois en cours pour chaque source d'incident de sécurité. Vous pouvez également comparer le nombre d'incidents de sécurité pour chaque type de source entre deux mois sélectionnés.
Analyse en backlog d'incidents de sécurité	Nombre total d'incidents de sécurité ouverts au cours de la période spécifiée et nombre moyen de jours pendant lesquels les incidents restent ouverts. Vous pouvez également comparer le nombre d'incidents de sécurité ouverts entre deux mois sélectionnés. La formule utilisée pour calculer la période moyenne du backlog est la suivante : `[[Âge cumulé des incidents de sécurité ouverts > Catégorie des incidents de sécurité = Activité du code malveillant]] / [[Nombre d'incidents de sécurité ouverts > Catégorie des incidents de sécurité = Activité du code malveillant]]) / 24`
Analyse des incidents de sécurité fermés	Nombre total d'incidents de sécurité fermés au cours de la période spécifiée et délai moyen de résolution de ces incidents. La formule utilisée pour calculer le délai de résolution moyen est `la suivante : [[Durée cumulée des incidents de sécurité fermés > Catégorie des incidents de sécurité = Activité du code malveillant]] / [[Nombre d'incidents de sécurité fermés > Catégorie des incidents de sécurité = Activité du code malveillant]]) / 24`

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Analyse du score de risque d'incident



Onglet Analyse du score de risque d'incident

Indicateur	Description
Analyse totale de l'exposition au risque	Nombre total d'incidents ouverts dans chaque catégorie de risque (faible, modéré et critique) au cours de la période spécifiée. Vous pouvez également comparer le nombre d'incidents dans les différentes catégories de risque entre deux mois.
Travail normalisé d'analyste de sécurité par score de risque	Le score de risque total pour chaque analyste de sécurité pour la période spécifiée. Cette valeur est calculée en fonction du nombre d'incidents de sécurité vrais positifs que l'analyste de sécurité a fermés. La formule utilisée est `la suivante : [[Cumul des scores de risque des incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité affectée à = Administrateur SI / SOMME par mois +]] - [[Score de risque cumulé d'incidents de sécurité signalés comme faux positifs > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité affectée à = Administrateur SI / SOMME par mois +]]`
Travail d'analyste de sécurité par score de risque moyen	Score de risque moyen pour chaque analyste de sécurité pour la période spécifiée. La formule utilisée est `la suivante : [[Cumul des scores de risque des incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité affectée à = Administrateur SI / MOY par`

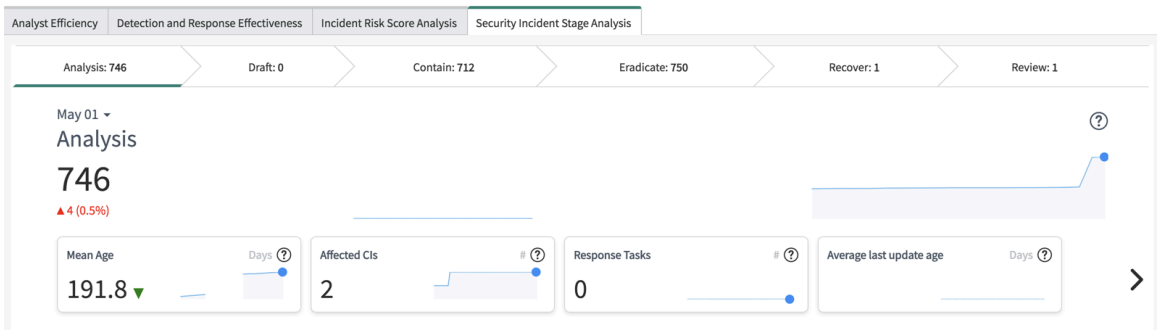
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Analyse du score de risque d'incident (suite)

Indicateur	Description
	mois +]] – [[Score de risque cumulé d'incidents de sécurité signalés comme faux positifs > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité affectée à = Administrateur SI / MOY par mois +]]

Onglet Analyse de l'étape de l'incident de sécurité



Vous pouvez afficher le nombre d'incidents ouverts un jour spécifique et l'état (analyse, brouillon, contenir, éliminer, récupérer ou examiner) de ces incidents. À chaque étape, vous pouvez afficher l'âge moyen, les CI affectés, les tâches de réponse, etc. Cliquez sur un lien pour afficher des détails supplémentaires ou la répartition de ces incidents.

Espace de travail de la Réponse aux incidents de sécurité

Il s'agit ServiceNow® Espace de travail de la Réponse aux incidents de sécurité d'une interface réinventée qui offre une expérience utilisateur de nouvelle génération aux analystes de la sécurité et aux responsables SOC. Les analystes de sécurité peuvent l'utiliser pour gérer le cycle de vie des incidents de sécurité, de l'analyse initiale à l'émancipation, à l'éradication et à la récupération.

Introduction à SIR Workspace

Sélectionnez une tuile pour commencer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer l’espace de travail



En savoir plus sur les concepts et les fonctionnalités de l’espace de travail SIR

Administrateurs utilisant l’espace de travail



Configurer l’espace de travail et les fonctionnalités SIR

Analystes utilisant Workspace



Découvrez comment les analystes utilisent l’espace de travail SIR

Afficher les tableaux de bord SIR



Afficher les tableaux de bord de l’espace de travail SIR

Traduction automatique

Demander des applications dans l’App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays. D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Important :

- L'installation de la Réponse aux incidents de sécurité version 13.4.5 ou ultérieure à partir de installe ServiceNow Store automatiquement la version 1.5.1 ou ultérieure Espace de travail de la Réponse aux incidents de sécurité (sn_si_aw) par défaut. Pour plus d'informations sur les applications dépendantes, reportez-vous à la SIR Workspace Modules d'extension et rôles section.
- Veuillez noter que les versions 1.5.1 et supérieures de l'espace de travail Réponse aux incidents de sécurité ne peuvent être installées/mises à niveau que via une installation/mise à niveau de Réponse aux incidents de sécurité et ne peuvent pas être installées indépendamment.

Plus de ressources

Visitez le Réponse aux incidents de sécurité forum sur le ServiceNow Community.

Explorer SIR Workspace

Explorez Espace de travail de la Réponse aux incidents de sécurité pour comprendre comment les analystes et les gestionnaires de sécurité effectuent leurs opérations quotidiennes avec une expérience utilisateur améliorée, effectuez une enquête complète sur les incidents et obtenez une vue d'ensemble des incidents de sécurité, des tâches de réponse et des SLA affectés à l'analyste et à l'équipe de sécurité.

Cette section décrit les points suivants :

- SIR Workspace Modules d'extension et rôles requis.
- Caractéristiques principales SIR Workspace .

SIR Workspace Modules d'extension et rôles

Voici les applications requises pour travailler avec Espace de travail de la Réponse aux incidents de sécurité le module d'extension (sn_si_aw).

Applications

L'installation de la Réponse aux incidents de sécurité version 13.4.5 ou ultérieure de l'application installe automatiquement les applications suivantes Espace de travail de la Réponse aux incidents de sécurité

- Gestion des tickets de sécurité d'entreprise PAD Commons [sn_escm_pad_cmn]
- Espace de travail commun Security Operations [sn_escm_ws_cmn]
- Incident de sécurité - Composant de la carte d'interface utilisateur [sn_sirw_evam]
- Spoke Security Operations [sn_sec_spoke]

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

- L'installation de la Réponse aux incidents de sécurité version 13.4.5 ou ultérieure à partir de installe ServiceNow Store automatiquement la version 1.5.1 ou ultérieure Espace de travail de la Réponse aux incidents de sécurité (sn_si_aw) par défaut. Pour plus d'informations sur les applications dépendantes, reportez-vous à la SIR Workspace Modules d'extension et rôles section.
- Veuillez noter que les versions 1.5.1 et supérieures de l'espace de travail Security Incident Response ne peuvent être installées/mises à niveau que via une installation/ mise à niveau de Security Incident Response et ne peuvent pas être installées indépendamment.

Enterprise Security Case Management PAD Commons nécessite le module d'extension Expérience de playbook [playbook_experience].

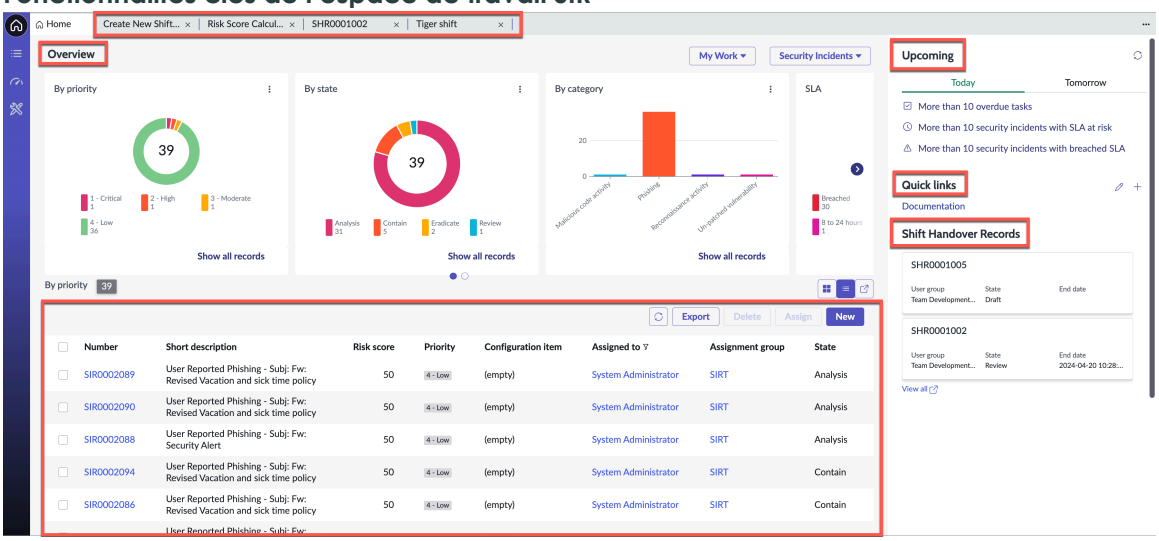
Pour en savoir plus sur les rôles, les tables, les propriétés et les Réponse aux incidents de sécurité travaux planifiés, consultez Composants installés avec Réponse aux incidents de sécurité

Fonctionnalités de l'espace de travail SIR

Il Espace de travail de la Réponse aux incidents de sécurité se compose des fonctionnalités clés suivantes.

- Section Vue d'ensemble
- Section À venir
- Section Liens rapides
- Section des enregistrements de transfert d'équipe
- Vue liste
- Interface multionglet qui prend en charge l'ouverture de plusieurs incidents de sécurité

Fonctionnalités clés de l'espace de travail SIR



SIR Workspace Vue d'ensemble de l'interface

La SIR Workspace page Vue d'ensemble contient les détails des incidents de sécurité et des tâches de réponse qui se trouvent sous les analystes de sécurité et leur équipe.

Traduction automatique

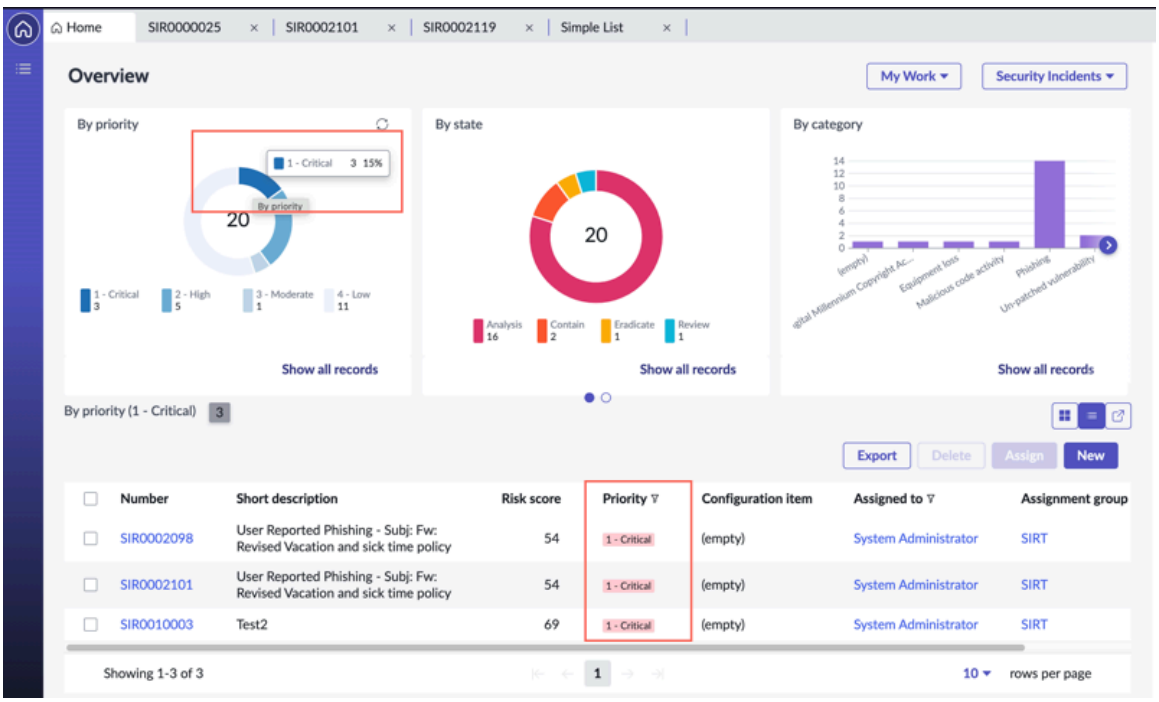
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sous chaque filtre, différents widgets sont regroupés par priorité, catégorie, état et SLA, qui se trouvent dans les files d'attente des analystes de sécurité et dans la file d'attente de l'équipe d'analystes de sécurité.

Lorsque des filtres sont appliqués aux widgets, la moitié inférieure de la page de vue d'ensemble est renseignée avec les incidents de sécurité ou les tâches de réponse correspondants, présentés sous forme de cartes ou d'éléments de liste. L'analyste peut basculer entre la vue de carte ou la vue de liste comme il le souhaite.

Par exemple, dans le widget **Priorité** , si vous souhaitez sélectionner tous les incidents critiques ou les tâches de réponse, cliquez sur le segment **Critique** (exemple de capture d'écran ci-dessous) du widget et les incidents ou tâches de réponse critiques s'affichent dans la vue de liste ou de carte.

Section Vue d'ensemble

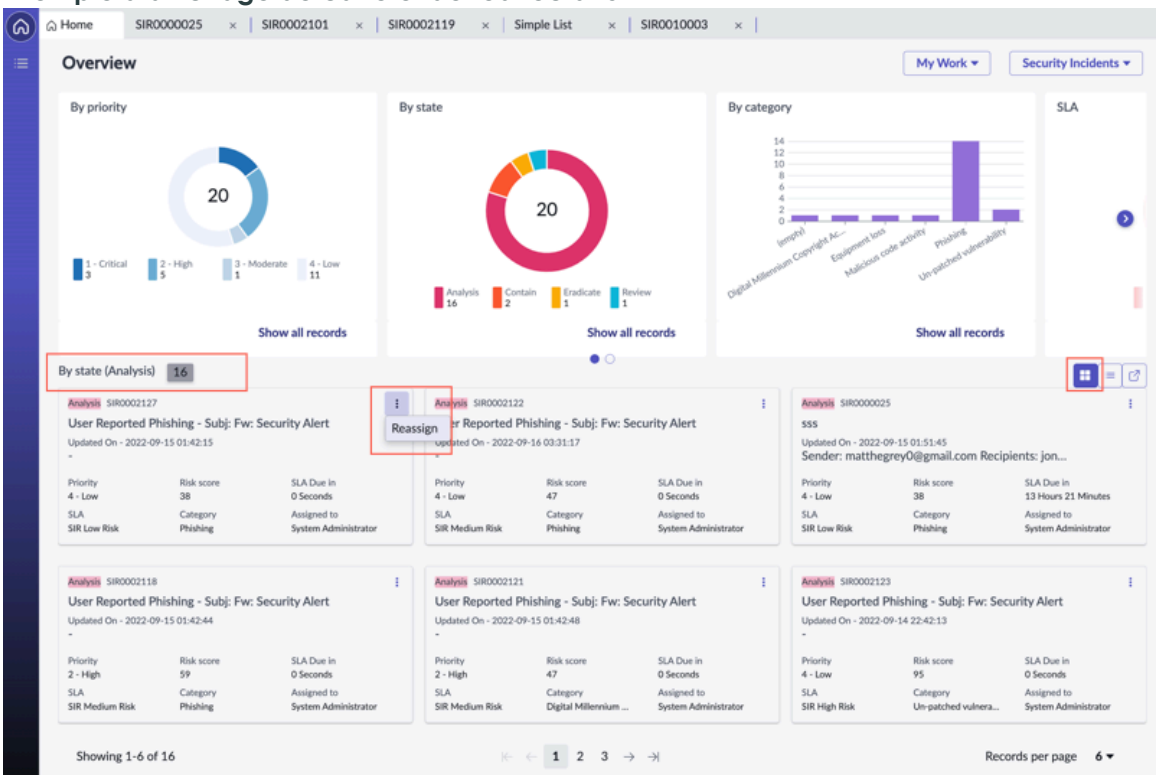


Vous pouvez affecter ou réaffecter les incidents de sécurité ou les tâches de réponse directement à partir de cette vue en cliquant sur l'icône en forme de ellipse et en sélectionnant le bouton **Affecter** (option dans la vue de carte) ou directement le bouton **Affecter** (option dans la vue de liste) en conséquence pour affecter un incident.

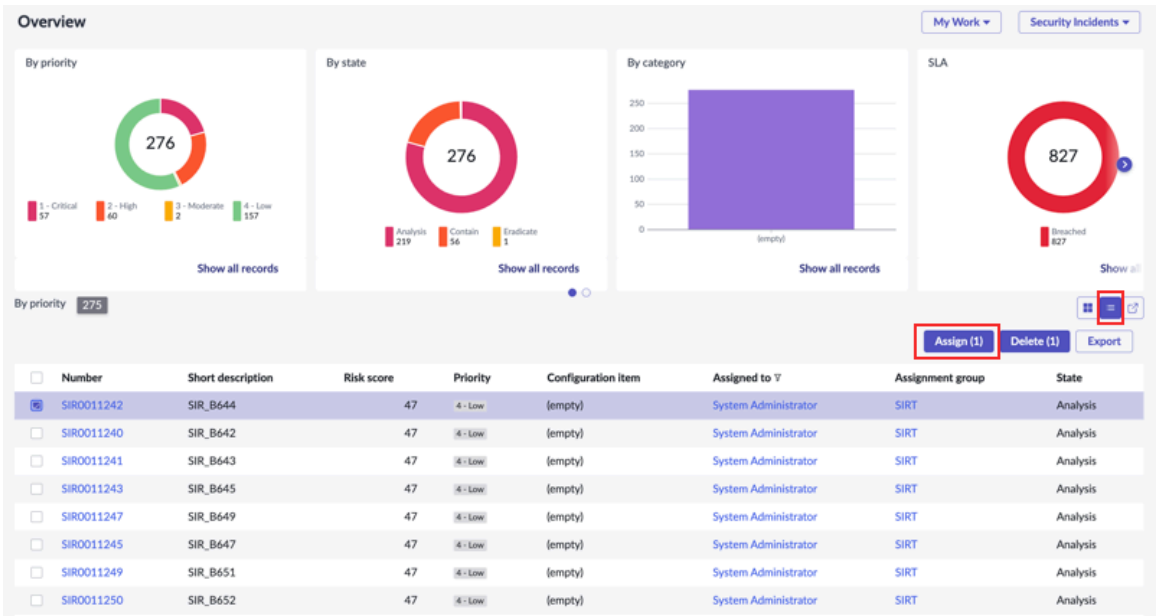
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple d'affichage de carte et de réaffectation



Affecter l'incident

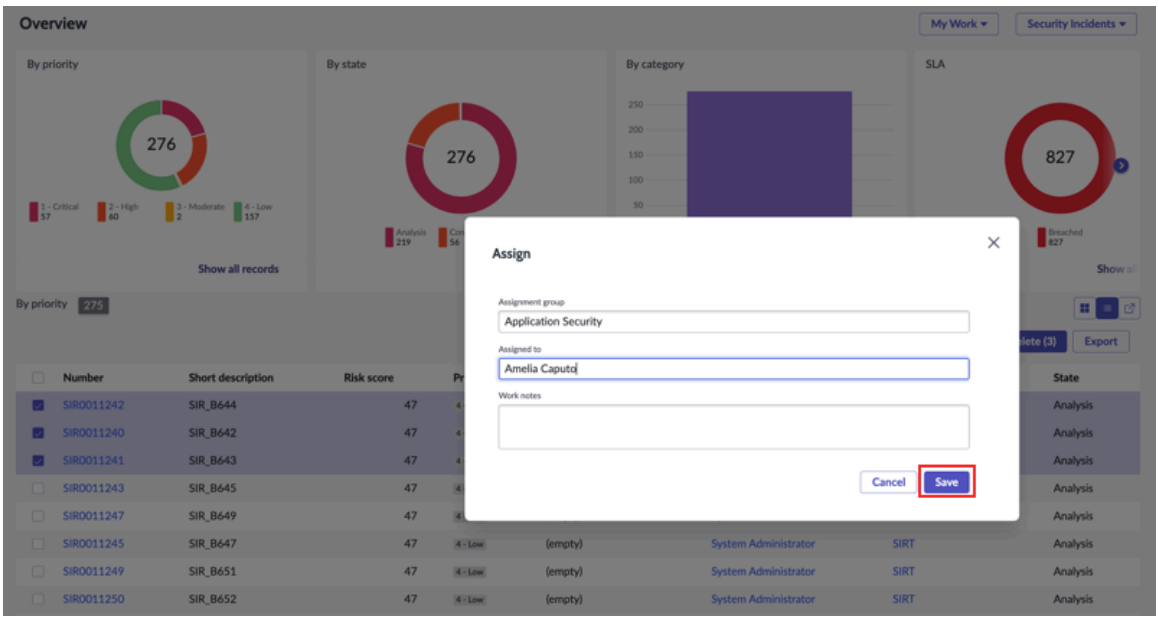


Voici un exemple de vue de liste. L'utilisateur peut également affecter des incidents à partir de la vue de liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affecter l'incident



Ajoutez ou modifiez les détails du délégataire, tels que le groupe d'affectation et Affecté à, puis ajoutez des notes de travail, si nécessaire.

Remarque : Vous pouvez affecter un ou plusieurs incidents de sécurité ou tâches de réponse aux groupes d'affectation. Le numéro sélectionné s'affiche sur le bouton **Attribuer** .

L'utilisateur peut supprimer des incidents de sécurité à partir de cette vue. Cliquez sur le bouton **Supprimer** pour supprimer l'incident de sécurité, l'enregistrement sera supprimé de la vue de liste.

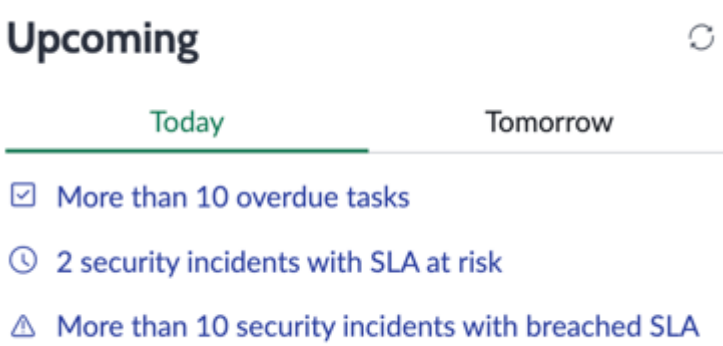
L'utilisateur peut également exporter le contenu de la liste. Cliquez sur le bouton **Exporter** pour exporter la liste au format souhaité.

Section À venir

Cette section affiche les tâches à venir telles que les incidents de sécurité et les tâches de réponse qui sont dues le jour même et le jour suivant.

La liste des incidents de sécurité et des tâches de réponse qui s'affiche est basée sur le champ de date d'échéance et la définition de SLA définis pour ces enregistrements.

Si cette section contient plusieurs tâches de réponse ou d'incident de sécurité, l'incident ou les enregistrements ouvrent tous ces enregistrements dans un nouvel onglet.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les tâches à venir

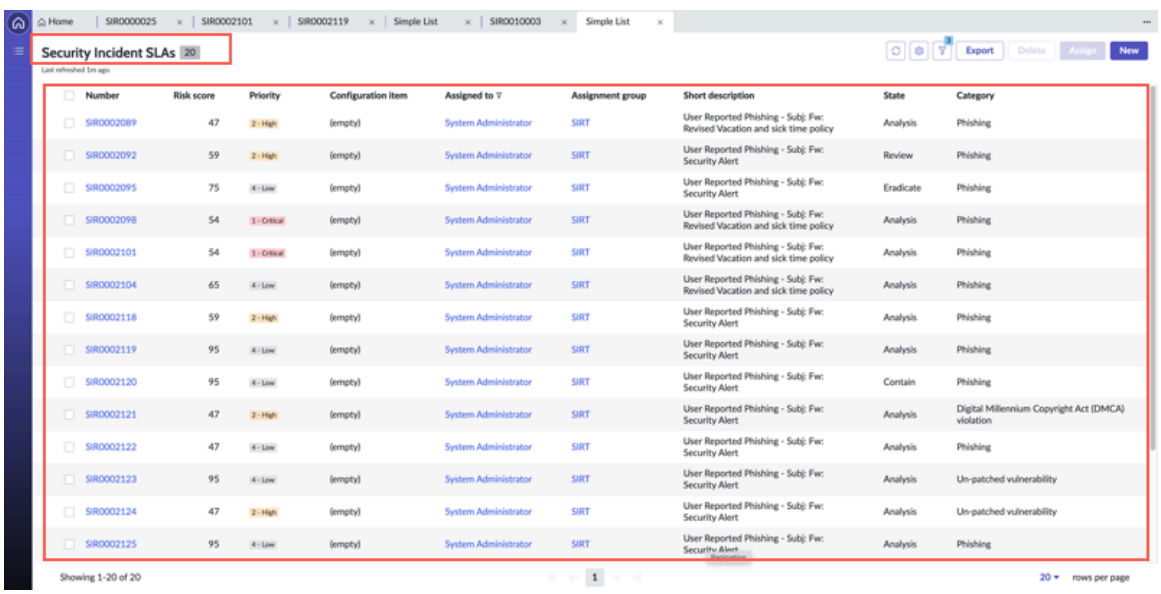
L'analyste de la sécurité peut afficher les tâches à venir liées aux incidents de sécurité et aux tâches de réponse qui sont dues, en retard ou qui ne respectent pas le SLA défini.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **À venir**.
2. Cliquez sur l'onglet **Aujourd'hui** pour afficher les tâches dues le même jour.
3. Sélectionnez **l'onglet Demain** pour afficher les tâches en retard pour le lendemain.
   La section À venir répertorie les incidents de sécurité ou les tâches de réponse qui sont en retard en fonction de la date d'échéance et qui ont enfreint la définition de SLA.
4. Cliquez sur l'icône **Actualiser** pour actualiser la liste des sections à venir.
   Par exemple, si vous cliquez sur le lien, **Plus de 10 incidents de sécurité avec violation de SLA** La liste des incidents de SLA violés s'affiche dans un nouvel onglet de l'espace de travail.



Remarque : Vous pouvez effectuer les opérations Nouveau, Affecter, Exporter et Supprimer à partir de n'importe quelle vue de liste.

Section Liens rapides

Les liens rapides fonctionnent comme des liens de signet. Vous pouvez ajouter des URL externes et y accéder rapidement à partir de l'espace de travail.

Utilisation de liens rapides

Ajoutez des liens rapides pour une référence facile.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

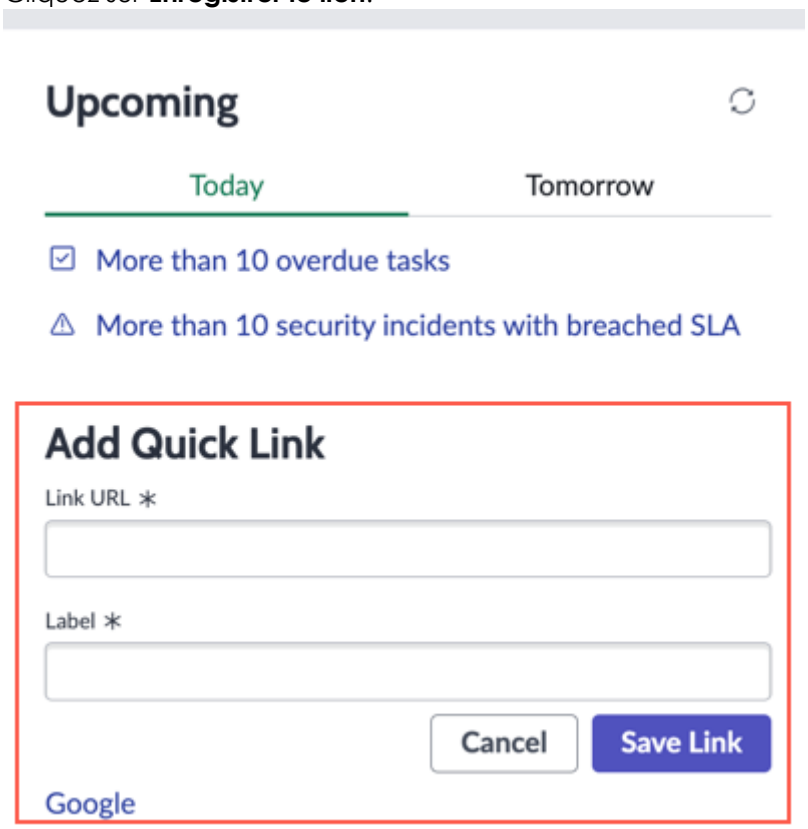
Vous pouvez ajouter et modifier des liens rapides utiles et les mettre en signet afin d'aider à la résolution de l'incident.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Liens rapides**.
2. Cliquez sur l'icône **Ajouter un lien rapide** pour ajouter les liens.
3. Entrez le lien vers l'URL et l'étiquette.
4. Cliquez sur **Enregistrer le lien**.



Le nouveau lien est ajouté sous la section des liens rapides.

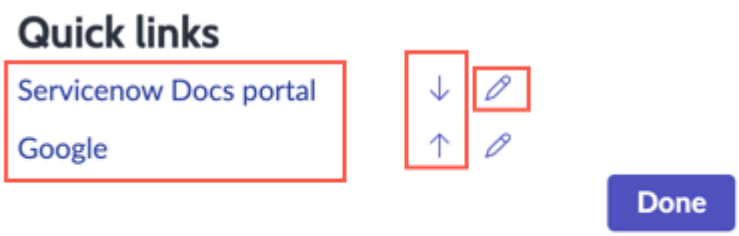
5. **Pour modifier ou supprimer les liens :**

   a. Cliquez sur **l'icône Modifier le lien** .

   b. Modifiez le lien souhaité ou affichez le texte qui est l'étiquette de l'URL.

   c. Cliquez sur **Enregistrer**.

   d. Cliquez sur **Terminé**.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Utilisez les flèches vers le haut et vers le bas pour déplacer la position des liens.

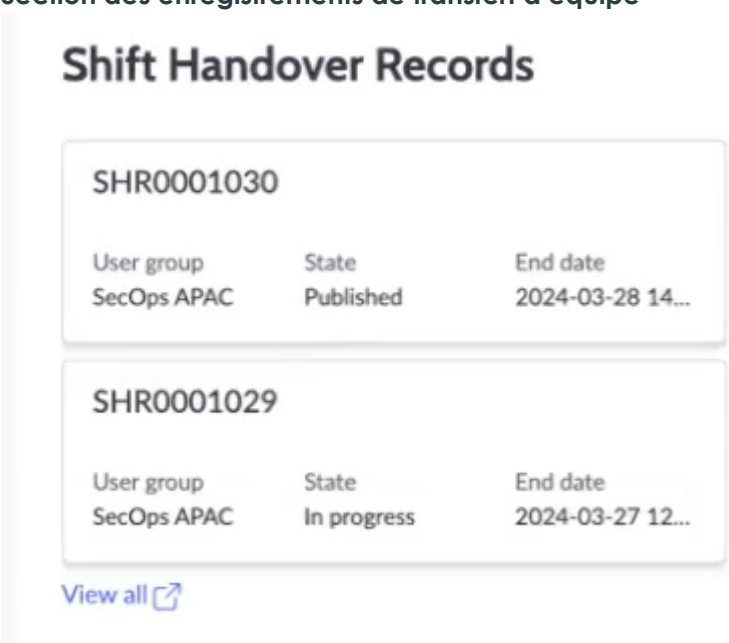
f. Cliquez sur **Supprimer** pour supprimer les liens qui ont été signets lors de la modification.

Section des enregistrements de transfert d'équipe

La section affiche la liste des enregistrements de transfert d'équipe dans l'espace de travail Réponse aux incidents de sécurité.

La section Enregistrements de transfert d'équipe de l'espace de travail Réponse aux incidents de sécurité affiche les deux derniers enregistrements de transfert d'équipe en fonction des champs Date de fin, État et Groupe d'utilisateurs définis pour ces enregistrements. Pour afficher tous les enregistrements de transfert d'équipe, sélectionnez **Afficher tout**.

Section des enregistrements de transfert d'équipe



Vue de liste dans SIR Workspace

La vue de liste comprend les incidents de sécurité, les tâches de réponse, les e-mails d'hameçonnage et les évaluations.

La vue de liste comporte des filtres pré-appliqués tels que Affecté à moi, Affecté à l'équipe, Non affecté, Tous ouverts, Tous, et ainsi de suite.

À l'aide de ces catégories de listes et de ces listes filtrées, les analystes peuvent rapidement trouver les enregistrements d'incidents de sécurité et de tâches de réponse requis sur lesquels ils doivent travailler.

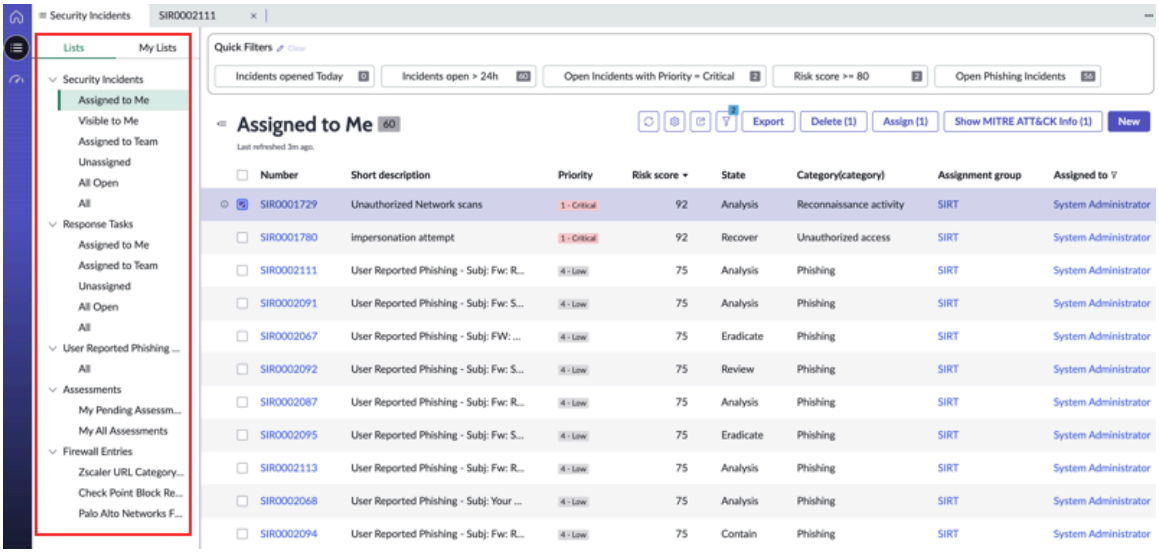
Pour accéder à la vue de liste, vous devez cliquer sur l'icône de liste ( ). Lorsque vous cliquez sur un enregistrement dans une vue de liste, l'enregistrement s'ouvre dans un nouvel onglet.

Types de listes

Vous trouverez ci-dessous un exemple de listes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le volet de liste contient les sections suivantes :

Listes

Élément de liste	Description	Option
Incidents de sécurité	Affichez la liste des incidents de sécurité et accédez à l'incident souhaité pour commencer à travailler dessus. Les listes suivantes sont disponibles : • **Visibles par moi** : incidents de sécurité visibles par l'utilisateur connecté. • **Affectés à moi** : incidents de sécurité qui sont affectés à l'analyste. • **Affectés à l'équipe** : incidents de sécurité qui sont affectés à toutes les équipes auxquelles appartient l'analyste. • **Non affecté** : liste des incidents de sécurité non affectés. • **Tous ouverts** : liste de tous les incidents de sécurité ouverts. • **Tous** : liste de tous les incidents de sécurité.	• Dans la vue de liste, l'analyste peut configurer la liste des colonnes en cliquant sur l'icône d'engrenage qui est disponible au-dessus des colonnes d'incident. • L'analyste peut sélectionner un ou plusieurs incidents de sécurité et affecter ces incidents aux autres utilisateurs. • L'analyste peut supprimer les incidents de sécurité. • L'analyste peut créer un nouvel incident de sécurité. • L'analyste peut appliquer les filtres rapides. Appliquez les filtres en cliquant sur l'option **Filtres rapides** au lieu d'utiliser l'option **Filtre** avancé. À l'aide des filtres rapides, vous pouvez filtrer rapidement la liste des incidents de sécurité qui nécessitent une attention immédiate. Pour plus d'informations, consultez Utilisation de filtres rapides.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Option
		• Les analystes peuvent actualiser la liste des incidents. • L'analyste peut exporter la vue de liste aux formats Excel, CSV, JSON et PDF.
Enregistrements de transfert d'équipe	Affichez la liste des enregistrements de transfert d'équipe. Les listes suivantes sont disponibles : • **Affecté à l'équipe** : enregistrements de transfert d'équipe qui sont affectés à toutes les équipes/groupes d'utilisateurs auxquels l'analyste appartient. • **Tous** : liste de tous les incidents de sécurité.	Le transfert d'équipe prend en charge les trois rôles suivants : • Administrateur : rôle du propriétaire de l'équipe • Analyste de la sécurité : rôle d'analyste d'équipe • Gestionnaire de sécurité : rôle de propriétaire d'équipe, mais n'a pas accès au groupe d'utilisateurs auquel l'enregistrement de transfert d'équipe est affecté. • Les utilisateurs disposant du rôle Propriétaire d'équipe/ Analyste qui font partie du groupe d'utilisateurs dans l'équipe active peuvent ajouter ou modifier du contenu dans les enregistrements de transfert d'équipe à l'état brouillon. • Les utilisateurs qui n'ont pas le rôle de propriétaire/ analyste d'équipe ou qui ne font pas partie du groupe d'utilisateurs de l'équipe active peuvent uniquement afficher le contenu des enregistrements de transfert d'équipe.
Tâches de réponse	Affichez la liste des tâches de réponse et accédez à la tâche de réponse souhaitée pour commencer à travailler dessus. La vue de	• Dans la vue de liste, l'analyste peut configurer la liste des colonnes en cliquant sur l'icône d'engrenage qui est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Option
	liste contient les éléments suivants : • **Affectées à moi** : tâches de réponse qui sont affectées à l'analyste. • **Affectées à l'équipe** : les tâches de réponse qui sont affectées aux équipes des analystes appartiennent. • **Non affectées** : liste des tâches de réponse non affectées. • **Toutes ouvertes** : liste de toutes les tâches de réponse ouvertes. • **Toutes** : liste de toutes les tâches de réponse.	disponible au-dessus des colonnes d'incident. • L'analyste peut sélectionner une ou plusieurs tâches de réponse et les affecter à d'autres utilisateurs. • L'analyste peut créer une nouvelle tâche de réponse. • L'analyste peut appliquer les filtres rapides. Appliquez les filtres en cliquant sur l'option **Filtres rapides** au lieu d'utiliser l'option **Filtre** avancé. À l'aide des filtres rapides, vous pouvez filtrer rapidement la liste des tâches de réponse qui requièrent une attention immédiate. • Les analystes peuvent actualiser la liste des tâches de réponse. • L'analyste peut exporter la vue de liste aux formats Excel, CSV, JSON et PDF. Pour plus d'informations, consultez Exporter les incidents de sécurité ou les tâches de réponse.
E-mails d'hameçonnage	Affichez la liste de tous les e-mails d'hameçonnage. La vue de liste sera triée en fonction de la dernière mise à jour.	• Signaler un e-mail d'hameçonnage. Pour plus d'informations, consultez l'article Signaler un e-mail d'hameçonnage Comment signaler un e-mail d'hameçonnage. • Supprimez les e-mails d'hameçonnage. • Exporter la vue de liste des e-mails d'hameçonnage aux formats Excel, CSV, JSON et PDF.
Évaluations	Consultez la liste des évaluations nécessaires pour	Faites des évaluations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Option
	effectuer une revue post-incident. • **Mes évaluations en attente** : liste des évaluations en attente. • **Toutes mes évaluations** : liste de toutes les évaluations.	

Personnaliser une liste

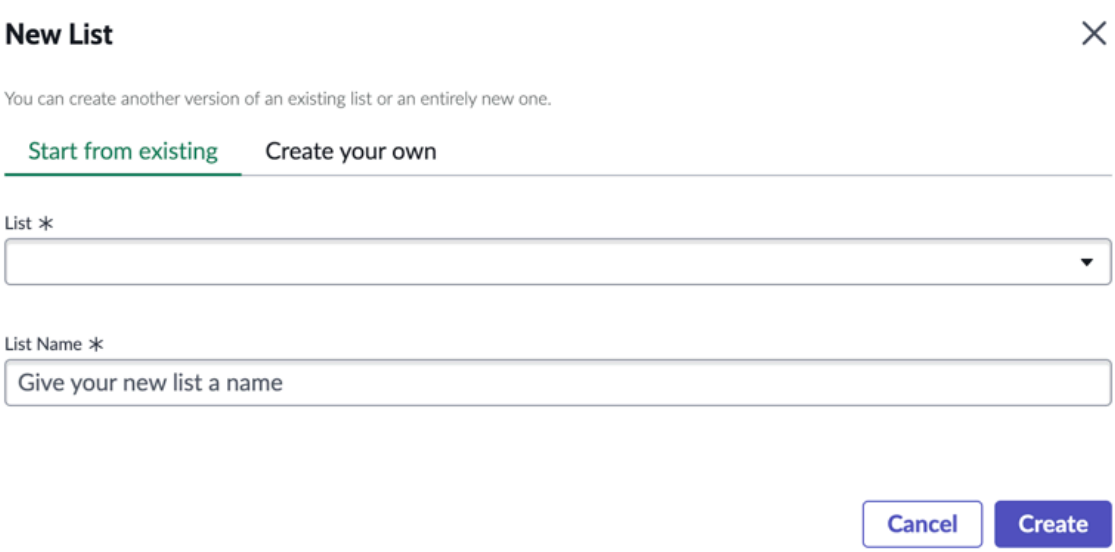
Les analystes ou gestionnaires de sécurité peuvent personnaliser la vue de liste personnalisée liée aux incidents de sécurité, aux tâches de réponse ou aux e-mails d'hameçonnage en fonction de leurs préférences individuelles.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur **Vue de liste**.
3. Cliquer sur **Mes listes**.
4. Cliquez sur **Ajouter une nouvelle liste**, disponible en bas de la vue **Mes listes** .



Les analystes de sécurité peuvent créer soit une autre version d'une liste existante, soit une liste entièrement personnalisée.

5. **Pour créer à partir d'une vue de liste existante :**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Cliquez sur **Démarrer à partir d'un lien existant** .

b. Sélectionnez la **liste** dans la liste déroulante.

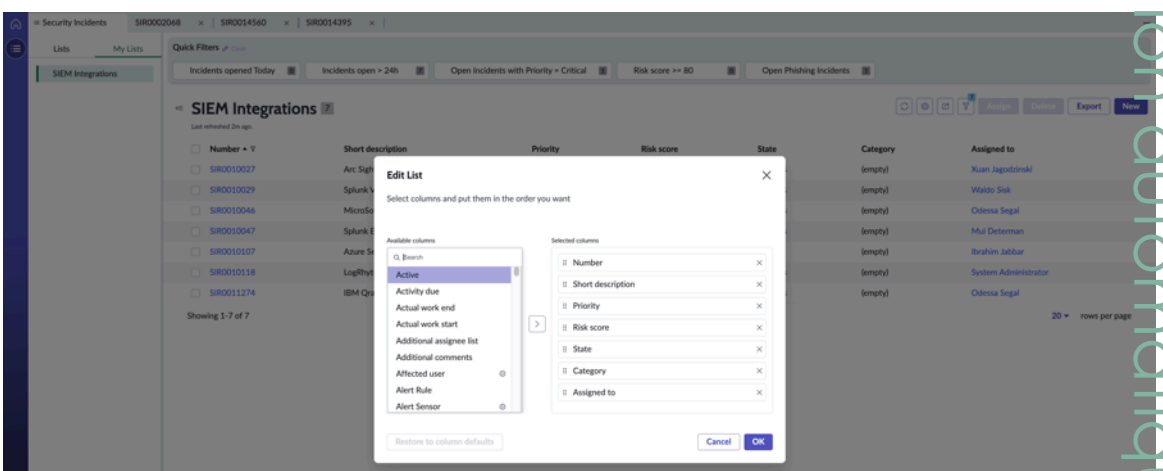
> **Remarque :** Quelle que soit la liste que vous sélectionnez dans la liste déroulante, le nom de la liste sera la copie de votre liste principale. Par exemple, si vous sélectionnez **Affectés à moi** dans la section Incidents de sécurité, le nom de la liste sera **Me l'affecter Copie** de la section des incidents de sécurité.

c. Sélectionnez les colonnes à personnaliser et ajoutez des filtres.
Créez un filtre en ajoutant des conditions qui contiennent un champ, un opérateur et une ou des valeurs.

d. Cliquez sur **Créer**.

> **Remarque :** Pour personnaliser votre propre vue de liste, vous pouvez ajouter des colonnes personnalisées, des filtres, définir des conditions, trier par ordre selon vos besoins.

e. Une fois qu'une vue de liste personnalisée est créée, cliquez sur l'icône d'engrenage et personnalisez les colonnes de la liste en choisissant l'option **Modifier les colonnes** pour modifier les colonnes et les placer dans l'ordre que vous préférez.



Vous pouvez également :

- **Renommez** la vue de liste personnalisée.
- **Supprimez** la vue de liste personnalisée.
- Enregistrez la vue de liste personnalisée comme vous le souhaitez à l'aide de l'option **Enregistrer sous** .
- **Réinitialiser la largeur** de la vue de liste.

> **Remarque :** Vous pouvez également effectuer directement ces opérations à l'aide des autres boutons d'actions de liste tels que l'affectation, la suppression, l'exportation de la vue de liste qui sont fournis.

6. Pour créer votre propre liste :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

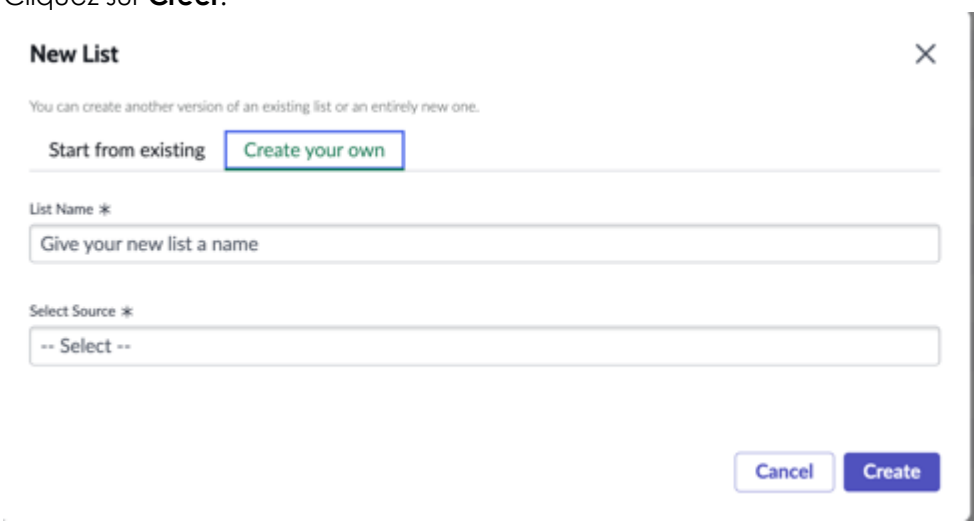
a. Cliquez sur **Créer votre propre** lien.

b. Fournissez un **nom de liste**.

c. Sélectionnez la **source** et les **colonnes**.

d. Ajoutez des filtres.
Créez un filtre en ajoutant des conditions et indiquez l'ordre dans lequel la liste doit être affichée.

e. Cliquez sur **Créer**.



Une nouvelle liste est créée telle que définie et personnalisée par vous sous la section **Mes listes** .

Remarque : Vous pouvez **réorganiser** votre vue personnalisée en déplaçant leurs positions.

Affecter des incidents de sécurité

Affecter des incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

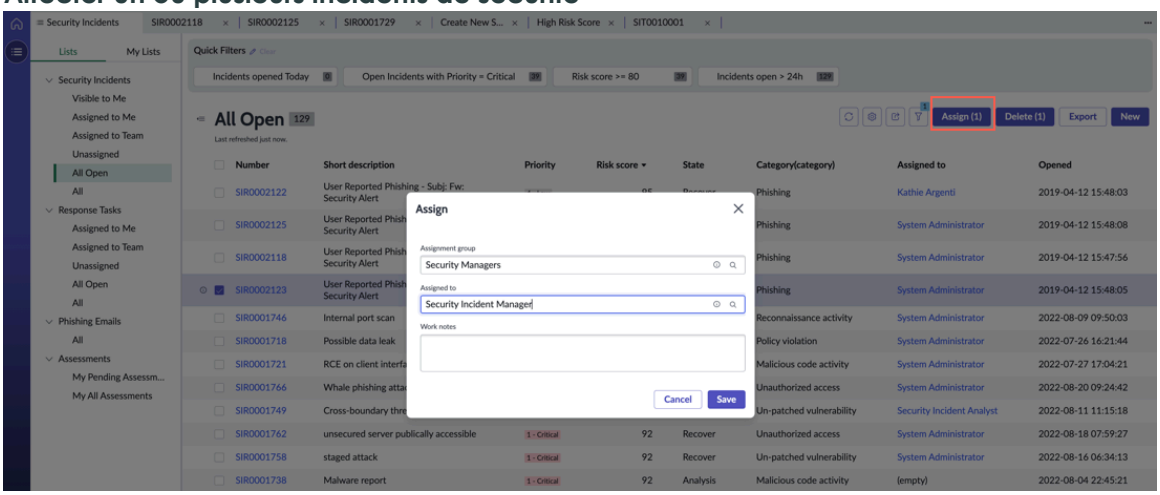
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône de liste ( ).
3. Cliquez sur **Listes**.
4. Par exemple, accédez à **Incidents de sécurité** > **Tous les éléments ouverts**.
5. Sélectionnez un ou plusieurs incidents de sécurité.
6. Cliquez sur **Affecter**.
7. Renseignez les détails tels que le groupe d'affectation, l'Affecté à, et ajoutez des notes de travail si nécessaire.
   L'incident sera alors affecté à l'utilisateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Cliquez sur **Enregistrer**.

Affecter un ou plusieurs incidents de sécurité



Affecter des tâches de réponse

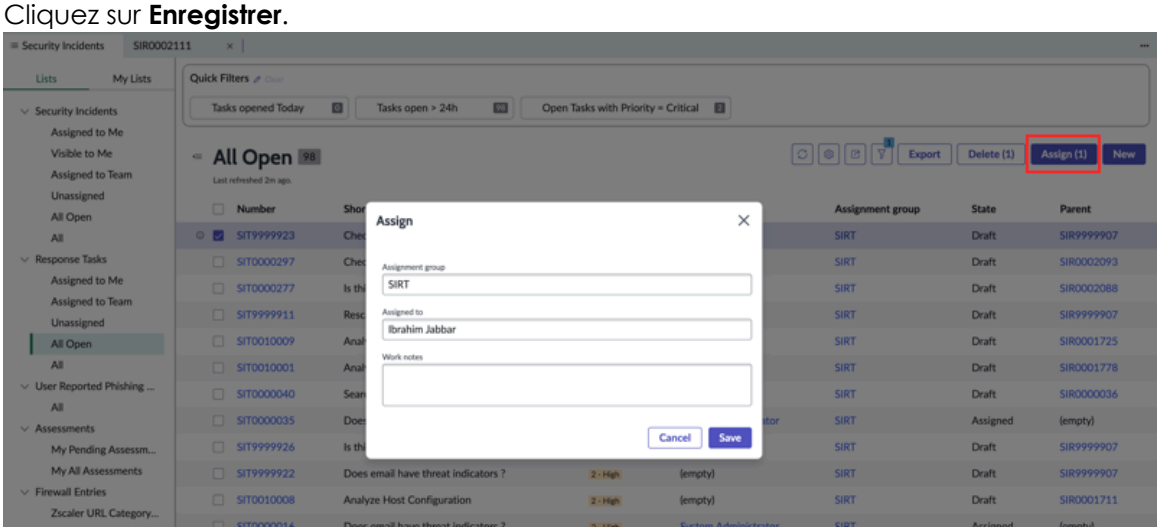
Affecter des tâches de réponse pour un problème de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône de liste ( ).
3. Cliquez sur **Listes**.
   Par exemple, accédez à **Tâches de réponse** > **Tous les éléments ouverts**.
4. Sélectionnez une ou plusieurs tâches de réponse.
5. Cliquez sur **Affecter**.
6. Renseignez les détails tels que le groupe d'affectation, l'Affecté à, et ajoutez des notes de travail si nécessaire.
   L'incident sera alors affecté à l'utilisateur.
7. Cliquez sur **Enregistrer**.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signaler un e-mail d'hameçonnage

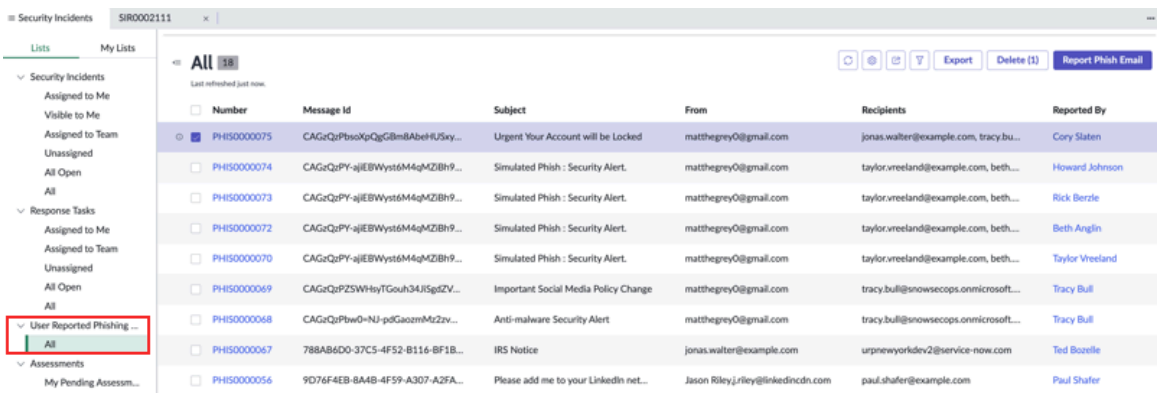
Signalez les e-mails d'hameçonnage à partir de la vue de listes.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône de liste ( ).
3. Accéder à **E-mails d'hameçonnage signalés par un utilisateur** > **Tout**.
   La liste des e-mails de hameçonnage signalés par l'utilisateur s'affiche.



4. Cliquez sur le bouton **Signaler un e-mail d'hameçonnage** .
   Signalez un e-mail d'hameçonnage en le téléchargeant.
5. Cliquez sur **Ajouter un fichier** pour ajouter des pièces jointes.
6. Cliquez sur **Charger**.

> **Remarque :** Signalez un e-mail d'hameçonnage en téléchargeant les pièces jointes. Vous ne pouvez charger qu'un seul e-mail d'hameçonnage à la fois. Il doit être au format .eml.

7. Cliquez sur **Envoyer**.
   L'e-mail d'hameçonnage permettant de consigner un incident de sécurité est créé.

Utilisation de filtres rapides

Les filtres rapides sont des filtres facilement accessibles, disponibles sur les listes d'incidents de sécurité et de tâches de réponse.

Avant de commencer

Rôle requis : sn_si.admin

Le SIR Workspace fournit une fonctionnalité de filtres rapides qui vous permet de filtrer facilement la liste des incidents de sécurité ou des tâches de réponse.

Vous pouvez utiliser des filtres rapides pour configurer de nouveaux filtres ou modifier les filtres existants qui s'affichent sur ces listes. Le système de base fournit les filtres rapides suivants pour chaque incident de sécurité :

- **Incidents ouverts aujourd'hui**
- **Incidents ouverts > 24 heures**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Incidents ouverts avec priorité = critique**
- **> de risque = 80**
- **Incidents d'hameçonnage ouverts**

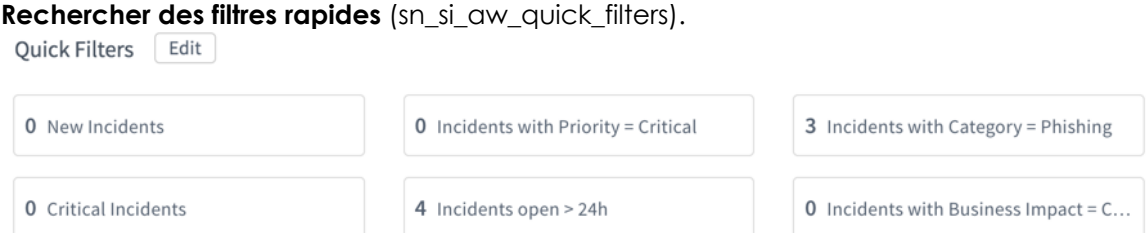
Le système de base fournit les filtres rapides suivants pour chaque tâche d'intervention :

- **Tâches ouvertes > 24h/24**
- **Tâches ouvertes avec priorité = critique**

Remarque : Un administrateur peut configurer la liste requise de filtres rapides en fonction des besoins de l'organisation.

Procédure

1. Accédez à la **Définition du système** > **Tables**.
2. **Rechercher des filtres rapides** (sn_si_aw_quick_filters).



3. Accéder à **Liens connexes** > **Afficher la liste** section.
   La page de liste **Filtres rapides** s'affiche. Prêts à l'emploi, vous trouverez ci-dessous la liste des filtres rapides fournis avec l'application.

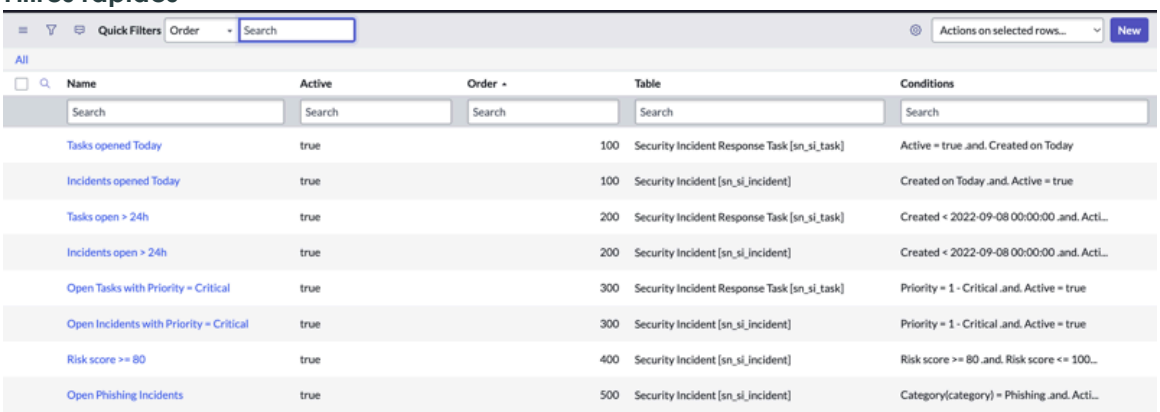
Nom	Table	Valeur
Tâches ouvertes aujourd'hui	Tâche d'incident de sécurité [sn_si_task]	Vrai
Incidents ouverts aujourd'hui	Incident de sécurité [sn_si_incident]	Vrai
Tâches ouvertes > 24h/24	Tâche Réponse aux incidents de sécurité [sn_si_task]	Vrai
Incidents ouverts > 24h	Incident de sécurité [sn_si_incident]	Vrai
Tâches ouvertes avec priorité = critique	Tâche Réponse aux incidents de sécurité [sn_si_incident]	Vrai
Incidents ouverts avec la priorité Critique	Incident de sécurité [sn_si_incident]	Vrai
Score de risque >= 80	Incident de sécurité [sn_si_incident]	Vrai
Incidents d'hameçonnage ouverts	Incident de sécurité [sn_si_incident]	Vrai

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

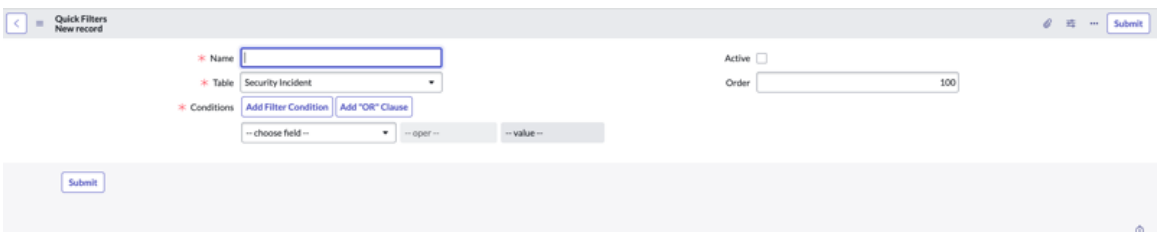
Remarque : L'administrateur de sécurité peut configurer ces filtres rapides. Selon les besoins de l'entreprise, l'administrateur peut modifier la valeur existante sur faux et créer un nouveau filtre rapide.

Filtres rapides



Name	Active	Order	Table	Conditions
Tasks opened Today	true	100	Security Incident Response Task [sn_si_task]	Active = true .and. Created on Today
Incidents opened Today	true	100	Security Incident [sn_si_incident]	Created on Today .and. Active = true
Tasks open > 24h	true	200	Security Incident Response Task [sn_si_task]	Created < 2022-09-08 00:00:00 .and. Acti...
Incidents open > 24h	true	200	Security Incident [sn_si_incident]	Created < 2022-09-08 00:00:00 .and. Acti...
Open Tasks with Priority = Critical	true	300	Security Incident Response Task [sn_si_task]	Priority = 1 - Critical .and. Active = true
Open Incidents with Priority = Critical	true	300	Security Incident [sn_si_incident]	Priority = 1 - Critical .and. Active = true
Risk score >= 80	true	400	Security Incident [sn_si_incident]	Risk score >= 80 .and. Risk score <= 100...
Open Phishing Incidents	true	500	Security Incident [sn_si_incident]	Category(category) = Phishing .and. Acti...

4. Cliquez sur **Nouveau** pour créer un nouveau filtre.
5. Entrez un nom pour le filtre, sélectionnez la table, spécifiez la condition de filtre.
6. Cliquez sur **Soumettre** pour revenir à la page de liste précédente.
   Vous verrez le filtre nouvellement ajouté répertorié sur la page.



Remarque :

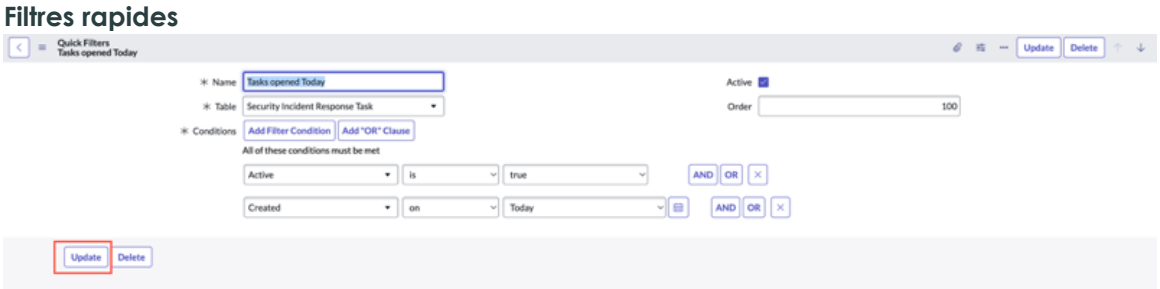
- Le filtre rapide ne s'applique que si la case **Actif** est cochée.
- Dans l'espace de travail, tout utilisateur connecté peut personnaliser les filtres rapides actifs disponibles dans l'application. Les utilisateurs peuvent masquer ou afficher les filtres rapides nouvellement créés. Cette fonctionnalité est basée sur les préférences de l'utilisateur.
- Si un utilisateur a modifié les préférences pour les filtres rapides et qu'un nouveau filtre rapide est créé par la suite, si le filtre rapide est défini sur actif, il ne s'appliquera pas à la préférence de l'utilisateur. L'utilisateur doit modifier manuellement les préférences dans la vue personnalisée.

7. Sélectionnez n'importe quel enregistrement de filtre existant pour modifier les filtres rapides existants.
8. Modifiez le nom et la condition de filtre.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Cliquez sur **Mettre à jour**.



Ajouter ou modifier des filtres rapides

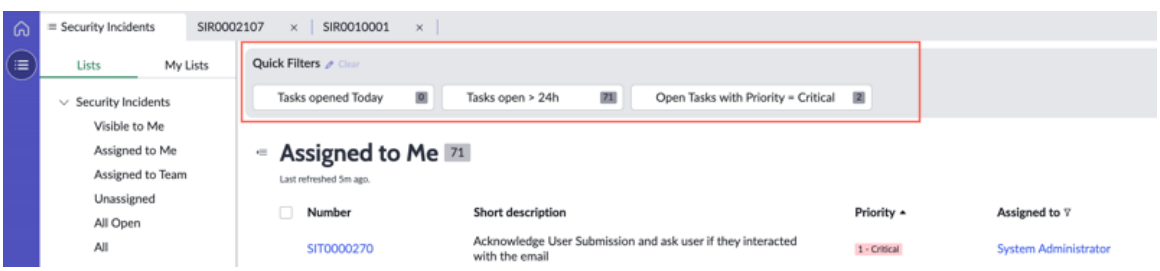
Ajoutez ou modifiez des filtres rapides pour les incidents de sécurité ou les tâches de réponse dans la vue de liste.

Avant de commencer

Rôle requis : sn_si.basic

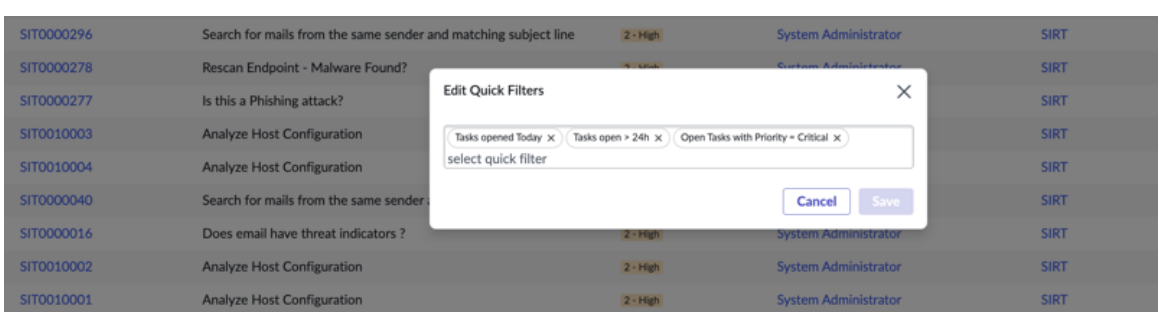
Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône de liste ( ).
3. Par exemple, accédez à **Listes** > **Incidents de sécurité** > **Filtres rapides** section.



4. Cliquez sur **l'icône Modifier** pour apporter les modifications.

> **Remarque :** La modification que vous apportez est conservée et, lorsque l'utilisateur revient sur cette page la prochaine fois, la préférence persistante s'affiche.



5. Cliquez sur **Enregistrer**.

Exporter les incidents de sécurité ou les tâches de réponse

Exportez les incidents de sécurité ou les tâches de réponse à partir de la vue de liste.

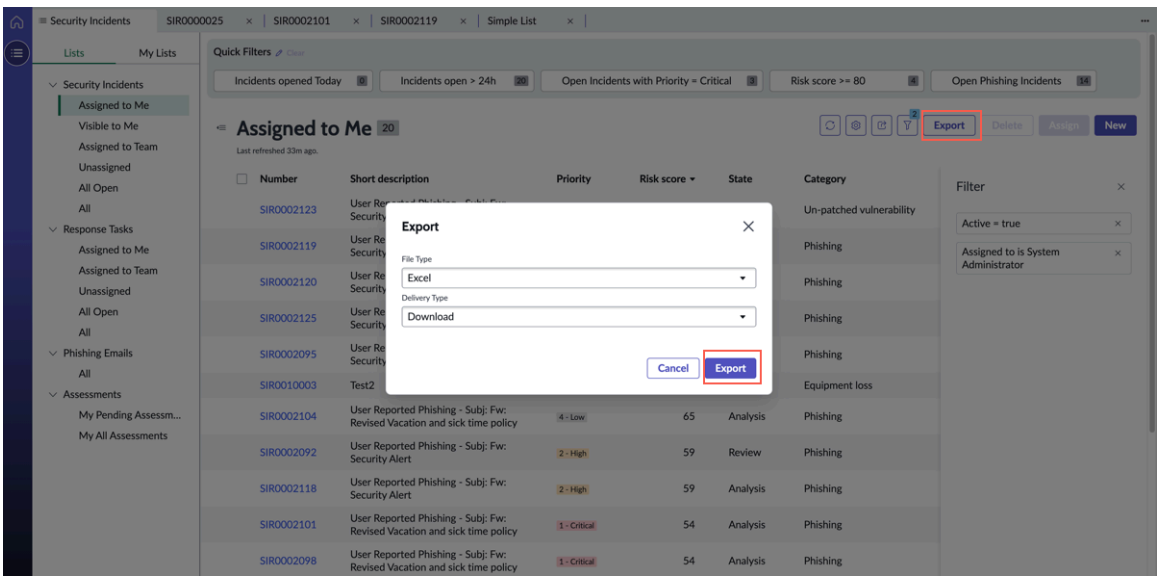
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône Liste .
3. Cliquez sur **Listes**.
4. Accéder à **Incidents de sécurité ou tâches de réponse** > **Tous les éléments ouverts**.
5. Affichez la liste et cliquez sur **Exporter**.



6. Sélectionnez le **type de fichier** et le **type de livraison**.
   Par exemple, **Excel** et **Télécharger** ou Envoyer la liste **par e-mail** .
7. Cliquez sur **Exporter**.
   Le fichier sera téléchargé ou envoyé par e-mail selon l'option choisie.

Gérer les enregistrements de transfert d'équipe

Utilisez la vue de liste des enregistrements de transfert d'équipe pour créer, modifier, copier ou supprimer des enregistrements de transfert d'équipe. Chaque enregistrement de transfert d'équipe est associé à un modèle de rapport de transfert d'équipe.

Avant de commencer
Rôle requis :

- sn_escm_sh.shift_analyst : configuration minimale requise pour accéder aux enregistrements de transfert d'équipe.
- sn_escm_sh.shift_owner : Créez, modifiez et supprimez des enregistrements de journal de transfert dans les groupes d'utilisateurs dont le propriétaire de l'équipe fait partie. Ce rôle hérite du rôle sn_escm_sh.shift_analyst.
- sn_escm_sh.shift_analyst : affiche tous les enregistrements du journal de transfert d'équipe, mais ne peut contribuer qu'aux enregistrements de transfert d'équipe en cours affectés au groupe de l'analyste d'équipe.
- sn_si.analyst : hérite du rôle sn_escm_sh.shift_analyst.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_si.admin : hérite du rôle sn_escm_sh.shift_admin.
- sn_escm_sh.shift_admin : hérite du rôle sn_escm_sh.shift_owner

Important : Pour savoir comment configurer le modèle de transfert d'équipe en tant qu'administrateur, reportez-vous à la section Configurer les modèles de transfert d'équipe.

Pourquoi et quand exécuter cette tâche

Le propriétaire d'équipe et l'équipe ou le groupe d'utilisateurs respectif créent les enregistrements du journal de transfert d'équipe. Le propriétaire de l'équipe doit choisir le modèle de transfert d'équipe et le groupe d'utilisateurs qui travailleront sur le rapport de transfert d'équipe. Une fois le rapport de transfert d'équipe terminé, il est partagé avec le propriétaire d'équipe actif suivant et son équipe.

Points clés du modèle de transfert d'équipe :

- Si un autre analyste de l'équipe active a déjà mis à jour le rapport avant vous et si des changements sont en cours de traitement, un message d'erreur indiquant que des mises à jour de contenu sont en attente peut s'afficher. Vous devez attendre 30 secondes, puis sélectionner à nouveau **Passer à l'état « Revue »**. Vous pouvez voir le rapport consolidé dans le volet droit se mettre à jour avec le contenu mis à jour par d'autres analystes.
- Si le propriétaire du quart a modifié le contenu d'une section à l'état Révision, le même contenu est reflété pour l'analyste lorsque l'enregistrement revient à l'état En cours.
- Le propriétaire de l'équipe doit être attentif lors de la modification du contenu à l'état Révision et effectuer des actions telles que la fusion de deux lignes, la fusion de deux sections, la suppression d'une section, car cela affectera le rapport de transfert d'équipe des autres analystes.
- Après avoir publié le rapport de transfert d'équipe, le propriétaire de l'équipe peut modifier le contenu, mais il ne peut pas changer l'état de l'enregistrement.
- Lorsque quelqu'un modifie le contenu et pendant ce temps, si l'état de l'enregistrement passe de En cours à Réviser, les changements de contenu non enregistrés sont ignorés.
- L'administrateur d'équipe a un accès en écriture à tous les enregistrements du journal de transfert d'équipe, quels que soient les groupes d'utilisateurs.

Procédure

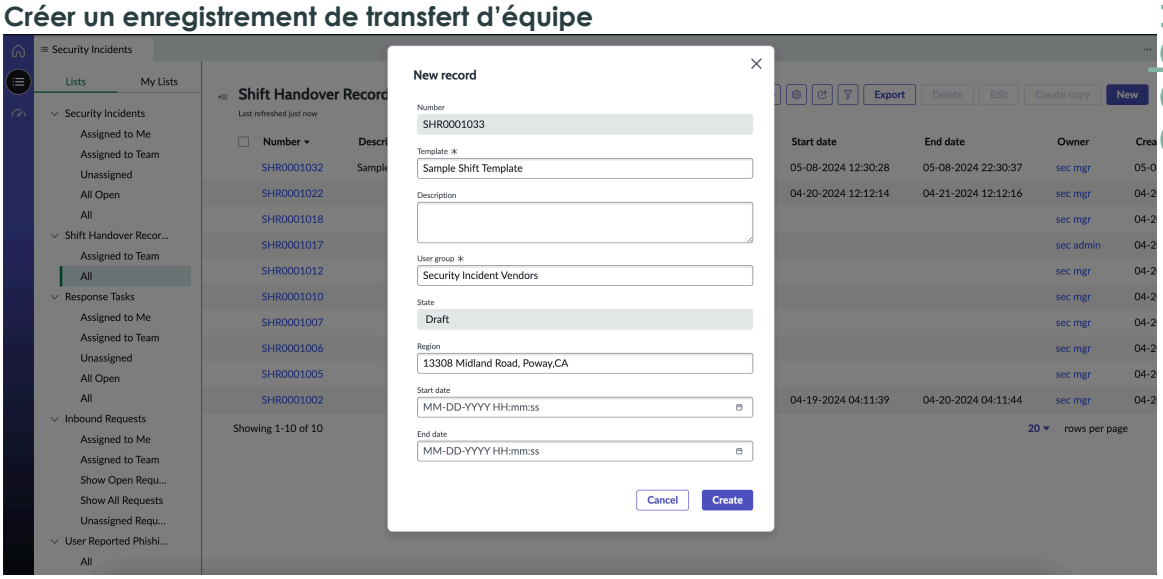
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez Liste des incidents de sécurité.
3. Sous l'onglet **Listes** , sélectionnez **Enregistrements de transfert d'équipe**.
4. Sélectionnez **Tous les enregistrements** pour afficher la liste de tous les enregistrements de transfert d'équipe.
5. Sélectionnez **Affecté à une équipe** pour afficher la liste des enregistrements de transfert d'équipe qui sont affectés à toutes les équipes/groupes d'utilisateurs auxquels les analystes appartiennent.
6. Pour créer un enregistrement de transfert d'équipe, sélectionnez **Nouveau**.
7. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Numéro	Numéro unique généré automatiquement pour un enregistrement de transfert d'équipe.
Modèle	Sélectionnez le modèle de transfert d'équipe à utiliser. Par exemple, Exemple de modèle d'équipe.
Description	Description de l'enregistrement de transfert d'équipe.
Groupe d'utilisateurs	Sélectionnez le groupe/l'équipe d'utilisateurs auquel l'enregistrement de transfert d'équipe sera affecté. Par exemple, Réviseurs de code de Développement de l'équipe.
État	État actuel de l'enregistrement de transfert d'équipe. Par défaut, l'état initial est Brouillon **Remarque :** L'état ne peut pas être modifié pendant la création d'un enregistrement. .
Région	Sélectionnez la région à laquelle l'enregistrement de transfert d'équipe sera affecté. Par exemple, APAC.
Date de début	Sélectionnez la date de début de l'enregistrement de transfert d'équipe.
Date de fin	Sélectionnez la date de fin de l'enregistrement de transfert d'équipe.

Créer un enregistrement de transfert d'équipe



8. Sélectionnez **Créer**.

Traduction automatique

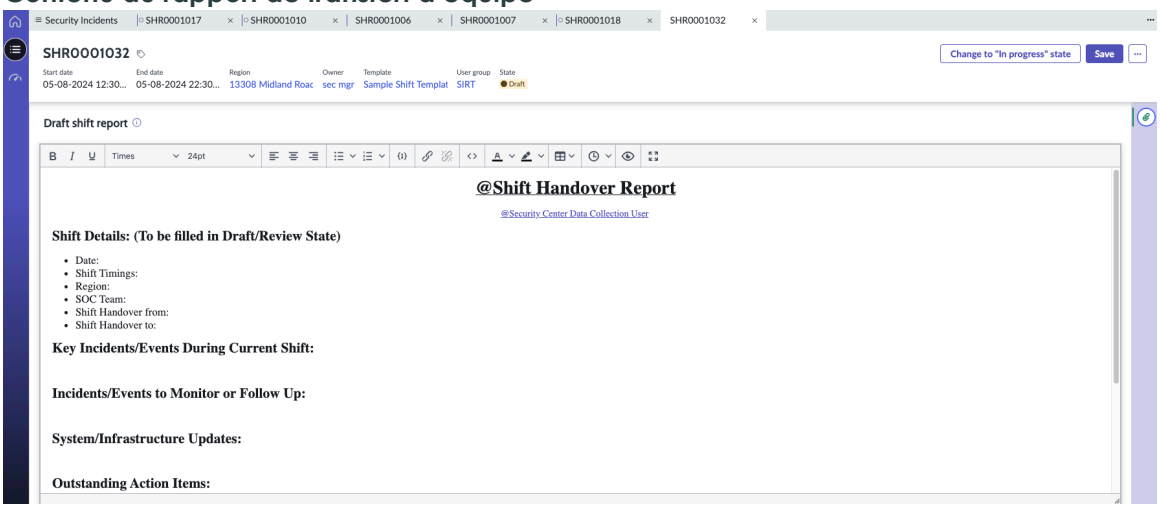
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un nouvel enregistrement de transfert d'équipe est créé en fonction du modèle que vous avez sélectionné et ajouté à la vue de liste.

9. Ouvrez le nouvel enregistrement de transfert d'équipe pour mettre à jour l'état et les détails des incidents de sécurité dans le rapport de transfert d'équipe.
   Par défaut, l'enregistrement de transfert d'équipe est à l'état **Brouillon** .

   Remarque : Seul le propriétaire de l'équipe peut modifier le contenu.

Contenu du rapport de transfert d'équipe



10. Dans l'éditeur de rapport de brouillon d'équipe, utilisez les sections de modèle de rapport de transfert d'équipe pour mettre à jour les détails des incidents de sécurité et des utilisateurs.

    Vous pouvez mettre en forme votre rapport avec toutes les options de l'éditeur, telles que les polices, les couleurs, les puces, les liens et les pièces jointes.

    Remarque : Le propriétaire de l'équipe et l'analyste de l'équipe peuvent tous deux modifier le contenu.

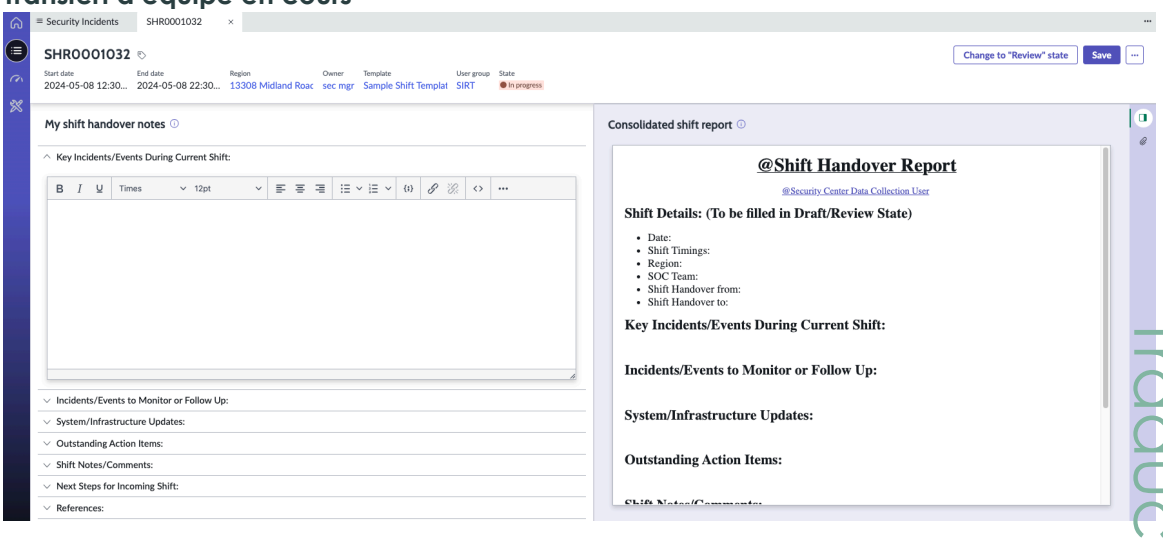
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Après avoir apporté les modifications requises au rapport de transfert d'équipe, sélectionnez **Enregistrer**.

b. Sélectionnez **l'action Passer à l'état « En cours »** pour faire passer l'enregistrement du transfert d'équipe à l'état En cours.

Transfert d'équipe en cours

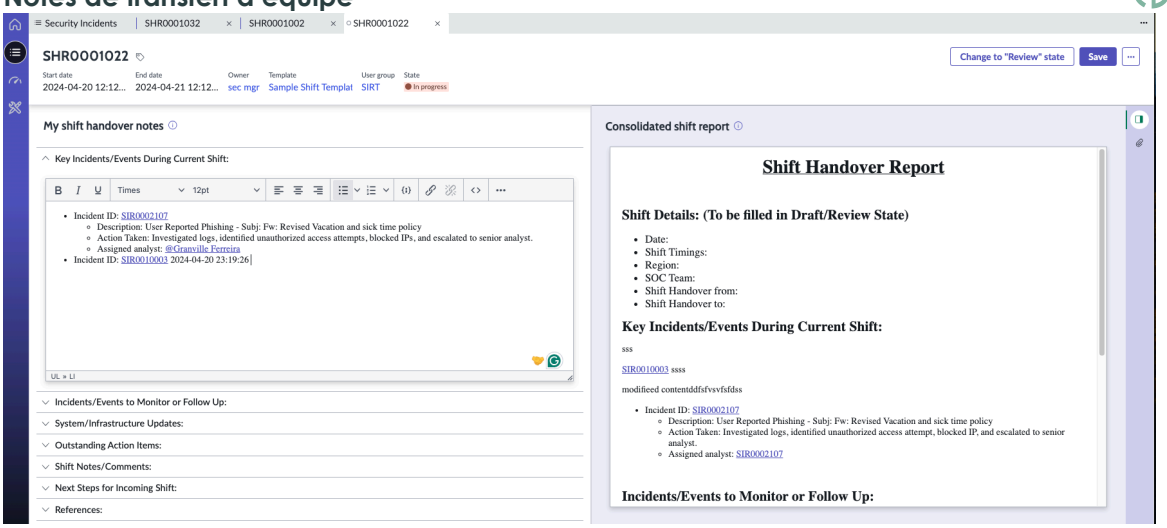


11. Dans l'éditeur de notes de transfert de mon équipe, mettez à jour les détails requis pour toutes les sections telles que l'incident de sécurité et les détails de l'utilisateur.

> **Remarque :** Le propriétaire de l'équipe et l'analyste de l'équipe peuvent tous deux modifier le contenu.

a. Pour mentionner un enregistrement particulier dans l'éditeur, utilisez **/** et choisissez **Sélectionner un enregistrement**, puis sélectionnez un enregistrement dans la liste des tables qui s'affiche.
Par exemple, si vous sélectionnez l'enregistrement **Incidents de sécurité** , une liste des incidents de sécurité s'affiche. Sélectionnez un (**SIR0010025**) d'incident de sécurité dans la liste et mettez à jour les détails du transfert d'équipe requis. Vous pouvez également mentionner les champs associés à l'incident de sécurité tels que description brève, convoitise de surveillance en utilisant **/** après le numéro d'incident de sécurité.

Notes de transfert d'équipe



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

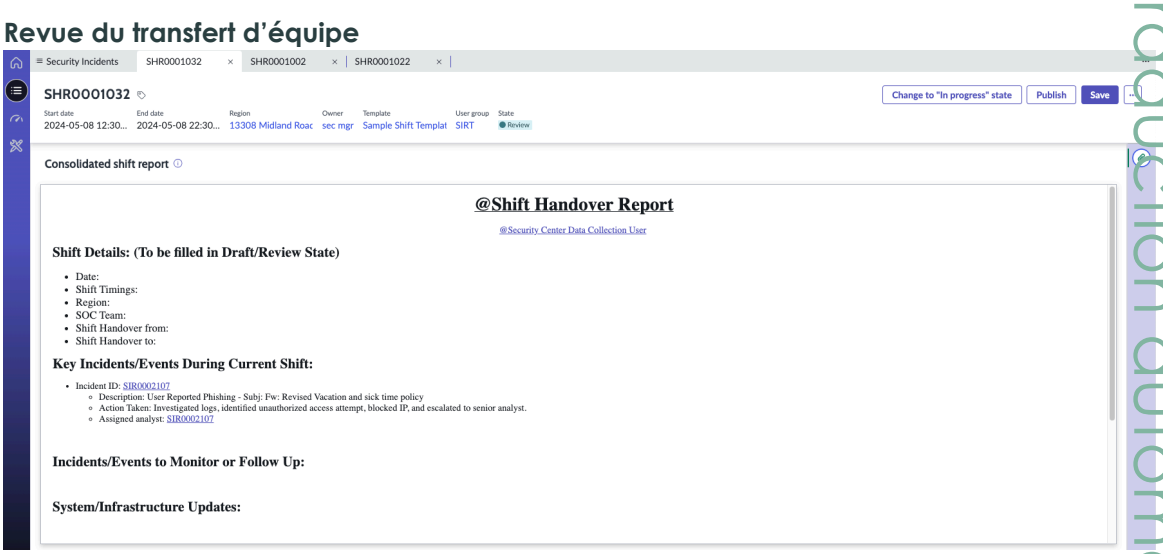
b. Pour mentionner un utilisateur particulier dans l'éditeur, utilisez **/** et choisissez **Sélectionner un utilisateur**, puis sélectionnez un utilisateur dans la liste qui s'affiche.

c. Vous pouvez mettre en forme votre rapport avec toutes les options de l'éditeur, telles que les polices, les couleurs, les puces, les liens et les pièces jointes.

d. Après avoir apporté les modifications requises aux notes de transfert d'équipe, sélectionnez **Enregistrer**.

e. Sélectionnez **l'action Passer à l'état « Revue »** pour faire passer l'enregistrement de transfert d'équipe à l'état Réviser.

Remarque : Si un autre analyste de l'équipe d'équipe active a déjà mis à jour le rapport avant vous et si les changements sont en cours de traitement, un message d'erreur peut s'afficher. Vous devez patienter quelques secondes, puis sélectionner à nouveau **Passer à l'état « Revue »**.



12. Dans le rapport d'équipe consolidé, examinez le rapport de transfert d'équipe et apportez les modifications requises.

Remarque : Seul le propriétaire de l'équipe peut modifier le contenu.

a. Après avoir apporté les modifications requises aux notes de transfert d'équipe, sélectionnez **Enregistrer**.

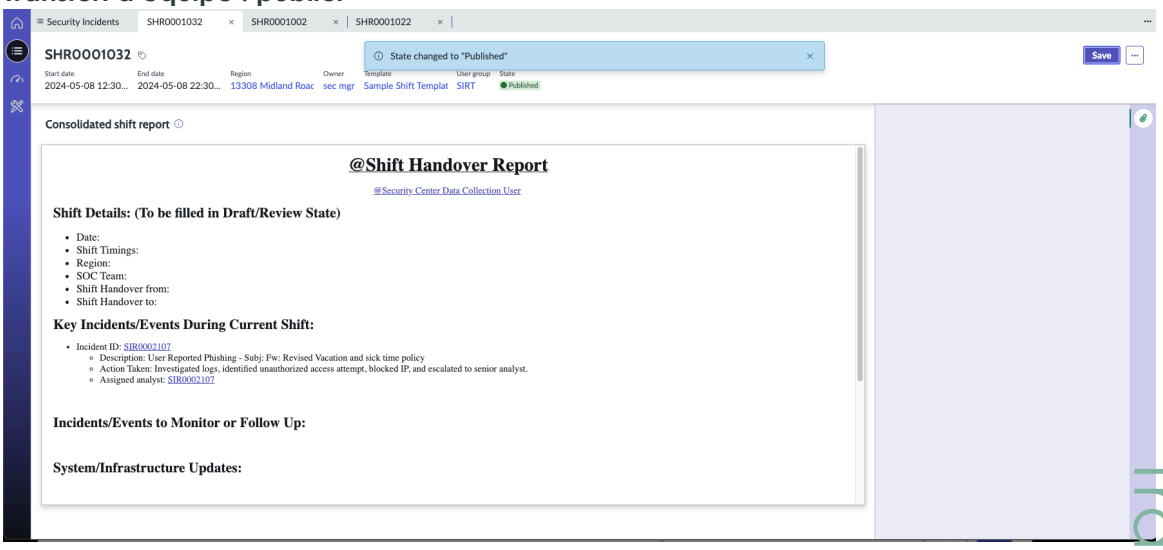
b. Si le rapport de transfert d'équipe nécessite d'autres mises à jour de la part des analystes, vous pouvez sélectionner **Passer à l'état « En cours »**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Sélectionnez **l'action Publier** pour publier le rapport de transfert d'équipe.

Transfert d'équipe : publier



13. Sélectionnez **Enregistrer** pour enregistrer le rapport de transfert d'équipe.
Une fois que vous avez enregistré, vous pouvez voir un aperçu du rapport de transfert d'équipe avec vos dernières mises à jour dans le volet Aperçu.

> **Remarque :** Bien que vous puissiez prévisualiser immédiatement les mises à jour que vous avez effectuées dans le rapport de transfert d'équipe, les autres analystes peuvent prendre quelques secondes pour voir les changements.

14. En tant que propriétaire d'équipe, vous pouvez également effectuer les actions suivantes dans la vue de listes Transfert d'équipe.

a. Pour modifier un enregistrement de transfert d'équipe existant, sélectionnez l'enregistrement et sélectionnez l'action **Modifier** .
Vous pouvez modifier uniquement l'heure de début, l'heure de fin, la description et la région.

b. Pour créer une copie d'un enregistrement de transfert d'équipe, sélectionnez l'enregistrement et sélectionnez **Créer une** action de copie.

c. Pour supprimer un enregistrement de transfert d'équipe existant, sélectionnez l'enregistrement et sélectionnez l'action **Supprimer** .

Configurer SIR Workspace

Cette section décrit les configurations nécessaires pour travailler avec le Espace de travail de la Réponse aux incidents de sécuritéfichier .

Configurer la vue des enregistrements SIR

Cette section décrit la façon dont les listes connexes sont regroupées et présentées dans l'onglet Enregistrements connexes SIR pour faciliter la navigation.

Les utilisateurs de l'espace de travail peuvent également facilement effectuer une recherche dans la liste connexe par nom.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'examen de l'heure de conception du SI

Utilisez cette section pour configurer la page d'enquête sur l'heure de conception de l'incident de sécurité afin d'ajouter plusieurs points d'entrée et ses enregistrements associés dans le Espace de travail de la Réponse aux incidents de sécurité.

Rôle requis : sn_si.admin.

Vous trouverez ci-dessous des détails sur les étapes de configuration de la page d'examen sur le Espace de travail de la Réponse aux incidents de sécurité.

- Création d'une vue pour les tables d'informations associées
- Ajout d'une liste de points d'entrée
- Vue du mappage des informations associées à la liste de points d'entrée
- Configurer chaque liste associée à partir de la vue pour gérer le rendu des données d'exécution

Information associée

Explorer le canevas d'enquête

Création d'une vue pour les tables d'informations associées

L'écran d'examen s'appuie sur les vues de listes connexes créées sur l'incident de sécurité pour configurer les listes associées.

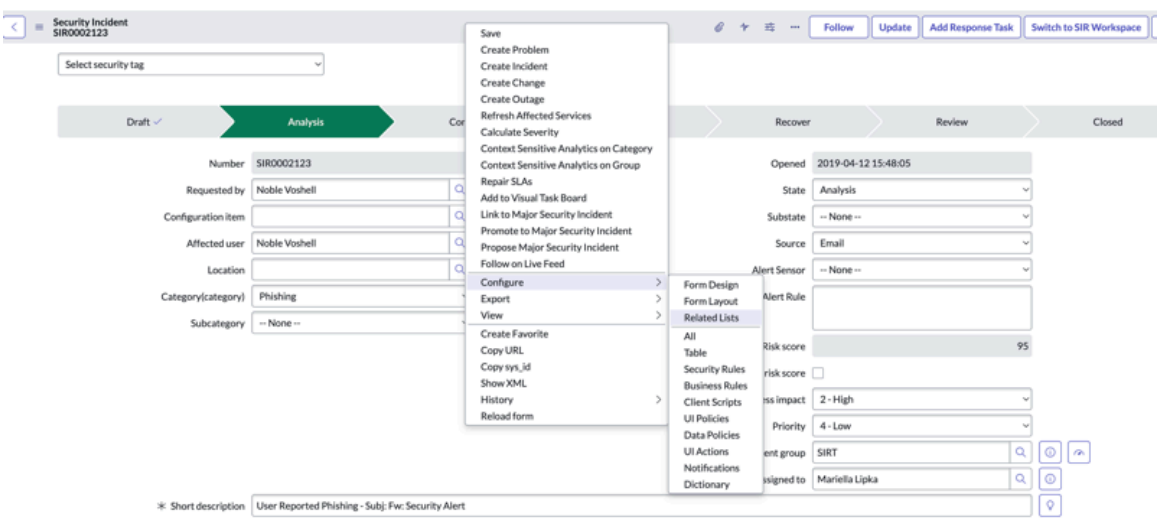
Avant de commencer

Rôle requis : sn_si.admin

Voici la procédure pour créer une vue et y ajouter des listes connexes.

Procédure

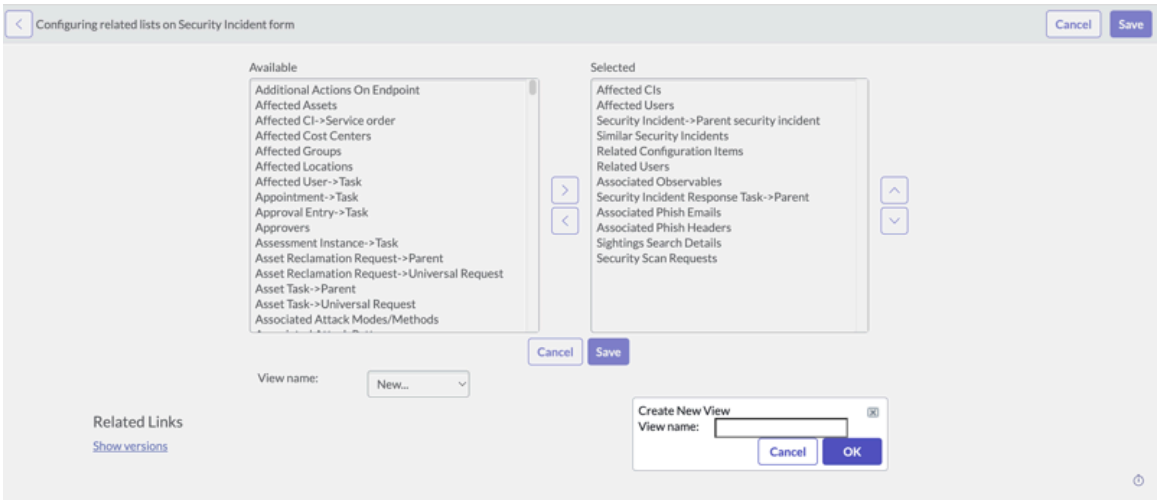
1. Accédez à la liste **des incidents de sécurité** .
2. Ouvrez n'importe quel incident de sécurité dans l'interface utilisateur classique.
3. À partir du menu contextuel du formulaire, accédez à **Configurer** > **Listes connexes**.
   La fenêtre de la zone de liste double s'affiche.



4. Accédez à la liste déroulante Nom de **la vue** , puis cliquez sur **Nouveau** pour créer une nouvelle vue.
   Vous devez ajouter un nom à la vue.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Ajoutez les listes connexes souhaitées au compartiment de droite sous la vue nouvellement créée et enregistrez la vue.
   Cette vue permet d'afficher les informations associées dans l'onglet Examen.

Ajout d'une liste de points d'entrée

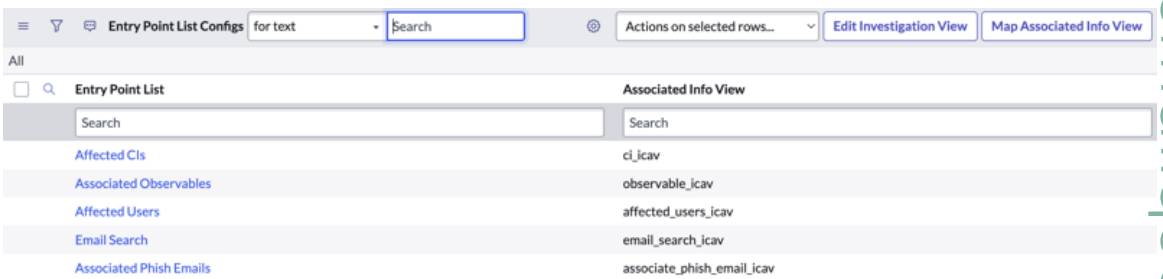
Configurez la nouvelle liste de points d'entrée pour l'ajouter à la page d'enquête.

Avant de commencer

Rôle requis : administrateur

Procédure

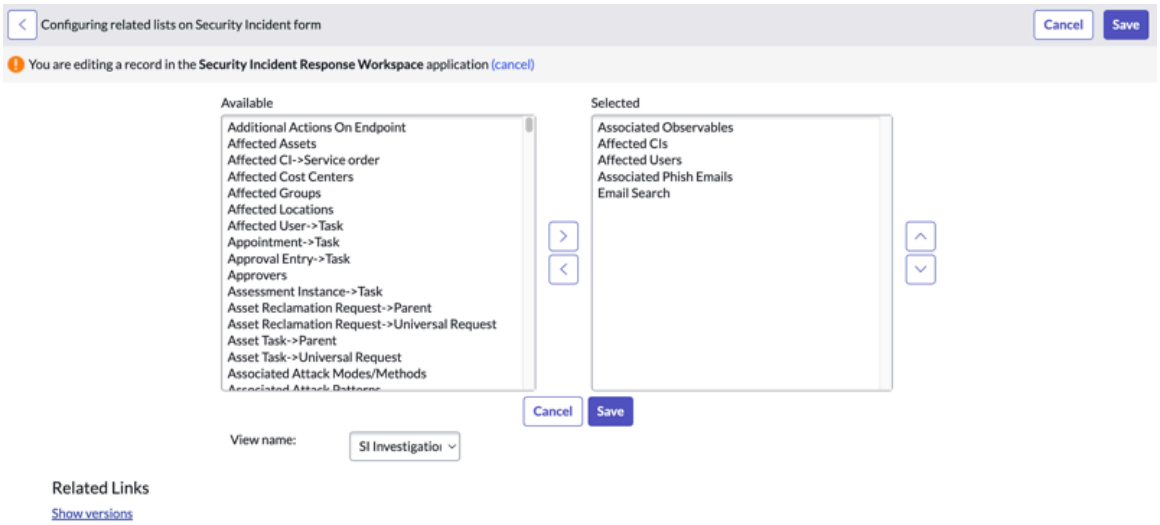
1. Accédez à la **sn_si_aw_entry_point_config.list**.
   La page **Configurations des listes de points d'entrée** s'affiche.



2. Cliquez sur le bouton **Modifier la vue d'enquête** pour ajouter une liste de points d'entrée à l'écran d'enquête.
   Le **formulaire Configuration des listes connexes sur l'incident de sécurité** s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Ajoutez ou supprimez la liste de points d'entrée de la vue de la zone de liste double.
4. Cliquez sur **Enregistrer**.

> **Remarque :** La vue correspondant à l'écran d'examen contenant les listes de points d'entrée est appelée **vue d'enquête SI** et est sélectionnée par défaut lorsque vous accédez à la page **Modifier la vue d'enquête** .
>
> L'ordre dans lequel les listes de points d'entrée sont affichées sur le canevas d'examen est déterminé par l'ordre dans la vue sélectionnée de la zone de sélection.

Vue du mappage des informations associées à la liste de points d'entrée

Mappez la vue d'informations associée à la liste de points d'entrée nouvellement ajoutée à l'aide de l'action Vue des informations associées à la carte.

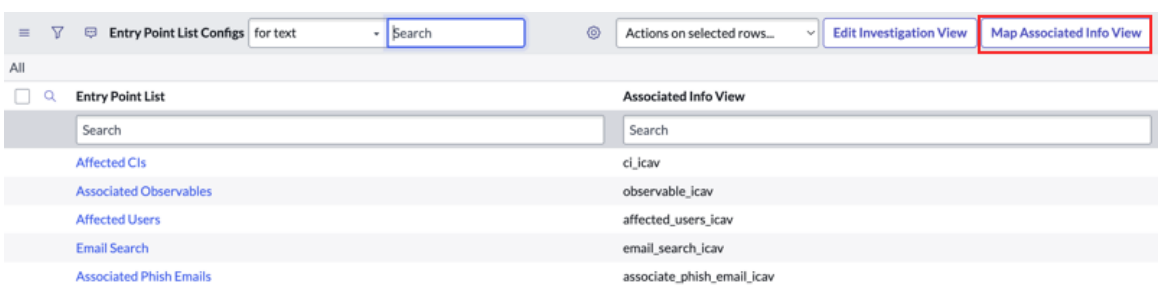
Avant de commencer

> **Remarque :** Cette étape est requise pour que la liste de points d'entrée soit visible sur la page Examiner. Même si vous ne souhaitez pas que des listes d'informations associées s'affichent sous un point d'entrée, vous devez tout de même créer une vue factice et la mapper.

Rôle requis : administrateur

Procédure

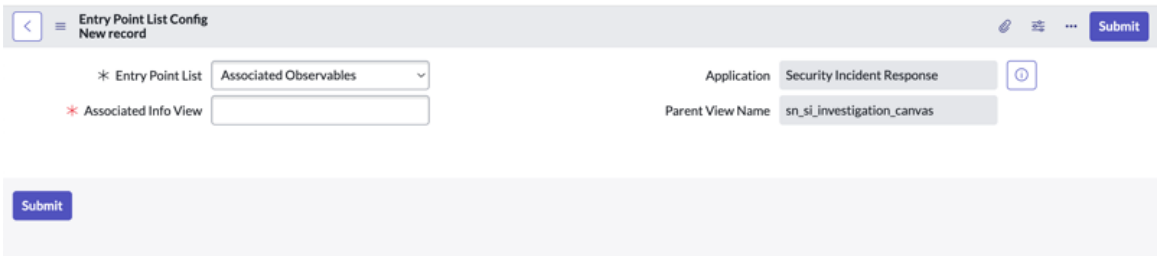
1. Cliquez sur le bouton **Afficher les informations associées à la carte** sur la page **Configurations de point d'entrée** .



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Sélectionnez la liste de points d'entrée nouvellement ajoutée dans la liste **déroulante Liste de points d'entrée** .
3. Saisissez le nom de la vue contenant les listes connexes des informations associées dans le champ **Vue des informations associées** .
   Pour en savoir plus sur la création d'une vue pour les listes connexes Informations associées, reportez-vous à la section Création d'une vue pour les tables d'informations associées.



4. **Enregistrez** le formulaire.
5. En outre, si nécessaire, vous pouvez ajouter ou supprimer d'autres listes associées à l'aide de la **vue Modifier les informations associées**.
   Vous pouvez également configurer la mise en page de la liste de points d'entrée à l'aide de l'action **Modifier la mise en page de la liste de points de terminaison** . Ajoutez ou supprimez des colonnes de la zone de sélection comme vous le souhaitez, puis enregistrez le formulaire.

Configurer chaque liste associée à partir de la vue pour gérer le rendu des données d'exécution

Configurez chaque liste associée à partir de la vue pour gérer le rendu des données d'exécution.

Avant de commencer

Remarque : Cette étape est obligatoire pour chaque liste associée configurée dans la vue d'informations associée. Dans le cas contraire, la liste associée ne sera pas disponible sur la page d'examen.

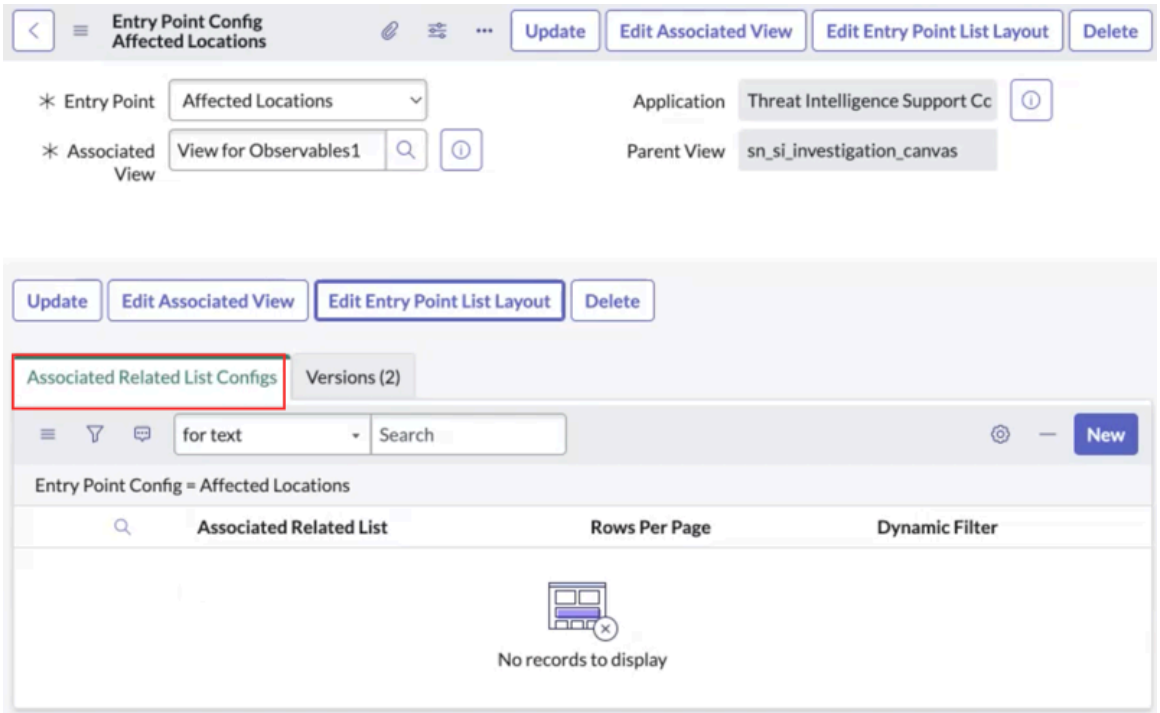
Chacune des listes associées ajoutées (lors du mappage d'une vue d'informations associée à une liste de points d'entrée) Vue du mappage des informations associées à la liste de points d'entrée (ou provenant directement de la vue) nécessite une configuration supplémentaire pour filtrer les données en ce qui concerne la sélection des enregistrements d'exécution et la sélection des filtres.

Rôle requis : administrateur

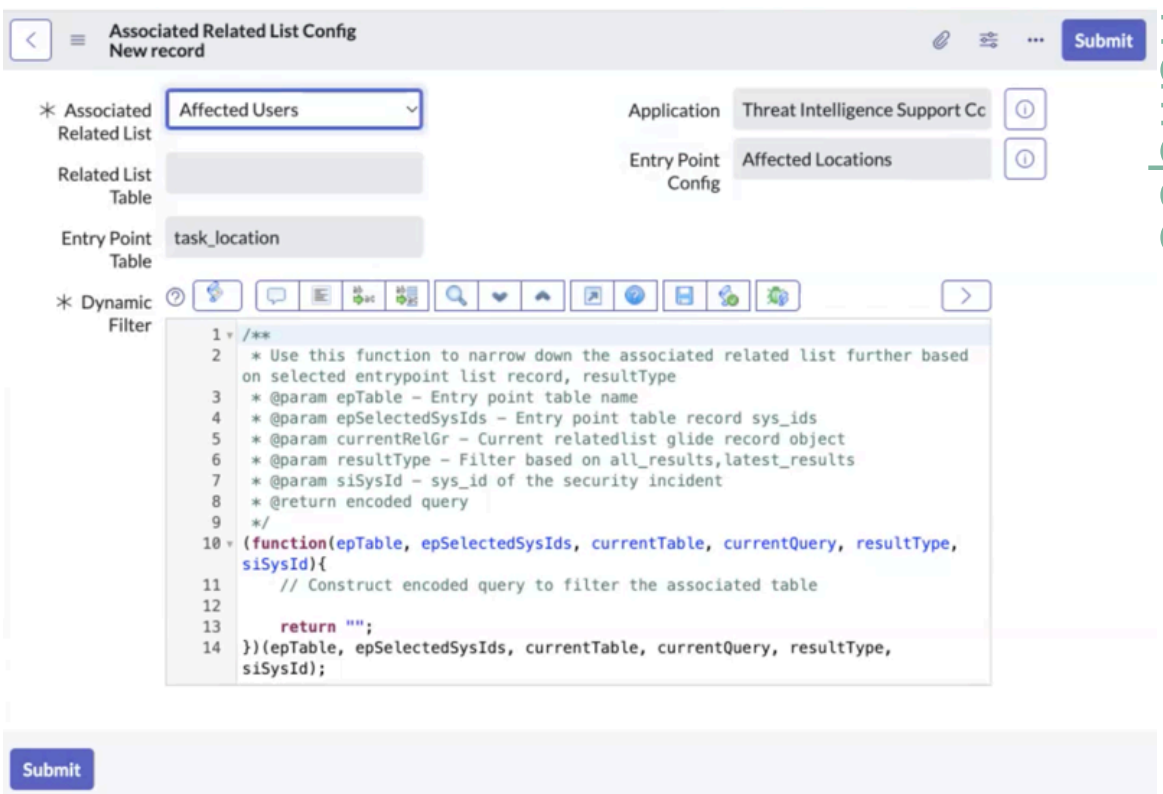
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Cliquez sur **Nouveau** dans les configurations de liste **associées**.



2. Sélectionner la valeur du champ **de la liste associée** .
3. Utilisez la colonne **Filtre dynamique** pour filtrer davantage la liste associée en fonction des enregistrements de liste de points d'entrée sélectionnés et du type de résultat (derniers résultats de chaque implémentation de fournisseur, tous les résultats).
   Reportez-vous aux exemples existants qui sont expédiés dans le produit.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Vous pouvez également configurer la mise en page de la liste associée à l'aide de l'action **Modifier la mise en page de la liste associée** .
   Dans la fenêtre de la zone de sélection, ajoutez ou supprimez des colonnes selon vos besoins.

SIR Workspace Enregistrements connexes

Cette section se compose des éléments des listes connexes qui sont regroupés en sections telles que les observables associés et les éléments de configuration.

La liste connexe suivante répertorie les groupes disponibles dans le cadre du système de base. Vous pouvez modifier ces groupes ou créer des groupes au sein de l'application et de leurs actions respectives.

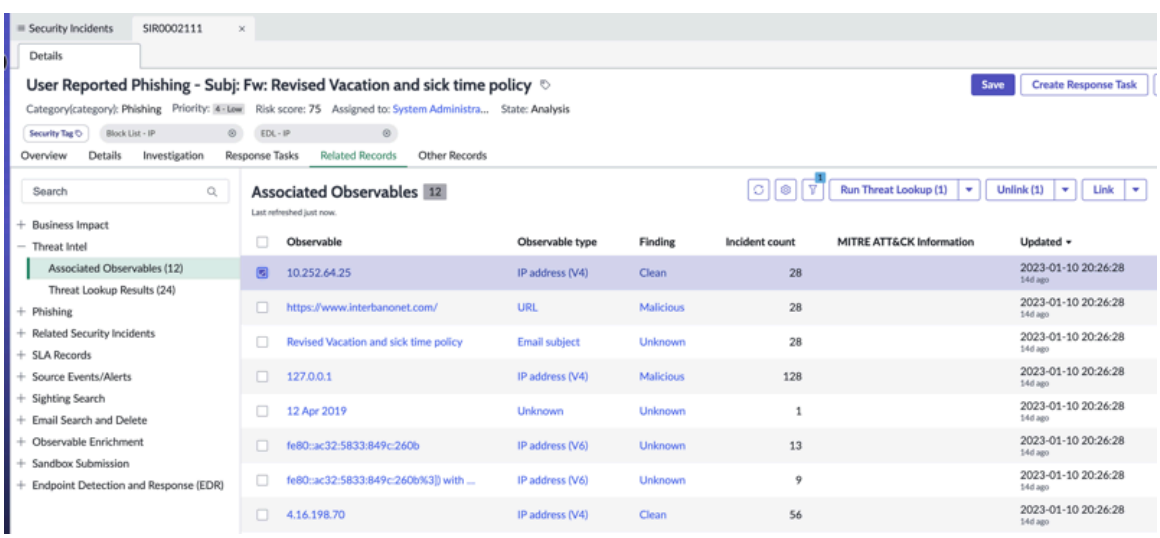
Vous pouvez modifier ces groupes ou en créer de nouveaux. Pour plus d'informations, consultez Configurer la liste connexe des incidents de sécurité comment configurer et regrouper la liste connexe pour les incidents de sécurité et les tâches de réponse. Chaque liste connexe est entièrement fonctionnelle dans le SIR Workspacefichier .

Liste connexe	Élément groupé
Impact sur l'entreprise	• Éléments de configuration • Utilisateurs affectés • Éléments de configuration associés • Utilisateurs associés • Services affectés
Connaissance de la menace	• Observables associés • Résultats de la recherche de menace
Hameçonnage	• E-mails associés Phish • En-têtes d'hameçonnage associés
Incidents de sécurité associés	• Incident de sécurité parent • Incident de sécurité enfant • Incident de sécurité similaire
Enregistrements SLA	SLA de tâche
Événements/alertes sources	Les événements ou alertes sources correspondent à la liste connexe Intégration SIEM activée, telle que l'e-mail source, les journaux d'analyse LogRhythm, les événements LogRhythm, l'attaque IBM QRadar agrégée, entre autres.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Élément groupé
	Remarque : Cette liste dépend entièrement de l'intégration que vous avez dans votre instance. Pour afficher la liste connexe de l'intégration SIEM pertinente, vous devez installer la version la plus récente.
Recherche de perception	• Résultats de recherche de perceptions • Détails de la recherche de perception • Perception
Enrichissement des éléments observables	• Résultats de l'enrichissement de l'observable • Événements MISP associés • Résultats de l'enrichissement MISP
EDR (Endpoint Detection and Response)	• Détails de l'hôte • Processus en cours • Services d'exécution • Utilisateurs connectés • Statistiques réseau • Obtenir un fichier • Isoler les entrées de l'hôte • Actions supplémentaires sur le point de terminaison • Détails des ordinateurs liés à Microsoft Defender pour point de terminaison



Remarque : En général, vous pouvez créer de nouveaux enregistrements, lier ou dissocier des enregistrements existants ou de nouveaux enregistrements par rapport au groupe de listes connexes, le cas échéant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Configurer la liste connexe des incidents de sécurité

Configurer la liste connexe des incidents de sécurité

Vous pouvez ajouter de nouvelles listes connexes ou de nouveaux groupes de listes connexes, et modifier les groupes ou listes connexes existants qui apparaissent dans le SIR Workspacefichier .

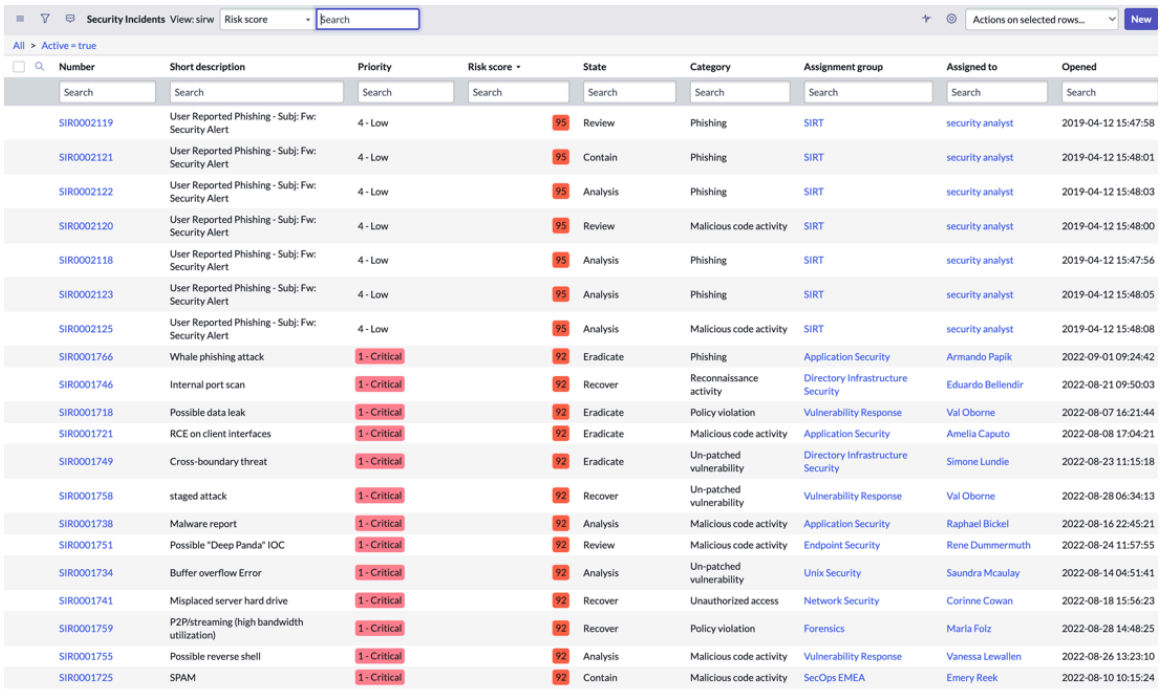
Avant de commencer

La liste connexe des incidents de sécurité est regroupée et affichée en tant qu'éléments de liste connexes de groupe dans l'onglet **Enregistrements connexes** de l'espace de travail.

Rôle requis : sn_si.admin

Procédure

1. Dans l'interface utilisateur classique, accédez à **Tout** > **Incident de sécurité** > **Afficher les incidents ouverts**.

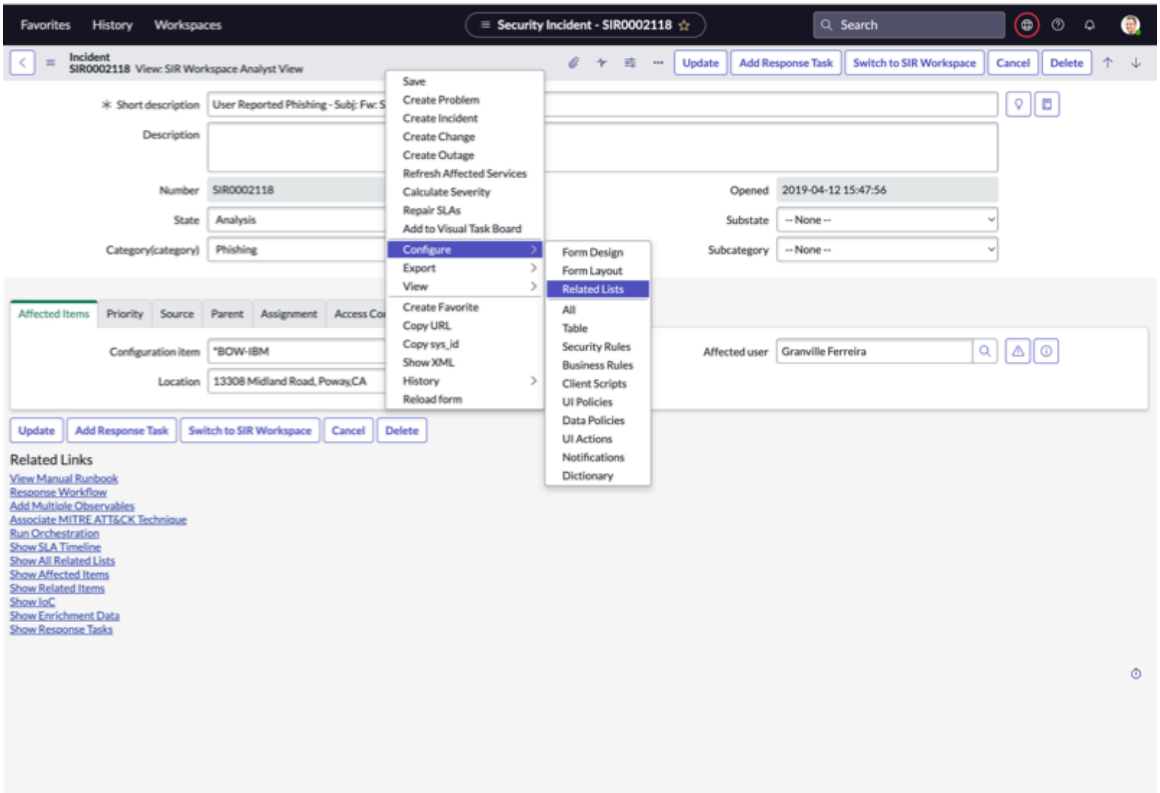


Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

2. Sélectionnez n'importe quel enregistrement d'incident.
3. Cliquez avec le bouton droit sur le menu contextuel de l'incident.
4. Accéder à **Configurer** > **Liste connexe**.

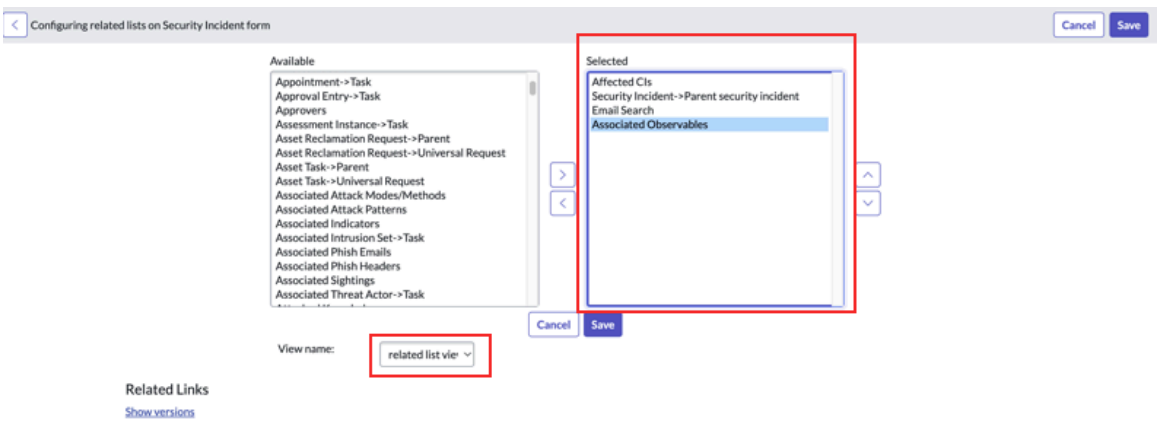
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le **formulaire Configuration des listes connexes sur l'incident de sécurité** s'affiche.

5. Accédez à **Nom de la vue** et sélectionnez **Nouveau**.
6. Entrez un nom pour la vue.
7. Sélectionnez la vue nouvellement créée.
   Une fois que vous avez sélectionné la vue, choisissez les champs de liste connexe requis dans la zone de sélection.

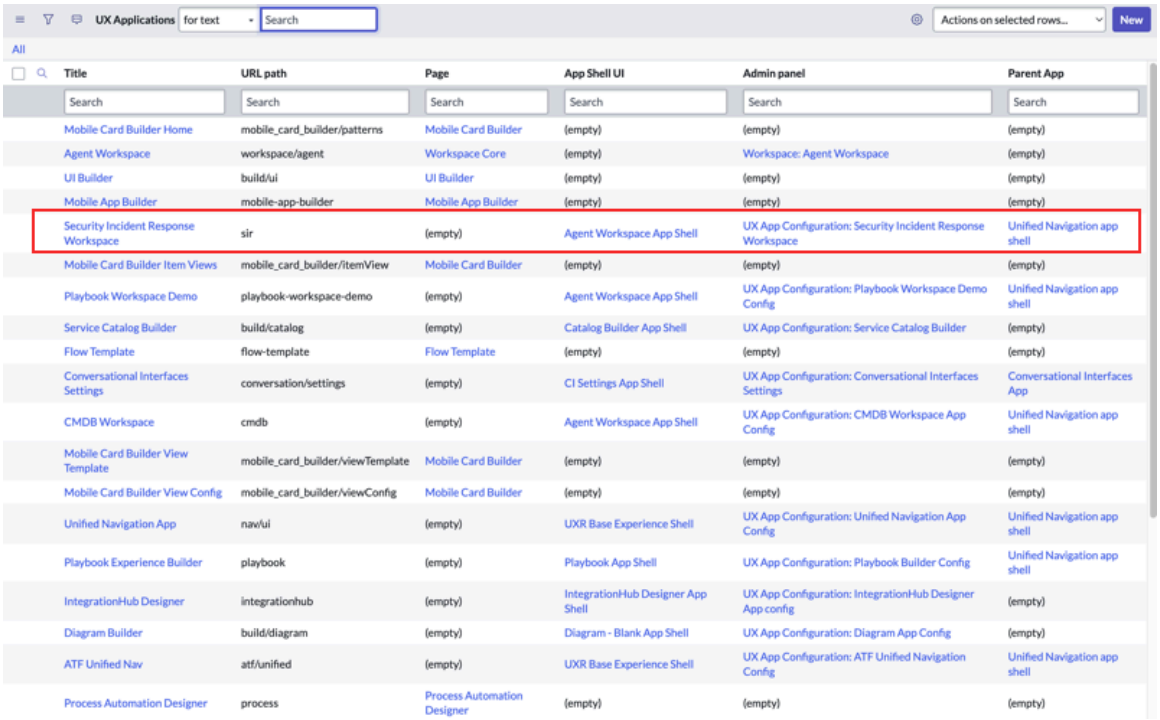


Remarque : Si vous souhaitez modifier quoi que ce soit, sélectionnez la vue et supprimez ou ajoutez les éléments.

8. Cliquez sur **Enregistrer**.
9. Dans le volet de navigation de gauche, accédez à **Tout** > **Cadre de travail Now Experience** > **Expériences**.
10. Sélectionnez **Espace de travail Réponse aux incidents de sécurité**.

Traduction automatique

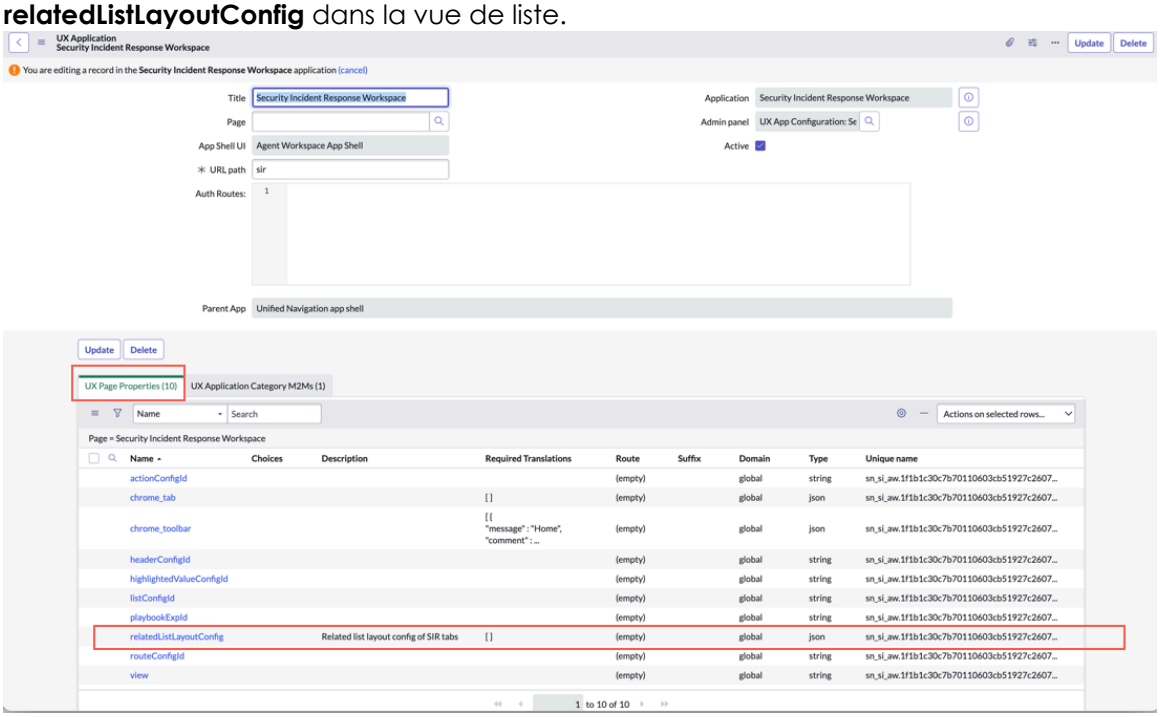
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Title	URL path	Page	App Shell UI	Admin panel	Parent App
Search	Search	Search	Search	Search	Search
Mobile Card Builder Home	mobile_card_builder/patterns	Mobile Card Builder	(empty)	(empty)	(empty)
Agent Workspace	workspace/agent	Workspace Core	(empty)	Workspace: Agent Workspace	(empty)
UI Builder	build/ui	UI Builder	(empty)	(empty)	(empty)
Mobile App Builder	mobile-app-builder	Mobile App Builder	(empty)	(empty)	(empty)
Security Incident Response Workspace	sir	(empty)	Agent Workspace App Shell	UX App Configuration: Security Incident Response Workspace	Unified Navigation app shell
Mobile Card Builder Item Views	mobile_card_builder/itemView	Mobile Card Builder	(empty)	(empty)	(empty)
Playbook Workspace Demo	playbook-workspace-demo	(empty)	Agent Workspace App Shell	UX App Configuration: Playbook Workspace Demo Config	Unified Navigation app shell
Service Catalog Builder	build/catalog	(empty)	Catalog Builder App Shell	UX App Configuration: Service Catalog Builder	(empty)
Flow Template	flow-template	Flow Template	(empty)	(empty)	(empty)
Conversational Interfaces Settings	conversation/settings	(empty)	CI Settings App Shell	UX App Configuration: Conversational Interfaces Settings	Conversational Interfaces App
CMDB Workspace	cmdb	(empty)	Agent Workspace App Shell	UX App Configuration: CMDB Workspace App Config	Unified Navigation app shell
Mobile Card Builder View Template	mobile_card_builder/viewTemplate	Mobile Card Builder	(empty)	(empty)	(empty)
Mobile Card Builder View Config	mobile_card_builder/viewConfig	Mobile Card Builder	(empty)	(empty)	(empty)
Unified Navigation App	nav/ui	(empty)	UXR Base Experience Shell	UX App Configuration: Unified Navigation App Config	Unified Navigation app shell
Playbook Experience Builder	playbook	(empty)	Playbook App Shell	UX App Configuration: Playbook Builder Config	Unified Navigation app shell
IntegrationHub Designer	integrationhub	(empty)	IntegrationHub Designer App Shell	UX App Configuration: IntegrationHub Designer App config	(empty)
Diagram Builder	build/diagram	(empty)	Diagram - Blank App Shell	UX App Configuration: Diagram App Config	(empty)
ATF Unified Nav	atf/unified	(empty)	UXR Base Experience Shell	UX App Configuration: ATF Unified Navigation Config	Unified Navigation app shell
Process Automation Designer	process	Process Automation Designer	(empty)	(empty)	(empty)

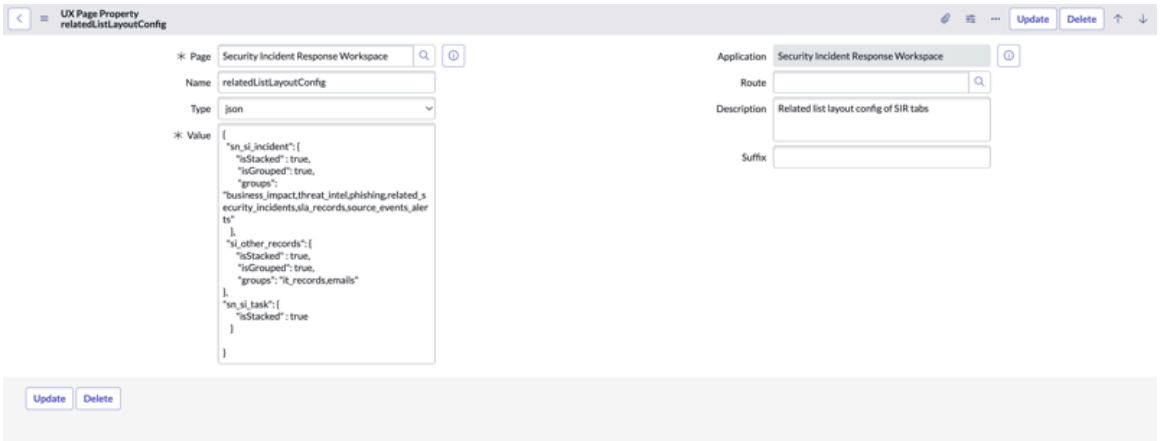
La page **Espace de travail de réponse aux incidents de sécurité de l'application UX** s'affiche.

11. Accédez à l'onglet Propriétés de la **page UX** et sélectionnez **l'option relatedListLayoutConfig** dans la vue de liste.

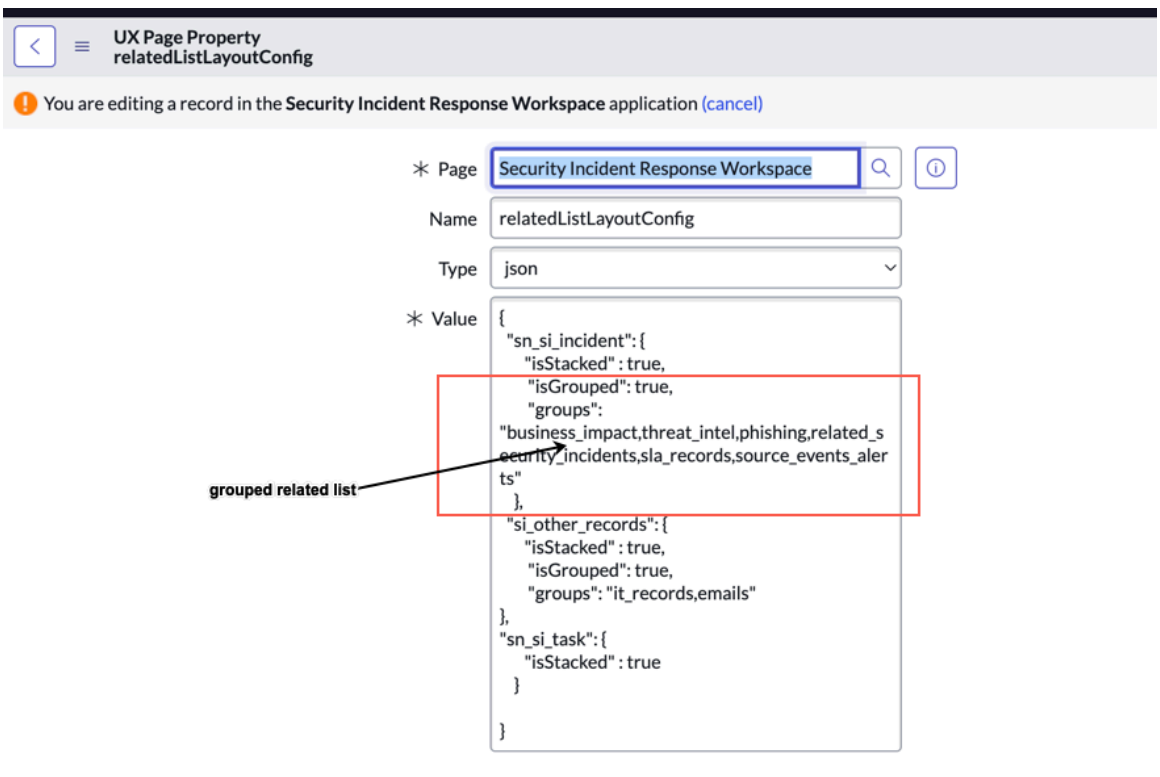


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



12. Ajoutez le nom de la vue nouvellement créée, séparée par une virgule, à une liste de valeurs déjà existante dans la zone de texte **Valeur** , sous le champ **sn_si_incident.viewsUsedForGrouping** .
Par exemple, si vous avez créé un nouveau nom de vue en tant **qu'Impact sur l'entreprise**, vous devez le spécifier en tant que **business_impact** dans la zone de texte **Valeur** (qui est séparé par un trait de soulignement dans le nom de la vue et séparé par une virgule après une valeur existante) sous le champ sn_si_incident :groups.

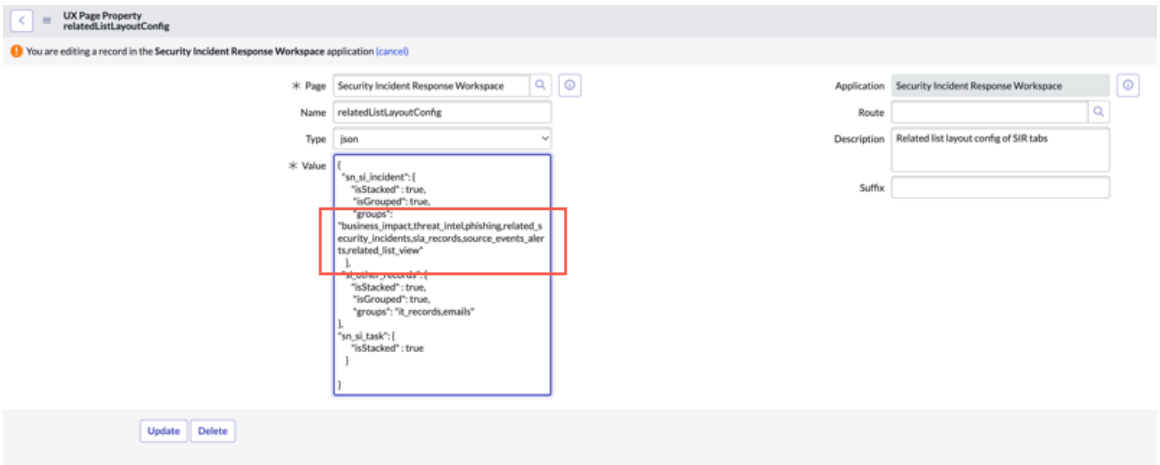


Remarque : Si vous ajoutez le nouveau nom de la vue sous **le champ sn_si_incident.viewsUsedForGrouping** , l'entrée est créée dans l'onglet **Enregistrements connexes** de l'espace de travail.

Si vous mettez à jour l'entrée de nom de la vue dans **si_other_records.viewsUsedForGrouping** , le groupe de listes connexes est ajouté dans l'onglet **Autres enregistrements** de l'espace de travail.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous trouverez ci-dessous un exemple de vue qui montre les vues nouvellement créées ajoutées.



Remarque : requiredRolesForGrouping contient des noms d'enregistrements sys_user_role séparés par des virgules. L'utilisateur de l'espace de travail SIR doit avoir au moins un de ces rôles pour utiliser les listes connexes groupées. Lorsqu'un utilisateur ne dispose d'aucun de ces rôles, la vue de listes connexes configurée pour le rôle d'utilisateur actuel à l'aide de la configuration de la règle de vue est représentée verticalement sans regroupement. Cette propriété est ignorée lorsque la propriété **isGrouped** est définie sur false. Si cette propriété est vide, tout utilisateur peut accéder aux listes connexes regroupées.

13. Cliquez sur **Enregistrer**.
14. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
15. Sélectionnez un incident de sécurité spécifique.
16. Accédez à l'onglet **Enregistrements connexes** de l'espace de travail.
    Les listes connexes groupées s'affichent.

Configurer la liste connexe des tâches de réponse

Utilisez cette section pour configurer les tâches de réponse de nouvelles listes connexes qui apparaissent sur l'application Réponse aux incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

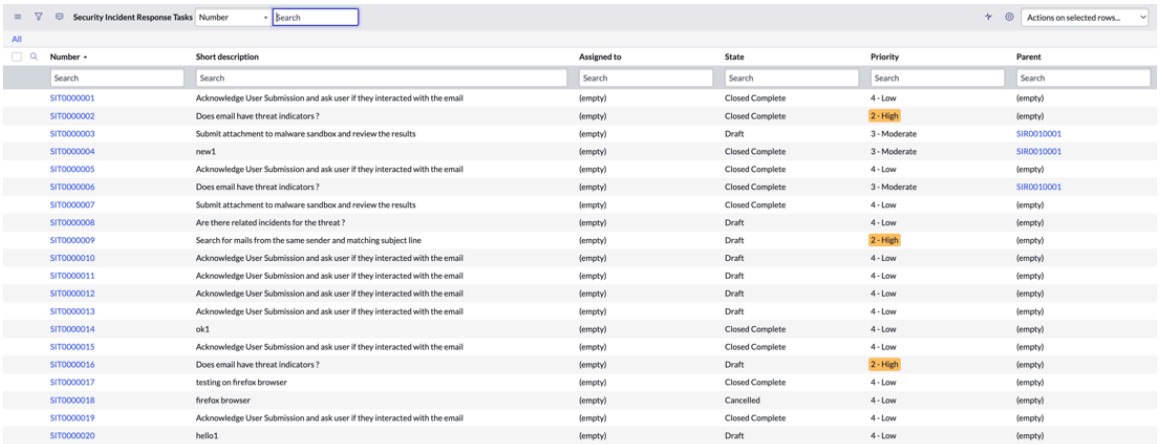
Pourquoi et quand exécuter cette tâche

La liste connexe des tâches de réponse n'est pas regroupée, mais affichée en tant qu'éléments de liste associés individuels, car il existe quelques listes par défaut. Affichez les éléments connexes des tâches de réponse à partir de l'onglet **Tâches de réponse** de l'enregistrement d'incident de sécurité de l'espace de travail.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

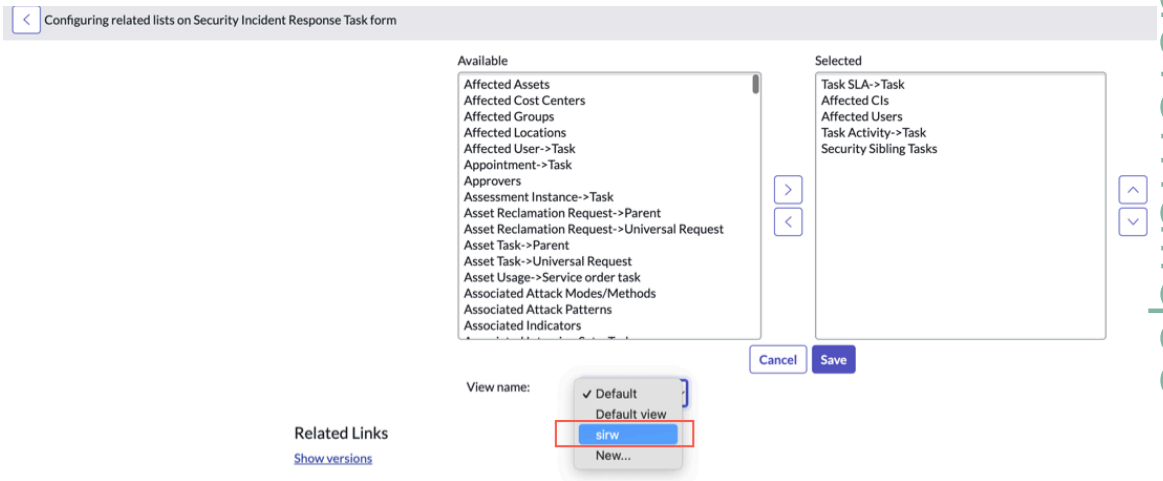
Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Tâches de réponse** > **Afficher toutes les tâches**.



Number	Short description	Assigned to	State	Priority	Parent
SIT0000001	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000002	Does email have threat indicators ?	(empty)	Closed Complete	2 - High	(empty)
SIT0000003	Submit attachment to malware sandbox and review the results	(empty)	Draft	3 - Moderate	SIR0010001
SIT0000004	new1	(empty)	Closed Complete	3 - Moderate	SIR0010001
SIT0000005	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000006	Does email have threat indicators ?	(empty)	Closed Complete	3 - Moderate	SIR0010001
SIT0000007	Submit attachment to malware sandbox and review the results	(empty)	Closed Complete	4 - Low	(empty)
SIT0000008	Are there related incidents for the threat ?	(empty)	Draft	4 - Low	(empty)
SIT0000009	Search for mails from the same sender and matching subject line	(empty)	Draft	2 - High	(empty)
SIT0000010	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000011	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000012	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000013	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000014	ok1	(empty)	Closed Complete	4 - Low	(empty)
SIT0000015	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000016	Does email have threat indicators ?	(empty)	Draft	2 - High	(empty)
SIT0000017	testing on firefox browser	(empty)	Closed Complete	4 - Low	(empty)
SIT0000018	firefox browser	(empty)	Cancelled	4 - Low	(empty)
SIT0000019	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000020	hello1	(empty)	Draft	4 - Low	(empty)

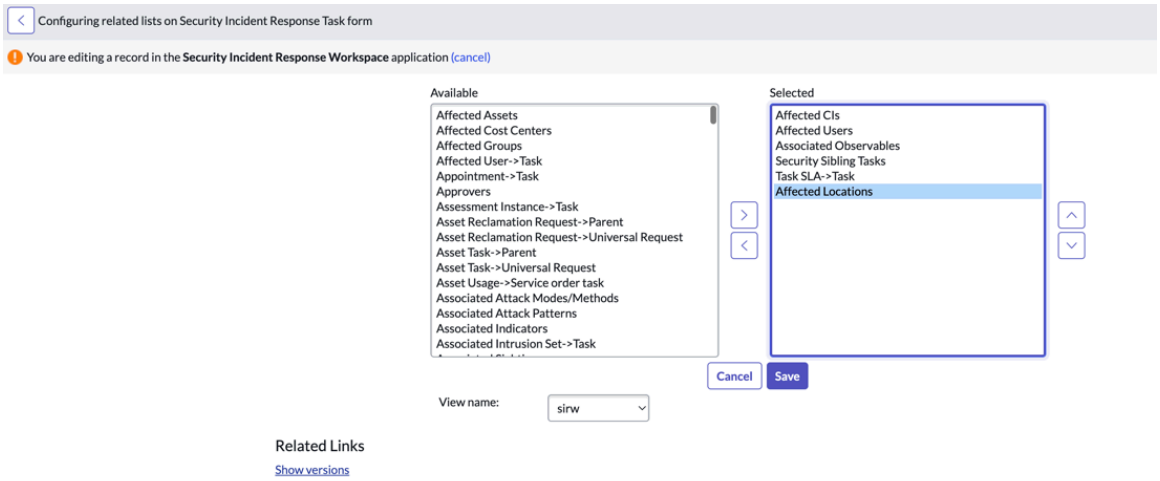
2. Sélectionnez n'importe quel enregistrement de tâche de réponse.
3. Cliquez avec le bouton droit sur le menu contextuel Tâche de réponse aux incidents de sécurité.
4. Accédez à la **Configurer** > **Liste connexe**.
   La **configuration des listes connexes sur le formulaire Tâche de réponse de sécurité** s'affiche.
5. Accédez à **Nom de la vue** et sélectionnez **vue sirw** .



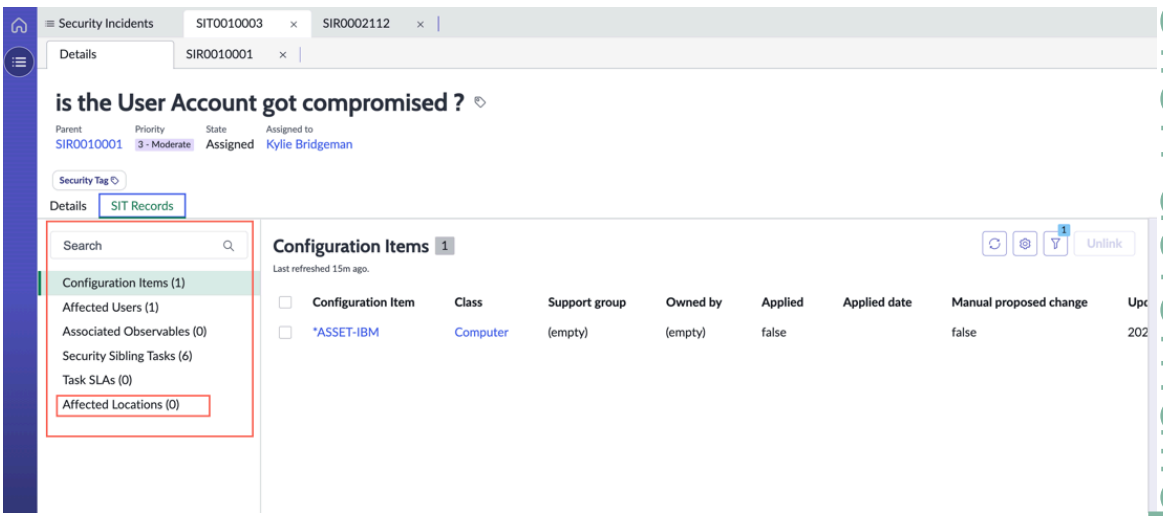
6. Sélectionnez les champs de liste connexe souhaités dans la zone de sélection.
   Par exemple, Emplacements affectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Cliquez sur **Enregistrer**.
8. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Tâches de réponse** > **Enregistrements SIT**.
   Les listes connexes configurées (par exemple, Emplacements affectés tels que sélectionnés) sont répertoriées dans la liste des enregistrements SIT.



Traduction automatique

Définir les nouvelles règles du calculateur de score de risque

Utilisez le nouveau calculateur de score de risque pour définir et calculer le score de risque des incidents de sécurité en fonction des critères définis par l'utilisateur, qui fournissent un score d'intelligence transparent des incidents de sécurité. Le score de risque est calculé automatiquement pour les enregistrements d'incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.admin.

Activez le nouveau calculateur de score de risque en définissant la propriété système `sn_si_aw.activate_new_risk_score_calculator` sur true.

Pourquoi et quand exécuter cette tâche

Définissez un score de risque pour les enregistrements d'incidents de sécurité qui sont générés en fonction des paramètres définis par l'utilisateur. Le système de base est doté d'une règle de définition du score de risque, qui peut être personnalisée et activée en conséquence.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Par défaut, la nouvelle règle du calculateur de score de risque est inactive, et vous devez activer la règle pour consulter le score de risque des incidents de sécurité.
- Pour calculer le score de risque pour d'autres tables connexes autres que celles disponibles dans le système de base, reportez-vous à Calculateur de score de risque pour les tables connexes supplémentaires.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Administration**.
2. Accédez à la **Moteur de règles** > **Règle du calculateur de score de risque**.
   La page Règle du calculateur de score de risque s'affiche.

   ### Remarque :

   - Dans le cadre du système de base, vous disposez d'un modèle de règle de score de risque prédéfini pour afficher, modifier ou modifier le score de risque. Toutefois, vous ne pouvez pas créer ou supprimer le modèle de règle de score de risque prédéfini.
   - Les modifications que vous apportez s'appliqueront à tous les nouveaux incidents de sécurité ou aux mises à jour des incidents existants. Pour retraiter les scores historiques, utilisez l'action **Recalculer le score** .

3. Sélectionnez la règle du **calculateur de score de risque** .
4. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom de la valeur de score de risque. Par exemple, Calculateur de score de risque.
Pondération globale (applicable au générateur de critères)	Pondération de ce champ dans la règle de risque. Ce champ n'est pas modifiable et affiche la pondération globale calculée par le système en fonction du poids correspondant aux critères activés. La pondération globale doit toujours être de 100 %.
Description	Description de l'enregistrement du score de risque. Par exemple, calcule le score de risque en fonction de la somme pondérée des scores de critères prédéfinis.
Critères de notation	Indique les critères de notation pour un incident de sécurité. Vous pouvez définir les **critères de score** de risque à l'aide des options suivantes : ◦ **Générateur de critères** : Utilisez cette option pour ajouter, modifier ou supprimer, activer et désactiver les critères qui contribuent au calcul

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	du score de risque et vérifier que la pondération totale agrégée est de 100 %. ◦ **Utiliser un script (avancé)** : la fonctionnalité de scripting est une fonctionnalité avancée permettant de créer un script personnalisé qui doit renvoyer le score de risque dans une plage comprise entre 0 et 100.

5. Pour définir les **critères de notation** à l'aide du **générateur de critères**, procédez comme suit :

   Remarque : Vous pouvez modifier les critères existants ou en ajouter un nouveau.

   a. Pour ajouter un nouveau critère, sélectionnez l'action **+Nouveau critère** .

   b. Sélectionnez la **table** pour laquelle vous souhaitez définir les critères.

   Remarque :

   - Si la table sélectionnée est un incident de sécurité, la condition est appliquée à l'enregistrement d'incident de sécurité pour lequel le score de risque est calculé. Si la table sélectionnée n'est pas un incident de sécurité, la condition n'est appliquée que si les enregistrements sont liés à l'incident de sécurité pour lequel le score de risque est calculé.
   - Un type d'agrégat supplémentaire est ajouté pour définir les scores en fonction du nombre de relations associées aux incidents de sécurité.

   c. Sélectionnez les critères **de type** pour la table sélectionnée.
   La valeur Type peut être **Champ** ou **Agrégat** en fonction de la table que vous choisissez.

   d. Sélectionnez les critères **de champ** pour la table sélectionnée.
   Si vous avez sélectionné la valeur Type **Champ**, les critères de champ affichent les valeurs de champ associées à la table. Si vous avez sélectionné la valeur Type **Agrégat,** les critères Champ affichent les valeurs d'agrégat associées à la table.

   Remarque : Le type Agrégat prend uniquement en charge la valeur Nombre.

   Par exemple, si vous sélectionnez les critères de table sur **Incident de sécurité**, les critères de type affichent uniquement l'option **Champ** . Les critères de champ affichent toutes les valeurs de champ associées à la table, qui peuvent être Gravité, Actif, etc. De même, si vous sélectionnez les critères de la table en tant **qu'Utilisateurs affectés**, les critères de type affichent à la fois l'option **Champ** et **Agrégat** . Si vous sélectionnez le type Agrégat, les critères de champ affichent les valeurs d'agrégat associées à la table, qui est **Nombre**.

   e. Entrez la **pondération** des critères entre 0 et 100.
   La pondération globale de tous les critères doit être de 100 %.

   f. Entrez le nom et une brève description des critères.

   g. Cochez la case **Activer les critères de notation** pour activer les critères de notation.

Traduction automatique

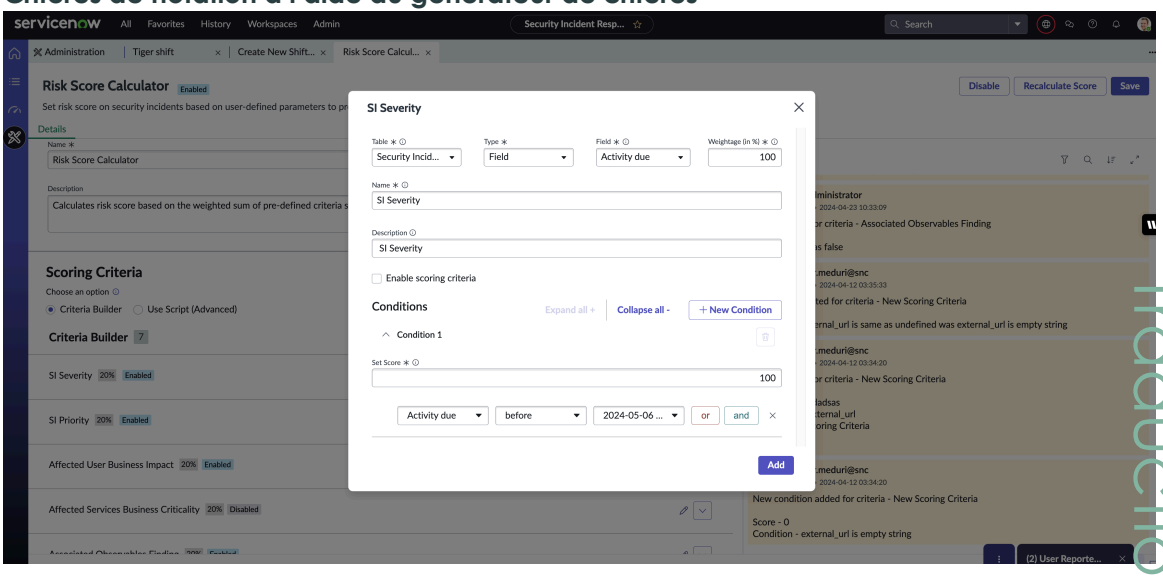
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

h. Définissez les **conditions** et définissez le score pour les conditions.

i. Vous pouvez également ajouter de nouvelles conditions à l'aide de l'option **Nouvelle condition** et supprimer les conditions existantes à l'aide de l'icône **Supprimer les critères** .

j. Sélectionnez **Ajouter** pour ajouter les critères configurés.

Critères de notation à l'aide du générateur de critères



6. Sélectionnez l'option **Recalculer le score** pour recalculer le score de risque.

Par exemple, si des changements sont apportés à la règle du score de risque. Dans ce cas, vous devez réappliquer la règle de notation aux incidents de sécurité dont le score de risque a déjà été calculé dans le passé. Utilisez l'action **Recalculer le score** pour déclencher la tâche de recalcul.

7. Sélectionnez **Confirmer**.

Remarque : Une fois que vous avez déclenché cette action, le processus s'exécute en arrière-plan et prend quelques minutes. Vous ne pouvez pas apporter de modifications tant qu'il n'est pas terminé.

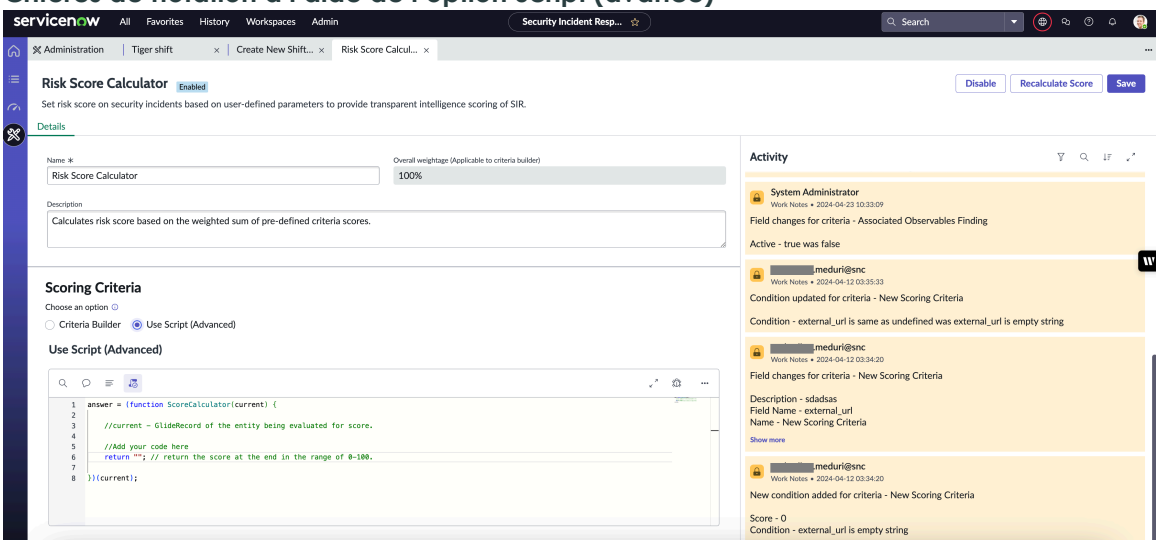
8. Pour définir les **critères de notation** à l'aide de l'option **Utiliser le script (avancé)**, procédez comme suit :

a. Utilisez ce script prédéfini pour créer un script personnalisé qui doit renvoyer le score de risque dans une plage comprise entre 0 et 100.
Le champ de script avancé est renseigné automatiquement avec une fonction, qui prend les paramètres **actuels** et cette fonction doit renvoyer le score de risque dans la plage de 0 à 100.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Critères de notation à l'aide de l'option Script (avancé)



Ici, le paramètre actuel est l'objet GlideRecord de l'entité (incident de sécurité) pour laquelle le score de risque est calculé. Pour les incidents de sécurité, il correspond au GlideRecord de la table sn_si_incident.

9. Pour désactiver le calculateur de score de risque, sélectionnez **Désactiver**.
10. Sélectionnez **Enregistrer**.

Calculateur de score de risque pour les tables connexes supplémentaires

Le calculateur de score de risque est fourni avec une règle de score de risque dans le cadre du système de base pour calculer le score de risque des incidents de sécurité en fonction de critères définis par l'utilisateur. Toutefois, vous pouvez personnaliser et inclure des tables connexes supplémentaires pour calculer le score de risque.

Avant de commencer

Rôle requis : sn_si.admin.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez n'importe quel enregistrement d'incident de sécurité.
3. Sélectionnez l'option **Actions supplémentaires** en regard du numéro d'incident de sécurité.
4. Accéder à **Configurer** > **Listes connexes**.
5. Accédez au nom de la vue, puis sélectionnez **Calculateur de score de risque**.
   Une fois que vous avez sélectionné la vue, choisissez la liste connexe requise que vous souhaitez ajouter à partir de la zone de sélection. Par exemple, Observations associées.
6. Sélectionnez **Enregistrer**.
   Vous avez ajouté avec succès les nouvelles listes ou tables connexes pour lesquelles vous souhaitez calculer le score de risque.

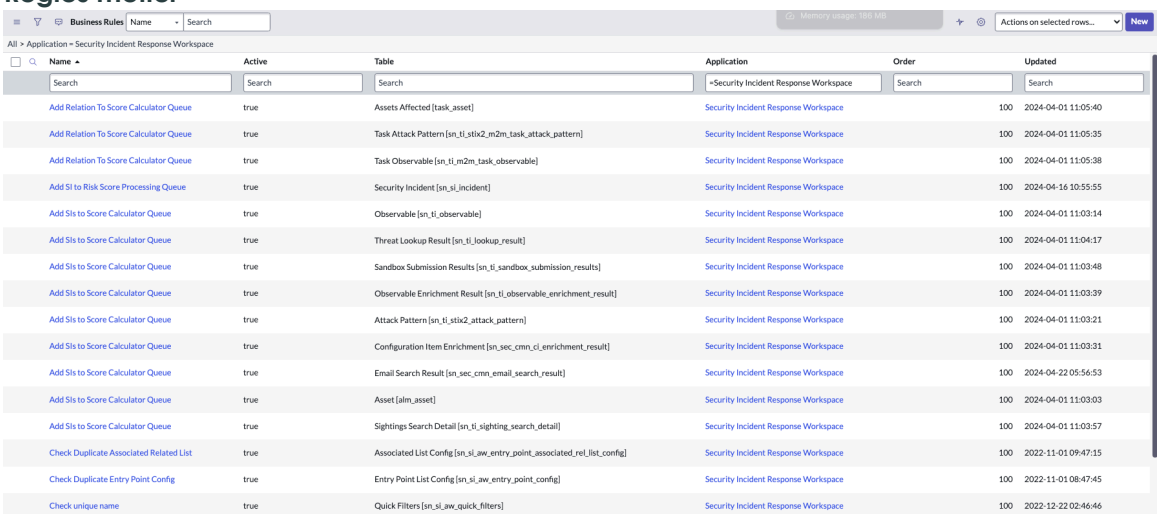
> **Important :** Pour calculer le score de risque pour les incidents de sécurité qui ont de nouveaux critères avec les listes connexes nouvellement créées, vous devez définir des règles métier sur la table de base de la liste connexe.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Accédez à la **Tout** > **Définition du système** > **Règles métier**.
   Vous pouvez utiliser les deux règles métier suivantes comme référence pour créer vos propres règles métier :
   - Ajouter des incidents de sécurité (SI) à la file d'attente du calculateur de score
   - Ajouter une relation à la file d'attente du calculateur de score (ceci s'applique aux tables m2m)

Règles métier



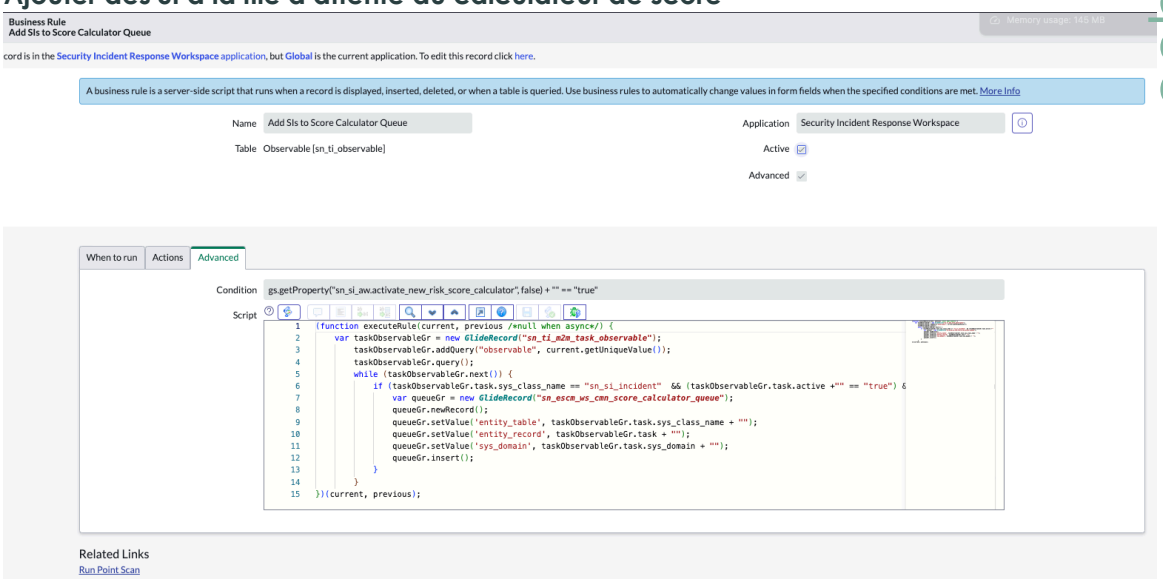
Name	Active	Table	Application	Order	Updated
Add Relation To Score Calculator Queue	true	Assets Affected [task_asset]	Security Incident Response Workspace	100	2024-04-01 11:05:40
Add Relation To Score Calculator Queue	true	Task Attack Pattern [sn_ti_stix2_m2m_task_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:05:35
Add Relation To Score Calculator Queue	true	Task Observable [sn_ti_m2m_task_observable]	Security Incident Response Workspace	100	2024-04-01 11:05:38
Add SI to Risk Score Processing Queue	true	Security Incident [sn_si_incident]	Security Incident Response Workspace	100	2024-04-16 10:55:55
Add SIs to Score Calculator Queue	true	Observable [sn_ti_observable]	Security Incident Response Workspace	100	2024-04-01 11:03:14
Add SIs to Score Calculator Queue	true	Threat Lookup Result [sn_ti_lookup_result]	Security Incident Response Workspace	100	2024-04-01 11:04:17
Add SIs to Score Calculator Queue	true	Sandbox Submission Results [sn_ti_sandbox_submission_results]	Security Incident Response Workspace	100	2024-04-01 11:03:48
Add SIs to Score Calculator Queue	true	Observable Enrichment Result [sn_ti_observable_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:39
Add SIs to Score Calculator Queue	true	Attack Pattern [sn_ti_stix2_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:03:21
Add SIs to Score Calculator Queue	true	Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:31
Add SIs to Score Calculator Queue	true	Email Search Result [sn_sec_cmn_email_search_result]	Security Incident Response Workspace	100	2024-04-22 05:56:53
Add SIs to Score Calculator Queue	true	Asset [alm_asset]	Security Incident Response Workspace	100	2024-04-01 11:03:03
Add SIs to Score Calculator Queue	true	Sightings Search Detail [sn_ti_sighting_search_detail]	Security Incident Response Workspace	100	2024-04-01 11:03:57
Check Duplicate Associated Related List	true	Associated List Config [sn_si_aw_entry_point_associated_rel_list_config]	Security Incident Response Workspace	100	2022-11-01 09:47:15
Check Duplicate Entry Point Config	true	Entry Point List Config [sn_si_aw_entry_point_config]	Security Incident Response Workspace	100	2022-11-01 08:47:45
Check unique name	true	Quick Filters [sn_si_aw_quick_filters]	Security Incident Response Workspace	100	2022-12-22 02:46:46

8. Par exemple, pour que les critères observables associés fonctionnent, nous avons défini deux règles métier.

   La première est la règle métier **Ajouter des SI à la file d'attente du calculateur de scores** .

   Par exemple, un nouvel incident de sécurité est créé et associé à une table d'observables (`Observables[sn_ti_observable]`). Après la recherche de menace, l'observable est considéré comme malveillant. Vous devez ensuite ajouter tous les incidents de sécurité associés à cet observable malveillant à la file d'attente pour recalculer le score de risque des incidents de sécurité.

Ajouter des SI à la file d'attente du calculateur de score



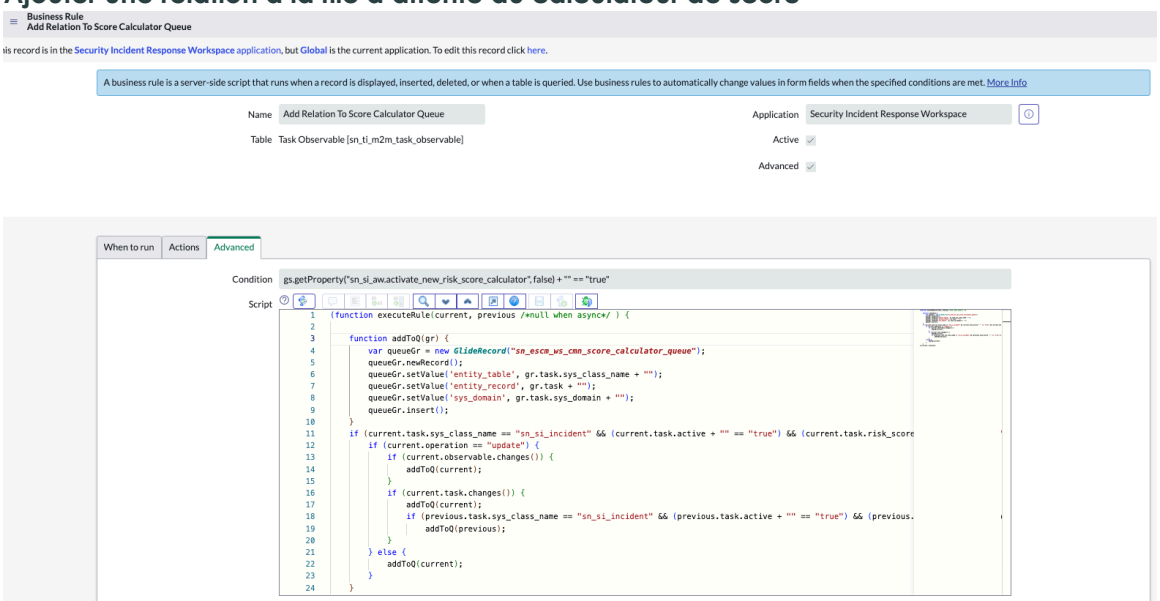
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La seconde est la règle métier **Ajouter une relation à la file d'attente du calculateur de score** .

Par exemple, un nouvel incident de sécurité est créé ou supprimé et associé à une table d'observables (`Observables de tâche[sn_ti_m2m_task_observable]`). Il y a donc un changement dans l'association de l'incident de sécurité. Vous devez ensuite ajouter cet incident de sécurité à la file d'attente pour recalculer le score de risque de l'incident de sécurité.

Ajouter une relation à la file d'attente du calculateur de score



Configurer les modèles de transfert d'équipe

L'administrateur peut définir et configurer différents modèles de transfert d'équipe pour que le propriétaire d'équipe crée des enregistrements de transfert d'équipe et les transmette à l'équipe d'équipe suivante.

Avant de commencer

Rôle requis :

- sn_escm_sh.shift_admin
- sn_si.admin hérite du rôle sn_escm_sh.shift_admin

Pourquoi et quand exécuter cette tâche

Pour configurer un modèle de transfert d'équipe, l'administrateur crée un nouveau modèle de transfert d'équipe ou ouvre un modèle existant dans le système de base avec le nom **Exemple de modèle d'équipe** et modifie les détails et les sections en fonction de vos besoins.

Le propriétaire d'équipe peut utiliser le modèle configuré pour créer des enregistrements de journal de transfert d'équipe, puis le rapport de transfert d'équipe est partagé avec le propriétaire d'équipe actif suivant et son équipe.

Remarque : Seuls les modèles de transfert d'équipe actifs sont visibles pour que le propriétaire d'équipe crée des enregistrements de journal de transfert.

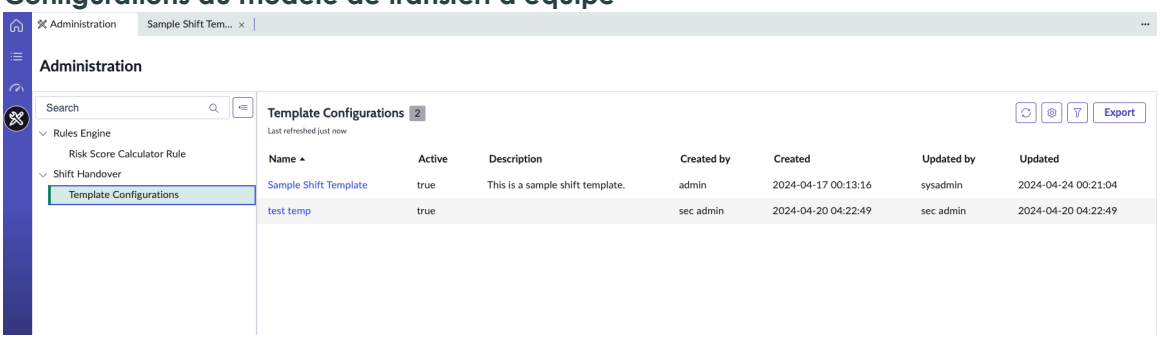
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Administration**.
2. Accédez à la **Transfert d'équipe** > **Configurations de modèles**.
   La page Configurations des modèles s'affiche.

> **Remarque :** Dans le cadre du système de base, vous disposez d'une configuration de modèle de transfert d'équipe prédéfinie pour afficher, modifier ou modifier le modèle de transfert d'équipe. Toutefois, vous ne pouvez pas créer ou supprimer la configuration prédéfinie du modèle de transfert d'équipe.

Configurations du modèle de transfert d'équipe



3. Pour créer un nouveau modèle de transfert d'équipe, sélectionnez **Nouveau**.
4. Renseignez les champs du formulaire Détails.

Créer un nouveau modèle de transfert d'équipe

Champ	Description
Nom	Nom du modèle de transfert d'équipe. Par exemple, Modèle SIR.
Application	Nom de l'application pour laquelle vous créez le modèle de transfert d'équipe. Par exemple, Espace de travail Réponse aux incidents de sécurité.
Actif	Option permettant d'indiquer si le modèle de transfert d'équipe est actif. Activez cette option pour activer le modèle de transfert d'équipe.
Description	Description du modèle de transfert d'équipe.
Enregistrer la configuration de la mention	Utilisez ce champ pour configurer les détails de mention de l'enregistrement de l'éditeur de texte enrichi (RTE). L'entrée est un tableau d'objets JSON avec les champs suivants : ◦ *sourceTable* : nom de la table source. ◦ *étiquette* : nom de l'étiquette à afficher.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ *filterCondition* : requête codée pour le filtrage ◦ *champs* : sélectionner les champs pour interroger le modèle Exemple de configuration que vous pouvez copier-coller dans le champ de configuration de la mention d'enregistrement. `[ { "sourceTable": "incident", "label": "Incidents", "filterCondition": "active=true", "fields": [ "number" ] } ]` Pour copier l'exemple de configuration, utilisez l'action **Copier dans le presse-papiers** du volet Assistance contextuelle. Ensuite, vous pouvez apporter des modifications supplémentaires en fonction de vos besoins.

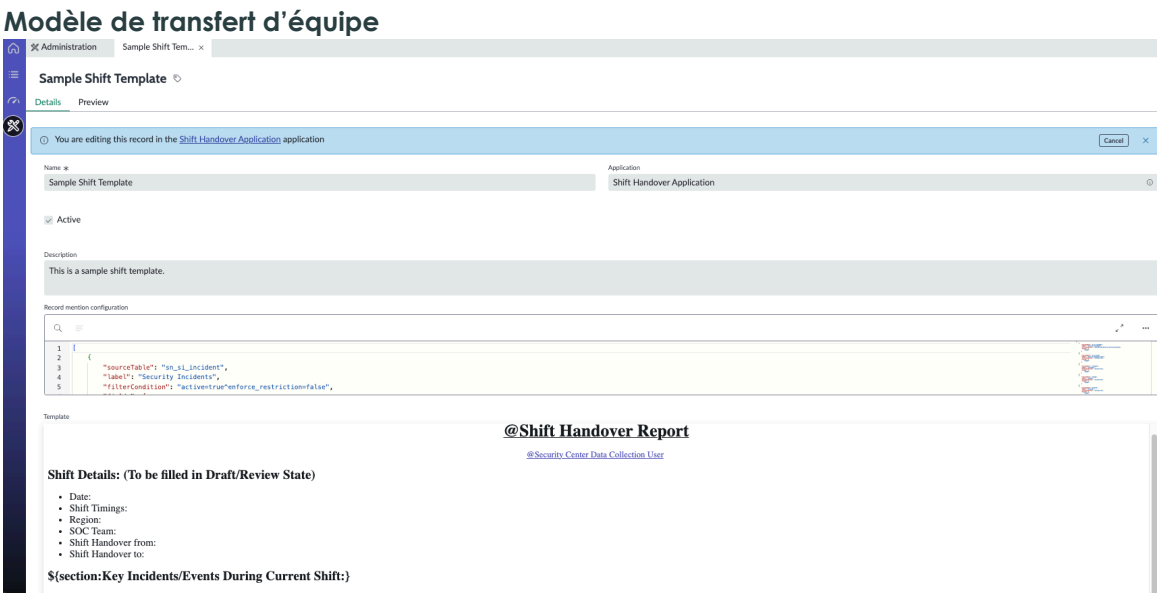
Modèle	Créez un modèle de transfert d'équipe à l'aide de sections. Assurez-vous qu'il existe au moins une section pour que les analystes puissent contribuer aux enregistrements du journal de transfert d'équipe basés sur le modèle.
	
	Le modèle peut contenir du texte statique, des images, etc., dans les sections appropriées. Vous pouvez copier et coller des images directement dans le champ Modèle. Vous pouvez créer des sections dans le modèle à l'aide du code suivant :
	
	`${section:Section Label}`
	
	Exemple :
	
	`${section:Key Incidents/Events During Current Shift} ${section:Incidents/Events to Monitor or Follow Up} ${section:System/Infrastructure Updates}`

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description

	`${section:Next Steps for Incoming Shift}`
	`${section:References}`
	
	Remarque : Pour plus d'informations, reportez-vous à **l'assistance contextuelle** dans le volet droit.

5. Pour utiliser et modifier un modèle de transfert d'équipe existant, sélectionnez **Exemple de modèle d'équipe**.

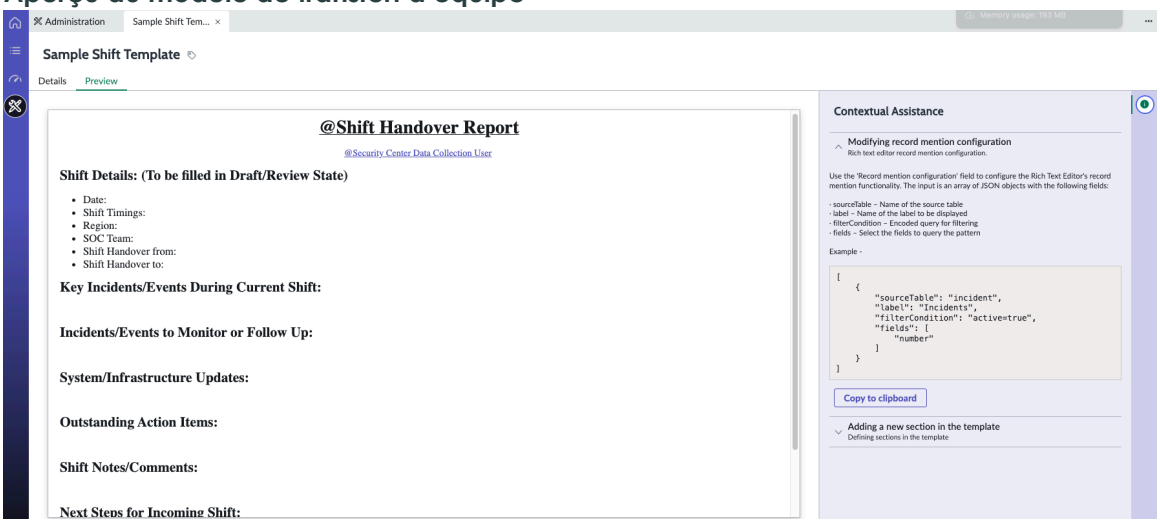


6. Mettez à jour le modèle de transfert d'équipe en fonction de vos besoins.
7. Sélectionnez **Aperçu** pour afficher l'aperçu de l'exécution du modèle de transfert d'équipe.

   Le rapport génère un aperçu basé sur la configuration du modèle de transfert d'équipe.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçu du modèle de transfert d'équipe



8. Sélectionnez **Enregistrer** pour enregistrer le modèle de transfert d'équipe.

Que faire ensuite

Pour apprendre à gérer les enregistrements de transfert d'équipe dans la vue de liste et à effectuer des actions telles que créer, modifier, copier ou supprimer des enregistrements de transfert d'équipe, reportez-vous à la section Gérer les enregistrements de transfert d'équipe.

Utiliser SIR Workspace

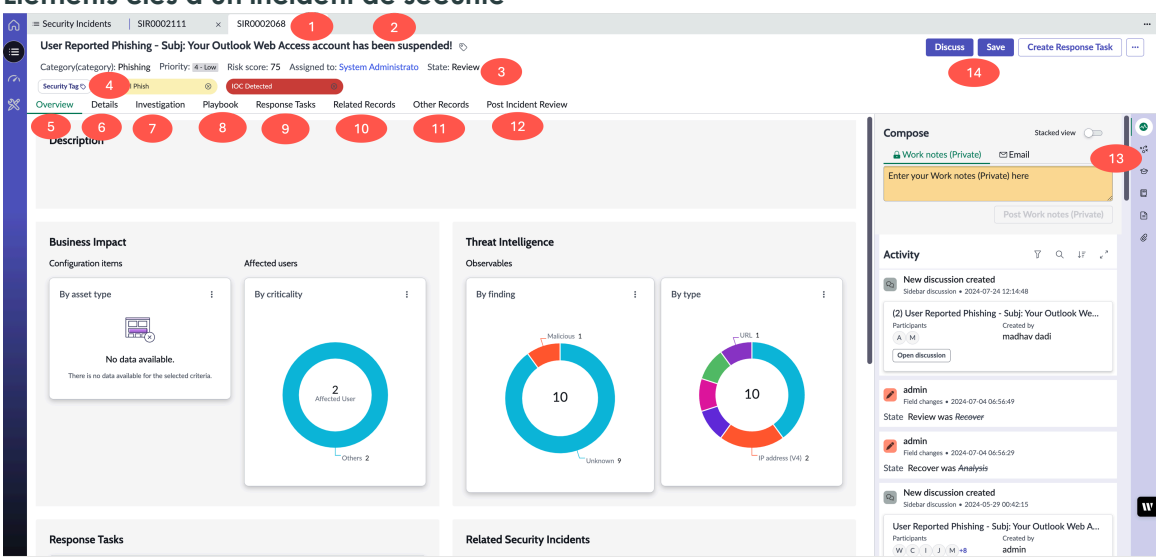
Les analystes et les gestionnaires de sécurité ont l'habitude SIR Workspace d'effectuer des opérations quotidiennes avec une expérience utilisateur améliorée, de terminer l'enquête sur les incidents et d'obtenir une vue d'ensemble.

Utilisation des enregistrements d'incidents de sécurité

L'enregistrement d'incident de sécurité se compose des éléments suivants.

Composants clés disponibles dans un enregistrement d'incident de sécurité :

Éléments clés d'un incident de sécurité



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Numéro	Nom	Description
1	Numéro d'incident de sécurité	Le numéro de l'incident de sécurité est disponible en regard du nom de l'onglet.
2	Description brève	Brève description de l'incident de sécurité qui s'affiche au-dessus de la bannière du formulaire.
3	Bannière de formulaire	Il s'agit d'une section en lecture seule qui contient les champs clés tels que la catégorie, la priorité, le score de risque, l'état et les détails d'affectation de l'incident. **Remarque :** Les balises de plate-forme régulières peuvent également être appliquées ici.
4	Balises de sécurité	Affiche les balises de sécurité associées à un incident de sécurité.
5	Vue d'ensemble	Fournit une vue d'ensemble instantanée de l'incident de sécurité telle que la description, l'impact sur l'entreprise comprenant les détails des actifs par type, les utilisateurs affectés par criticité, les éléments de renseignements sur les menaces comprenant des observables par résultat et par type, les tâches de réponse, les incidents de sécurité connexes comprenant des incidents de sécurité enfants et des incidents de sécurité similaires.
6	Détails	L'onglet Détails affiche le formulaire d'incident de sécurité.
7	Examen	L'onglet Examiner affiche l'expérience d'enquête sur l'incident.
8	Playbook	Le Playbook est déclenché via Concepteur d'automatisation de processus (PAD). Si un processus est créé et si une condition de déclenchement est définie pour déclencher le Playbook pour un incident de sécurité. Ensuite, un playbook s'affiche.
9	Tâches de réponse	Les tâches de réponse capturent toutes les tâches de réponse associées à un incident de sécurité.
10	Enregistrements connexes	L'onglet Enregistrements connexes se compose de toutes les listes connexes de l'interface utilisateur classique sous cette section. Les listes connexes sont regroupées sous différentes sections telles que l'impact sur l'entreprise, les informations sur les menaces, etc., pour faciliter la navigation.
11	Autres enregistrements	L'onglet Autres enregistrements comprend les enregistrements informatiques tels que les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Numéro	Nom	Description
		demandes de changements, les incidents et les e-mails, regroupés et affichés dans cette section.
12	Onglet Revue post-incident	Au fur et à mesure que l'incident de sécurité progresse vers l'état de révision, l'onglet Revue post-incident s'affiche avec les évaluations et rapports post-incident dans l'onglet.
13	Menu contextuel	Fournit un accès facile aux actions rapides et est disponible dans tous les onglets pour que l'analyste puisse y accéder quand il en a besoin. Le menu contextuel permet d'accéder facilement aux multiples ressources telles que : **1.** Flux d'activité **2.** Playbook **3.** Assistant analyste **4.** Runbook **5.** Modèles **6.** Pièces jointes
14	Actions d'interface utilisateur du formulaire	Les différentes actions d'interface utilisateur du formulaire d'incident de sécurité sont affichées en haut à droite du formulaire d'incident. Les actions d'interface utilisateur de formulaire disponibles sont : • Discuter • Enregistrer • Créer une tâche de réponse • Composer un e-mail • Ajouter un Playbook • Ouvrir les workflows associés • Incident en Crète • Créer un problème • Créer une demande de changement • Créer une panne • Calculer la gravité • Lier à Incident de sécurité majeur • Proposer en tant que Incident de sécurité majeur • Promouvoir à Incident de sécurité majeur • Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison • Associer la technique MITRE ATT&CK • Basculer vers l'interface utilisateur classique

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Numéro	Nom	Description
		• Ajouter au ticket de sécurité • Supprimer Pour plus d'informations, consultez Utiliser les actions d'interface utilisateur de formulaire.

Section Vue d'ensemble de l'incident de sécurité

La section Vue d'ensemble de l'espace de travail présente les informations clés associées à l'incident de sécurité.

L'exploration vers le bas des graphiques en anneau est activée, lorsqu'un analyste sélectionne l'un des éléments de graphique, il vous dirige vers l'enregistrement respectif avec une vue de liste filtrée des éléments de cet onglet correspondant. Par exemple, si l'option **Observables malveillants** est sélectionnée, vous êtes redirigé vers les observables avec une vue de liste filtrée des observables malveillants dans l'onglet **Enregistrements connexes** .

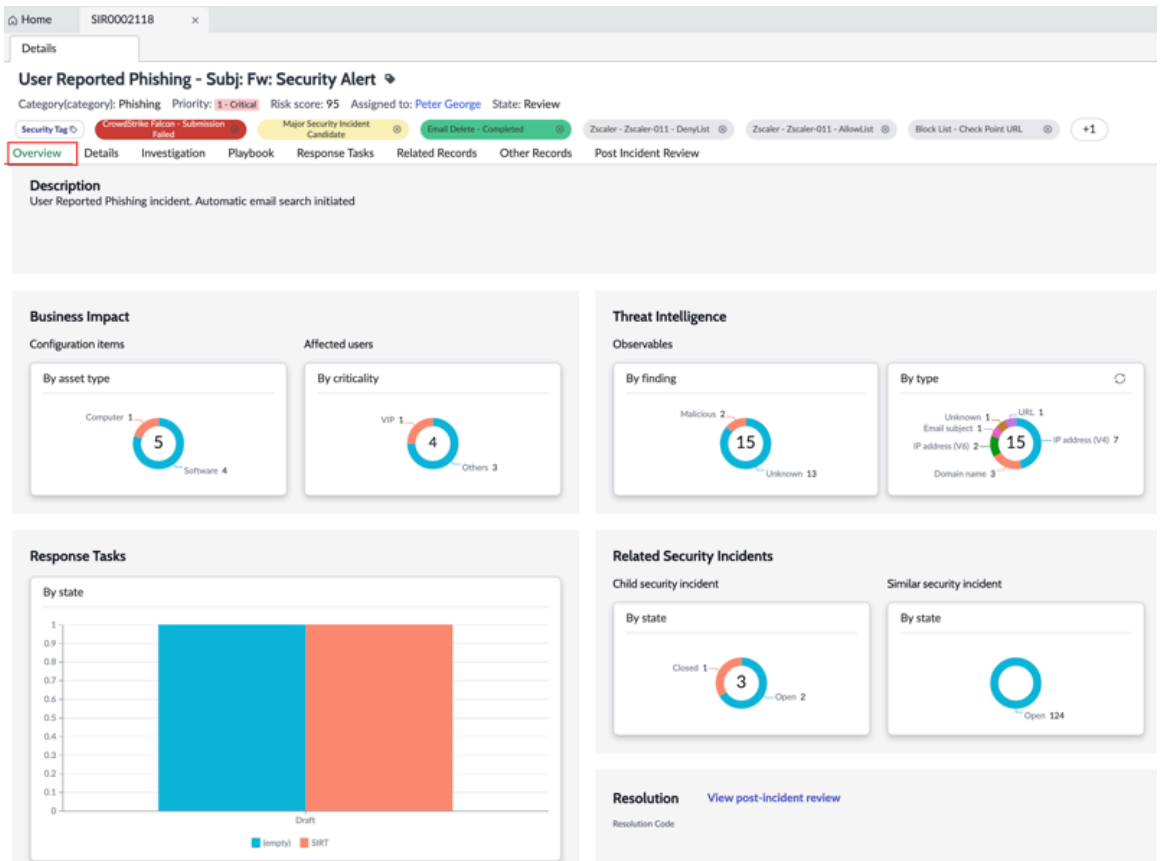
La section Vue d'ensemble affiche les éléments suivants :

- Description de l'incident de sécurité.
- Détails de l'impact sur l'entreprise, tels que les éléments de configuration par type d'actif et les utilisateurs affectés par criticité, qu'il s'agisse d'utilisateurs VIP ou d'autres utilisateurs.
- Éléments de Threat Intelligence tels que les observables en déterminant s'il s'agit d'observables, de malveillants ou inconnus, et par type.
- Tâches de réponse par état et groupe d'affectation.
- Incidents de sécurité associés comprenant des incidents de sécurité enfants par état, ouverts ou fermés, et des incidents de sécurité similaires par état, qu'ils soient ouverts ou fermés.
- La section Résolution s'affiche lorsqu'un incident passe à l'état Examen, puis la section Résolution s'affiche dans la section **Vue d'ensemble** avec la possibilité d'afficher la revue post-incident.
- Résolution : afficher la revue post-incident : sélectionnez le lien pour accéder à la page de **revue post-incident** .
- Une fois l'incident fermé, la section Résolution affiche le code de résolution, les notes de résolution et Résolu par (utilisateur), ainsi que les détails de la revue post-incident.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Section Vue d'ensemble



Incident de sécurité Section Détails

Cette section affiche les champs de formulaire d'incident de sécurité qui sont rendus à partir de l'interface utilisateur classique de l'incident de sécurité.

L'interface utilisateur classique dispose d'une vue appelée **Vue SIRW** créée. Cette vue est mappée à l'onglet **Détails** dans le nouvel espace de travail. Toutes les personnalisations requises doivent être implémentées dans cette vue.

Les champs de formulaire sont regroupés dans les sections suivantes et affichés dans la vue de formulaire de l'onglet Détails, cliquez sur l'une des sections ou accédez à la section respective dans le formulaire :

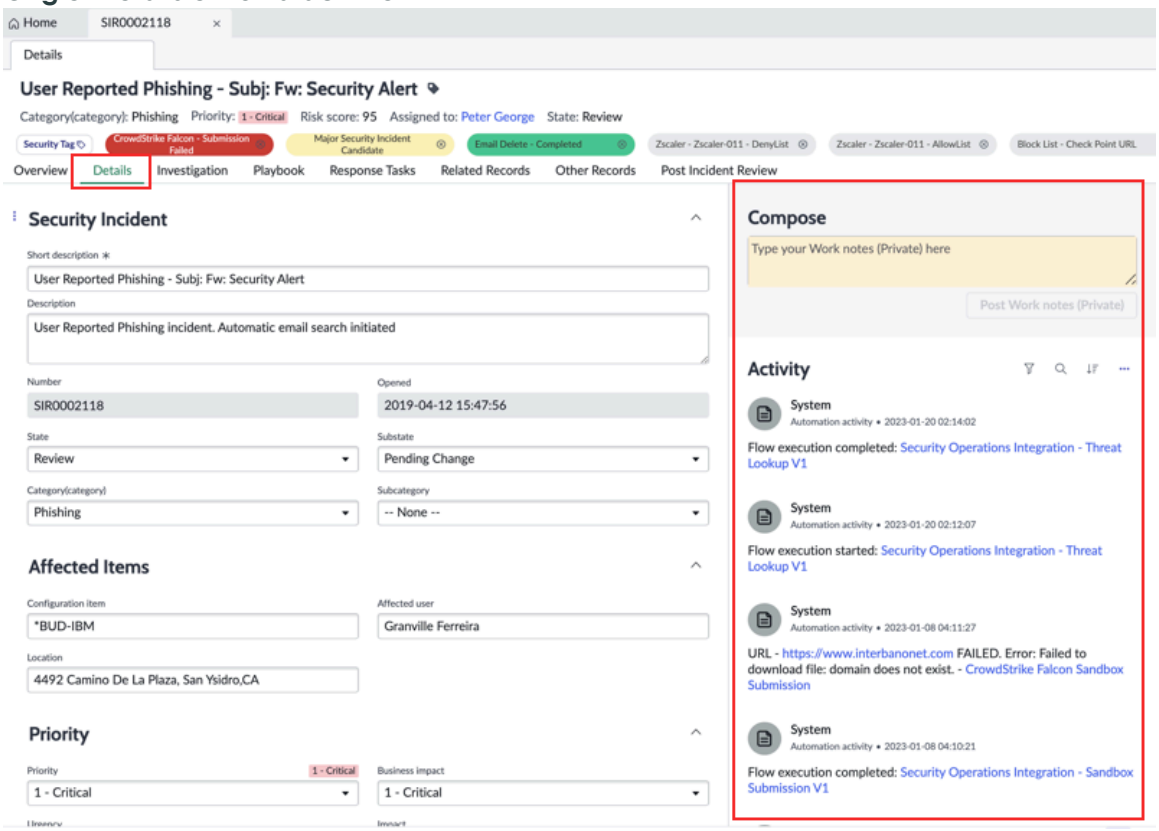
- Incident de sécurité
- Priorité
- Source
- Parent
- Affectation
- Contrôles des accès
- Éléments affectés
- Résolution

L'onglet **Détails** contient la section **Flux d'activité** dans le formulaire de détails lui-même pour un accès rapide aux analystes de sécurité pour ajouter des commentaires et le publier.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

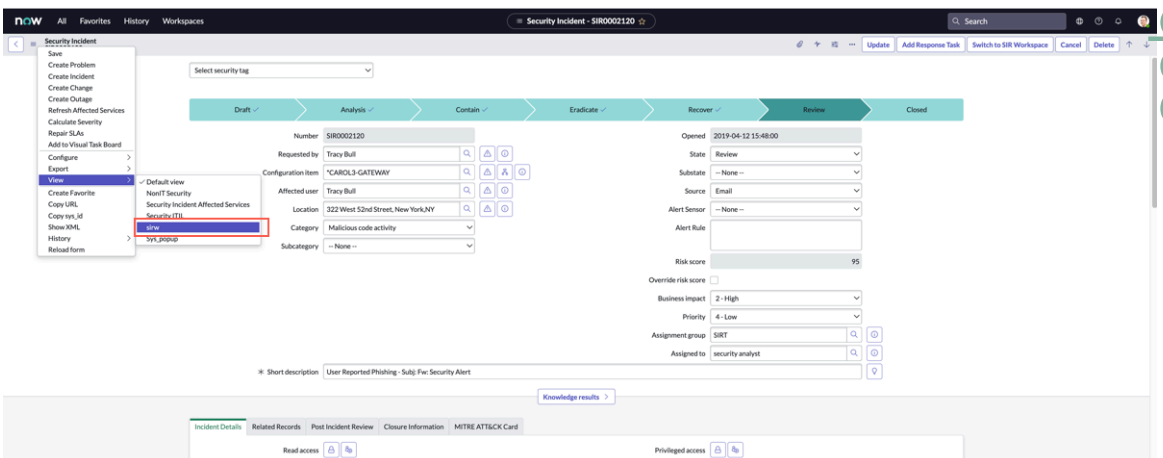
Onglet Détails et flux d'activité



Affichez la vue Espace de travail de l'analyste SIR :

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. Sélectionnez n'importe quel enregistrement d'incident de sécurité.
3. Cliquez sur le menu contextuel et sélectionnez **Vue** > **SIRW**.

> **Remarque :** Vous pouvez personnaliser à l'aide de la vue de l'espace de travail **sirw** dans le formulaire d'interface utilisateur classique.

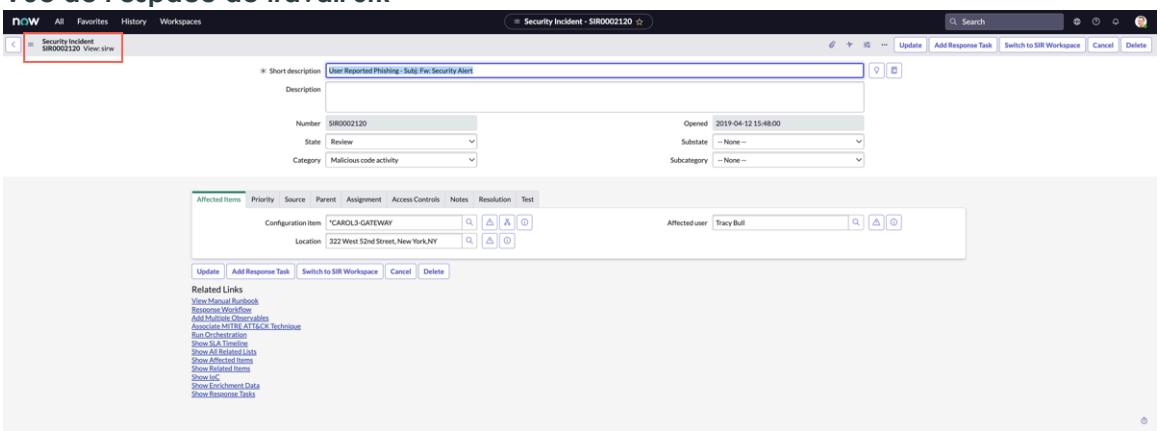


4. La vue de l'espace de travail d'incident de sécurité est affichée comme indiqué ci-dessous.

Traduction automatique

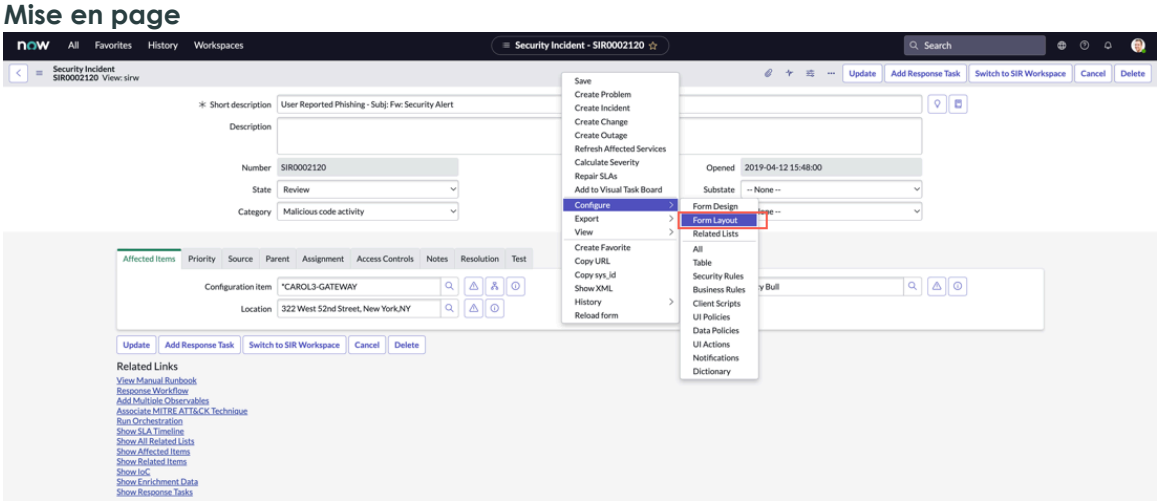
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue de l'espace de travail SIR



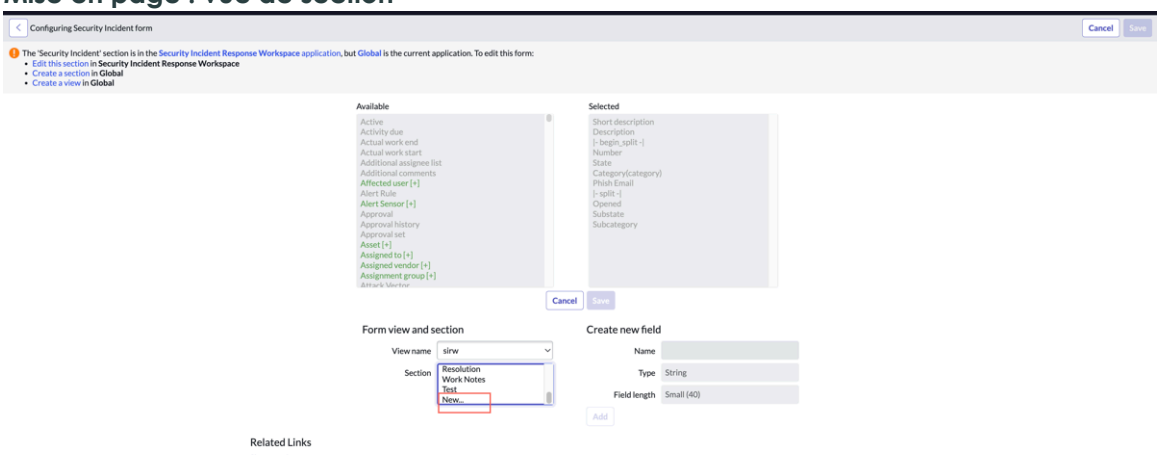
5. Dans l'enregistrement d'incident de sécurité, cliquer avec le bouton droit et accéder à **Configurer** > **Mise en page**.

Mise en page



6. Explorez la **vue et la section du formulaire** et sélectionnez **Nouveau** à partir de **la section** pour créer une nouvelle section.

Mise en page : vue de section



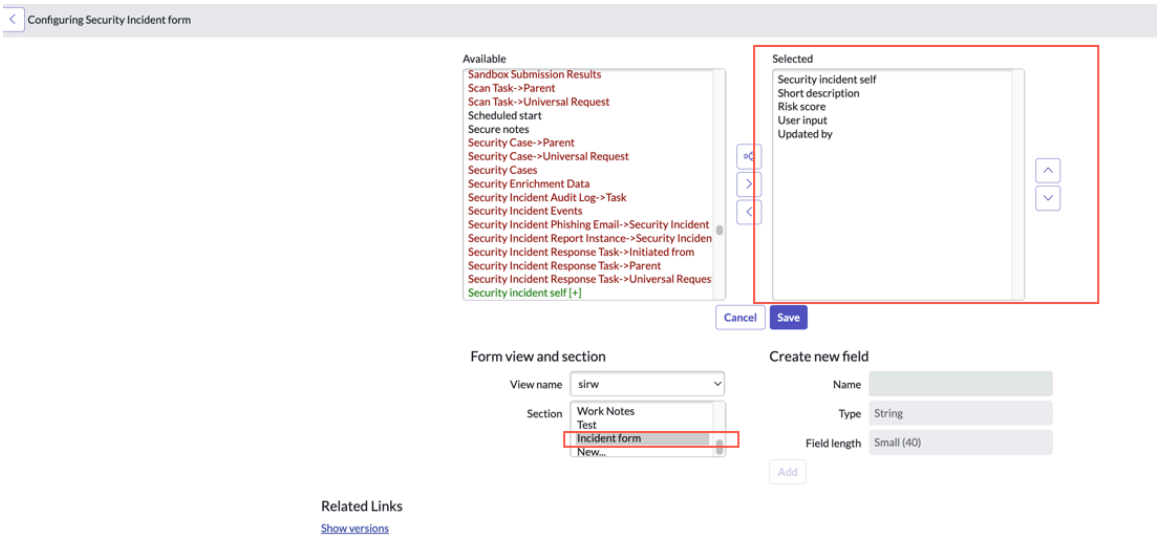
7. Fournissez le nouveau nom de la section , puis cliquez sur OK.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

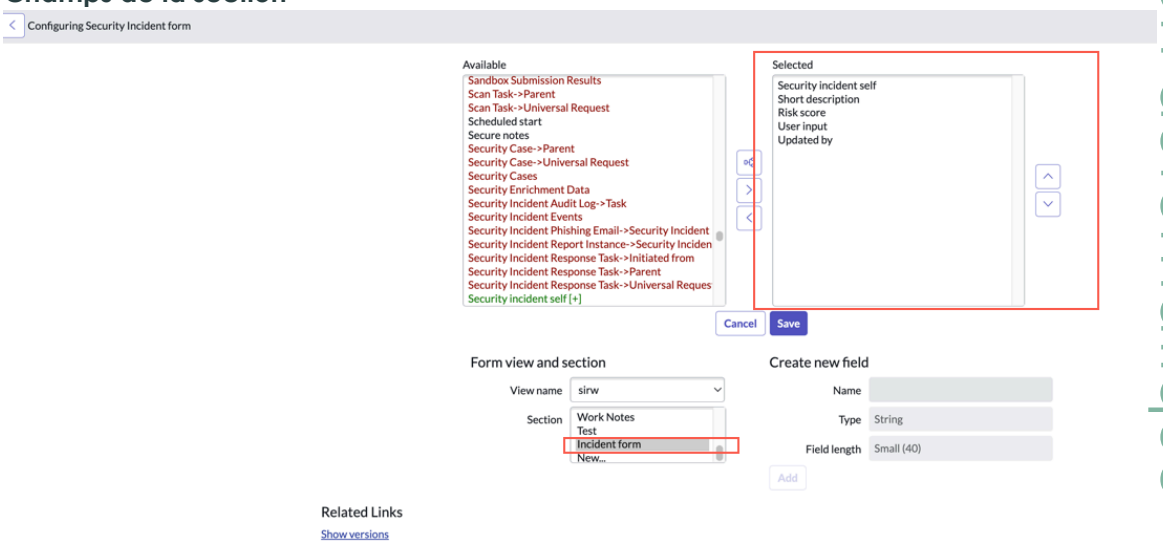
Par exemple, Formulaire Incident.

8. La nouvelle section est créée et ajoutée à la **section**.



9. Sélectionnez votre nouvelle section et ajoutez les champs de section requis à la zone de sélection et cliquez sur **Enregistrer**.

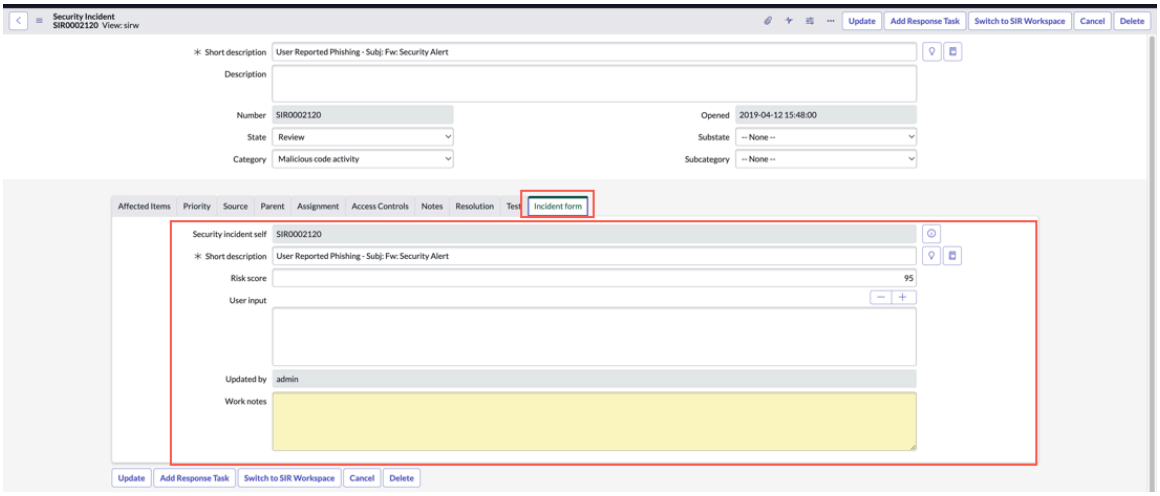
Champs de la section



10. La section nouvellement ajoutée s'affiche avec la disposition de section existante dans le formulaire d'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



11. Maintenant, cliquez sur **Basculer vers l'espace de travail SIR** pour accéder au formulaire d'incident de sécurité et à la section personnalisée dans l'onglet **Détails** de l'espace de travail.

SIR Workspace Orchestration

Espace de travail de la Réponse aux incidents de sécurité Les activités d'orchestration aideront les analystes de sécurité à afficher le canevas d'enquête et à effectuer diverses actions applicables.

SIR Workspace Canevas d'examen

Espace de travail de la Réponse aux incidents de sécurité permet aux analystes de sécurité de consulter les informations clés associées à l'incident de sécurité pendant le processus de correction de l'incident. Les informations clés comprennent également les listes connexes telles que les observables, les résultats de la recherche de menace, la recherche de perception, l'enrichissement des observables, etc.

Dans l'interface utilisateur classique, la plupart des actions d'orchestration associées aux intégrations prêtes à l'emploi sont disponibles sur les listes connexes. Par exemple, Exécuter une recherche de menace, Exécuter l'enrichissement des observables... sont présents sur la liste connexe Observables associés. De même, Obtenir les détails de l'hôte, Obtenir les statistiques réseau, etc., sont disponibles par rapport à la liste connexe Éléments de configuration.

Lorsqu'un analyste de la sécurité effectue ces actions, les résultats sont renseignés dans une liste connexe différente. Par exemple, lorsqu'un utilisateur exécute Exécuter une recherche de menace, les résultats sont disponibles dans la table Résultats de la recherche de menace. Parfois, les résultats sont disponibles dans plusieurs tables différentes. Au cours de ce processus, les analystes de la sécurité ont une expérience utilisateur décousue et désorganisée dans la co-relation des informations provenant de plusieurs endroits.

Dans la nouvelle SIR Workspaceversion réinventée, le canevas **d'enquête** (onglet) fournit toutes les informations nécessaires regroupées logiquement en un seul endroit pour que l'analyste puisse effectuer l'enquête.

Explorer le canevas d'enquête

L'objectif principal du canevas d'enquête est de présenter les données nécessaires sur les incidents de sécurité en un seul endroit commun.

Dans le SIR Workspace, l'enquête sur les incidents de sécurité s'articule principalement autour de quelques points d'entrée clés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voici quelques points d'entrée clés qui sont provisionnés pour les analystes de sécurité dans le système de base :

- Observables associés
- Éléments de configuration
- Utilisateurs affectés
- E-mails associés Phish
- Recherche d'e-mail

Vous pouvez également configurer les points d'entrée ci-dessus en ajoutant, en modifiant ou en supprimant les points d'entrée selon le cas. Pour plus d'informations, consultez Configurer l'examen de l'heure de conception du SI.

Dans l'onglet **Examen** , la table de points d'entrée fait office de table parente. Toutes les tables contenant les résultats d'une action d'orchestration effectuée sur la table parente sont présentées comme des tables enfants au sein du point d'entrée.

Par exemple, pour le point d'entrée **Observables associés** , la table **Observables associés** est la table parente et d'autres tables telles que Résultats de la recherche de menace, Résultats de soumission du bac à sable, entre autres, sont la table enfants.

L'analyste de sécurité peut effectuer toutes les actions d'orchestration sur la table Observables associés et peut afficher toutes les informations associées sur la même page, sans avoir besoin de naviguer à plusieurs endroits.

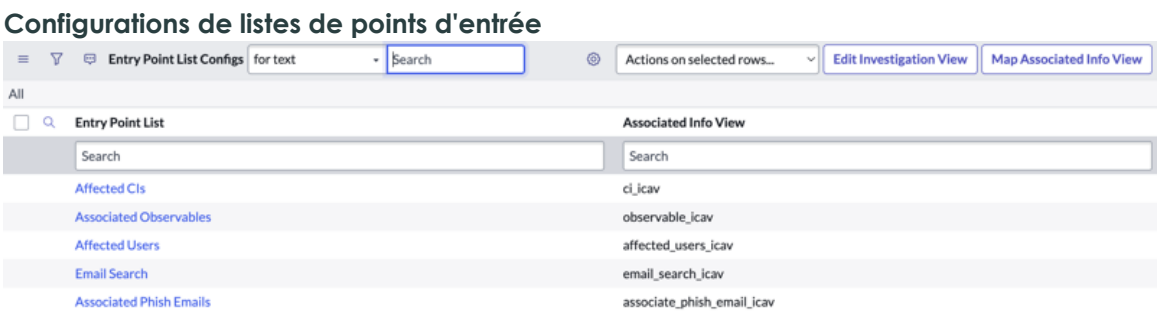
Remarque : Lorsqu'un utilisateur clique sur les graphiques interactifs de la page **Vue d'ensemble** , tels que les observables malveillants, il est dirigé vers la vue filtrée des observables malveillants dans le canevas d'examen. Alternativement, l'utilisateur peut directement commencer l'enquête en naviguant vers le canevas d'enquête qui contiendra toutes les données.

La table de liste des enfants sous un point d'entrée est également configurable. Pour plus d'informations, consultez Configurer l'examen de l'heure de conception du SI.

Voici un exemple détaillé de point d'entrée (observable associé) configuré et approvisionné dans le système de base :

1. Sélectionnez le point d'entrée **Observables associés** dans la liste déroulante.

   Ici, la table parente est également **un observable associé**.



2. Sélectionnez un ou plusieurs observables dans la table parente.
3. Exécuter l'aptitude souhaitée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

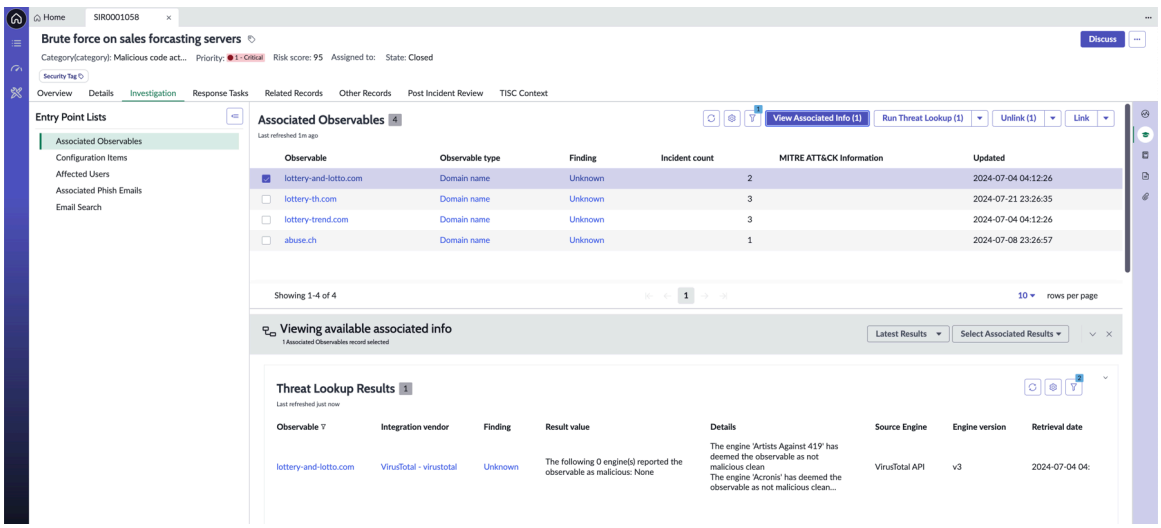
Par exemple, sélectionnez **Exécuter la recherche de menace** pour extraire les résultats de la recherche de menace pour un observable sélectionné.

Remarque : Lorsqu'une action observable correspondante est exécutée, le processus est exécuté dans le back-end et les résultats sont affichés sous la liste Observables.

4. Cliquez sur **Afficher les informations associées** pour afficher les résultats des observables. Les résultats sont affichés sur la même page.

   Remarque : Vous pouvez afficher les résultats à l'aide de filtres par résultats, sélectionner **Tous les résultats** ou **Derniers résultats**, selon la valeur souhaitée. Par défaut, les derniers résultats sont affichés. S'il existe plusieurs implémentations (d'intégrations), les derniers résultats par implémentation s'affichent.

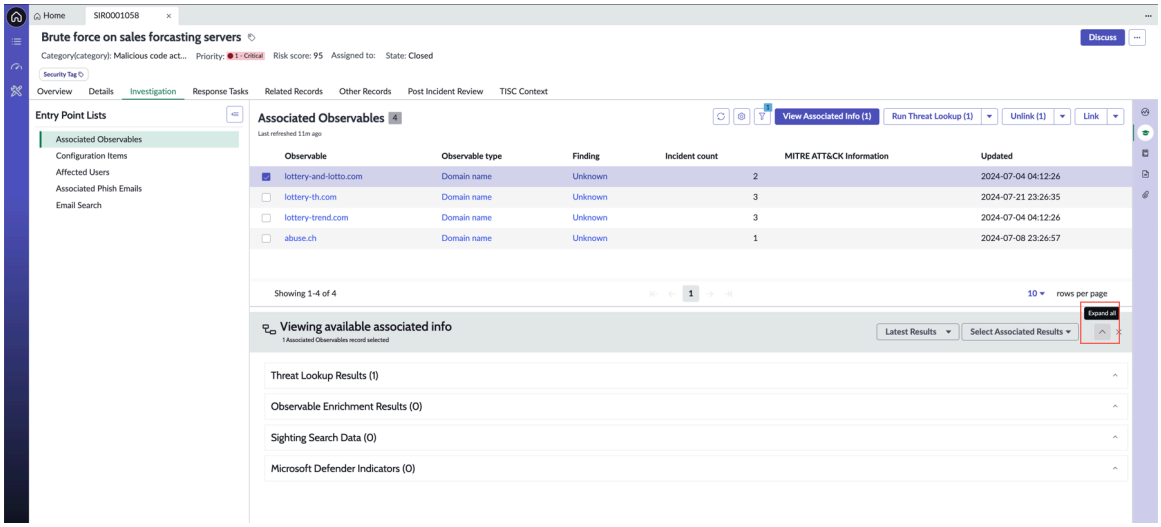
   En outre, vous pouvez filtrer les résultats **par des listes connexes associées** qui sont les résultats de la table enfant. Par défaut, toutes les listes connexes des tables enfants configurées sont affichées. Pour plus d'informations, consultez Configurer l'examen de l'heure de conception du SI. Toutefois, vous pouvez choisir de sélectionner uniquement les tables enfants requises.



5. En cliquant sur **Afficher les informations associées** , vous pouvez afficher toutes les données de table enfants associées en un seul endroit. Cependant, vous pouvez fermer la vue des listes connexes en sélectionnant le bouton **Fermer la vue** . Une fois que vous fermez la vue, vous pouvez uniquement voir la table parente des observables, comme précédemment.
6. Cliquez sur l'icône **Développer tout** vers le haut dans la table **Affichage des résultats des informations associées disponibles** pour développer toutes les données de table enfants de listes connexes.

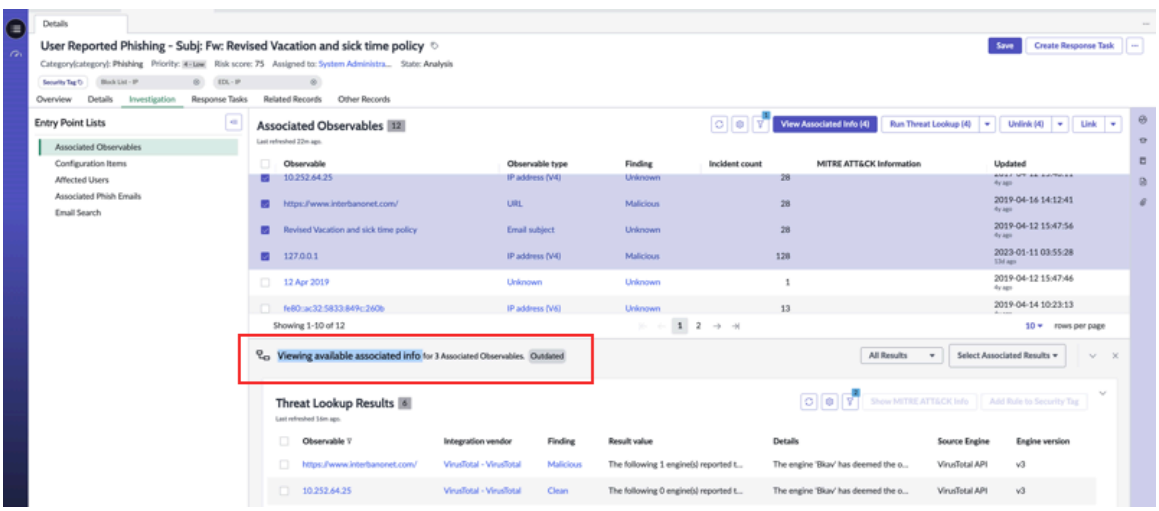
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Cliquez sur l'icône **Réduire tout** vers le bas pour réduire toutes les données de table enfants de listes connexes.

Remarque : La bannière en haut de la section d'informations associée, qui contient toutes les données de la table enfant, indique le nombre d'informations observables connexes présentées à l'utilisateur. Par exemple, initialement, si vous sélectionnez deux observables et cliquez sur **Afficher les informations associées**, la bannière affiche **Affichage des informations associées disponibles pour 2 observables associés.** Si vous sélectionnez par exemple, un autre observable, la bannière indique que l'information est obsolète (capture d'écran ci-dessous). Vous devrez cliquer à nouveau sur **Afficher les informations associées** pour obtenir les données les plus récentes.



En plus de la vue complète ci-dessus des informations associées aux observables, si vous souhaitez afficher plus d'informations sur un enregistrement sur la table parente, cliquez sur l'observable et le formulaire d'enregistrement de la table parente s'ouvre dans un onglet différent avec une vue plus détaillée de l'enregistrement sélectionné. Toutes les données de table enfants associées de cet enregistrement sélectionné particulier sont également présentées sous la section **Informations associées** .

Toutefois, la section d'informations associée affiche uniquement les derniers résultats de la table enfants, tels qu'ils apparaissent dans le canevas d'examen, en mode lecture seule. Aucune action n'est possible dans cette vue. La page de formulaire de la table enfants

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

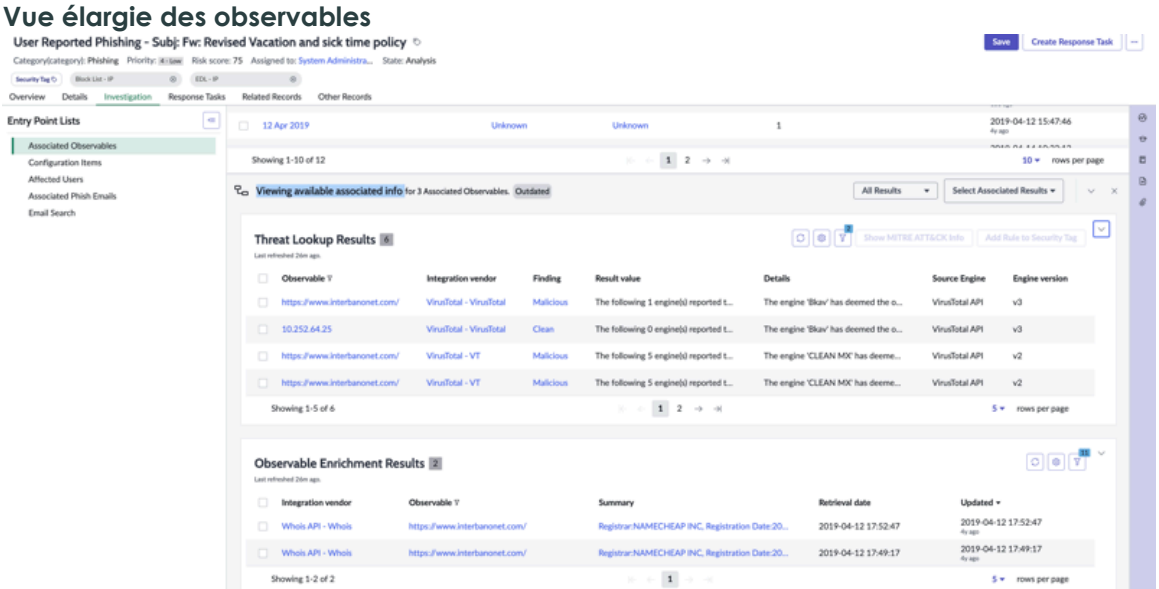
peut être ouverte dans un nouvel onglet qui affichera la page entièrement fonctionnelle avec toutes les actions, le cas échéant.

Vous pouvez passer d'une table à l'autre à l'aide de la liste déroulante. Vous pouvez également développer ou réduire chaque formulaire dans la section d'informations associée.

Dans la page **de formulaire Observable** (page de formulaire d'enregistrement de table parente), vous pouvez effectuer certaines actions selon les disponibilités. Chaque fois que vous effectuez une action, vous pouvez cliquer sur Actualiser sur la bannière d'informations associée pour actualiser les données.

8. Cliquez sur **Développer tout** pour développer la table enfant de toutes les listes connexes. Par défaut, tous les enfants sont développés.

Vue élargie des observables



Information associée

Configurer l'examen de l'heure de conception du SI

Cadre de travail de l'expérience unifiée pour les intégrations optimisées par le cadre de travail d'aptitude

Dans l'interface utilisateur classique, l'expérience est disjointe lors de l'exécution d'activités d'orchestration telles que l'exécution d'une recherche de menace, l'exécution d'une recherche de perception, etc. Chaque option a sa propre expérience lors de son exécution. Dans le nouvel espace de travail, il existe une expérience unifiée sur toutes les options.

L'expérience unifiée ne s'applique qu'aux intégrations et activités d'orchestration qui relèvent du cadre de travail d'aptitude. Il peut y avoir des actions spécifiques à l'intégration, par exemple, Créer des indicateurs dans Microsoft Defender. Ces actions auront leur propre expérience en fonction des besoins du cas d'utilisation.

Le nouveau cadre se compose d'écrans modaux en trois étapes, comme expliqué ci-dessous.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. **Implémentations** : la première étape consiste à sélectionner une ou plusieurs implémentations présentes par rapport à l'aptitude sélectionnée.

   Par exemple, lorsque l'analyste clique sur **Exécuter une recherche de menace**, il est en mesure de sélectionner une ou plusieurs implémentations présentes pour **l'option Exécuter la recherche de menace**.

   Chaque implémentation aura les détails de la source d'intégration. Reportez-vous au tableau ci-dessous. Des informations supplémentaires sont également présentées pour chaque implémentation.

   Les informations supplémentaires peuvent inclure, par exemple, des informations sur les filtres, les types d'observables pris en charge, etc. Les informations supplémentaires peuvent être configurées comme vous le souhaitez. Pour plus d'informations, consultez la procédure de configuration technique du cadre UX.

Fenêtre modale du cadre de travail de l'implémentation unifiée

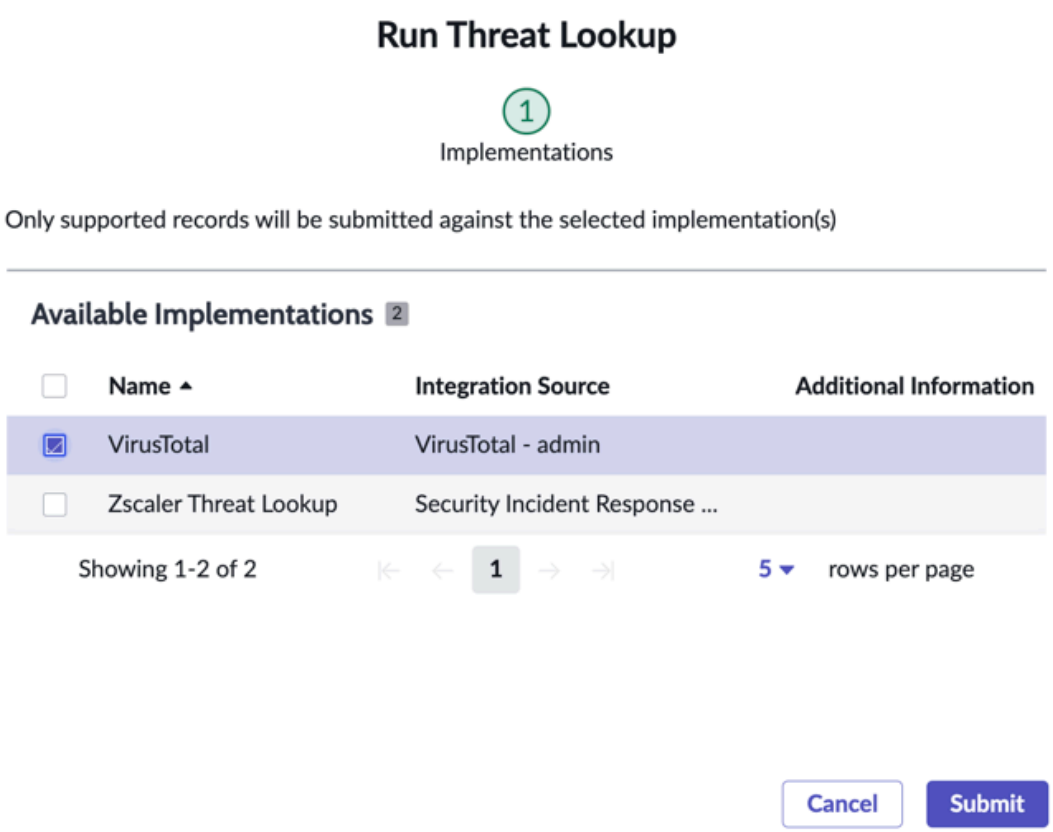
Implémentation	Description
Nom	Nom de l'implémentation.
Source d'intégration	La source de l'implémentation, telle que la configuration utilisée.
Informations supplémentaires	Cette colonne capture les informations statiques qui permettent à l'analyste de sécurité de disposer de plus de contexte par rapport à la ou aux implémentations sélectionnées pour procéder à une action. Par exemple, la prise en charge ou les informations filtrées. En outre, si une implémentation ne prend en charge qu'un certain type d'observables tels que le domaine ou l'URL, vous pouvez ajouter ces informations supplémentaires ici dans cette colonne pour fournir le contexte à l'utilisateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Implémentation	Description
	Remarque : Le cadre d'interface utilisateur permettrait essentiellement de sélectionner n'importe quel type d'implémentation et n'importe quel type d'observables. Lors de la soumission, les intégrations de systèmes de base existantes qui sont expédiées prendront en charge le filtrage dans le back-end et soumettront uniquement le type d'observables pris en charge. Les autres enregistrements qui ne correspondent pas à la prise en charge seront ignorés. Par conséquent, un message d'information de l'interface utilisateur s'affiche lorsque vous sélectionnez l'aptitude : **Seuls les enregistrements pris en charge seront soumis pour la ou les implémentations sélectionnées.**

Écran 1 : Implémentation(s)



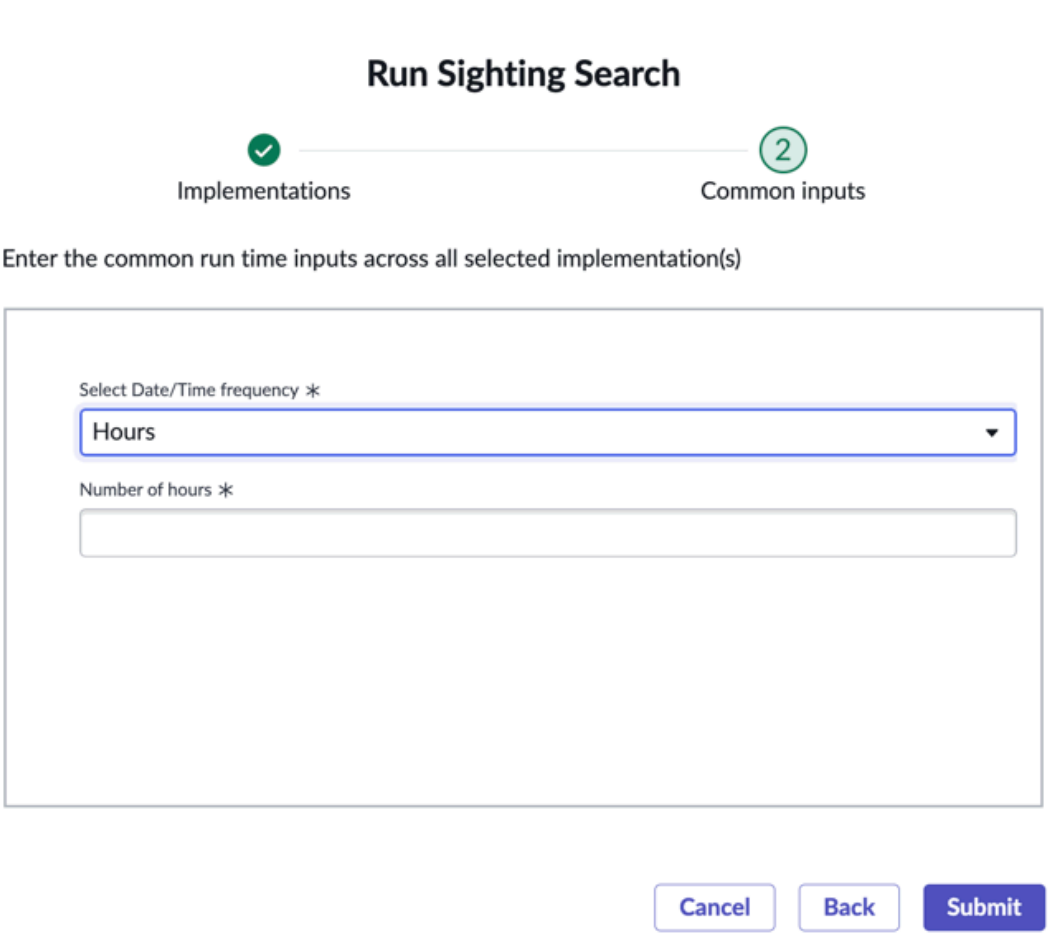
2. **Entrées communes** : ajoutez des entrées communes pour les implémentations sélectionnées ou pour toutes les implémentations applicables sélectionnées. Il s'agit

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de l'écran 2 de votre implémentation. Par exemple, à partir de maintenant, seule **la recherche de perceptions** dispose de l'écran d'entrées communes. Cette implémentation est une combinaison de l'écran 1 (Implémentations) et de l'écran 2 (entrées communes).

Écran 1 + Écran 2



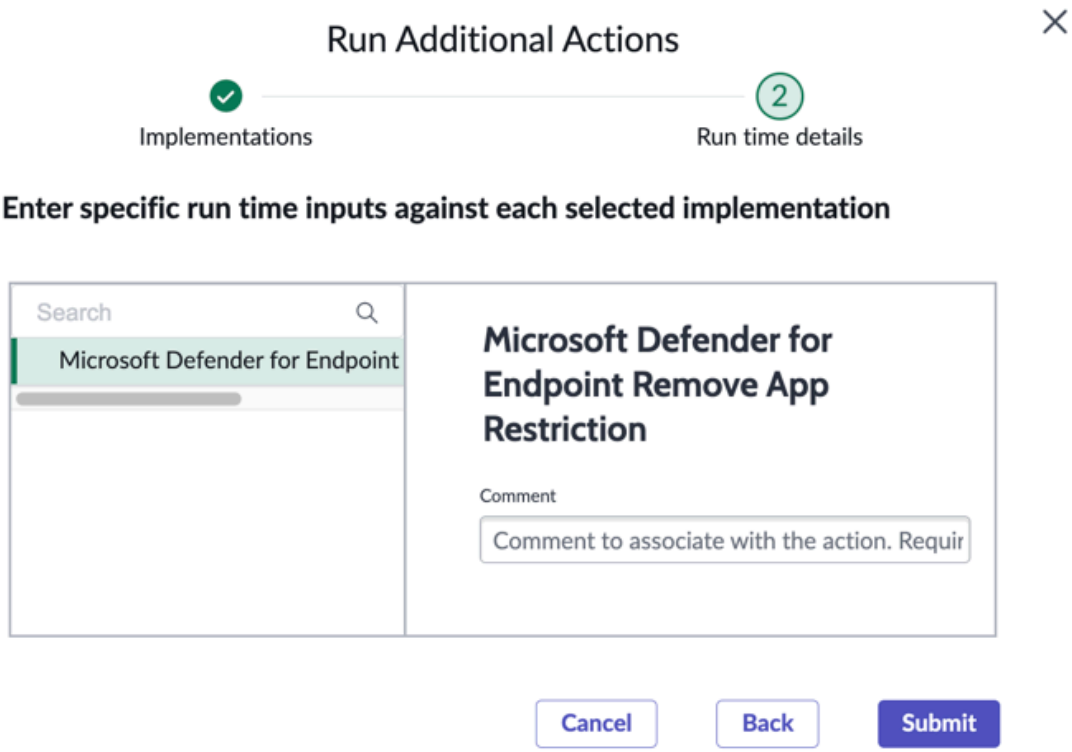
3. **Détails de temps d'exécution** : ajoutez des entrées de temps d'exécution spécifiques pour les implémentations sélectionnées qui sont différentes les unes des autres. Il s'agit de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'écran 3 de votre implémentation. Cette implémentation est une combinaison de l'écran 1 (Implémentations) et de l'écran 3 (entrées de temps d'exécution spécifiques).

Entrées spécifiques



Remarque : Les trois étapes ne sont pas toujours requises. En fonction de l'aptitude et du type d'entrées requises, l'étape des détails de l'exécution et l'étape des entrées communes sont visibles.

Options d'expérience unifiée et écrans modaux

Le tableau suivant ci-dessous décrit les fonctionnalités et les écrans applicables.

Option	Écrans des cadres de travail UX applicables	Intégrations prises en charge
Exécuter une recherche de menace	Seul l'écran 1 – Sélectionner les implémentations s'applique. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Exécuter une recherche de menace. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité est en mesure de soumettre l'action.	• Virus Total • Hybrid Analysis • Intégration de Security Incident Response à Zscaler • Phistank • Metadefender (en anglais seulement) • Foule menacée • Ai-je été mis en gage ? • Intelligence du faucon Crowd Strike

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Écrans des cadres de travail UX applicables	Intégrations prises en charge
Exécuter l'enrichissement de l'élément observable	Seul l'écran 1 – Sélectionner les implémentations est applicable Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Exécuter l'enrichissement des observables. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité est en mesure de soumettre l'action.	• MISP • Point de terminaison Microsoft Defender • Shodan • RiskIQ (en anglais seulement) • LE WHOIS • Inverser le WHOIS
Exécuter la recherche de perception/Exécuter la recherche de perception Web/Exécuter la recherche de perception des e-mails	Écran 1 – **Sélectionner les implémentations** et Écran 2 – **Les entrées communes** sont applicables. La recherche de perception utilise la date et la fréquence comme entrées communes à plusieurs implémentations de Splunk et d'autres intégrations. Cet écran sera présenté à l'analyste de la sécurité pour capturer les fréquences de date et d'heure. Pour les intégrations qui ne nécessitent pas ces entrées, par exemple FireEye HX, elles sont ignorées. Après avoir sélectionné une ou plusieurs implémentations et fourni des entrées communes, l'analyste de la sécurité est en mesure de soumettre l'action.	• Enrichissement des incidents Splunk • Carbon Black • Recherche élastique • FireEye HX • McaFee ESM • MSFT Defender pour point de terminaison • Observation Splunk • Recherche de perception Qradar • MISP
Soumettre au bac à sable (sandbox)	Écran 1 – Sélectionner les implémentations et Écran 3 – Implémentation, les entrées spécifiques sont applicables. Soumettre au bac à sable accepte différentes entrées pour différentes implémenta-	• Intégration de CrowdStrike Falcon X Sandbox • Intégration de Security Incident Response à Zscaler

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Écrans des cadres de travail UX applicables	Intégrations prises en charge
	tions. Il n'existe actuellement aucune entrée commune pour cette option. Par exemple, lorsque l'analyste sélectionne Analyse rapide Crowdstrike Falcon X, Crowdstrike Falcon X Windows 64, Crowdstrike Falcon X Linux et Zscaler, les entrées varient. L'analyse rapide Crowdstrike Falcon X et Zscaler n'ont pas besoin d'autres entrées de temps d'exécution. Crowdstrike Falcon X Windows 64 prend en charge des entrées d'exécution facultatives qui diffèrent de celles de Crowdstrike Falcon X Linux. Ainsi, ceux-ci peuvent être fournis dans l'écran 3 spécifiquement par rapport aux implémentations sélectionnées individuelles, le cas échéant.	
Publier dans la liste de surveillance	Seul l'écran 1 – Sélectionner les implémentations s'applique. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour **Publier dans la liste de surveillance**. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité est en mesure de soumettre l'action.	Hôte Crowdstrike Falcon
Demande d'autorisation/de blocage	Seul l'écran 1 – Sélectionner les implémentations s'applique. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour la **demande d'autorisation/de blocage**.	• Réseau Palo Alto NGFW • Check Point NGFW • Intégration de Security Incident Response à Zscaler

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Écrans des cadres de travail UX applicables	Intégrations prises en charge
	Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité est en mesure de soumettre l'action.	
Obtenir les détails de l'hôte	Seul l'écran 1 – Sélectionner les implémentations s'applique. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Obtenir les détails de l'hôte. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité est en mesure de soumettre l'action.	• FireEye HX • Microsoft Defender pour point de terminaison
Obtenir un fichier	Écran 1 – Sélectionner les implémentations et Écran 2 – Les entrées communes sont applicables. Obtenir un fichier prend le nom du fichier et le chemin d'accès comme entrées communes. Après avoir sélectionné une ou plusieurs implémentations et fourni des entrées communes, l'analyste de la sécurité est en mesure de soumettre l'action.	FireEye HX
Obtenir les statistiques réseau	Seul l'écran 1 – Sélectionner les implémentations s'applique. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Obtenir les statistiques réseau. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour	• FireEye HX • NetStat

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Écrans des cadres de travail UX applicables	Intégrations prises en charge
	sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité est en mesure de soumettre l'action.	
Obtenir l'exécution des processus	Seul l'écran 1 – Sélectionner les implémentations s'applique. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour l'exécution des processus. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité est en mesure de soumettre l'action.	• FireEye HX • Carbon Black • Commande système
Obtenir les services d'exécution	Seul l'écran 1 – Sélectionner les implémentations s'applique. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour les services d'exécution. Ainsi, seul l'écran 1 est présenté à l'analyste pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste est en mesure de soumettre l'action.	FireEye HX
Isoler l'hôte/Ne pas isoler l'hôte	Écran 1 – Sélectionner les implémentations et Écran 3 – Implémentation, les entrées spécifiques sont applicables. Isoler l'hôte/Ne pas isoler l'hôte prend des entrées différentes pour différentes implémentations.	• FireEye HX • Point de terminaison Microsoft Defender • Carbon Black

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Écrans des cadres de travail UX applicables	Intégrations prises en charge
	Il n'existe actuellement aucune entrée commune pour cette option. Par exemple, lorsque l'analyste sélectionne FireEye HX et Microsoft Defender pour point de terminaison, les entrées varient. FireEye HX n'a pas besoin d'entrées de temps d'exécution. D'autre part, Microsoft Defender accepte des entrées telles que le type d'isolement et les commentaires. Ainsi, ceux-ci peuvent être fournis dans l'écran 3 spécifiquement par rapport aux implémentations sélectionnées individuelles, le cas échéant.	
Exécuter des actions supplémentaires	Écran 1 – Sélectionner les implémentations et Écran 3 – Implémentation, les entrées spécifiques sont applicables. Exécuter des actions supplémentaires L'hôte prend des entrées différentes pour différentes implémentations. Il n'existe actuellement aucune entrée commune pour cette option. Par exemple, lorsque l'analyste sélectionne le script Détails d'enquête standard FireEye HX, l'acquisition du triage FireEye HX et le déchargement reg de Crowdstrike Falcon Insight, les entrées varient. Le script des détails d'enquête standard FireEye HX et l'acquisition du triage FireEye HX prennent les commentaires comme entrée qui peuvent être différents pour les deux. Le déchargement de l'enregistrement de Crowdstrike Falcon Insight prend la sous-clé comme entrée.	• FireEye HX • Microsoft Defender pour point de terminaison • Crowdstrike Falcon Insight

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Écrans des cadres de travail UX applicables	Intégrations prises en charge
	Ainsi, ceux-ci peuvent être fournis dans l'écran 3 spécifiquement par rapport aux implémentations sélectionnées individuelles, le cas échéant. **Remarque :** Ne prend actuellement en charge qu'une seule sélection d'implémentation. Dans les versions futures, la sélection multiple d'implémentation sera prise en charge.	

Exemple d'expérience unifiée

Cet exemple présente les options de Unified Experience Framework.

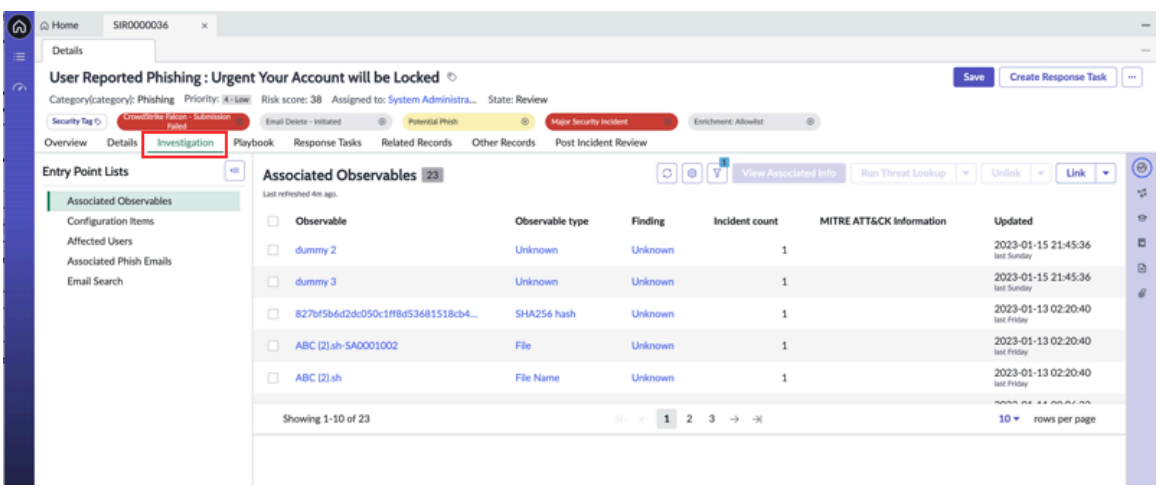
Exemple 1 : sélectionner les implémentations : Recherche de menace

L'exemple ci-dessous illustre la ou les implémentations.

Exemple 1 : Écran 1 uniquement : Recherche de menace

Vous pouvez effectuer **l'action d'options d'intégration connexes Exécuter une recherche de menace** à l'aide de l'onglet **Examiner** du SIR Workspace.

1. Dans l'onglet **Examen** , accédez à la section **Listes de points d'entrée** affichée sur le côté gauche de la page.
2. Sélectionnez n'importe quel point d'entrée et exécutez l'action d'aptitude d'intégration.



Remarque : Vous pouvez également accéder à l'onglet **Enregistrements connexes** de l'espace de travail pour effectuer l'action d'options d'intégration.

La recherche de menace est l'un des exemples qui est décrit en détail sur la façon d'effectuer les intégrations.

Sélectionner des implémentations

Sélectionnez une ou plusieurs implémentations selon le cas.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

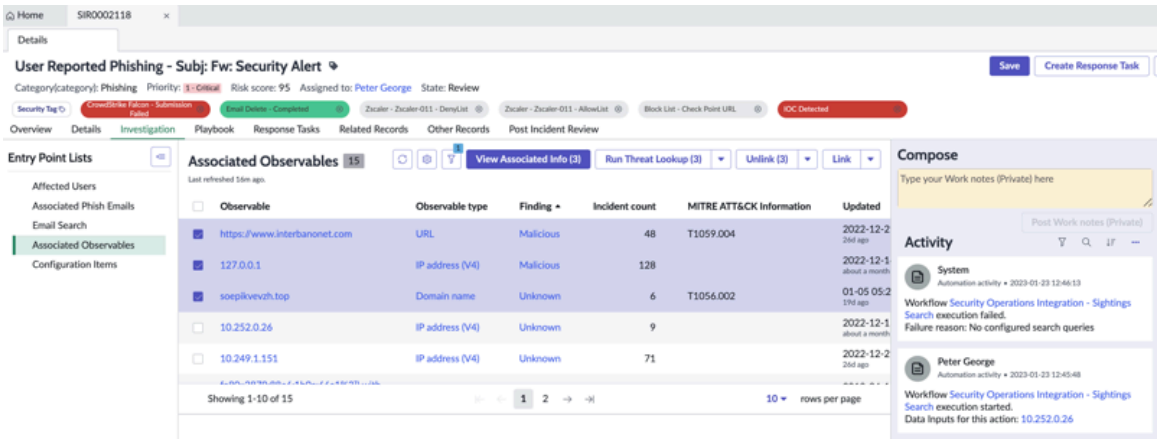
Avant de commencer

Rôle requis : sn_si.analyst

Les implémentations disponibles sont répertoriées. Sélectionnez la ou les implémentations. Après les avoir sélectionnées, seuls les enregistrements pris en charge sont soumis pour chaque implémentation sélectionnée.

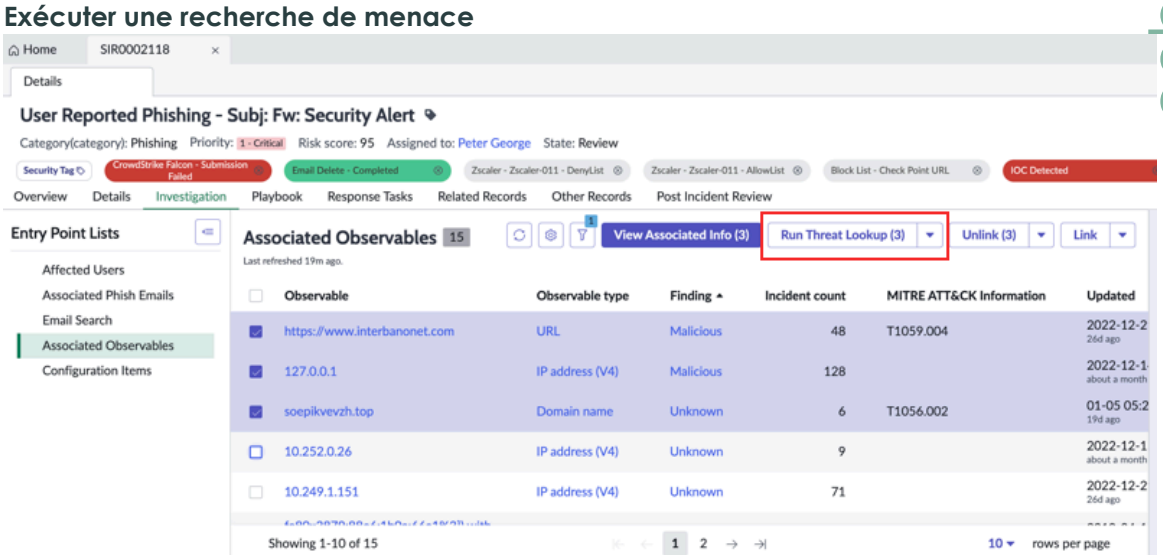
Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Accédez à l'onglet **Examiner** de l'espace de travail.
   L'onglet Examiner avec les listes de points d'entrée s'affiche.



4. Sélectionnez l'observable associé dans les listes de points d'entrée.
   Par exemple, sélectionnez **Observables associés** liste connexe. Les enregistrements d'observables correspondants s'affichent.

> **Remarque :** Vous pouvez sélectionner une implémentation pour effectuer une recherche sur les observables sélectionnés, ou vous pouvez effectuer la recherche en sélectionnant toutes les implémentations.



5. Cochez la case Observable que vous souhaitez pour effectuer la recherche de menace.

Traduction automatique

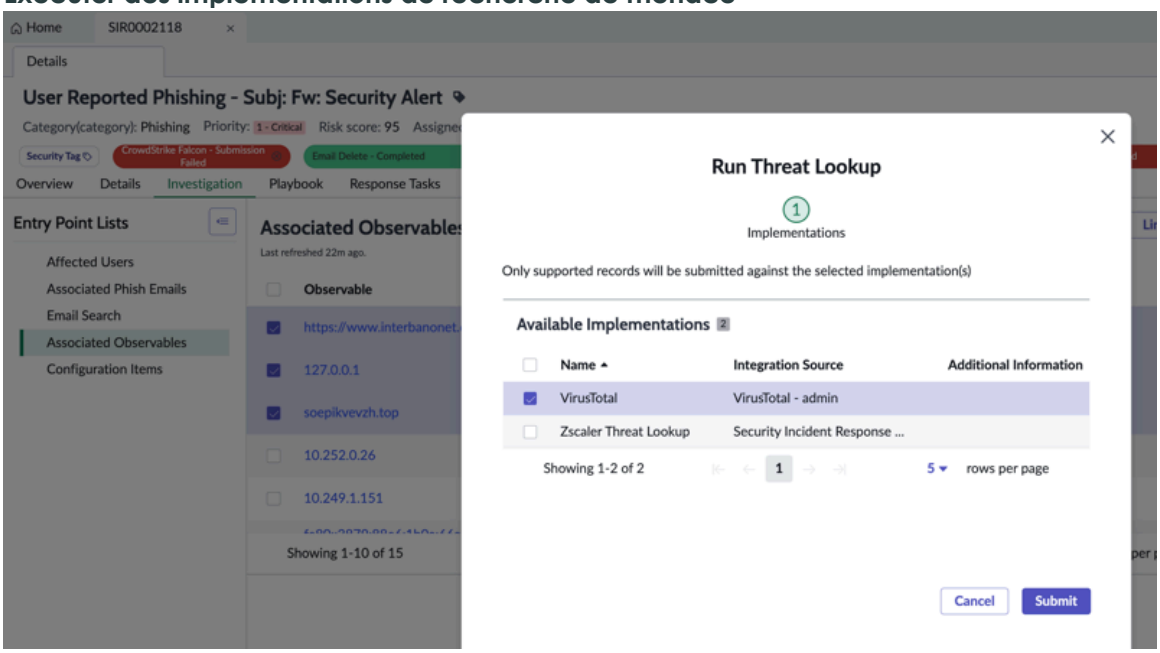
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Accédez à la liste déroulante des actions des listes connexes qui s'affiche en haut de la page des listes connexes.
7. Sélectionnez Exécuter une recherche de menace pour effectuer **l'action des options d'intégration** liées aux informations sur les menaces.

> **Remarque :** L'option Exécuter des recherches de menace effectue des recherches de renseignements sur les menaces pour déterminer si un ou plusieurs éléments observables sont associés avec des menaces de sécurité connues.

L'écran modal **Exécuter la recherche de menaces Implémentations** s'affiche.

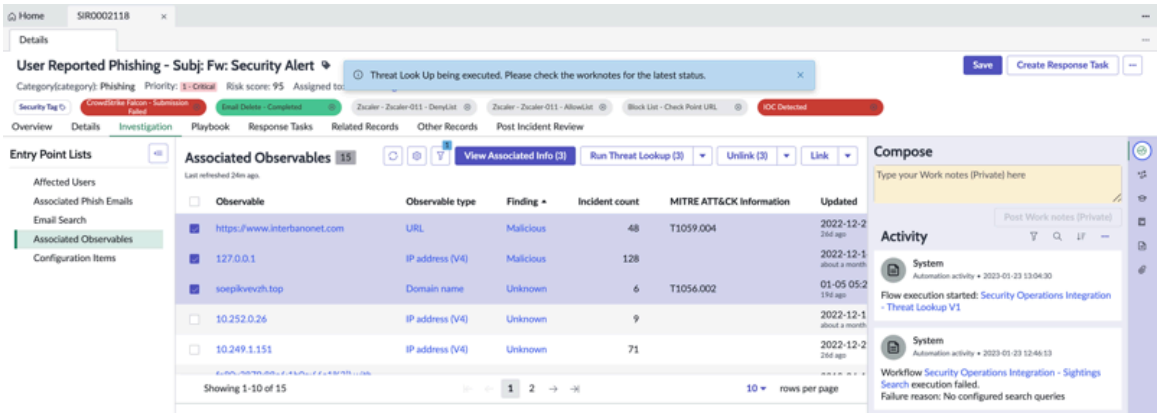
Exécuter des implémentations de recherche de menace



8. Sélectionnez une ou plusieurs implémentations dans la liste.
9. Cliquez sur **Envoyer**.
   Une fois les enregistrements sélectionnés soumis, un message s'affiche indiquant que la recherche est en cours d'exécution. Une fois l'implémentation traitée dans le back-end, les résultats sont affichés dans la section de liste connexe **Résultats de la recherche de menace** . De plus, l'activité d'implémentation respective est affichée dans la section **Activité** . Deux activités s'affichent, l'une lorsque l'exécution de l'implémentation est démarrée et l'autre lorsque l'exécution est terminée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Les listes connexes **Threat Intelligence** telles que les listes connexes des observables associés sont affichées dans la section **Résultats de la recherche de menace** , et les listes connexes de **recherche de perceptions** sont affichées dans la section **Résultats de recherche de perceptions** sous les enregistrements connexes.

Exemple 2 : Entrées communes : Recherche de perception

L'exemple ci-dessous illustre l'action d'aptitude Entrées courantes.

Vous pouvez effectuer **l'action d'options** d'intégration connexes Exécuter la recherche de perception à l'aide de l'onglet **Examiner** du SIR Workspace.

1. Dans l'onglet **Examen** , accédez à la section **Listes de points d'entrée** affichée sur le côté gauche de la page.
2. Sélectionnez le point d'entrée respectif et exécutez l'action d'aptitude d'intégration.

Remarque : Vous pouvez également accéder à l'onglet **Enregistrements connexes** de l'espace de travail pour effectuer l'action d'options d'intégration.

Ajouter des entrées communes à une implémentation

Ajoutez des entrées de temps d'exécution communes qui s'appliquent à toutes les implémentations sélectionnées, le cas échéant.

Avant de commencer

Rôle requis : sn_si.analyst

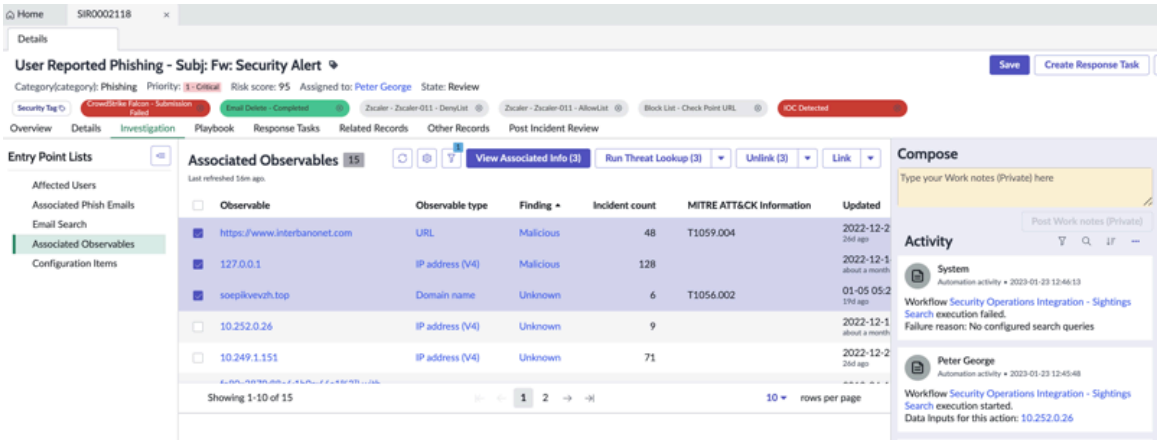
Les implémentations disponibles sont répertoriées. Sélectionnez la ou les implémentations. Après les avoir sélectionnées, seuls les enregistrements pris en charge sont soumis pour chaque implémentation sélectionnée.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Accédez à l'onglet **Examiner** de l'espace de travail.
   L'onglet Examiner avec les listes de points d'entrée s'affiche.

Traduction automatique

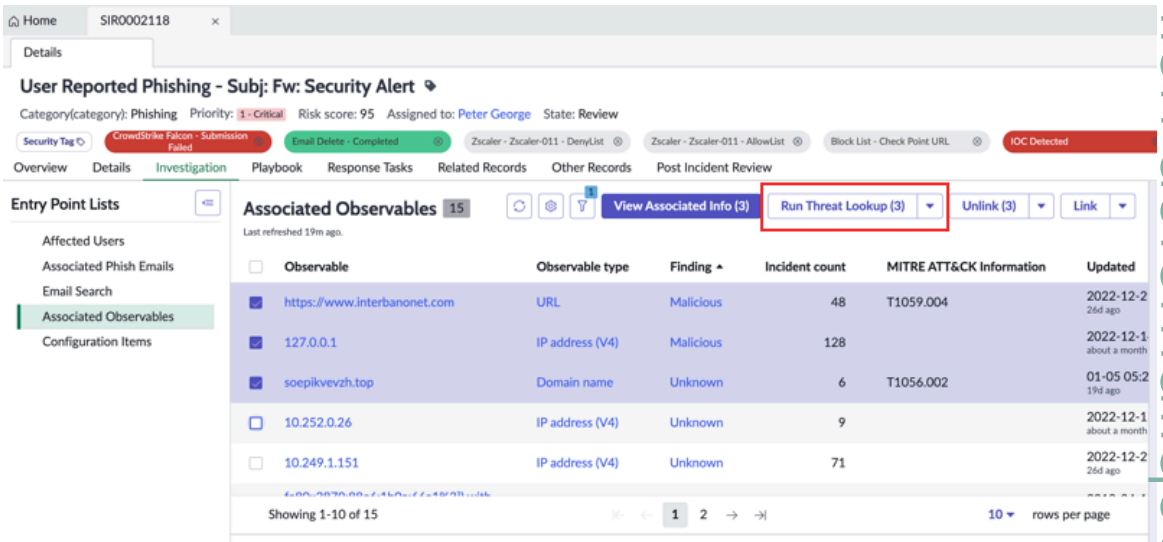
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez l'observable associé dans les listes de points d'entrée.
   Par exemple, sélectionnez **Observables associés** liste connexe. Les enregistrements d'observables correspondants s'affichent.

   Remarque : Vous pouvez sélectionner une implémentation pour effectuer une recherche de perception pour les observables sélectionnés ou en sélectionnant plusieurs implémentations.

Exécuter une recherche de menace

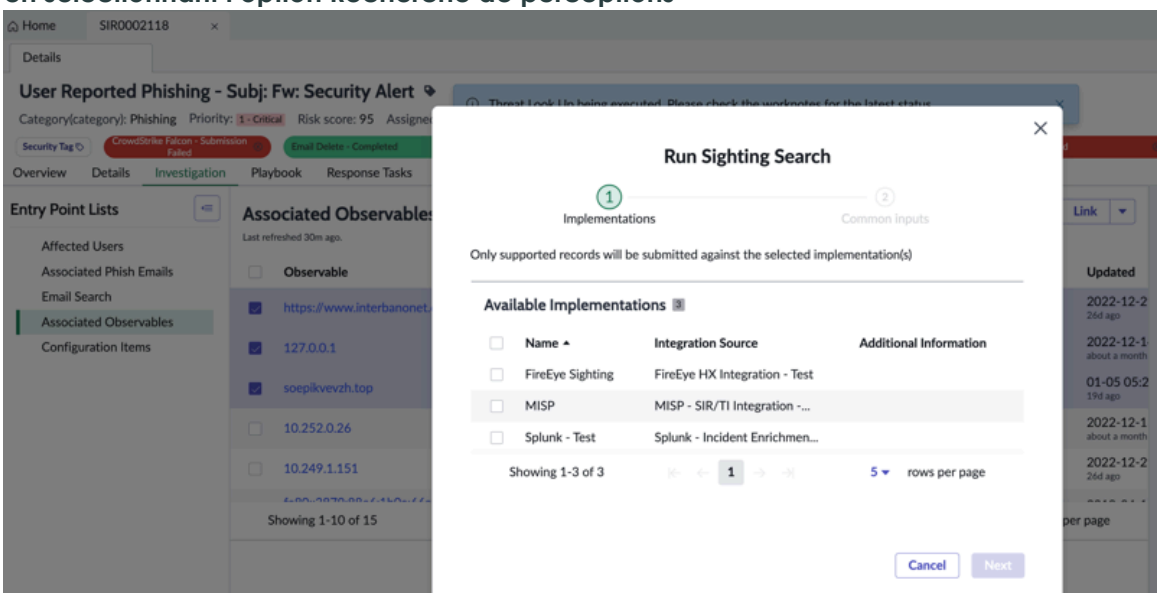


5. Cochez la case Observable que vous souhaitez pour effectuer la recherche de menace.
6. Sélectionnez **Exécuter la recherche de perception** pour effectuer une recherche d'e-mails.
   La boîte de dialogue modale Exécuter les implémentations de la recherche de perception s'affiche.

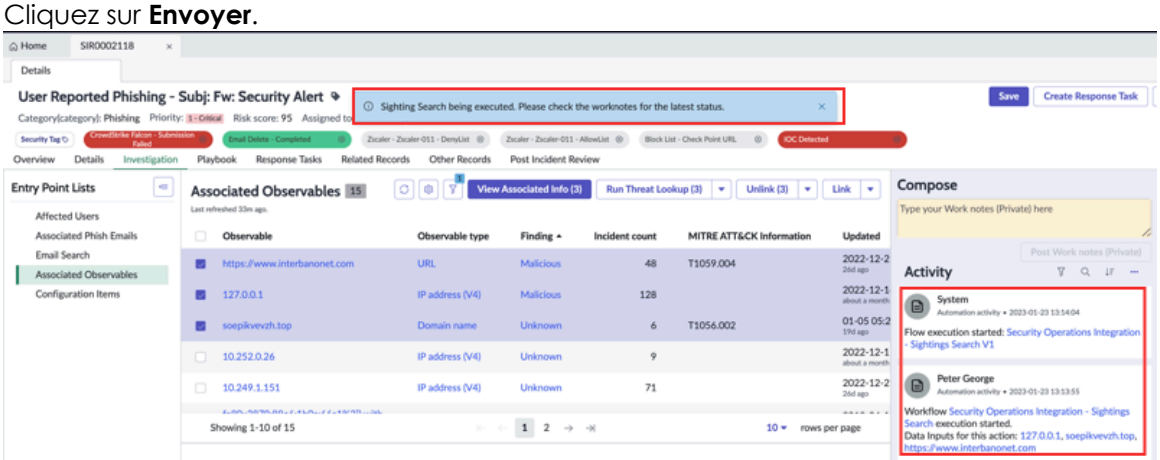
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un exemple qui montre comment ajouter des entrées d'exécution communes en sélectionnant l'option Recherche de perceptions



7. Sélectionnez une ou plusieurs implémentations dans la liste.
8. Cliquez sur **Suivant**.
   Une fois les enregistrements sélectionnés soumis, un message s'affiche indiquant que la recherche de perception est demandée. Une fois l'implémentation traitée dans le back-end, les résultats sont affichés dans la section de liste connexe **Recherche de perceptions** . De plus, l'activité d'implémentation respective est affichée dans la section Activité. Deux activités s'affichent, l'une lorsque l'exécution de l'implémentation est démarrée et l'autre lorsque l'exécution est terminée.
9. Sélectionnez la valeur d'entrée de temps d'exécution commune.
10. Cliquez sur **Envoyer**.



Une fois les enregistrements sélectionnés soumis, un message s'affiche indiquant que la recherche de perception est demandée. Une fois l'implémentation traitée dans le back-end, les résultats sont affichés dans la section de liste connexe **Résultats de recherche de perceptions** . De plus, l'état de traitement de l'activité d'implémentation respective est affiché dans la section **Activité** .

Exemple 3 : Ajouter des entrées de détails d'exécution spécifiques à une implémentation : Exécuter des actions supplémentaires

Ajoutez des entrées de détails d'exécution spécifiques à une implémentation, exécutez des actions supplémentaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez effectuer **l'action d'options** d'intégration connexes Exécuter des actions supplémentaires à l'aide de l'onglet **Examiner** du SIR Workspace.

1. Dans l'onglet **Examen** , accédez à la section **Listes de points d'entrée** affichée sur le côté gauche de la page.
2. Sélectionnez le point d'entrée respectif et exécutez l'action d'aptitude d'intégration.

> **Remarque :** Vous pouvez également accéder à l'onglet **Enregistrements connexes** de l'espace de travail pour effectuer l'action d'options d'intégration.

Ajouter des entrées spécifiques à une implémentation

Ajoutez des entrées de temps d'exécution spécifiques pour chacune des implémentations sélectionnées, le cas échéant.

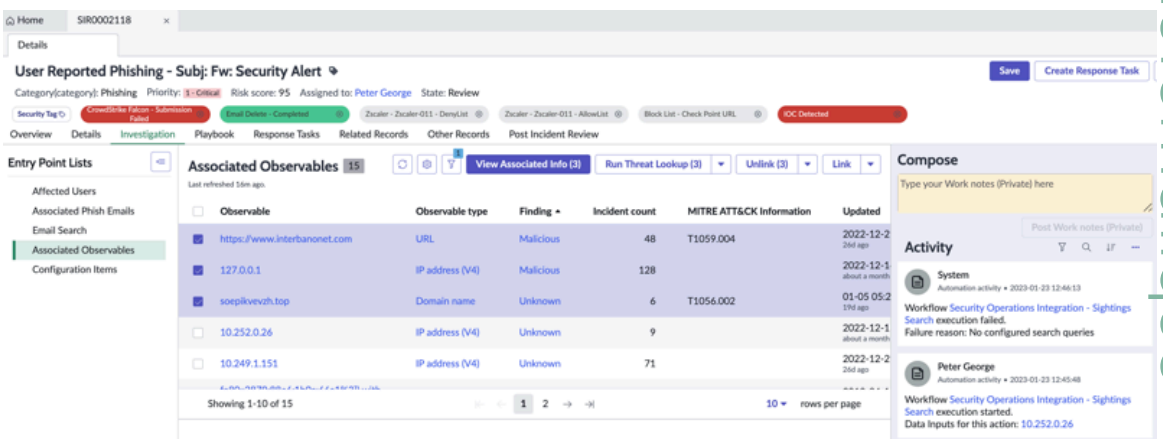
Avant de commencer

Rôle requis : sn_si.analyst

Les implémentations disponibles sont répertoriées. Sélectionnez la ou les implémentations. Après les avoir sélectionnées, seuls les enregistrements pris en charge sont soumis pour chaque implémentation sélectionnée.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Accédez à l'onglet **Examiner** de l'espace de travail.
   L'onglet Examiner avec les listes de points d'entrée s'affiche.

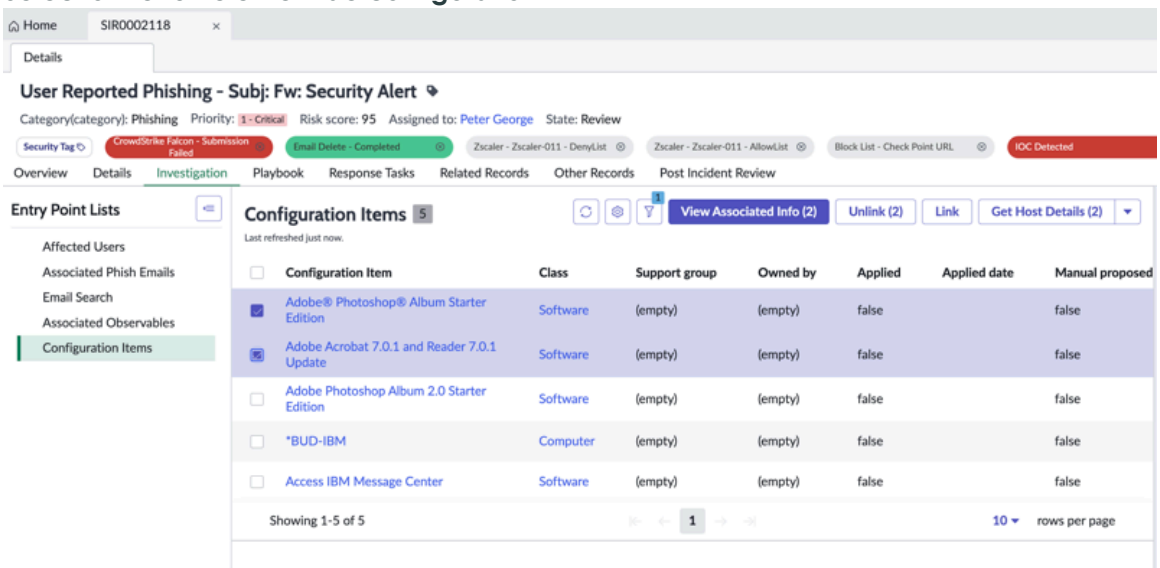


4. Sélectionnez l'élément de configuration dans la liste de points d'entrée.
   Par exemple, sélectionnez la liste de points d'entrée **Élément de configuration** . Les enregistrements d'éléments de configuration correspondants s'affichent.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

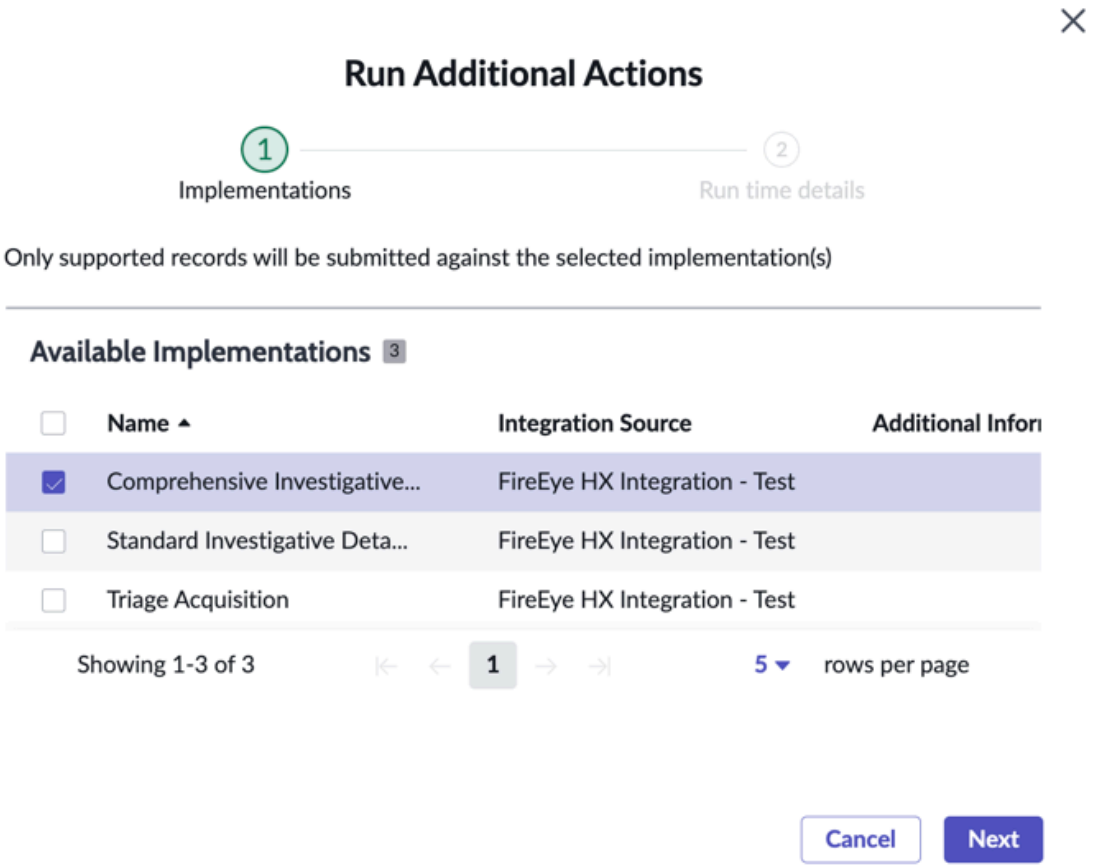
Sélectionner un élément de configuration



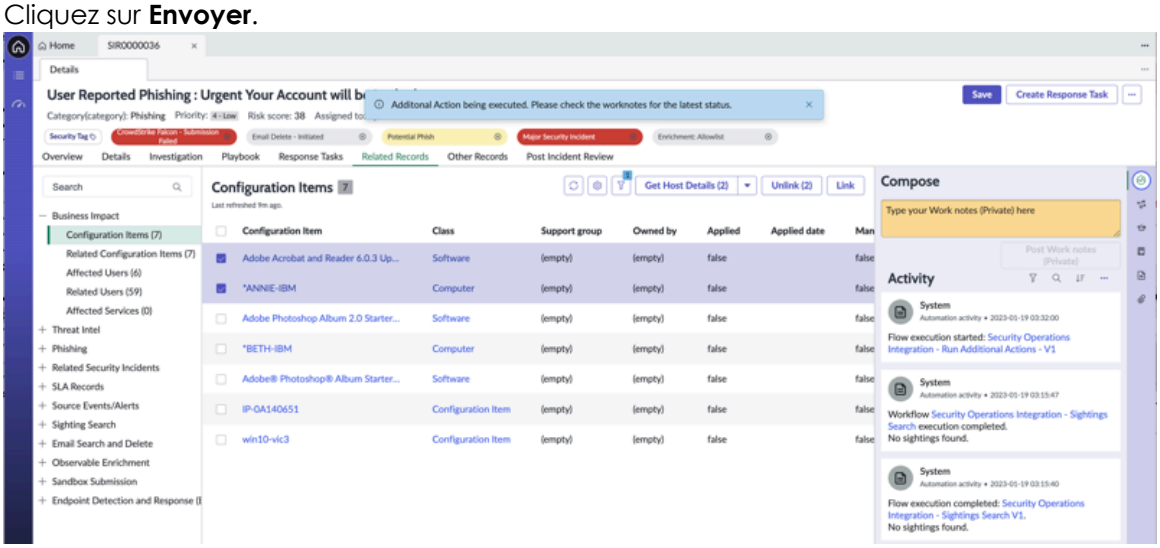
5. Sélectionnez **n'importe quel élément de configuration**.
6. Accédez à la liste déroulante des listes connexes qui s'affiche en haut de la page. Pour l'élément de configuration (CI) d'incident de sécurité, la liste déroulante contient la liste suivante d'actions d'options. Les actions de CI répertoriées collectent les résultats et les stockent en tant que données d'enrichissement sur un incident de sécurité :
   - Obtenir un fichier : cette aptitude effectue l'action pour obtenir les fichiers avec une valeur de hachage spécifique ou un nom de fichier.
   - Isoler l'hôte : cette fonctionnalité limite les connexions du système à d'autres périphériques.
   - Obtenir les détails de l'hôte : cette fonctionnalité récupère les détails de l'hôte, les détails des utilisateurs connectés et d'autres options d'enrichissement.
   - Exécuter des actions supplémentaires : cette aptitude exécute les actions supplémentaires au-delà des actions standard.
   - Obtenir les statistiques réseau : cette fonctionnalité récupère les statistiques réseau d'une ressource affectée.
   - Obtenir l'exécution du processus : cette aptitude récupère une liste des processus en cours sur un élément de configuration (CI) à partir d'un hôte.
   - Obtenir les utilisateurs connectés : cette fonctionnalité collecte les données des utilisateurs connectés et les associe à l'incident de sécurité.
7. Sélectionnez **Exécuter des actions supplémentaires** pour effectuer l'action des options d'intégration liées aux informations sur les menaces.
   La boîte de dialogue modale Exécuter des implémentations supplémentaires s'affiche.
8. Sélectionnez une ou plusieurs implémentations dans la liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Cliquez sur **Suivant**.
   Vous allez maintenant passer à l'étape suivante pour ajouter les détails de temps d'exécution.
10. Saisissez un commentaire à associer à l'action.
11. Cliquez sur **Envoyer**.



Une fois les enregistrements sélectionnés soumis, un message s'affiche indiquant que la demande d'action supplémentaire est en cours d'exécution. De plus, la progression des actions d'implémentation respectives est affichée dans la section **Activité** .

12. Affichez les résultats de la section de la liste connexe EDR.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

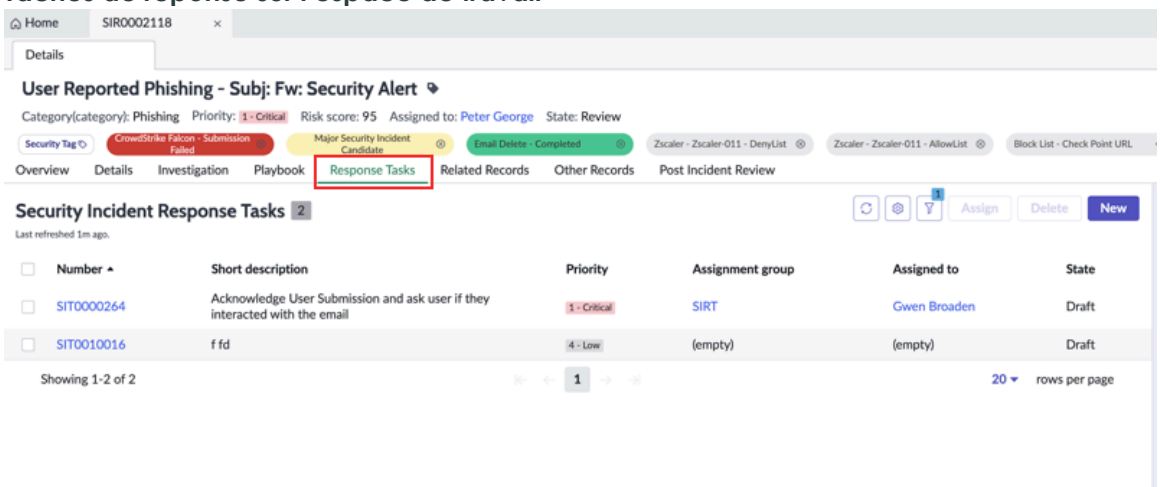
Tâches Réponse aux incidents de sécurité

Toutes les tâches de réponse associées à un incident de sécurité sont affichées dans la section Tâches de réponse.

L'analyste sera en mesure de :

- Créer une tâche de réponse
- Affecter des tâches de réponse à soi-même ou à d'autres personnes
- Supprimer les tâches de réponse

Tâches de réponse sur l'espace de travail



Remarque : Pour apporter des modifications rapides aux tâches de réponse. Sélectionnez la tâche de réponse et une liste de tâches de réponse s'affiche, sélectionnez l'enregistrement et apportez des modifications et enregistrez la tâche de réponse.

Créer une tâche de réponse

Créez des tâches de réponse pour suivre les actions distinctes à effectuer pour répondre au problème de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

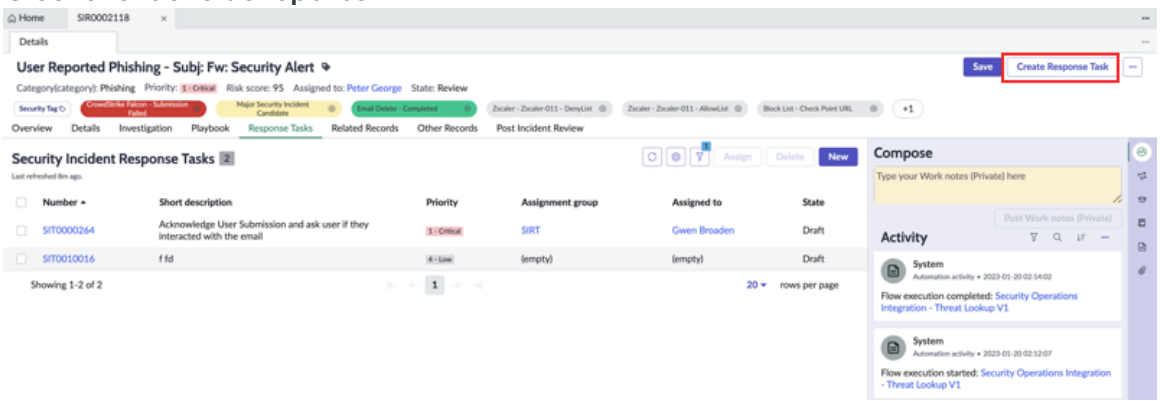
Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur **Créer une tâche de réponse** à partir des actions d'interface utilisateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une tâche de réponse



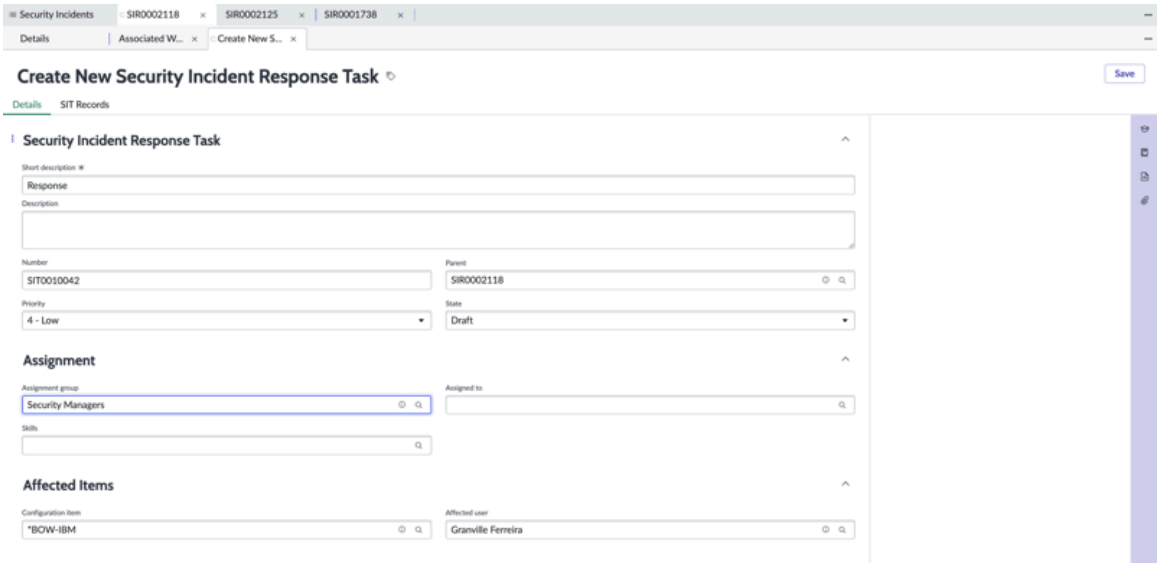
3. Renseignez les champs du formulaire comme il convient.

Incident de sécurité

Champ	Description
Description brève	Description de la Réponse aux incidents de sécurité tâche.
Description	Description de la tâche sélectionnée.
Numéro	Numéro unique généré automatiquement pour un incident de sécurité.
Parent	Numéro de l'incident de sécurité associé.
Priorité	Priorité utilisée pour déterminer le moment d'exécution de cette tâche.
État	État actuel de la tâche de réponse de sécurité. Par défaut, l'état initial est **Brouillon**.
Groupe d'affectation	Groupe d'affectation à partir duquel l'agent affecté est sélectionné.
Affecté à	Personne affectée à l'exécution de la tâche.
Compétences	Compétence requise pour effectuer cette tâche. Effectuez une recherche dans la recherche et sélectionnez la compétence requise.
Éléments affectés	Éléments affectés par le problème de sécurité.
ID d'élément de configuration	Élément de configuration affecté par le problème de sécurité.
Utilisateur affecté	La personne affectée par le problème de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



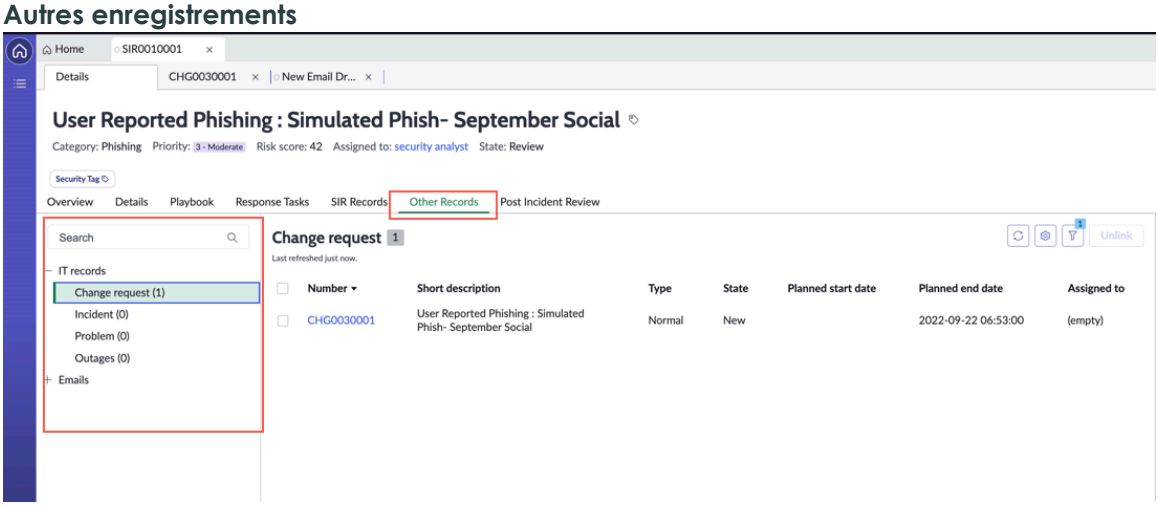
4. Cliquez sur **Enregistrer**.
   La nouvelle tâche de réponse (SIT) est créée.

Autres enregistrements de Réponse aux incidents de sécurité

Cette section affiche les autres enregistrements tels que les enregistrements informatiques et les enregistrements d'e-mails. Sous Enregistrements informatiques, Incident, Demande de changement, Problème et Pannes s'affichent.

Sous E-mail, Brouillon, E-mails envoyés et E-mails reçus s'affichent.

Autres enregistrements



Créer un incident

Créer un incident au sein d'un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst.

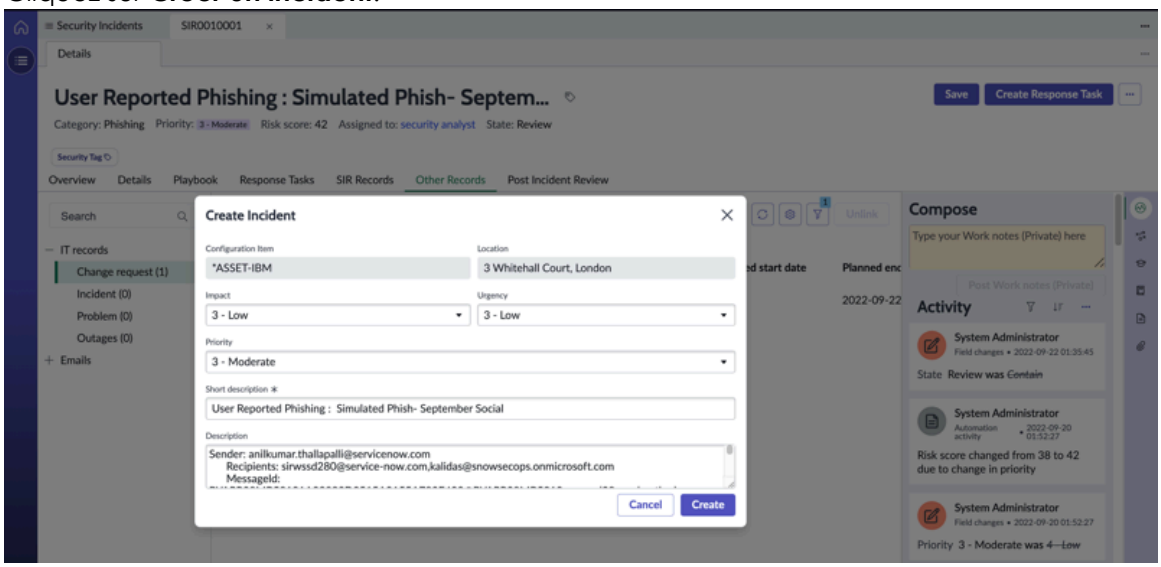
Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel enregistrement d'incident.

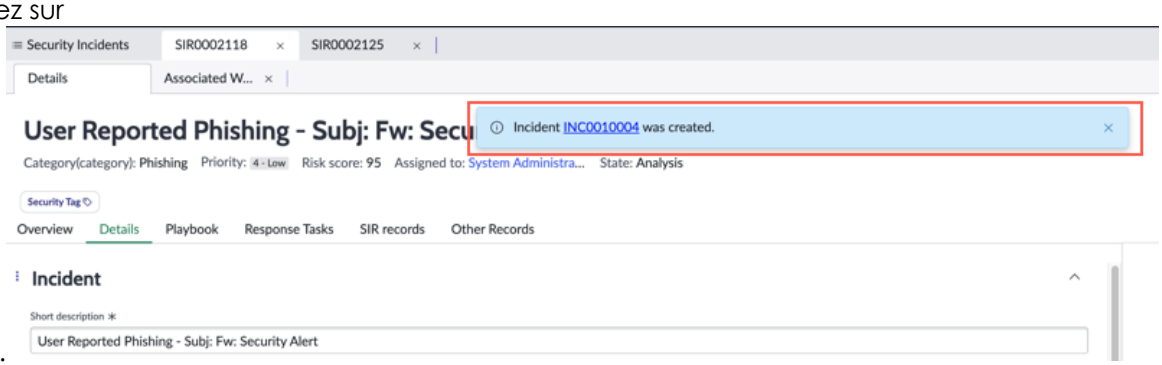
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Créer un incident**.



4. Saisissez les détails tels que l'élément de configuration, l'impact, l'urgence, l'emplacement, la priorité et la description courte.
5. Cliquez sur



Créer.

6. Un incident est créé.

Création d'une tâche de problème

Créez une tâche de problème.

Avant de commencer

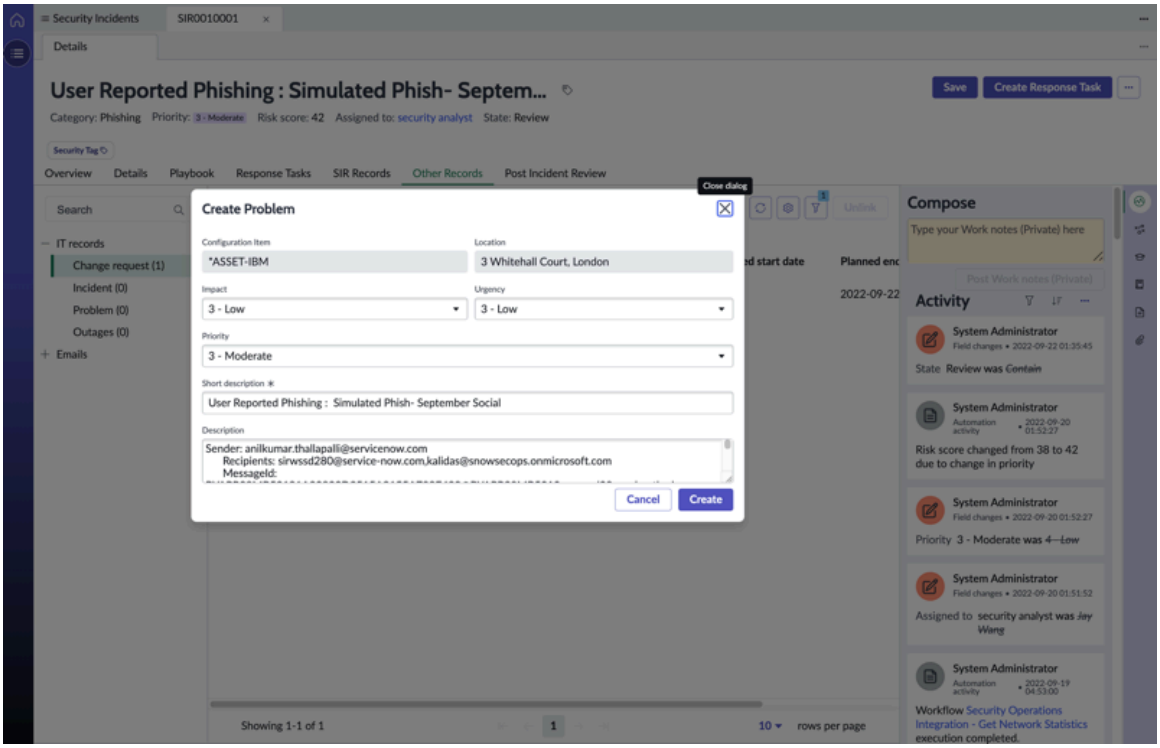
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel enregistrement d'incident.
3. Cliquez sur **Créer un problème**.

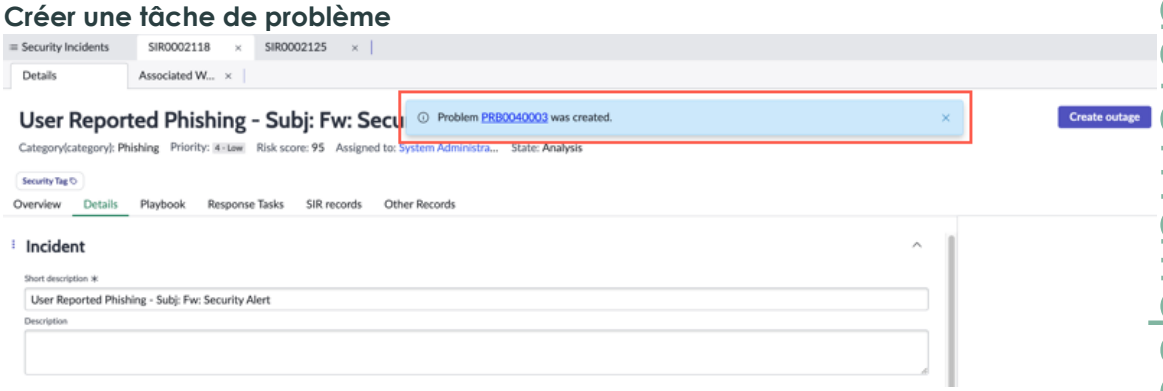
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Renseignez les détails tels que l'élément de configuration, l'emplacement, l'impact, l'urgence, la priorité et la description courte.
5. Cliquez sur **Créer**.

Créer une tâche de problème



6. Une tâche de problème est créée.

Créer une demande de changement

Créez une demande de changement.

Avant de commencer

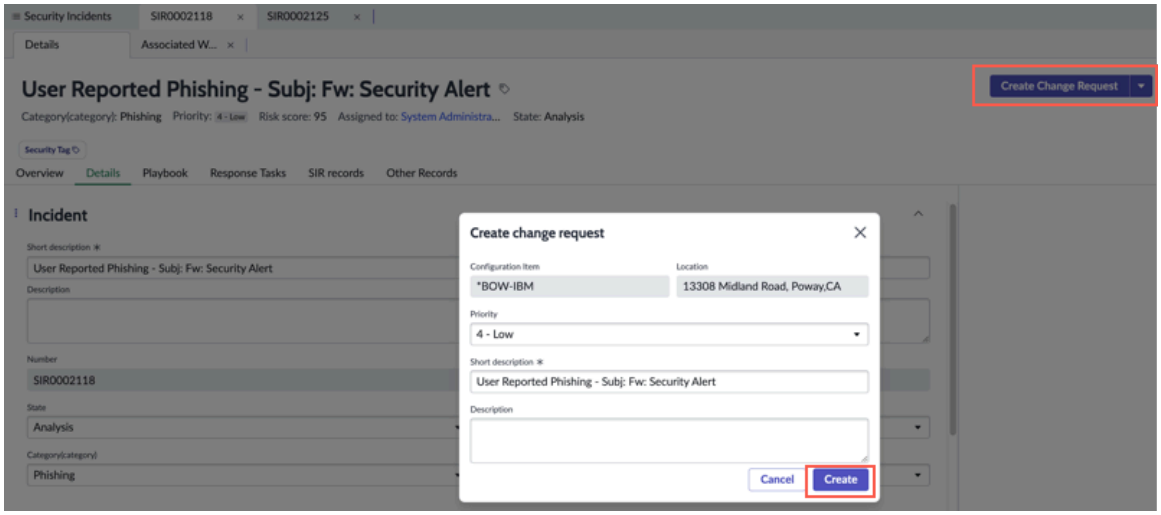
Rôle requis : sn_si.analyst.

Procédure

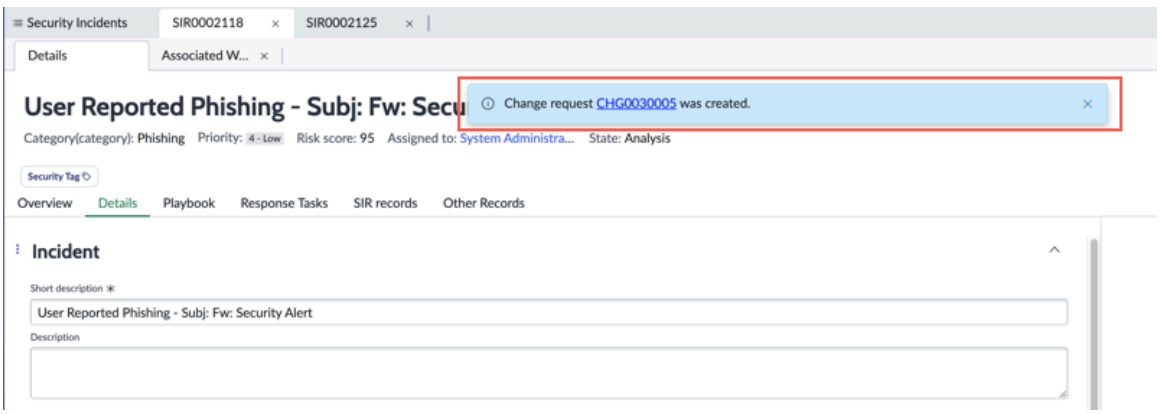
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel enregistrement d'incident.
3. Cliquez sur **Créer une demande de changement**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Entrez les détails tels que l'élément de configuration, l'emplacement, la priorité et la description courte.
5. Cliquez sur **Créer**.



6. Une demande de changement est créée.

Créer une panne

Créez une panne à partir d'un incident pour suivre le temps d'indisponibilité d'un élément de configuration.

Avant de commencer

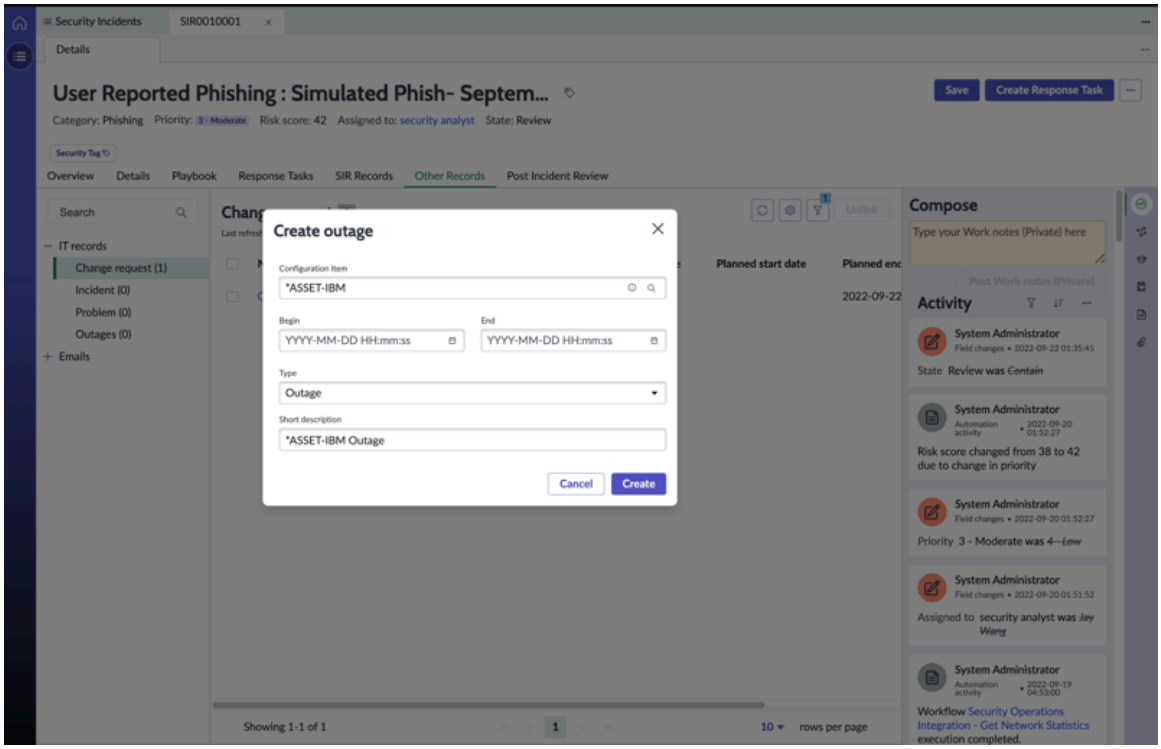
Rôle requis : sn_si.analyst

Procédure

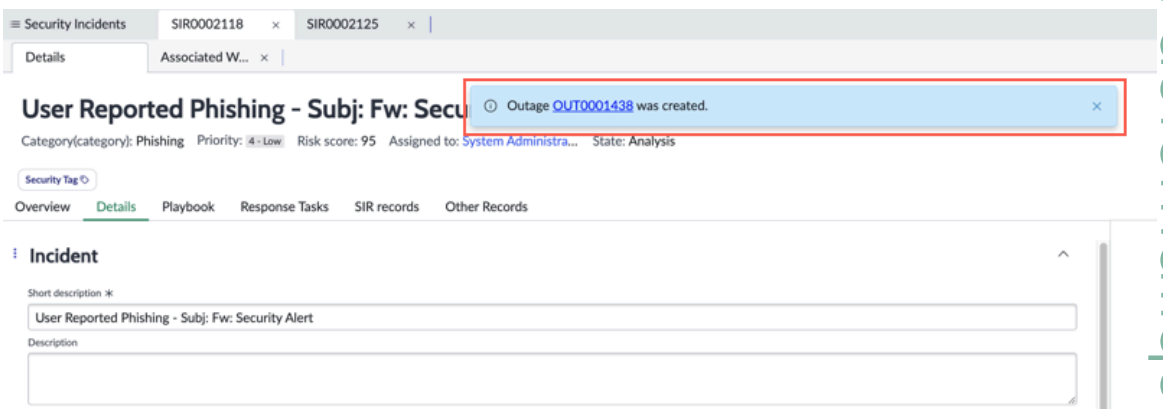
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel enregistrement d'incident.
3. Cliquez sur **Créer une panne**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Entrez les détails tels que l'élément de configuration, la date de début, la date de fin, le type et la description courte.
5. Cliquez sur **Créer**.



Composer des e-mails

En tant qu'analyste, vous pouvez rédiger des e-mails directement à partir d'incidents de sécurité.

Avant de commencer

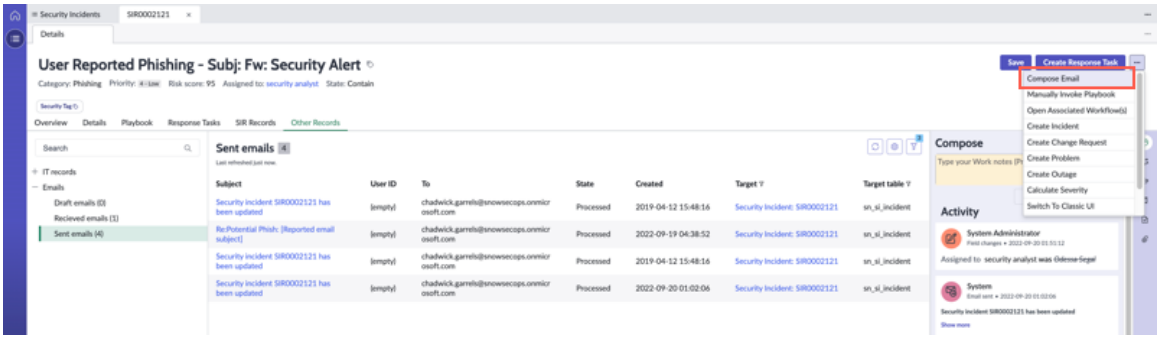
Rôle requis : sn_si.analyst

Procédure

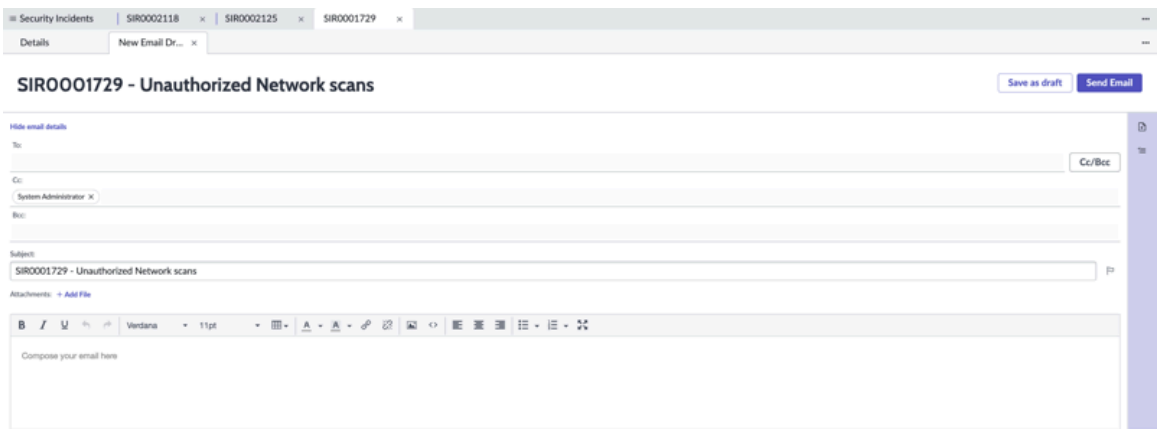
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez et ouvrez l'incident pour lequel vous souhaitez rédiger un e-mail.
3. Cliquez sur le débordement et sélectionnez **Composer un e-mail**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

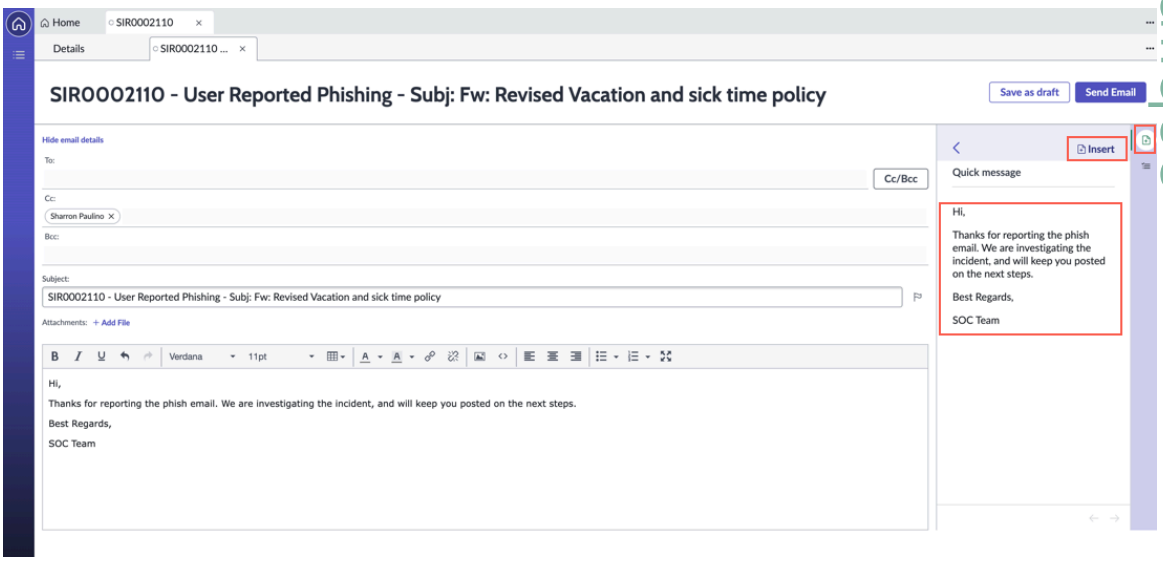


4. Saisissez les champs **À** et **CC** .



5. Ajoutez des pièces jointes, le cas échéant.

6. Dans le formulaire E-mail, cliquez sur **Messages rapides** pour afficher les messages rapides qui s'affichent sur le côté droit de la section **Composer des e-mails** .
Les messages rapides disponibles s'affichent. Sélectionnez le message et cliquez sur **Insérer**. Les messages sont insérés dans le corps de l'e-mail.



7. Composez votre e-mail et cliquez sur **Envoyer un e-mail**.

Traduction automatique

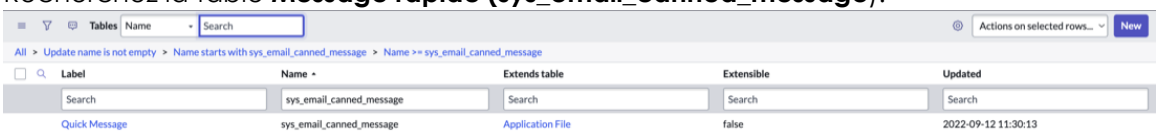
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez enregistrer un e-mail en tant que brouillon. Ces brouillons d'e-mails sont disponibles sous l'onglet Autres enregistrements.

Comment configurer les messages rapides :

a. Accédez à la **Définitions système** > **Tables**.

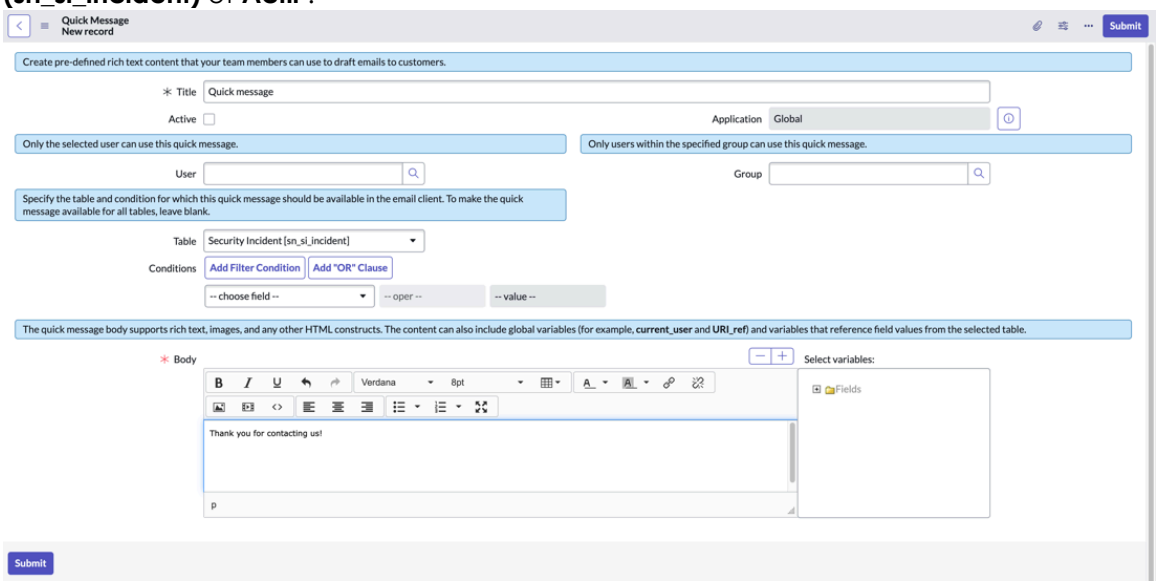
b. Recherchez la table **Message rapide (sys_email_canned_message)**.



c. Accéder à **Liens connexes** > **Afficher la liste**.

d. Créez-en un nouveau.

e. Saisissez le **titre** et **le corps du message**, cochez la case **Table : Incident de sécurité (sn_si_incident)** et **Actif** .



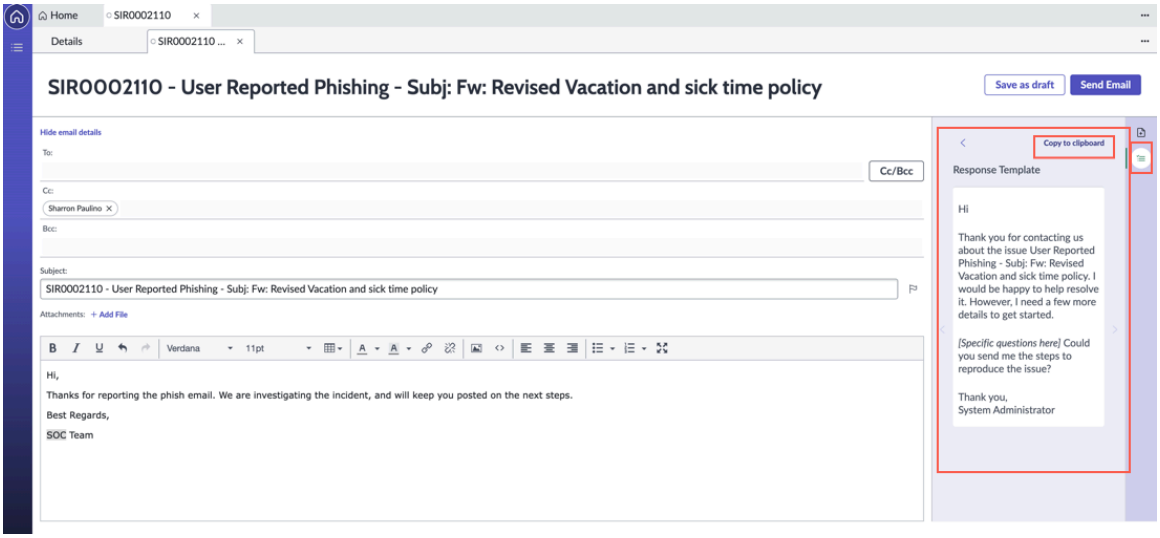
f. Cliquez sur **Envoyer**.
Une fois qu'une nouvelle entrée est créée dans la table, le message rapide apparaît dans le menu contextuel.

8. Cliquez sur **Modèles** pour ajouter un modèle si nécessaire.

9. Sélectionnez le **modèle de réponse** , puis cliquez sur **Copier dans le presse-papiers** et appliquez le modèle, si nécessaire.

Traduction automatique

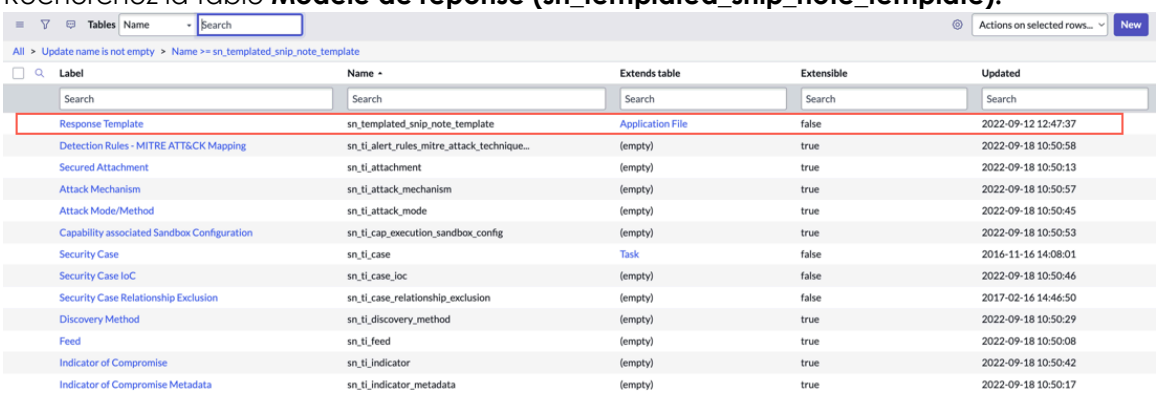
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Comment configurer les modèles de réponse :

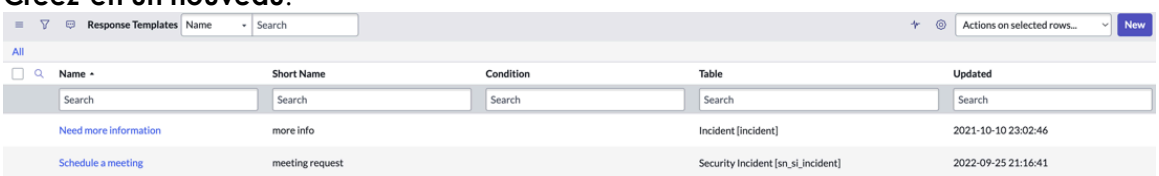
a. Accédez à la **Définitions système** > **Tables**.

b. Recherchez la table **Modèle de réponse (sn_templated_snip_note_template).**



c. Accéder à **Liens connexes** > **Afficher la liste**.

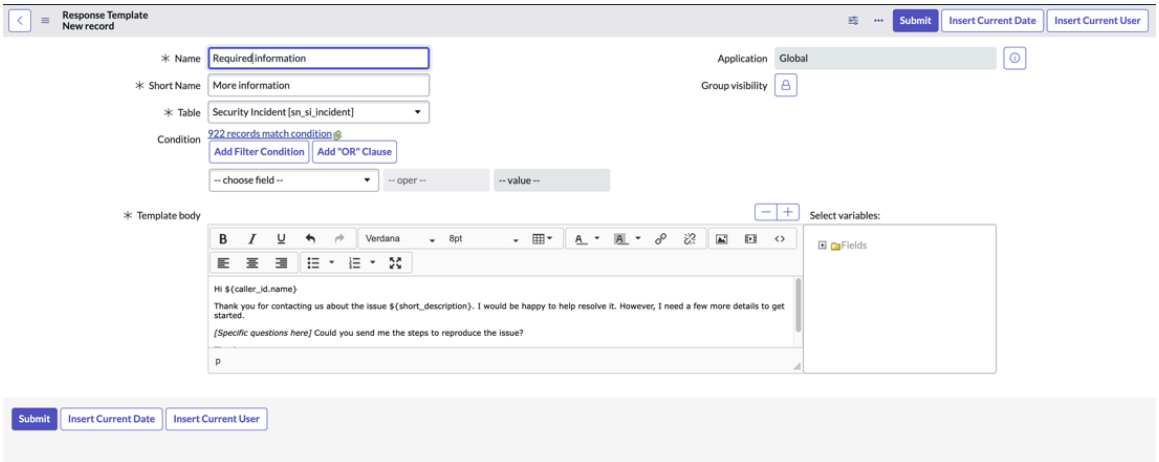
d. Créez-en un nouveau.



e. Entrez le **nom**, le **nom court**, sélectionnez la **table : incident de sécurité (sn_si_incident)** et **le corps du modèle**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



f. Cliquez sur **Envoyer**.
Une fois qu'une nouvelle entrée est créée dans la table, le nouveau modèle apparaît dans le menu contextuel.

Revue post-incident de Security Incident Response

La revue post-incident apparaît lorsqu'un incident est passé à l'état Réviser.

Pour plus d'informations sur la conduite des activités post-incident, consultez Rapport de revue post-incident

La revue post-incident comprend les sections suivantes :

1. Évaluations
2. Rapports

Depuis l'espace de travail Réponse aux incidents de sécurité, vous pourrez demander et effectuer des évaluations à l'aide de ces deux nouvelles actions d'interface utilisateur.

Nom	Description
Évaluations	L'évaluation affiche toutes les évaluations associées à l'incident de sécurité et aux autres évaluations. L'analyste sera en mesure de prendre des évaluations et de demander des évaluations. • **Passer les évaluations** : cliquez sur **Effectuer des évaluations** pour passer les évaluations (le cas échéant) et terminer l'évaluation. Avant de terminer l'évaluation, l'état de l'incident de sécurité est Prêt et la date d'échéance de l'incident est indiquée en rouge. • Évaluations de demande : cliquez sur Évaluation de la **demande** pour toute évaluation supplémentaire et vous pouvez

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
	ajouter les nouveaux utilisateurs que vous souhaitez demander. **Remarque :** Les utilisateurs qui ont déjà fait la demande n'apparaîtront pas dans cette section. Toute évaluation de cet incident a été configurée en fonction des conditions définies lors de la revue post-incident ; elle soit obligatoire ou facultative.
Rapports	Modifiez les configurations d'exécution et générez le rapport. Sélectionnez l'instance de rapport, modifiez les filtres et enregistrez le rapport. L'analyste peut prévisualiser et télécharger le rapport PIR.

Intégration de TISC dans l'espace de travail SIR

La section suivante inclut des informations sur l'intégration de Centre de sécurité des renseignements sur les menaces à partir du contexte de l'espace de travail SIR.

Envoyer des données de l'espace de travail SIR à TISC

Découvrez comment les données sont collaboratives et partagées entre les espaces de travail Centre de sécurité des renseignements sur les menaces (TISC) et Réponse aux incidents de sécurité (SIR) en suivant les procédures expliquées dans les sections suivantes.

Propriétés système pour envoyer des données

Passez en revue les propriétés système des intégrations TISC à combiner avec SIRW. Vous pouvez configurer ces propriétés pour contrôler la façon dont les deux applications gèrent les intégrations.

Principaux éléments à prendre en compte

Les propriétés système pour les intégrations TISC offrent des options de configuration avancées sur la façon dont l'application gère les observables et les enrichissements.

1. Pour définir les propriétés système des intégrations TISC dans SIRW, accédez aux **propriétés système** pour Renseignements sur les menaces et accédez à la table [sys_properties].
2. Les propriétés système contrôlent et gèrent le comportement de chaque opération de transmission de données.
3. Lorsque la propriété est activée, les données sont transmises automatiquement lorsque les données observables ou d'enrichissement sont générées dans l'espace de travail SIR.
4. Si la propriété est désactivée, les données sont transmises manuellement et les utilisateurs peuvent les transmettre par push à l'aide des actions d'interface utilisateur de l'espace de travail SIR.

La liste suivante présente les propriétés système pour l'intégration TISC - SIR :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Transmettre les données observables par push automatiquement et manuellement à partir de SIR : activez la propriété sn_ti.allow_observable_and_enrichment_records_push pour transmettre les données automatiquement ou manuellement. Si elle est désactivée, cette propriété désactive à la fois le mode automatique et le mode manuel pour toutes les transmissions de données à partir de SIR.
- Résultats de la recherche de menaces push : activez cette propriété système sn_ti.automatic_push_threat_lookup_results pour transmettre automatiquement les données de recherche de menaces à TISC. Si cette option est désactivée, les analystes de sécurité peuvent toujours transmettre manuellement les données de recherche de menaces.
- Transmettre les résultats de la recherche de perception à TISC : activez sn_ti.automatic_push_sighting_results_to_tisc cette propriété système pour transmettre automatiquement les données de recherche de perception à TISC. Si cette option est désactivée, les analystes de sécurité peuvent toujours transmettre manuellement les données de recherche de perception.
- Observables push : activez sn_ti.automatic_push_observable_to_tisc cette propriété système pour transmettre automatiquement les données observables à TISC. Si cette option est désactivée, les analystes de sécurité peuvent toujours transmettre manuellement les données observables.
- Transmettre par push les résultats d'enrichissement : activez sn_ti.automatic_push_enichment_results cette propriété système pour transmettre automatiquement les données de résultats d'enrichissement à TISC. Si cette option est désactivée, les analystes de sécurité peuvent toujours transmettre manuellement les données de résultats d'enrichissement.

Ajouter un incident de sécurité au ticket TISC

Ajoutez des incidents de sécurité aux enregistrements de tickets TISC.

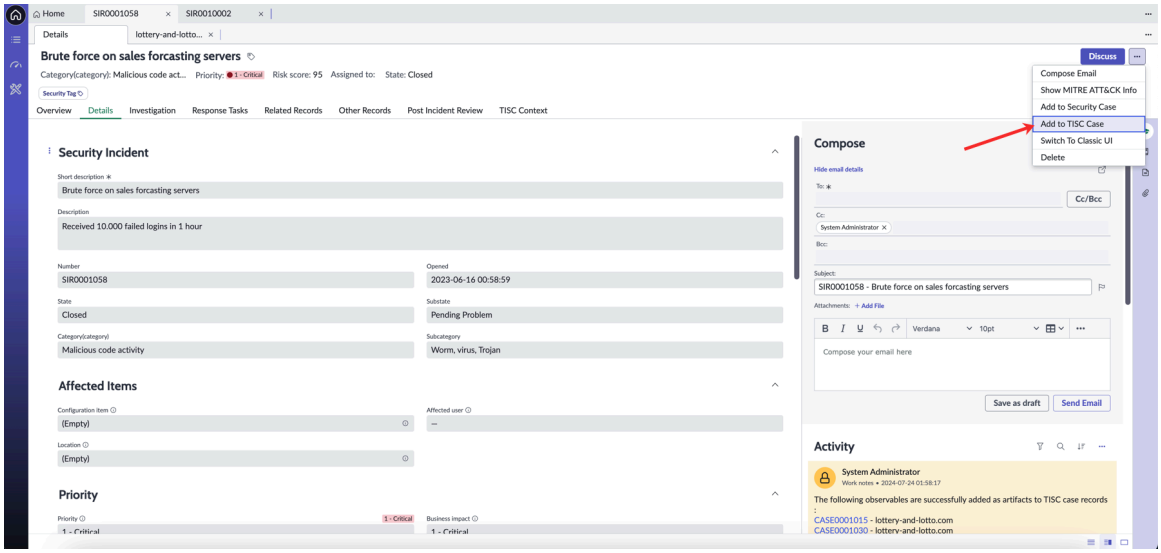
Avant de commencer

Rôle requis : sn_si.analyst, sn_sec_tisc.case_write

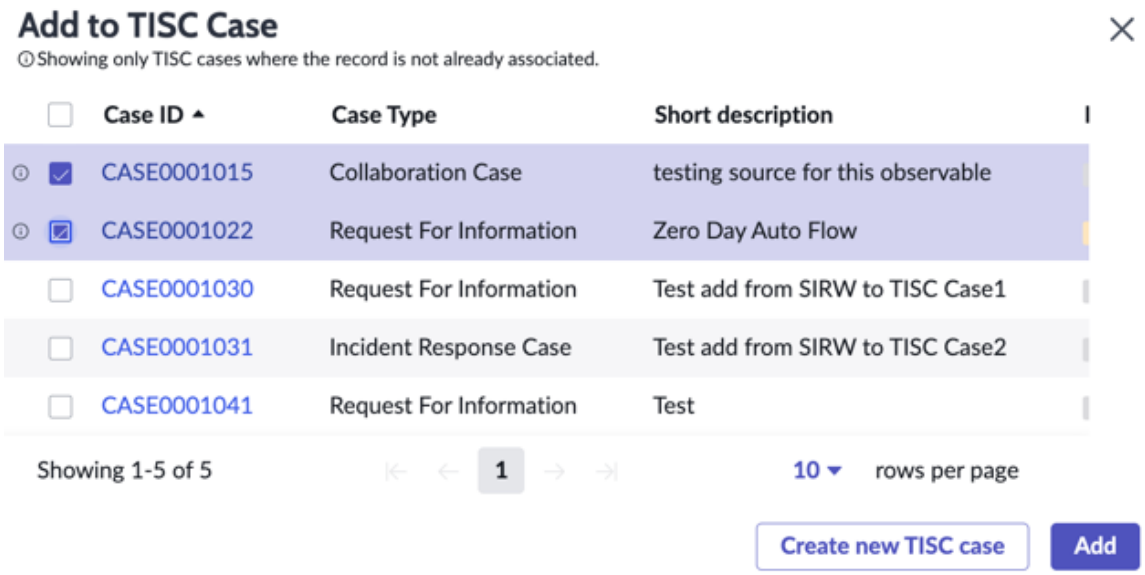
Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tout**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez.
   Cela peut également être fait en recherchant l'ID d'incident, en naviguant dans la section Filtres rapides ou en filtrant l'état de l'incident.
3. Cliquez sur l'icône **Actions supplémentaires** .
4. Cliquez sur **Ajouter à l'action de ticket TISC** .
   La boîte de dialogue Ajouter au ticket TISC s'affiche. Cela ne montre que les tickets TISC pour lesquels l'incident n'est pas déjà associé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Sélectionnez le ou les tickets dans la boîte **de dialogue Ajouter au ticket** .

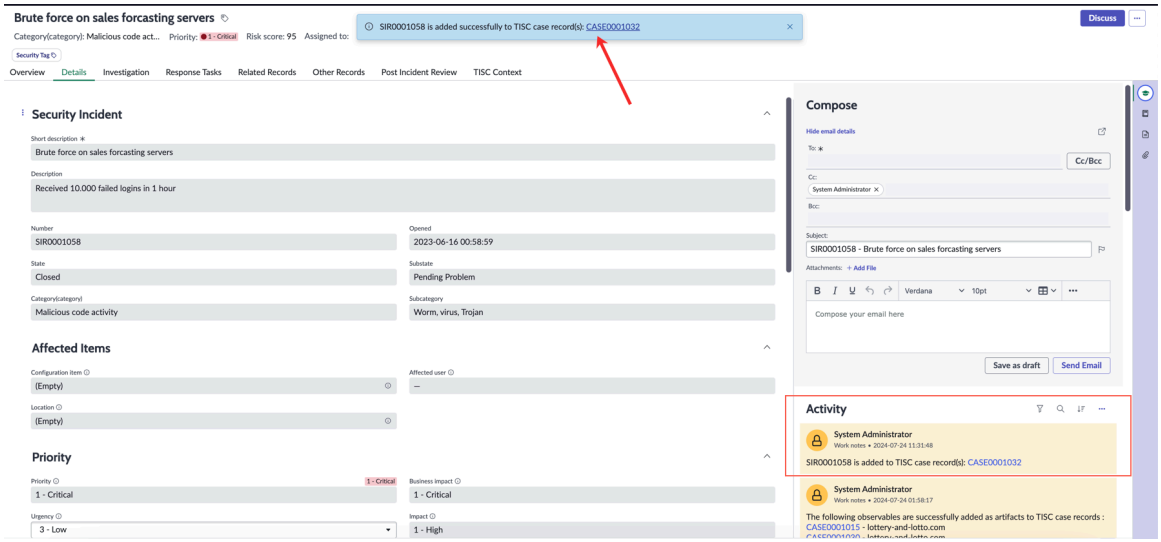


Remarque : Créez un nouveau ticket TISC s'il n'y a aucun enregistrement de ticket. Pour en savoir plus sur la création d'un ou de plusieurs tickets, reportez-vous à Création de tickets à l'aide de Threat Analyst Workbench.

6. Cliquez sur **Ajouter**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Cliquez sur l'enregistrement du ticket pour afficher le ticket dans TISC à partir du message d'information affiché ou à partir du flux **d'activité** .

> **Remarque :** Pour afficher les incidents de sécurité liés, cliquez sur l'enregistrement de cas particulier à partir du flux **d'activité** de l'incident de sécurité. En cliquant dessus, vous accéderez à l'enregistrement de ticket dans l'espace de travail TISC et les incidents de sécurité seront ajoutés sous l'onglet Artefacts du module de gestion des **tickets** .

Ajouter des observables au ticket TISC

Ajoutez des observables aux enregistrements de tickets TISC.

Avant de commencer

Rôle requis : sn_si.analyst, sn_sec_tisc.case_write

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tout**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez.
   Cela peut également être fait en recherchant l'ID d'incident, en naviguant dans la section Filtres rapides ou en filtrant l'état de l'incident.
3. Cliquez sur l'onglet **Enregistrements connexes** de l'espace de travail.
   Vous pouvez effectuer l'action d'ajout d'observables au(x) ticket(s) TISC à l'aide de différents onglets de l'espace de travail Security Incident Response.

> **Remarque :** Vous pouvez accéder au modèle suivant :
>
> - Page Détails des observables dans l'onglet Enregistrements connexes.
> - **Examination** , accédez à la section **Listes de points d'entrée** affichée sur le côté gauche de la page et sélectionnez **Observables associés** pour ajouter des observables au ticket TISC.

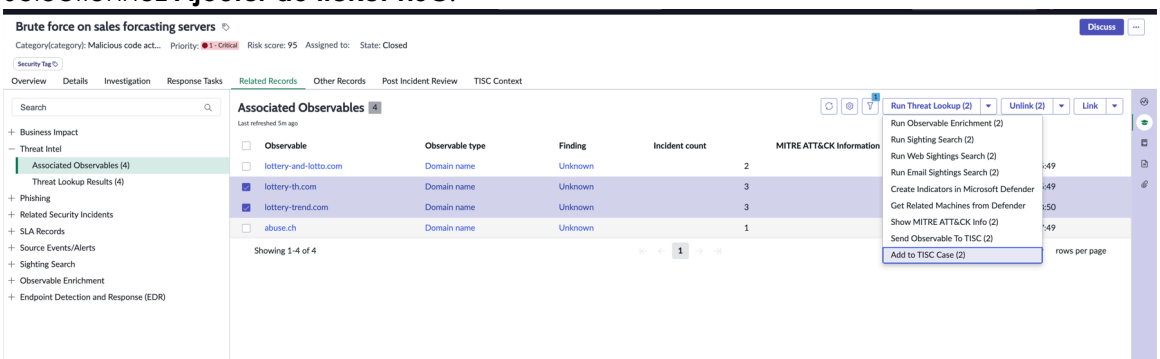
4. Par exemple, sélectionnez **Connaissance de la menace** > **Observables associés**.
5. Sélectionnez un ou plusieurs observables pour ajouter les observables sélectionnés aux enregistrements de ticket.

Traduction automatique

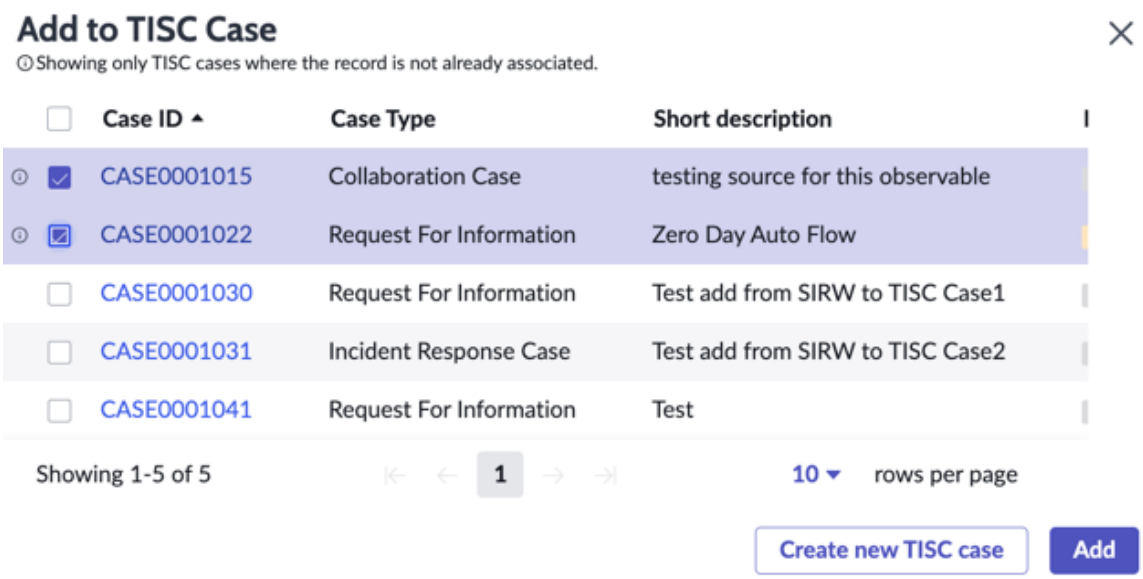
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez également cliquer sur l'un des enregistrements d'observables pour ouvrir la page des détails des observables dans un onglet différent et vous pouvez ajouter des enregistrements de tickets à partir d'ici en cliquant sur Ajouter au ticket TISC.

6. Cliquez sur le bouton de fractionnement des **actions d'aptitude** .
7. Sélectionnez **Ajouter au ticket TISC**.



8. Sélectionnez le ou les tickets dans la boîte **de dialogue Ajouter au ticket** .



Remarque : Créez un nouveau ticket TISC s'il n'y a aucun enregistrement de ticket. Pour en savoir plus sur la création d'un ou de plusieurs tickets, reportez-vous à Création de tickets à l'aide de Threat Analyst Workbench.

9. Cliquez sur **Ajouter**.
10. Cliquez sur l'enregistrement du ticket pour afficher le ticket dans TISC à partir du message d'information affiché ou à partir du flux **d'activité** .

Remarque : Si l'observable n'a pas d'observable TISC correspondant, l'observable sélectionné dans l'espace de travail SIR est envoyé automatiquement à TISC et ajouté par la suite à l'/aux enregistrement(s) de tickets TISC sélectionné(s). Pour afficher les observables liés, cliquez sur l'enregistrement de cas particulier dans le flux **d'activité** . En cliquant dessus, vous accéderez à l'enregistrement de ticket dans l'espace de travail TISC et les observables seront ajoutés sous l'onglet **Artefacts** du module Gestion des tickets.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Vous avez correctement envoyé les données observables à la gestion des tickets du Centre de sécurité des renseignements sur les menaces.

Envoyer des observables à TISC

À l'aide de cette fonctionnalité, l'analyste de sécurité peut transmettre les données observables de SIR à TISC. À l'aide du contexte TISC, vous pouvez vérifier si les observables sont présents dans TISC, sinon l'analyste de la sécurité peut transmettre les données par push chaque fois que nécessaire.

Avant de commencer

Rôle requis : sn_si.analyst

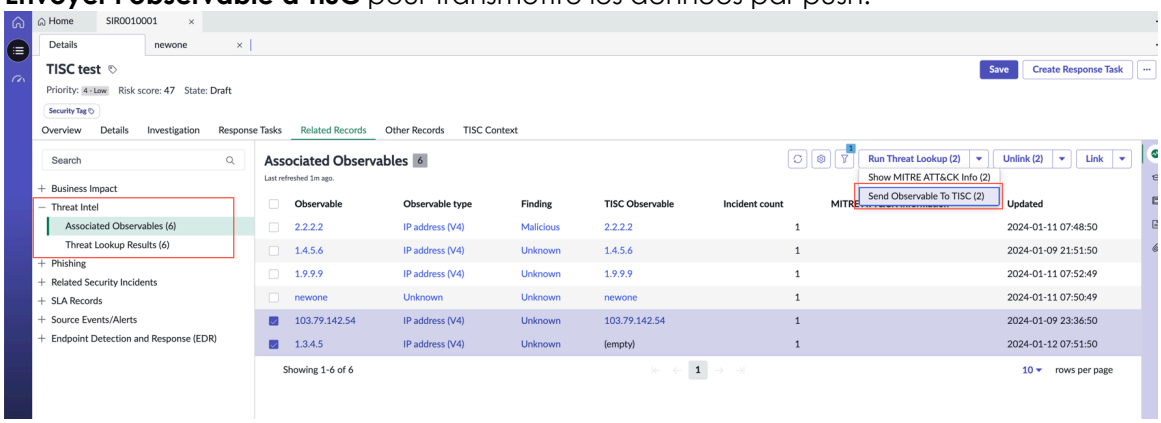
Procédure

1. Accédez à l'onglet **Enregistrements connexes** dans l'espace de travail SIR pour effectuer l'action d'aptitude d'intégration TISC.

   Remarque :

   - Vous pouvez également naviguer vers l'onglet **Examiner** et naviguer vers la section **Listes de points d'entrée** affichée sur le côté gauche de la page et sélectionner **les observables associés** pour effectuer l'opération push.
   - Dans l'onglet **Investigation** , cliquez sur **Afficher les informations connexes** pour afficher toutes les données associées de recherche de menace, de recherche de perception et d'enrichissement pour l'observable sélectionné. Pour plus d'informations, consultez Explorer le canevas d'enquête.

2. Par exemple, sélectionnez **Connaissance de la menace** > **Observables associés** pour effectuer l'opération push et pousser manuellement les données dans TISC.
3. Sélectionnez un ou plusieurs enregistrements d'observables pour effectuer l'opération **Envoyer l'observable à TISC** pour transmettre les données par push.



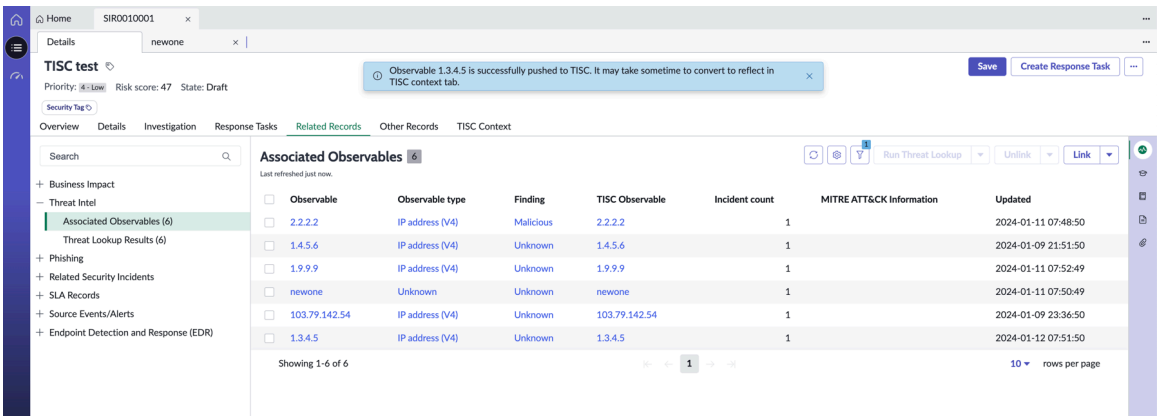
4. Cliquez sur **Envoyer l'observable à TISC**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si l'observable sélectionné n'est pas présent dans TISC, l'observable est d'abord créé en tant que source d'observable, puis une fois que l'observable source crée un enregistrement d'observable TISC, l'enregistrement de l'observable est automatiquement associé à l'observable nouvellement créé.
- Une fois l'opération push de l'observable effectuée, un message d'information s'affiche indiquant que `l'observable 0.0.0.0 a été transmis avec succès à TISC. La conversion peut prendre un certain temps pour refléter dans l'onglet` contextuel TISC.



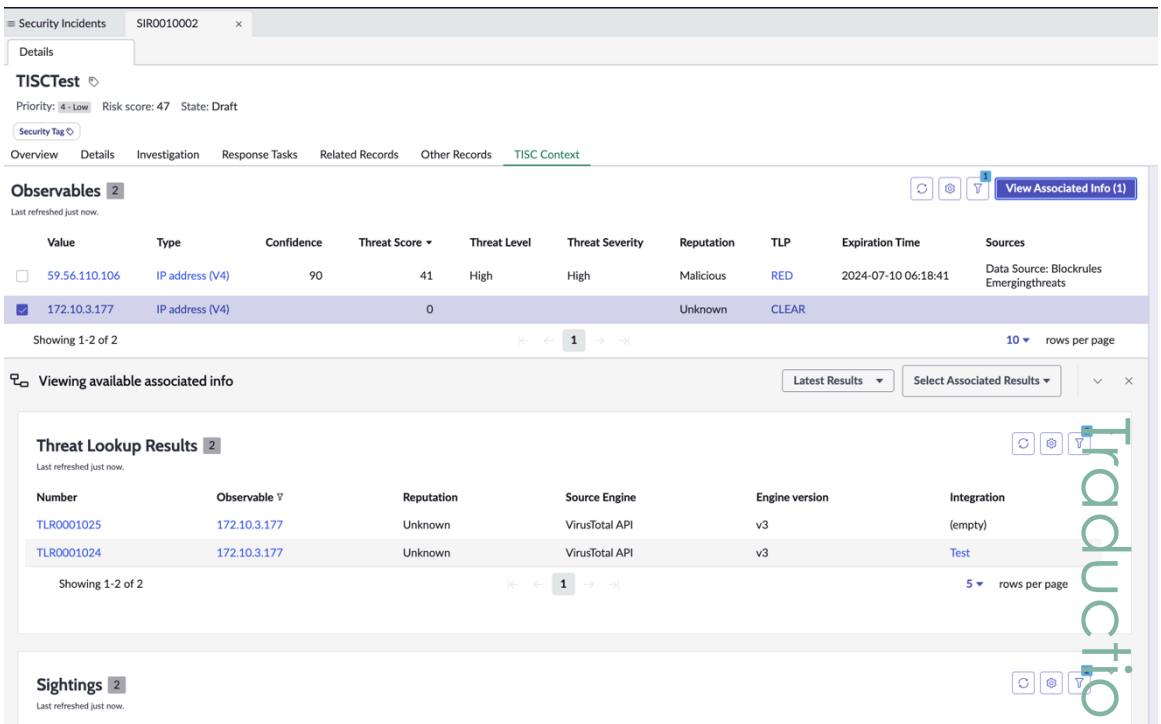
5. Sélectionnez **le contexte TISC**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : :

- Vous verrez maintenant l'observable qui est transmis par push à TISC à partir de l'application SIR.



- **Dans une opération push manuelle** : les données observables ne peuvent être transmises que si elles sont liées aux incidents de sécurité. Une fois que l'observable est transmis par push à partir de SIR, ces données peuvent être identifiées à l'aide de sources qui font référence à l'incident de sécurité lié à l'observable.
- **Dans une opération push automatique** : les données observables ou d'enrichissement sont poussées automatiquement lorsqu'elles sont associées à un incident de sécurité.
- **Le contexte TISC** affiche tous les observables associés au SIR qui sont également présents dans TISC.
- À l'aide du contexte TISC, les analystes SIR peuvent voir toutes les données d'enrichissement TISC, y compris les recherches de menaces, la recherche de perception et les résultats d'enrichissement des observables.
- **Afficher les informations associées** affiche toutes les données d'enrichissement observable associées des observables sélectionnés.

6. Affichez les résultats.

Envoyer une recherche de menace à TISC

Grâce à cette fonctionnalité, l'analyste en sécurité peut transmettre les données de recherche de menaces de SIR à TISC. À l'aide du contexte TISC, vous pouvez vérifier si les résultats de la recherche de menace sont présents dans TISC, sinon l'analyste de la sécurité peut transmettre les données par push chaque fois que nécessaire.

Avant de commencer
Rôle requis : sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

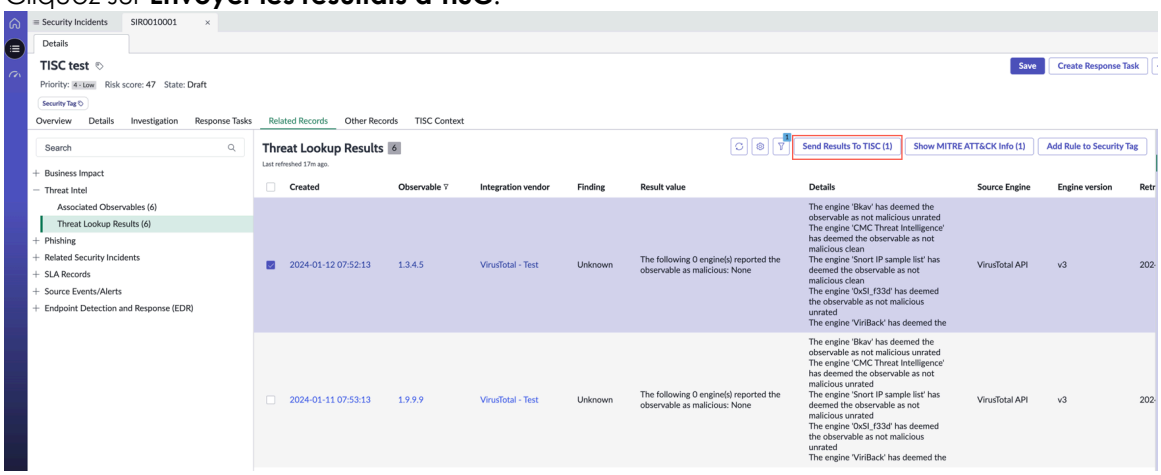
Procédure

1. Accédez à l'onglet **Enregistrements connexes** dans l'espace de travail SIR pour effectuer l'action d'aptitude d'intégration TISC.

Remarque :

- Vous pouvez également naviguer vers l'onglet **Examiner** et naviguer vers la section **Listes de points d'entrée** affichée sur le côté gauche de la page et sélectionner **les observables associés** pour effectuer l'opération push.
- Dans l'onglet **Investigation** , cliquez sur **View Associated Info (Afficher les informations associées**) pour afficher toutes les données associées de recherche de menace, de recherche de perception et d'enrichissement pour l'observable sélectionné. Pour plus d'informations, consultez Explorer le canevas d'enquête.

2. Sélectionner **Connaissance de la menace** > **Résultats de la recherche de menace** pour effectuer l'opération push et pousser manuellement les données dans TISC.
3. Sélectionnez un ou plusieurs enregistrements des résultats de la recherche de menace.
4. Cliquez sur **Envoyer les résultats à TISC**.



Remarque :

- Si l'observable de recherche de menace sélectionné n'est pas présent dans TISC, l'observable est d'abord créé en mode manuel en tant que source d'observable, puis une fois que l'observable source crée un enregistrement d'observable TISC, l'enregistrement de l'observable est automatiquement associé à l'observable nouvellement créé. En outre, la recherche de menaces sélectionnée sera également transmise à l'observable de recherche de menaces nouvellement créé en mode manuel.
- En mode automatique, les observables ne seront pas poussés si l'observable est présent, puis les recherches de menaces seront poussées automatiquement. Si les observables ne sont pas présents, les recherches de menaces ne sont pas poussées.

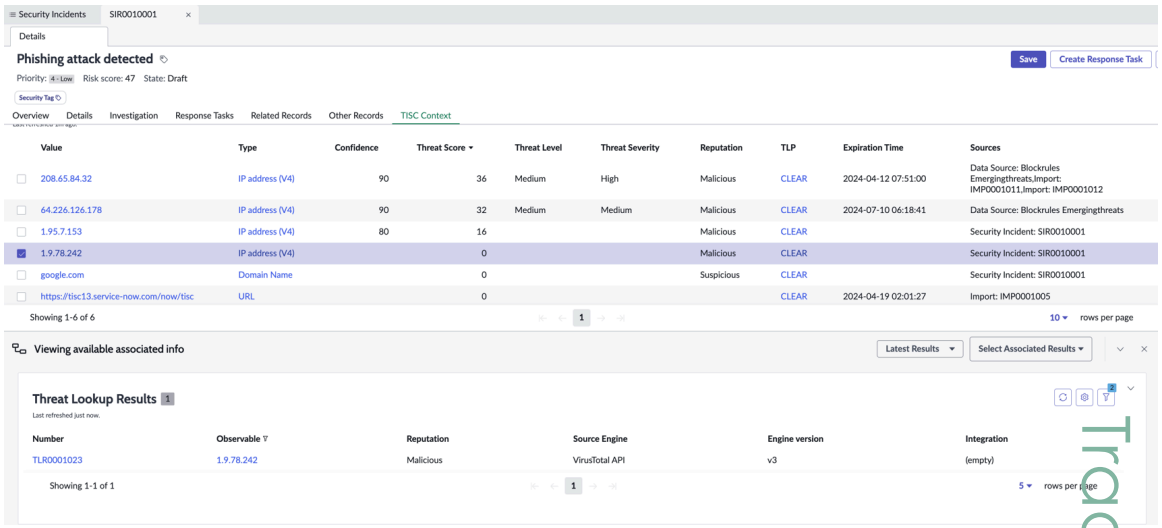
5. Un message de confirmation s'affiche indiquant que `l'observable (1.9.78.242) pour l'enregistrement de recherche de menaces sélectionné n'existe pas dans TISC. La création d'un observable et l'association automatique de l'enregistrement de recherche de menace observable dans TISC prennent un certain temps.`
   Une fois que cela est traité et transmis, vous pouvez voir les résultats.
6. Sélectionnez **le contexte TISC**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : :

- Vous verrez maintenant l'observable qui est transmis par push à TISC à partir de l'application SIR.



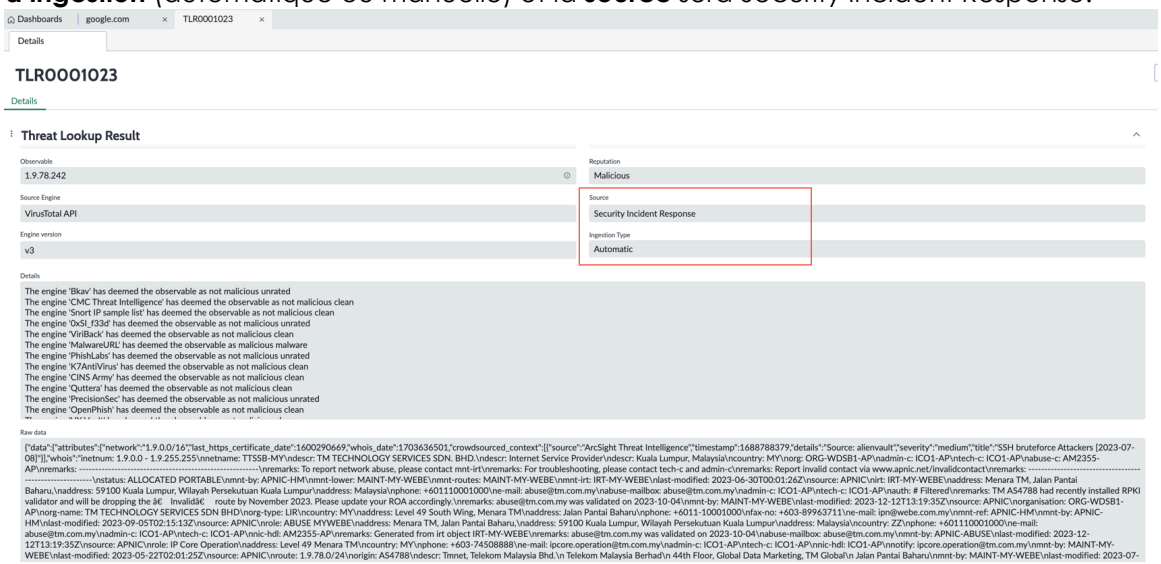
- **Dans une opération push manuelle** : les données observables ne peuvent être transmises que si elles sont liées aux incidents de sécurité. Une fois que l'observable est transmis par push à partir de SIR, ces données peuvent être identifiées à l'aide de sources qui font référence à l'incident de sécurité lié à l'observable.
- **Dans une opération push automatique** : les données observables ou d'enrichissement sont poussées automatiquement lorsqu'elles sont associées à un incident de sécurité.
- **Le contexte TISC** affiche tous les observables associés au SIR qui sont également présents dans TISC.
- À l'aide du contexte TISC, les analystes SIR peuvent voir toutes les données d'enrichissement TISC, y compris les recherches de menaces, la recherche de perception et les résultats d'enrichissement des observables.
- **Afficher les informations associées** affiche toutes les données d'enrichissement observable associées des observables sélectionnés.

7. La vue de liste affiche tous les résultats de la recherche de menace, cependant sélectionnez n'importe quel enregistrement et cliquez sur le bouton **Afficher les informations associées** .
8. Affichez les résultats de la recherche de menaces.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Cliquez sur n'importe quel enregistrement des résultats de la recherche de menaces pour afficher l'enregistrement dans la vue de formulaire, qui affiche également le type push ou **d'ingestion** (automatique ou manuelle) et la **source** sera Security Incident Response.



Envoyer la recherche de perception à TISC

Grâce à cette fonctionnalité, l'analyste de la sécurité peut transférer les données de recherche de perception de SIR vers TISC. À l'aide du contexte TISC, l'analyste peut vérifier si les données de recherche de perception sont présentes dans TISC, sinon l'analyste de sécurité peut transmettre les données par push chaque fois que nécessaire.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

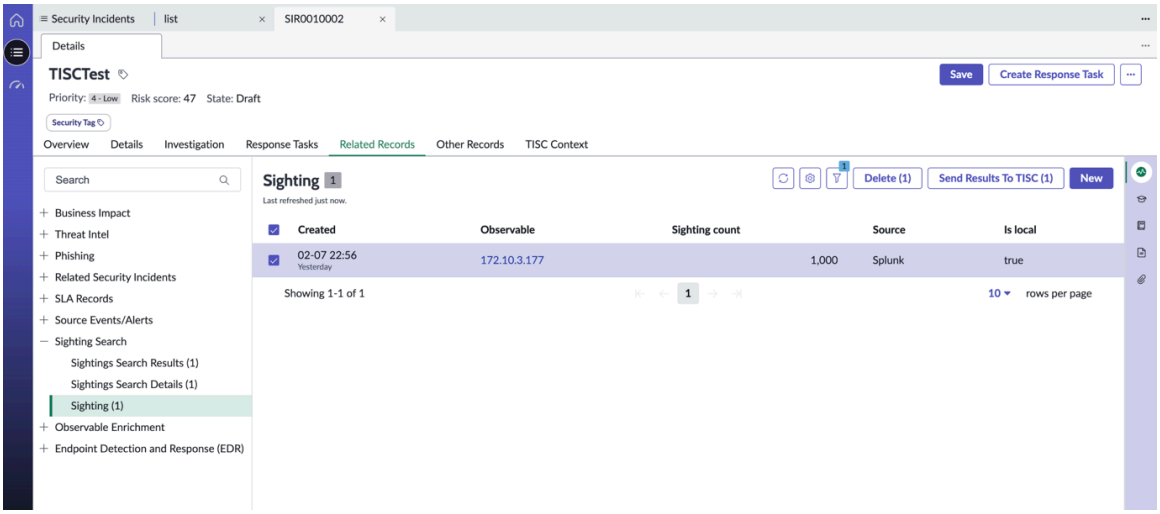
1. Accédez à l'onglet **Enregistrements connexes** dans l'espace de travail SIR pour effectuer l'action d'aptitude d'intégration TISC.

Remarque :

- Vous pouvez également naviguer vers l'onglet **Examiner** et naviguer vers la section **Listes de points d'entrée** affichée sur le côté gauche de la page et sélectionner **les observables associés** pour effectuer l'opération push.
- Dans l'onglet **Investigation** , cliquez sur **View Associated Info (Afficher les informations associées**) pour afficher toutes les données associées de recherche de menace, de recherche de perception et d'enrichissement pour l'observable sélectionné. Pour plus d'informations, consultez Explorer le canevas d'enquête.

2. Sélectionner **Recherche de perception** > **Résultats de recherche de perception** pour effectuer l'opération push et pousser manuellement les données dans TISC.
3. Sélectionnez un ou plusieurs enregistrements de résultats de recherche de perceptions.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

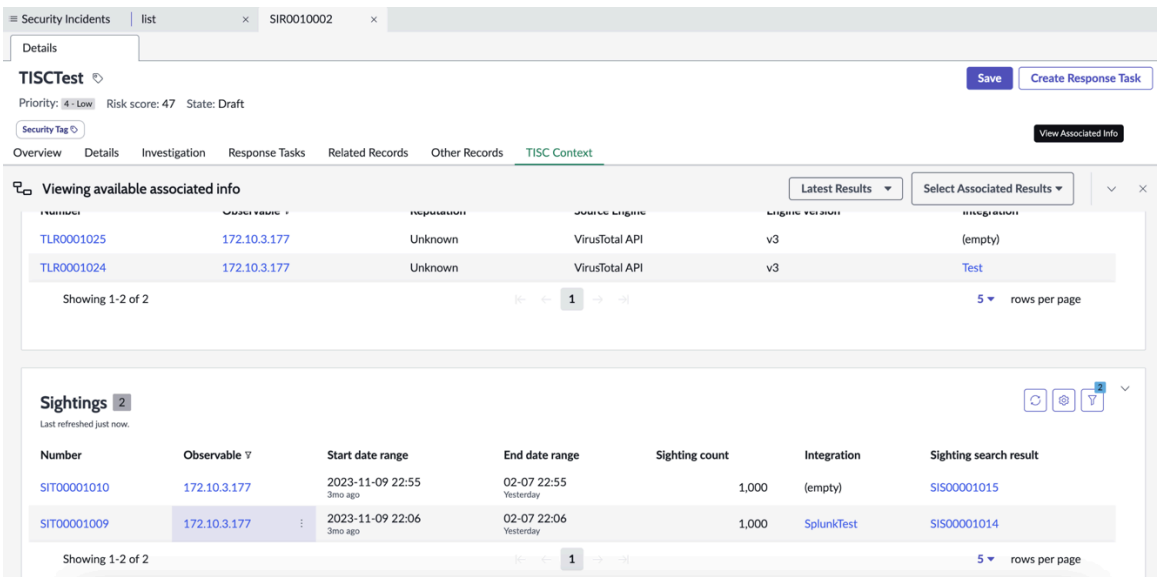


4. Cliquez sur **Envoyer les résultats à TISC**.

Remarque :

- Si l'observable de recherche de perception sélectionné n'est pas présent dans TISC, l'observable est d'abord créé en mode manuel en tant que source d'observable, puis une fois que l'observable source crée un enregistrement d'observable TISC, l'enregistrement de l'observable est automatiquement associé à l'observable nouvellement créé. En outre, la recherche d'observation sélectionnée sera également transmise à l'observable de recherche de menaces nouvellement créé en mode manuel.
- En mode automatique, les observables ne seront pas poussés si l'observable est présent, puis les recherches de menaces seront poussées automatiquement. Si les observables ne sont pas présents, les recherches de menaces ne sont pas poussées.

5. Sélectionnez **le contexte TISC**.



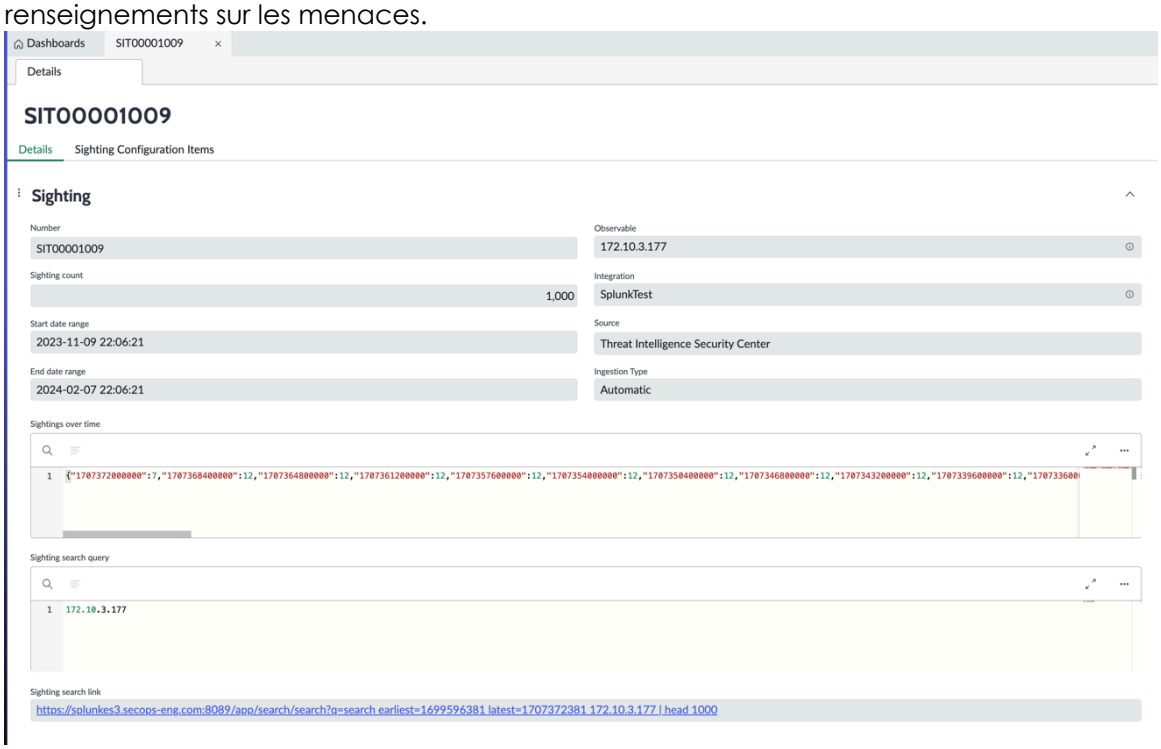
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : :

- Vous verrez maintenant l'observable qui est transmis par push à TISC à partir de l'application SIR.
- **Dans une opération push manuelle** : les données observables ne peuvent être transmises que si elles sont liées aux incidents de sécurité. Une fois que l'observable est transmis par push à partir de SIR, ces données peuvent être identifiées à l'aide de sources qui font référence à l'incident de sécurité lié à l'observable.
- **Dans une opération push automatique** : les données observables ou d'enrichissement sont poussées automatiquement lorsqu'elles sont associées à un incident de sécurité.
- **Le contexte TISC** affiche tous les observables associés au SIR qui sont également présents dans TISC.
- À l'aide du contexte TISC, les analystes SIR peuvent voir toutes les données d'enrichissement TISC, y compris les recherches de menaces, la recherche de perception et les résultats d'enrichissement des observables.
- **Afficher les informations associées** affiche toutes les données d'enrichissement observable associées des observables sélectionnés.

6. Une fois l'enregistrement traité, sélectionnez-le et cliquez sur **Afficher les informations associées**.
7. Affichez les résultats.
8. Cliquez sur n'importe quel enregistrement de résultats de recherche de perception pour afficher l'enregistrement dans la vue de formulaire, qui affiche également le type push ou **d'ingestion** (automatique ou manuel) et la **source** sera Centre de sécurité des renseignements sur les menaces.



Envoyer l'enrichissement de l'observable à TISC

Grâce à cette fonctionnalité, l'analyste de la sécurité peut transférer les données de recherche de perception de SIR vers TISC. À l'aide du contexte TISC, l'analyste peut vérifier

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

si les données de recherche de perception sont présentes dans TISC, sinon l'analyste de sécurité peut transmettre les données par push chaque fois que nécessaire.

Avant de commencer

Rôle requis : sn_si.analyst

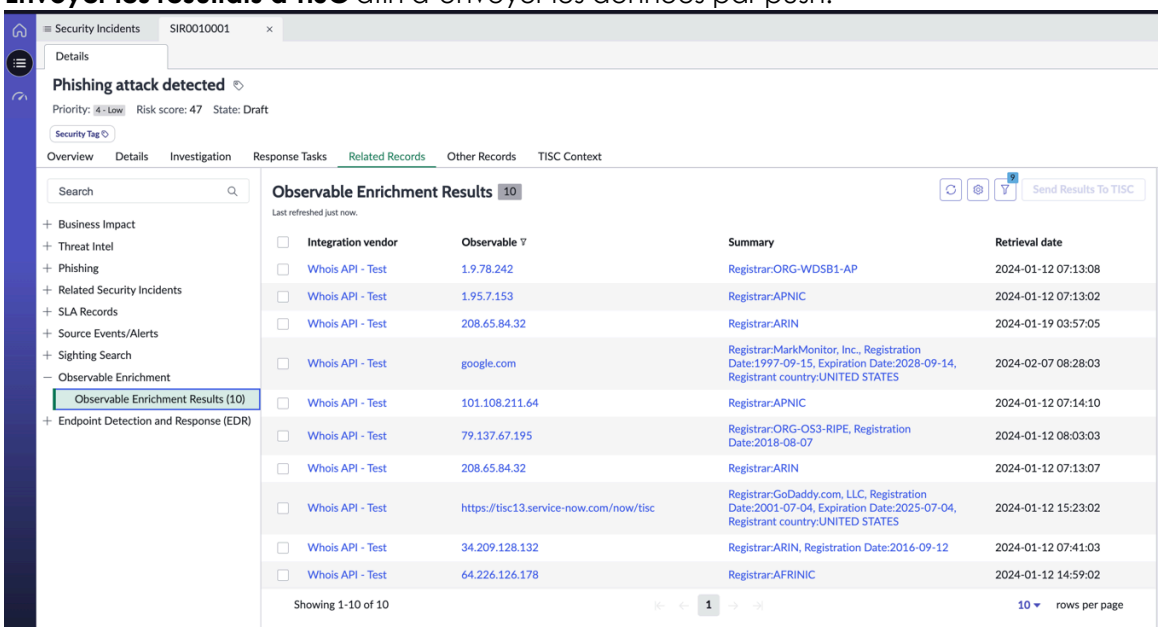
Procédure

1. Accédez à l'onglet **Enregistrements connexes** dans l'espace de travail SIR pour effectuer l'action d'aptitude d'intégration TISC.

   Remarque :

   - Vous pouvez également naviguer vers l'onglet **Examiner** et naviguer vers la section **Listes de points d'entrée** affichée sur le côté gauche de la page et sélectionner **les observables associés** pour effectuer l'opération push.
   - Dans l'onglet **Investigation** , cliquez sur **View Associated Info (Afficher les informations associées**) pour afficher toutes les données associées de recherche de menace, de recherche de perception et d'enrichissement pour l'observable sélectionné. Pour plus d'informations, consultez Explorer le canevas d'enquête.

2. Sélectionner **Enrichissement des éléments observables** > **Résultats de l'enrichissement de l'observable** pour effectuer l'opération push et pousser manuellement les données dans TISC.
3. Sélectionnez un ou plusieurs enregistrements d'observables pour effectuer l'opération **Envoyer les résultats à TISC** afin d'envoyer les données par push.



4. Cliquez sur **Envoyer les résultats à TISC**.

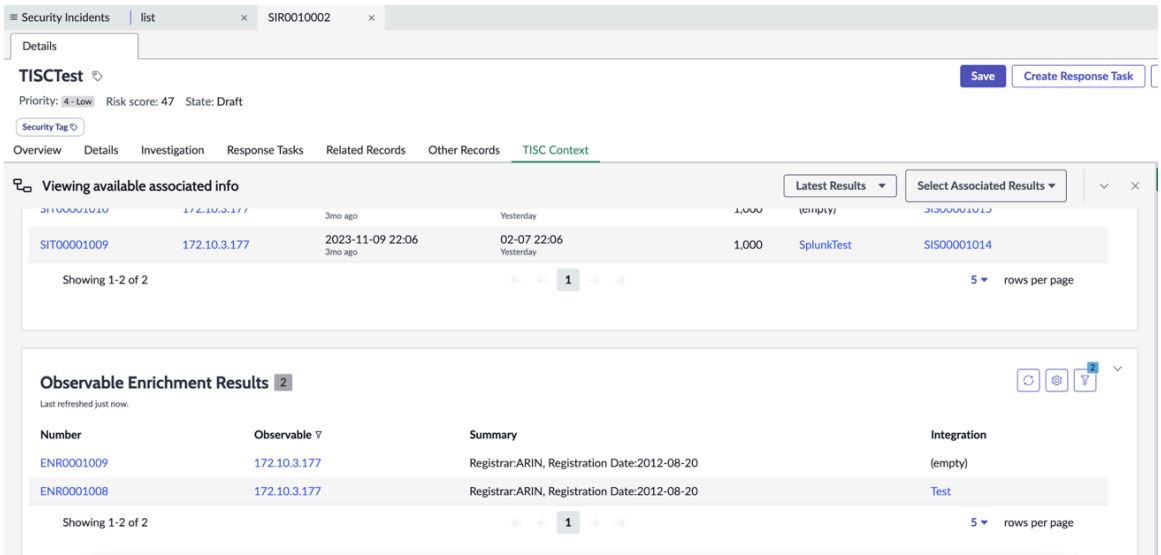
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si l'observable sélectionné n'est pas présent dans TISC, l'observable est d'abord créé en tant que source d'observable, puis une fois que l'observable source crée un enregistrement d'observable TISC, l'enregistrement de l'observable est automatiquement associé à l'observable nouvellement créé.
- Une fois l'opération push de l'observable effectuée, un message d'information s'affiche indiquant que `l'observable 0.0.0.0 a été transmis avec succès à TISC. La conversion peut prendre un certain temps pour refléter dans l'onglet` contextuel TISC.

5. Sélectionnez **le contexte TISC**.



Remarque : :

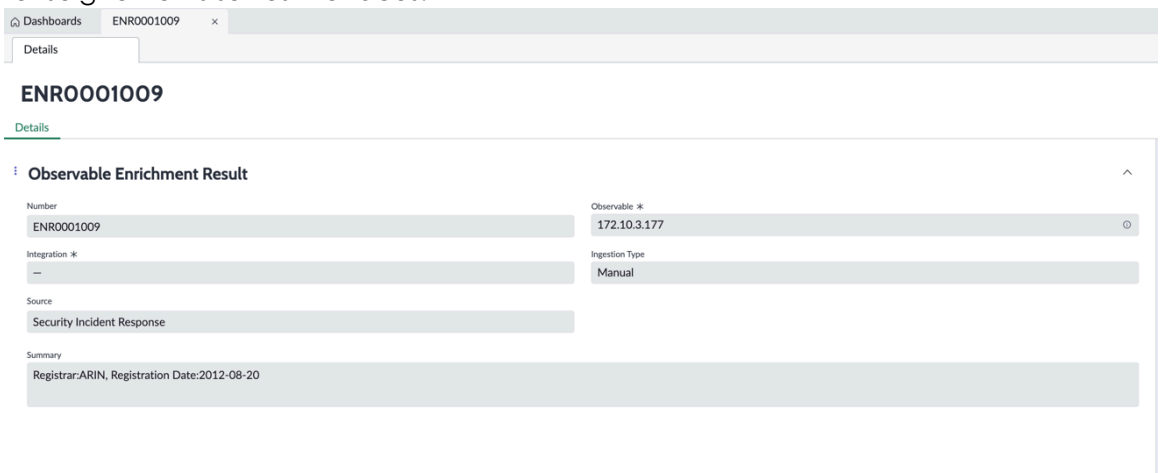
- Vous verrez maintenant l'observable qui est transmis par push à TISC à partir de l'application SIR.
- **Dans une opération push manuelle** : les données observables ne peuvent être transmises que si elles sont liées aux incidents de sécurité. Une fois que l'observable est transmis par push à partir de SIR, ces données peuvent être identifiées à l'aide de sources qui font référence à l'incident de sécurité lié à l'observable.
- **Dans une opération push automatique** : les données observables ou d'enrichissement sont poussées automatiquement lorsqu'elles sont associées à un incident de sécurité.
- **Le contexte TISC** affiche tous les observables associés au SIR qui sont également présents dans TISC.
- À l'aide du contexte TISC, les analystes SIR peuvent voir toutes les données d'enrichissement TISC, y compris les recherches de menaces, la recherche de perception et les résultats d'enrichissement des observables.
- **Afficher les informations associées** affiche toutes les données d'enrichissement observable associées des observables sélectionnés.

6. Affichez les résultats.

7. Cliquez sur n'importe quel enregistrement de résultats d'enrichissement d'observable pour afficher l'enregistrement dans la vue de formulaire, qui affiche également le type

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

push ou **d'ingestion** (automatique ou manuel) et la **source** sera Centre de sécurité des renseignements sur les menaces.



Utilisation du contexte TISC

Le contexte TISC facilite l'affichage des données Threat Intelligence telles que les observables dans l'espace de travail Security Incident Response.

Cela aide les analystes de sécurité à détecter, examiner et répondre aux incidents de sécurité plus efficacement à partir de l'espace de travail.

Le contexte TISC dans l'espace de travail Réponse aux incidents de sécurité permet aux analystes de sécurité d'ajouter des incidents de sécurité ou des observables au(x) ticket(s) TISC directement à partir de l'espace de travail, également afficher les résultats de l'enrichissement et afficher les informations relatives aux observables (acteurs de menace, modèles d'attaque, campagnes, etc.).

À l'aide de cette section, vous pouvez effectuer les opérations suivantes :

1. Associez des observables à un ticket TISC.
2. Affichez les informations sur les observables associés.
3. Affichez les résultats de l'enrichissement des observables.

Pour plus d'informations détaillées et la procédure, reportez-vous aux sections suivantes, et pour plus d'informations sur le fonctionnement de l'intégration entre les espaces de travail TISC et SIR, reportez-vous Intégration de TISC à l'espace de travail SIR à la section Threat Intelligence Security Center.

Ajouter des observables au ticket TISC

Utilisez cette section pour ajouter des incidents de sécurité ou des observables à un ticket TISC.

Avant de commencer

Rôle requis : sn_si.analyst

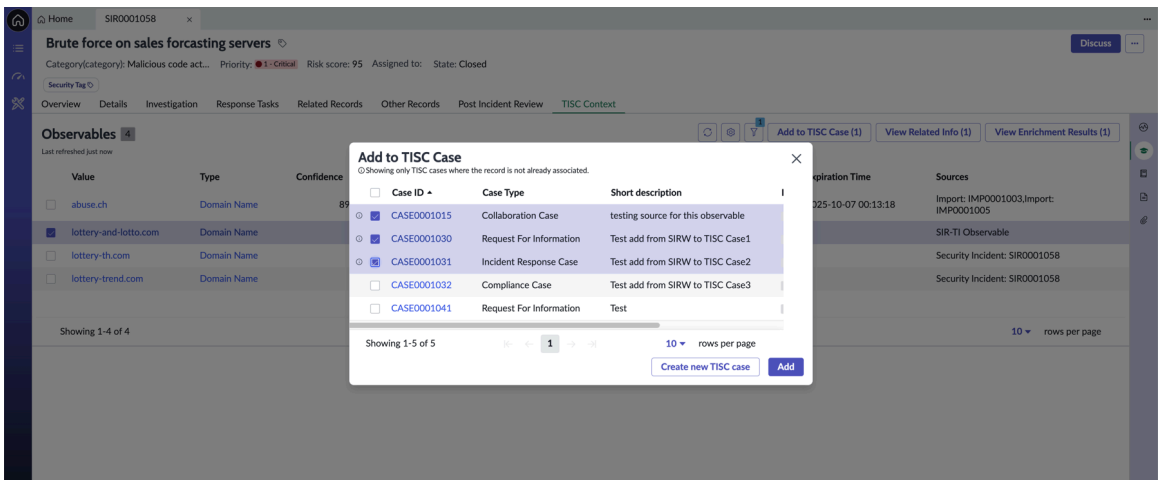
Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tout**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez. Cela peut également être fait en recherchant l'ID d'incident, en filtrant à l'aide de la section Filtres rapides ou en parcourant un état d'incident.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez **l'onglet Contexte TISC** .
4. Cliquez sur **le bouton Ajouter au ticket TISC** .
   La boîte de dialogue Ajouter au ticket TISC s'affiche. Cela permet d'afficher uniquement les tickets TISC pour lesquels l'enregistrement n'est pas déjà associé.
5. Sélectionnez les observables.
6. Sélectionnez un ou plusieurs tickets et cliquez sur **Ajouter** pour ajouter les tickets aux observables et les associer à l'incident de sécurité.



Remarque : Vous pouvez également créer un nouveau ticket en cliquant sur **Créer un nouveau ticket TISC**, au cas où vous n'auriez pas de tickets existants.

Les messages de confirmation suivants s'affichent :

- Les observables suivants sont ajoutés avec succès en tant qu'artefacts.
- Les observables suivants sont envoyés à TISC et ajoutés ultérieurement aux enregistrements de tickets TISC sélectionnés.

Remarque : Le traitement et l'association des activités des observables sont publiés dans le flux d'activité au fur et à mesure que l'association est terminée.

7. Affichez les enregistrements de tickets associés en vous connectant à l'espace de travail du centre de sécurité Renseignements sur les menaces pour connaître les étapes suivantes.
   Pour plus d'informations, reportez-vous à la section Intégration de TISC à l'espace de travail SIR.

Remarque :

Depuis l'espace de travail Réponse aux incidents de sécurité, vous pouvez également associer des observables à des enregistrements de tickets à partir des onglets **Enquête** et **Enregistrements connexes** .

Remarque : Pour associer des observables à partir de **l'enquête**, suivez la procédure ci-dessous et pour les associer à partir des **enregistrements connexes** expliqués ici Ajouter des observables au ticket TISC. Vous pouvez également naviguer vers l'onglet **Examiner** et naviguer vers la section **Listes de points d'entrée** affichée sur le côté gauche de la page et sélectionner **Observables associés** pour ajouter des observables au ticket TISC.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les informations connexes de TISC

Utilisez cette section pour afficher les informations connexes telles que les acteurs de menace connexes, les modèles d'attaque, les campagnes et les tickets de TISC dans l'espace de travail SIR.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tout**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez.
   Cela peut également être fait en recherchant l'ID d'incident, en naviguant dans la section Filtres rapides ou en filtrant l'état de l'incident.
3. Une fois l'incident ouvert, accédez à l'onglet **Contexte TISC** .
   Affichage des informations connexes de la vue :

   Dans les détails de l'incident, vous pouvez afficher les informations connexes dans plusieurs sections.

   a. Sélectionnez un ou plusieurs observables.

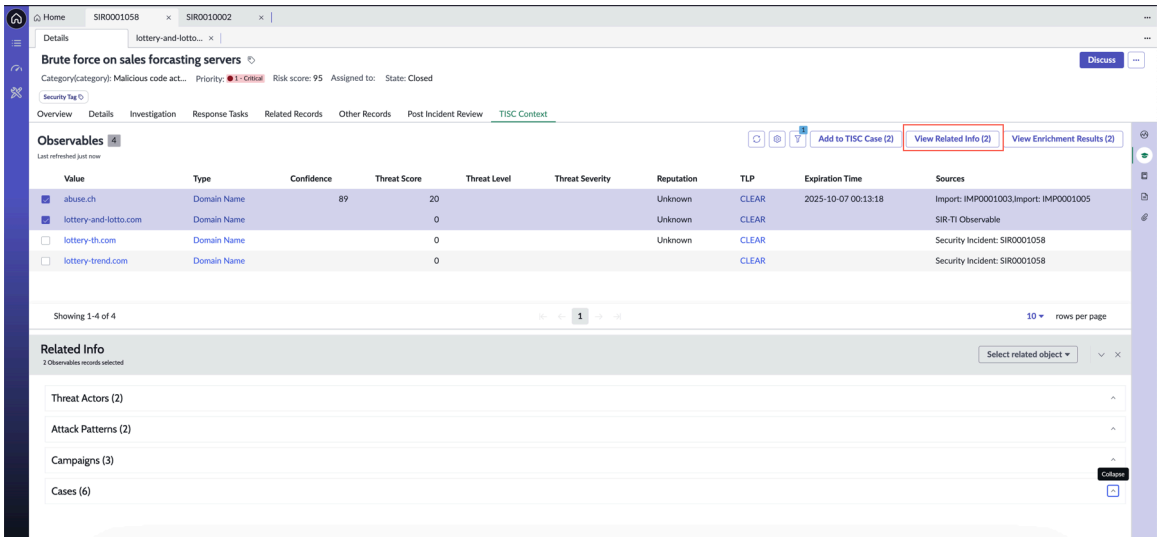
   b. Cliquez sur le bouton **Afficher les informations connexes** .
   Cette section affiche les informations associées aux observables sélectionnés.

Nom	Description
Acteurs de menace	Affiche les informations de TISC pour les acteurs de menace liées aux observables sélectionnés.
Schémas d'attaque	Affiche les informations de TISC pour les schémas d'attaque liés aux observables sélectionnés.
Campagnes	Affiche les informations de TISC pour les campagnes associées aux observables sélectionnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
Tickets	Affiche les informations de TISC pour les tickets TISC associés aux observables sélectionnés.



Afficher les résultats de l'enrichissement

Utilisez cette section pour afficher les résultats de l'enrichissement des observables tels que les résultats de la recherche de menace, les perceptions et les résultats de l'enrichissement des observables à partir de TISC dans l'espace de travail SIR.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tout**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez.
   Cela peut également être fait en recherchant l'ID d'incident, en naviguant dans la section Filtres rapides ou en filtrant l'état de l'incident.
3. Une fois l'incident ouvert, accédez à l'onglet **Contexte TISC** .
   Affichage des résultats de l'enrichissement :

   Dans les détails de l'incident, vous pouvez afficher les informations connexes dans plusieurs sections.

   a. Sélectionnez un ou plusieurs observables.

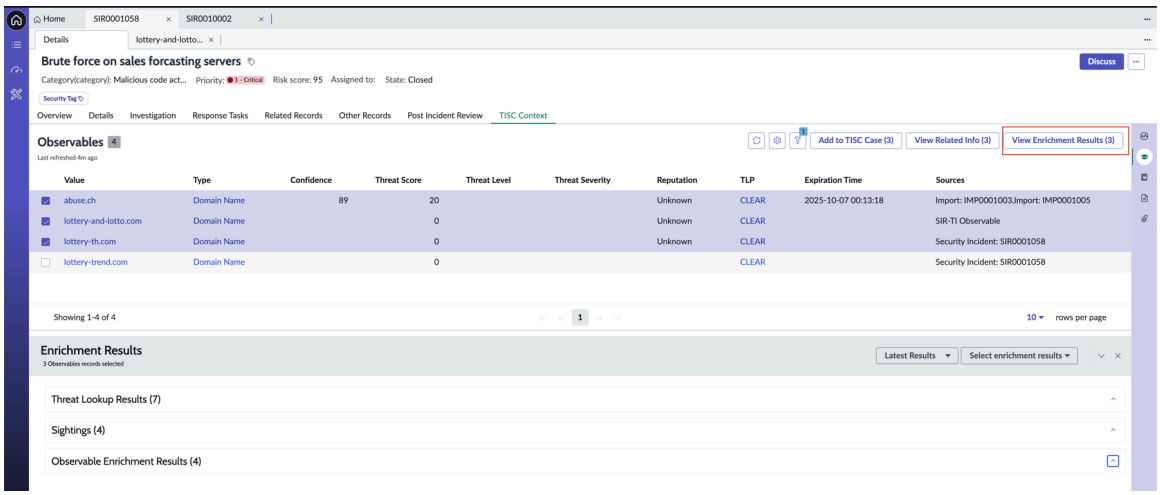
   b. Cliquez sur le bouton **Afficher les résultats de l'enrichissement** .
   Cette section affiche les détails associés aux observables sélectionnés.

Nom	Description
Résultats de la recherche de menace	Répertorie tous les résultats de la recherche de menace associés pour les observables TISC sélectionnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
Perceptions	Répertorie toutes les observations associées aux observables TISC sélectionnés.
Résultats de l'enrichissement de l'observable	Répertorie tous les résultats d'enrichissement observable associés pour les observables TISC sélectionnés.



Lancer une messagerie instantanée Sidebar dans Security Incident Response

À l'aide de Sidebar, les analystes de sécurité peuvent collaborer avec d'autres personnes en temps réel sur la base d'un enregistrement basé sur l'interaction ou une tâche de l'espace de travail. Ces discussions dans la barre latérale facilitent l'échange d'informations et de connaissances pour aider à résoudre les problèmes plus rapidement et avec des résultats de meilleure qualité.

Avant de commencer

Rôle requis : sn_si.read

Vérifiez que vous avez activé le module d'extension Omni-Experience Standard Feature Set. Pour plus d'informations, consultez Installer Barre latérale .

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez .
3. Ouvrez un incident de sécurité pour lequel vous souhaitez lancer une discussion dans la barre latérale.
4. Sélectionnez **Discuter**.
   La boîte de dialogue Démarrer une discussion dans la barre latérale s'affiche.

   Remarque : L'intégration de Sidebar à Microsoft Teams permet aux utilisateurs de Sidebar et de Microsoft Teams de communiquer entre eux à partir de leurs plateformes respectives. Pour plus d'informations, consultez Barre latérale et Microsoft Teams .

5. Renseignez les champs de la boîte de dialogue Démarrer une discussion dans la barre latérale.

Traduction automatique

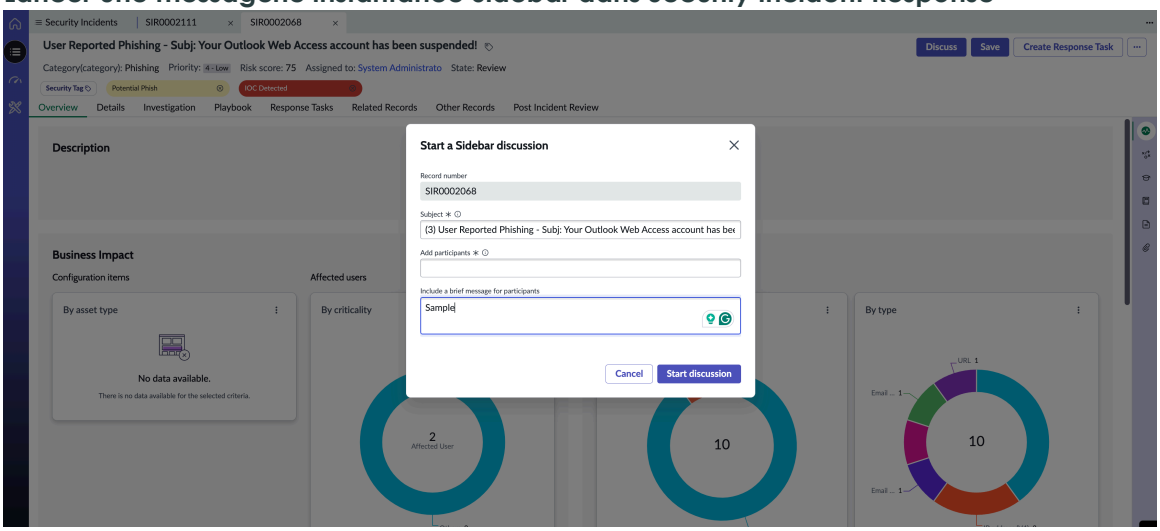
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Numéro d'enregistrement	Numéro de tâche ou d'incident associé à la discussion dans la barre latérale.
Objet	Donnez un titre à la discussion dans la barre latérale.
Ajouter des participants	Option permettant d'ajouter des participants à la discussion dans la barre latérale. Si vous avez intégré la messagerie instantanée Sidebar à Microsoft Teams, vous pouvez également ajouter des participants à partir de Microsoft Teams. **Remarque :** ◦ Vous devez ajouter au moins un participant pour créer une nouvelle discussion. ◦ Si Sidebar et Microsoft Teams sont intégrés, les utilisateurs de Microsoft Teams sont différenciés des utilisateurs de Sidebar avec une icône Microsoft Teams. ◦ Par défaut, tous les utilisateurs qui disposent d'un accès en lecture aux enregistrements SIR ont également accès aux messageries instantanées de barre latérale, mais cela peut être contrôlé à l'aide de la requête de membre. Pour plus d'informations, consultez Configuration de la Barre latérale requête de membre .
Inclure un bref message	Résumez brièvement la question qui sera abordée dans la discussion de la barre latérale.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lancer une messagerie instantanée Sidebar dans Security Incident Response



6. Sélectionnez **Démarrer une discussion**.
7. Vous pouvez effectuer des configurations supplémentaires telles que des actions rapides. Pour limiter l'utilisation de l'action, vous pouvez utiliser le champ **Appliquer au groupe** sur la page d'action rapide. Pour plus d'informations, consultez Création d'une action rapide .

Playbook d'incident de sécurité

Invoquer le flux du playbook d'incident de sécurité automatiquement ou manuellement.

Un Playbook n'est visible que si au moins un Playbook est associé à un incident de sécurité. Le composant Playbook fonctionne uniquement pour les processus créés par Concepteur d'automatisation de processus (PAD) et non pour les flux créés par Flow Designer. Pour les flux existants activés par Flow Designer, cela continuera de fonctionner et les activités continueront d'être restituées en tant que tâches de réponse.

Il existe deux façons d'associer le playbook à l'incident de sécurité :

- Invoquer automatiquement le playbook
- Ajouter manuellement un playbook

Appeler automatiquement le playbook

Pour qu'un Playbook soit invoqué automatiquement, un processus doit être défini à l'aide **de Process Automation Designer (PAD)**, et lorsque la condition de déclenchement est remplie, l'onglet Playbook s'affiche automatiquement avec les activités Playbook affichées.

Ajouter un playbook manuellement

Pour qu'un Playbook soit invoqué manuellement, accédez à la liste déroulante Action d'interface utilisateur du formulaire et sélectionnez **Ajouter un Playbook**. Pour plus d'informations, reportez-vous à la section Ajouter un Playbook

Remarque : S'il existe déjà un playbook disponible, les nouveaux playbooks ajoutés s'exécuteront en parallèle des playbooks existants.

- Dans le playbook, l'analyste peut filtrer les cartes du playbook par état.
- L'analyste peut annuler un playbook en le sélectionnant à partir de l'icône d'ellipse.

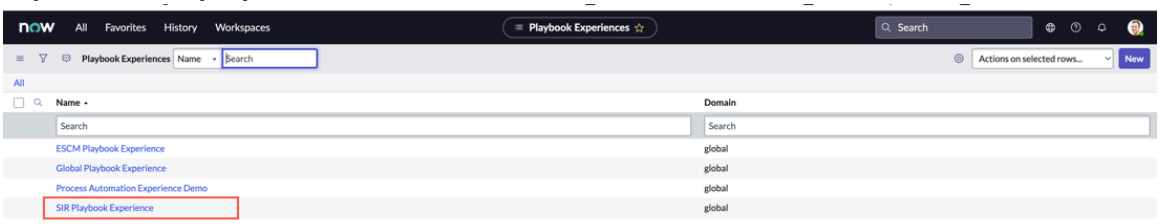
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Dans chaque activité, l'analyste pourra effectuer les actions définies dans les cartes d'activité, telles que Ignorer, Marquer comme terminé, Annuler, ou des actions d'orchestration telles que Soumettre au bac à sable, Rechercher des e-mails, etc.
- Chacune de ces actions est définie dans la définition d'activité, et la carte complète visible est personnalisable au moment de la création de la définition d'activité elle-même.

Remarque : Toutes les définitions d'activités futures et les prochaines étapes à effectuer sont affichées avec une icône de verrouillage et sont en mode lecture seule pour l'utilisateur. Le mode d'affichage du playbook est contrôlé par une configuration comme expliqué ci-dessous.

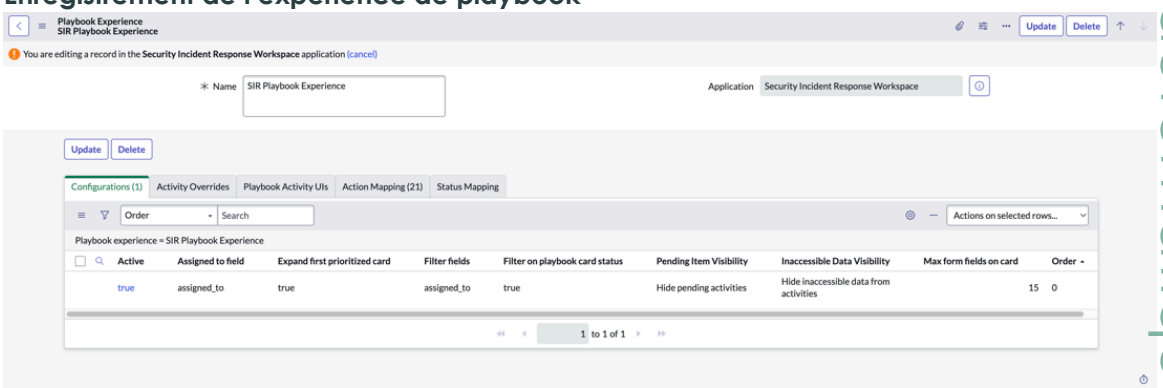
1. Accédez à la **Tout** > **Expériences Playbook**.
2. Sur la page Expériences de playbook, sélectionnez une **expérience de playbook SIR**.

Expérience de playbook

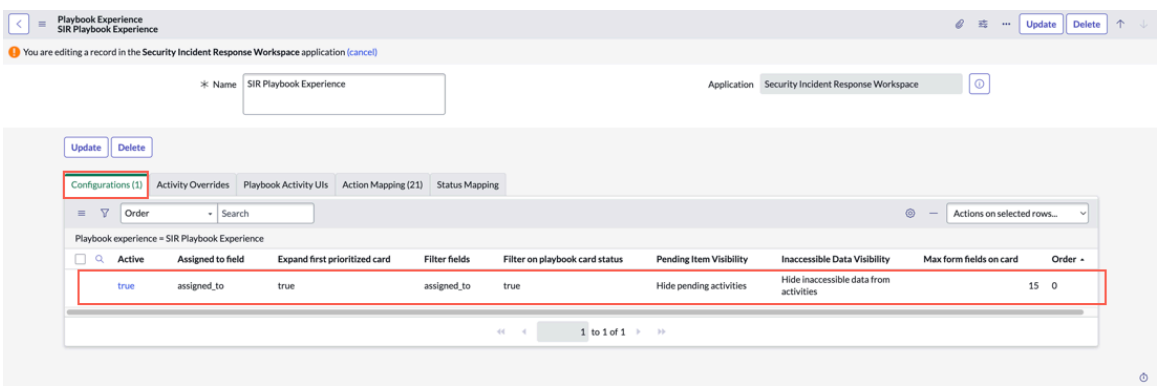


La page **Expérience de playbook SIR Expérience de playbook** s'affiche.

Enregistrement de l'expérience de playbook



3. Cliquez sur l'enregistrement **de configuration** .

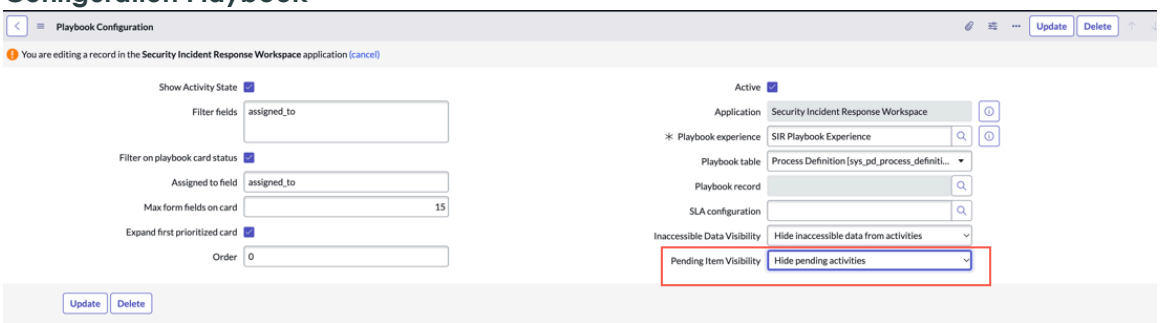


4. Dans l'onglet Configuration, cliquez sur Configuration de l'expérience de playbook SIR.

Traduction automatique

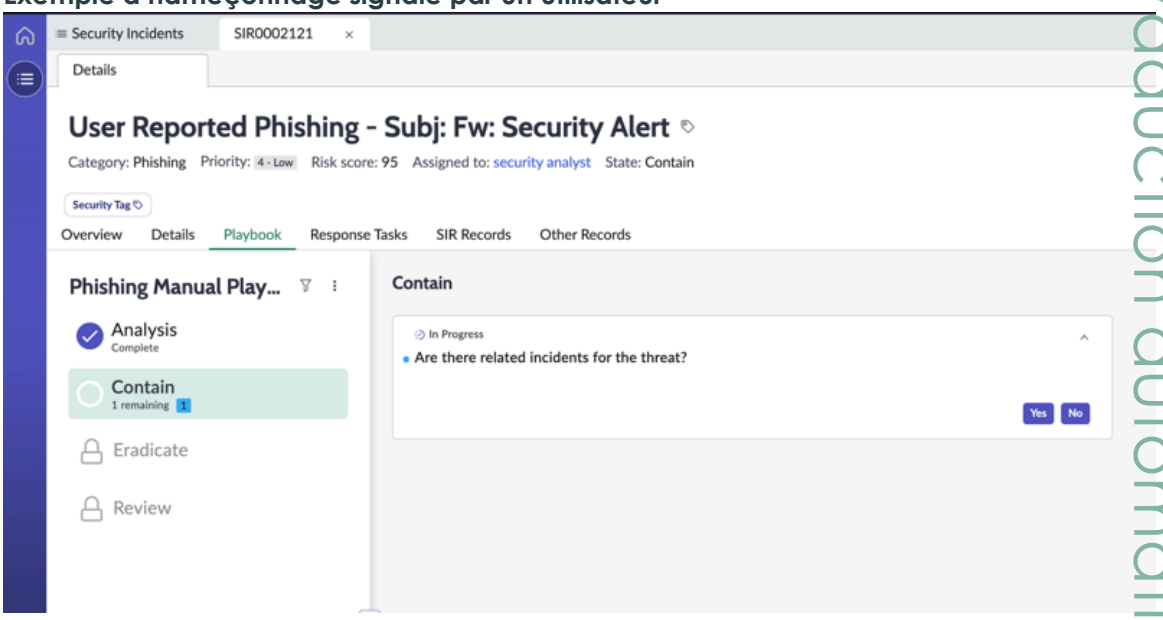
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration Playbook



5. Accédez à la liste déroulante du champ **Visibilité de l'élément en attente** , sélectionnez l'option souhaitée et enregistrez l'enregistrement. Choisissez parmi les options suivantes :
   - **Masquer les activités en attente** : sélectionnez cette option pour masquer les activités en attente que vous souhaitez afficher dans la section playbook de l'espace de travail.

Exemple d'hameçonnage signalé par un utilisateur

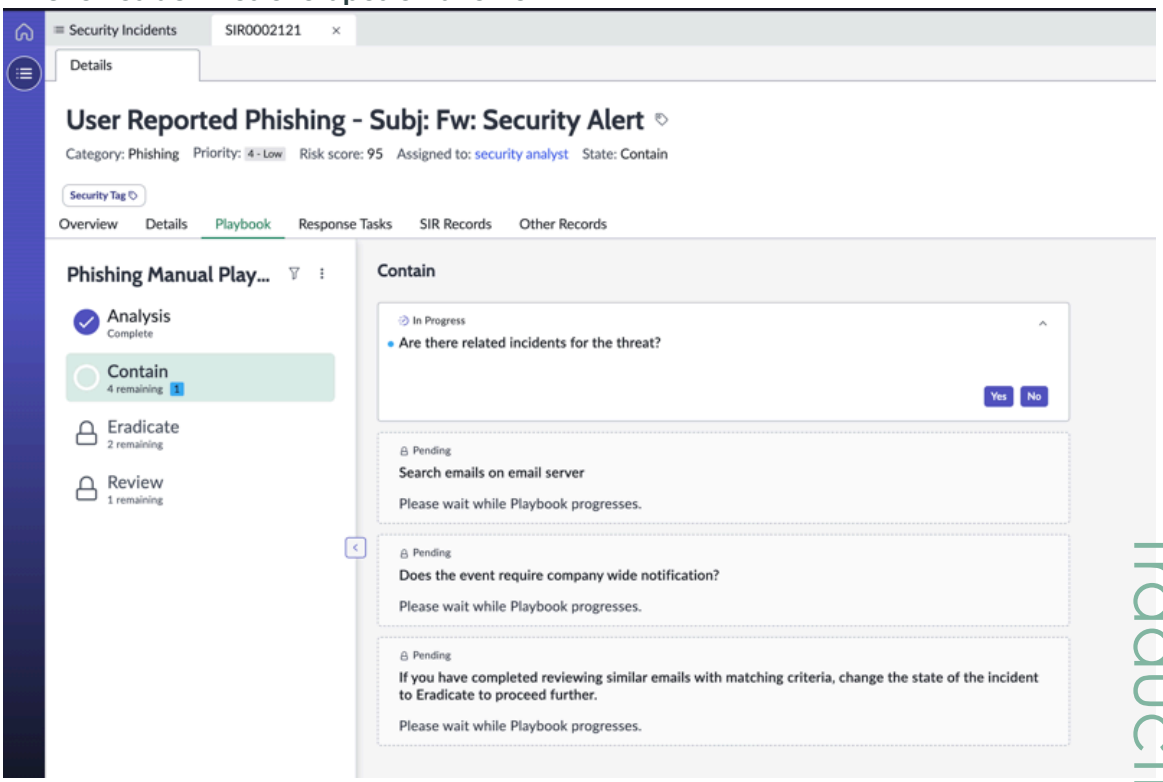


   - **Afficher les étapes et les activités en attente** : sélectionnez cette option pour afficher les étapes et les activités en attente que vous souhaitez afficher dans la section playbook de l'espace de travail.

Traduction automatique

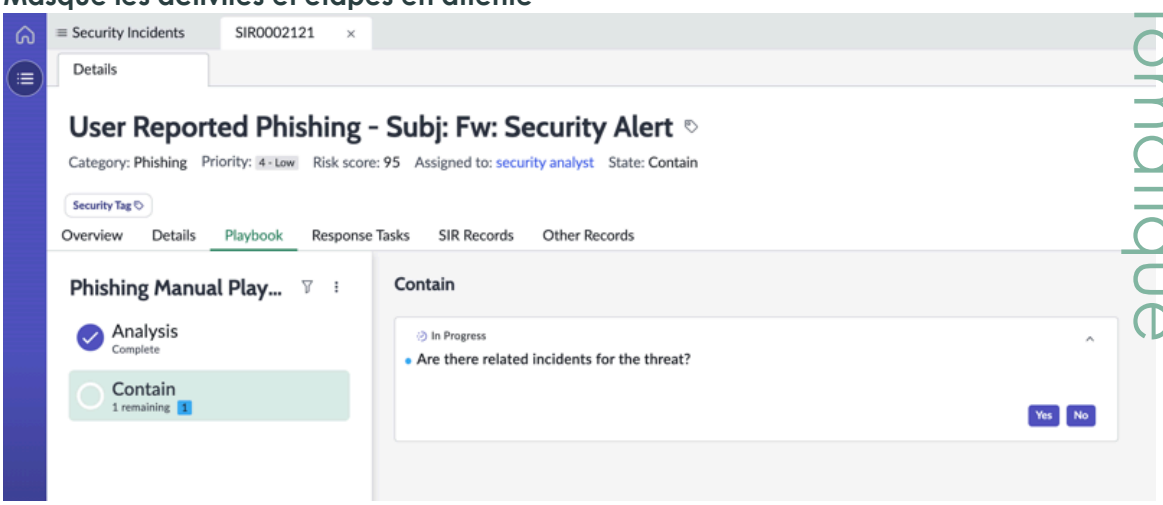
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les activités et étapes en attente



- **Masquer les activités et étapes en attente** : sélectionnez cette option pour masquer les activités et les étapes en attente que vous souhaitez afficher dans la section Playbook de l'espace de travail.

Masque les activités et étapes en attente

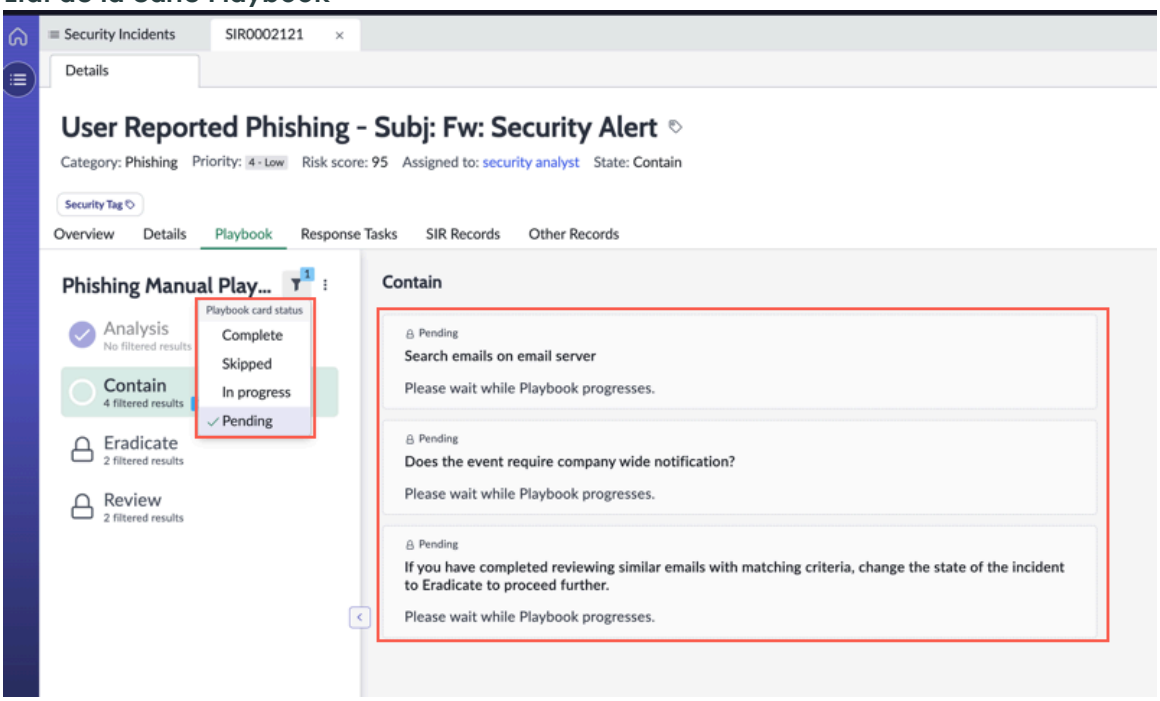


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans la section Playbook, utilisez l'option de filtre pour filtrer les activités par état de carte Playbook (définition d'activité).

État de la carte Playbook



Ajouter un Playbook

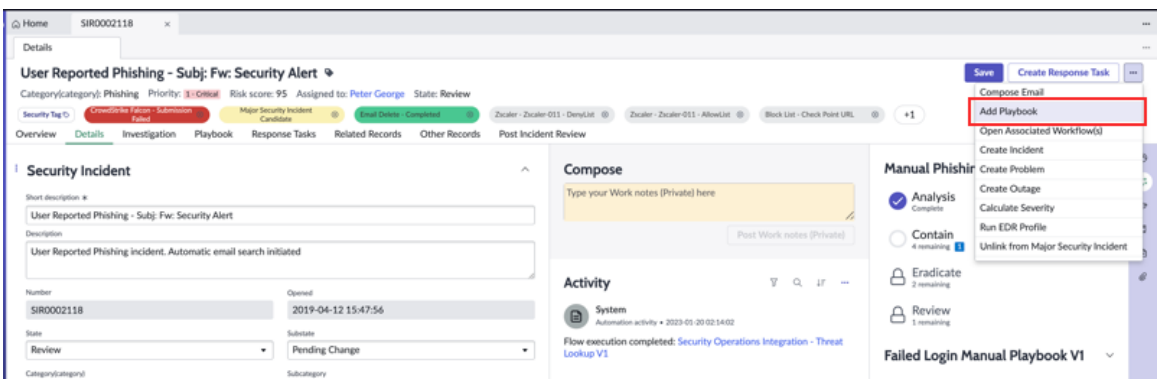
Utilisez cette section pour ajouter un playbook manuellement.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

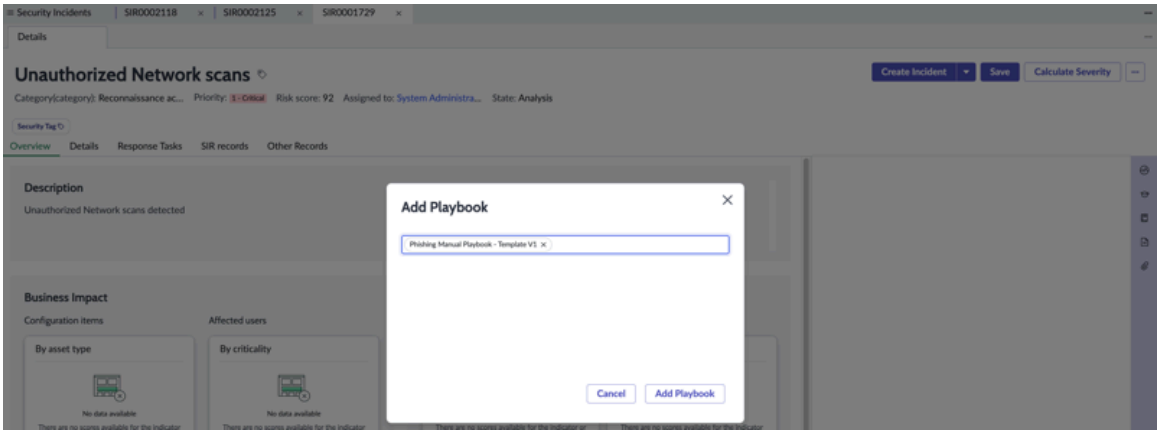
1. Accédez à la **Tout** > **Incident de sécurité** > **Security Analyst Workspace**.
2. Ouvrez un enregistrement d'incident.
3. Cliquez sur **Ajouter un playbook**.



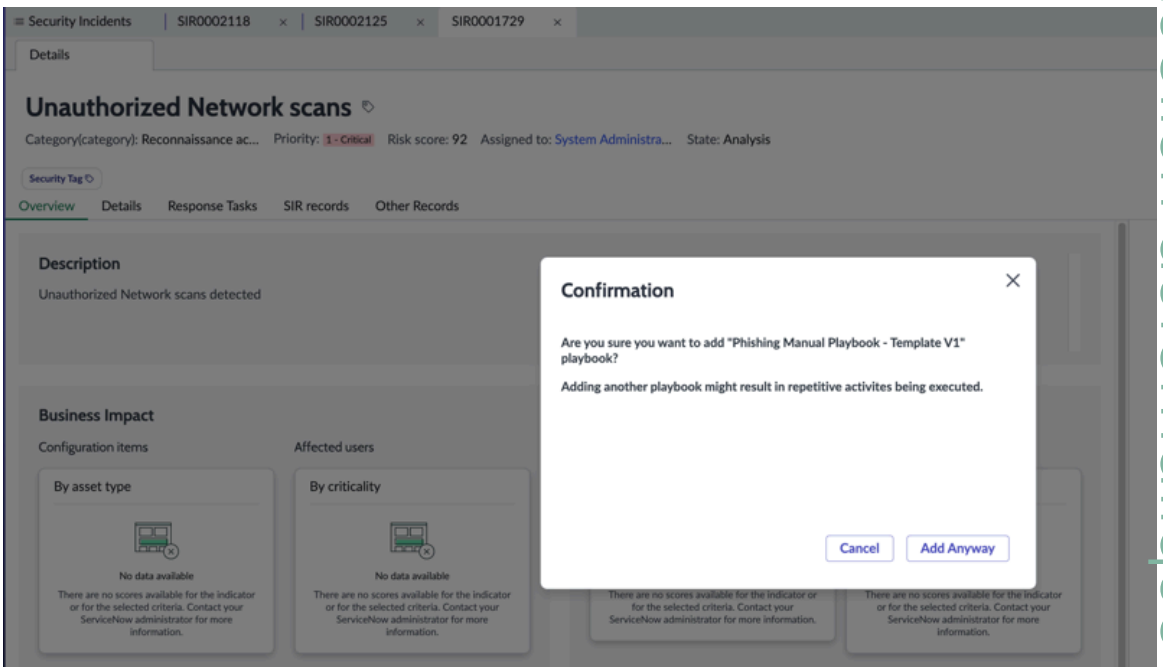
La boîte **de dialogue Ajouter un playbook** s'affiche.

Traduction automatique

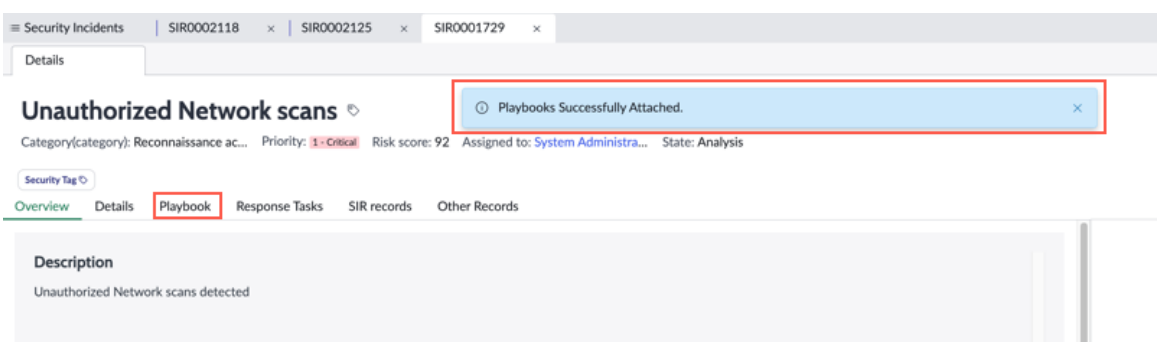
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez le modèle de playbook.
5. Cliquez sur **Ajouter un playbook**.
   Une boîte de dialogue de message de confirmation s'affiche pour vous permettre de confirmer.
6. Cliquez **quand même sur Ajouter**.



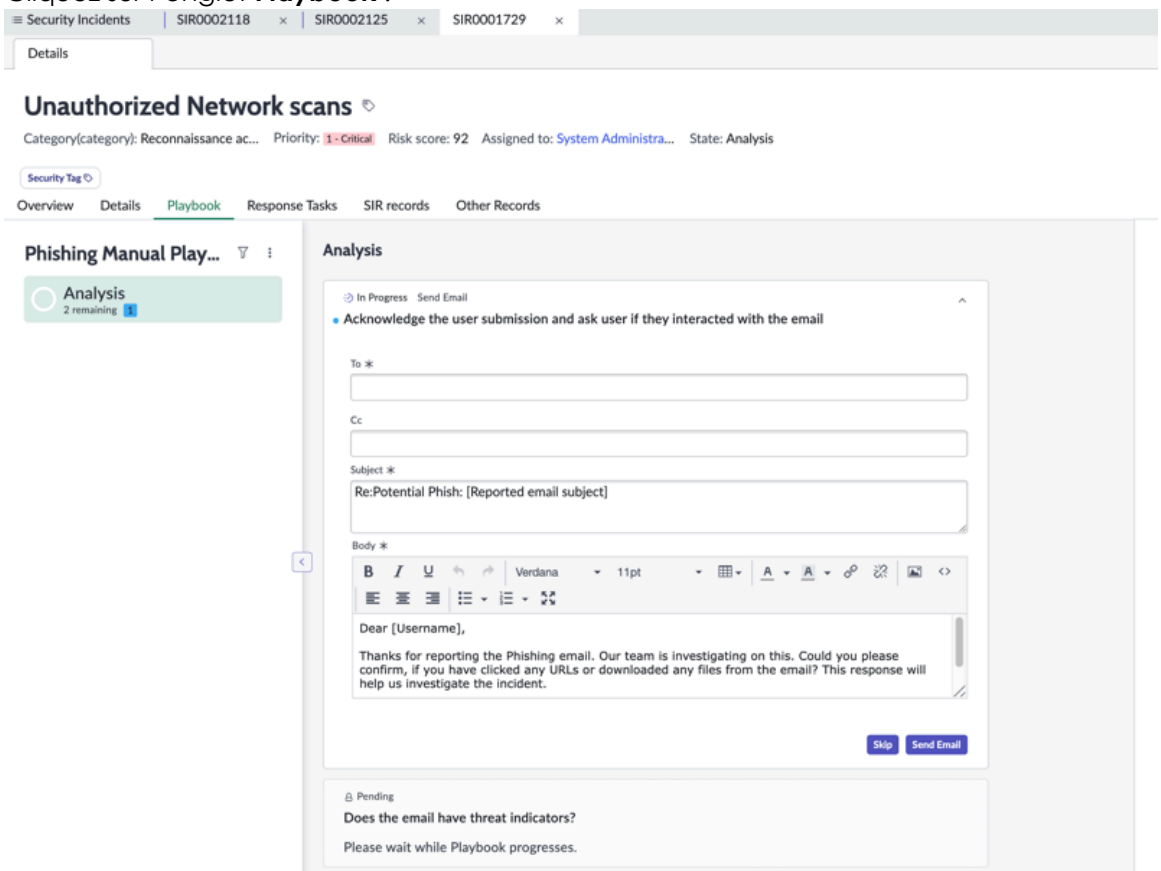
7. Le **Playbook** est ajouté à côté de l'onglet **Détails** .



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Cliquez sur l'onglet **Playbook** .



9. Effectuez la série d'activités répertoriées pour passer au niveau suivant.

> **Remarque :** Si un incident de sécurité est associé à un playbook, l'utilisateur ne peut pas associer le même playbook au même incident de sécurité tant que celui-ci n'est pas fermé ou annulé.

Conditions préalables pour les Playbooks

Vous avez besoin des rôles et modules d'extension suivants pour créer les Playbooks.

Rôle requis : admin.

- Activez le module d'extension Process Automation Designer (PAD) [com.glide.pad.license].
- Activez les modules d'extension suivants pour une expérience de playbook :
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- Activez le spoke Security Operations pour accéder aux flux [com.snc.secops.spoke].
- PAD Commons de gestion des tickets de sécurité d'entreprise.

Assurez-vous d'avoir lu la documentation de la plateforme sur Expérience de playbook et Concepteur d'automatisation de processus avant de commencer ce guide.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Reconstruire des playbooks existants dans Studio de workflow

Vous ne pouvez pas convertir les flux existants directement en playbooks dans Studio de workflow. Chaque étape de Flow Designer qui crée une tâche de réponse pour guider l'analyste doit être décomposée en actions ou flux secondaires distincts.

Vous n'êtes pas autorisé à convertir des flux existants directement en playbooks dans Studio de workflow. Chaque étape de Flow Designer qui crée une tâche de réponse pour guider l'analyste doit être décomposée en actions ou flux secondaires distincts. À l'aide de ces flux secondaires ou actions granulaires, vous devez créer des définitions d'activité. Une fois ces définitions d'activité créées, elles sont ajoutées en tant qu'activités au sein de l'étape de la définition de processus. Vous pouvez réutiliser les définitions d'activité dans plusieurs playbooks.

Vous pouvez personnaliser chaque activité pour afficher les actions requises et l'apparence que doit avoir la carte lors de la création de la définition d'activité. L'activité peut afficher des clients de messagerie, des tables, des actions, des articles de la base de connaissances, des URL, etc. Vous pouvez définir comment la définition d'activité et l'action ou les flux secondaires sous-jacents sont créés.

Pour plus d'informations, reportez-vous aux sections suivantes.

- Définitions d'activité
- Process Automation Designer

Définitions d'activités

Le Now Platform fournit quelques définitions d'activité dans le système de base. En outre, pour les playbooks que le système de base de l'espace de travail SIR, quelques définitions d'activité sont définies dans le système de base sous l'application Enterprise Security Case Management PAD Commons.

Rôle requis : sn_si.admin.

Voici la liste des définitions d'activité qui font partie du système de base :

Définition d'activité	Table	Description	Application
Attendre une condition sans expérience	Global[global]	Attendre une condition sans expérience	Gestion des tickets de sécurité d'entreprise PAD Commons
Soumettre au bac à sable CSF X	Incident de sécurité [sn_si_incident]	Soumettre au bac à sable (sandbox)	Gestion des tickets de sécurité d'entreprise PAD Commons
Envoyer un e-mail	Incident de sécurité [sn_si_incident]	Activité d'envoi d'e-mail pour les playbooks SIR.	Gestion des tickets de sécurité d'entreprise PAD Commons
Rechercher un e-mail	Incident de sécurité [sn_si_incident]	Rechercher des e-mails sur un serveur de messagerie	Gestion des tickets de sécurité d'entreprise PAD Commons
Mettre à jour l'état de la tâche	Incident de sécurité [sn_si_incident]	Mettre à jour l'état de la tâche	Gestion des tickets de sécurité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définition d'activité	Table	Description	Application
			d'entreprise PAD Commons
Supprimer l'e-mail	Incident de sécurité [sn_si_incident]	Supprimer les e-mails	Gestion des tickets de sécurité d'entreprise PAD Commons
Résultat avec oui/ non	Tâche [task]	Résultat attendu	Gestion des tickets de sécurité d'entreprise PAD Commons

Exemple de définition d'activité : envoyer un e-mail

Voici un exemple de définition d'activité Envoyer un e-mail.

Élémentaire

Les détails de base capturent le nom (étiquette), l'application, la description, la table et toutes les applications à partir desquelles elle est accessible.

Ajoutez le plan d'automatisation, l'expérience d'activité et soumettez. Après l'envoi, modifiez le document pour ajouter plus de détails à chaque onglet.

Plan d'automatisation

Le plan d'automatisation associe l'action back-end ou les flux secondaires créés à l'aide du Flow Designer. Cet exemple utilise : **Envoyer un e-mail - Flux secondaire d'activité ESCM** .

Ce flux secondaire permet l'envoi d'un e-mail. Il a la logique de base pour envoyer un e-mail. Tous les champs d'entrée et de sortie sont définis.

Tous les champs d'entrée sont affichés dans la section du plan d'automatisation. Chaque champ d'entrée peut être activé pour être visible uniquement par l'administrateur, dans le modal standard, dans le modal standard et le panneau de configuration :

- **Visibilité de l'administrateur uniquement** : lorsqu'elle est définie sur administrateur, seul l'administrateur peut l'afficher.
- **Inclure dans le modèle standard** : lorsqu'il est défini sur Afficher dans le modal standard, il n'apparaît que dans le modal des propriétés.
- **Inclure dans le modèle standard et le panneau de configuration** : lorsqu'il est défini sur Afficher dans le modal standard et le panneau de configuration, il apparaît dans le panneau de configuration PAD ainsi que dans le modal des propriétés. Pour plus d'informations, consultez Définitions d'activité

Vous pouvez définir les champs d'entrée au moment de la définition de l'activité elle-même, à condition que vous n'ayez pas besoin de modifier ces valeurs au moment de la configuration. Cela permet au propriétaire du processus business de gagner du temps lors de la configuration d'une activité au sein d'un processus.

Expérience de l'activité

L'onglet Expérience d'activité définit le mode de rendu de la carte d'activité lors de l'exécution. Le système de base fournit les types d'expérience suivants :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Approbation
- Élément de catalogue
- Créer un enregistrement
- Instructif
- Base de connaissances
- Liste
- Notification
- Enregistrement

Selon le type d'expérience que vous sélectionnez, les champs suivants sont renseignés. Pour plus d'informations, consultez la documentation Now Platform.

Dans cet exemple, **le type d'enregistrement** est sélectionné.

Remarque : Par exemple, si vous souhaitez afficher une table, vous pouvez choisir liste comme type d'expérience.

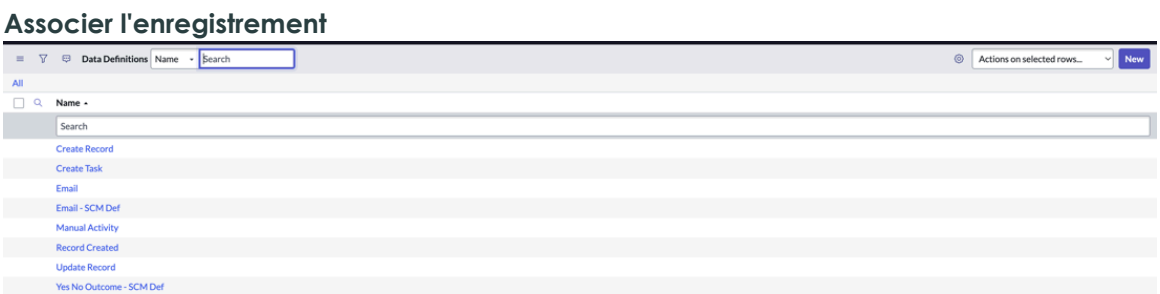
Enregistrement associé

Utilisez cet enregistrement pour stocker les données associées relatives à l'activité en cours. Cela capturerait les données de temps d'exécution, ainsi que l'état de l'expérience.

- Table associée : données de flux
- Enregistrement associé : VL
- Table de l'état de l'expérience : données de flux
- Enregistrement de l'état de l'expérience : VL

Dans cet exemple, la table de données de flux est utilisée pour capturer les données de temps d'exécution. Les données d'exécution peuvent varier en fonction du cas d'utilisation. Dans cet exemple, les données d'exécution sont des champs tels que À, cc, Objet et corps. Pour chaque cas d'utilisation, une définition de données de flux doit être créée afin de définir le type de données d'exécution.

1. Naviguez vers le volet gauche et saisissez **sys_flow_data_definition.list**. Il affiche la liste des définitions créées pour la table de données de flux.

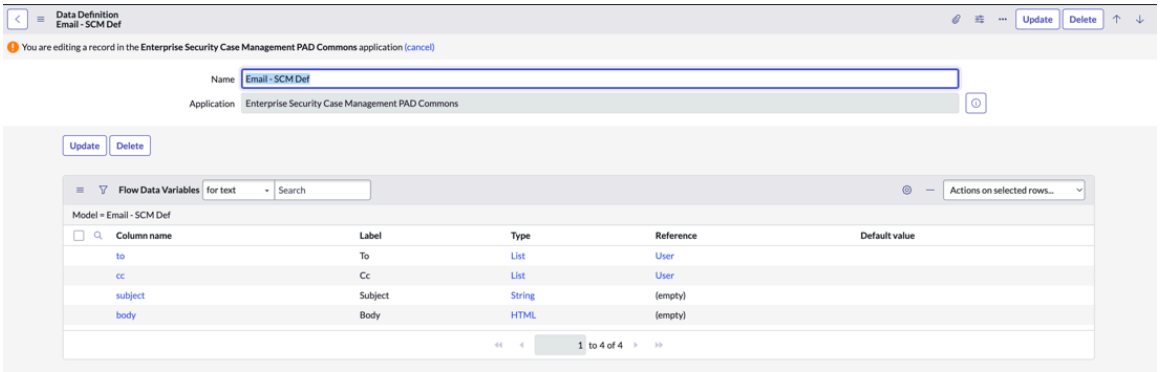


2. **Ouvrez E-mail - Définition du SCM** pour afficher la définition associée à cet exemple.

Traduction automatique

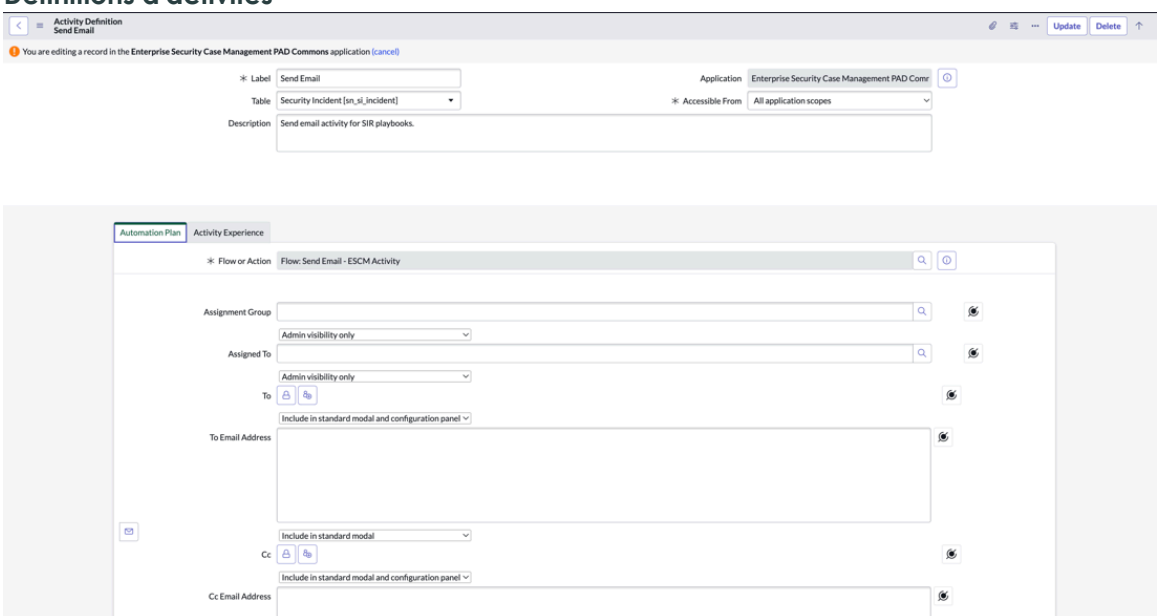
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

E-mail : définition SCM



Cette définition de données de flux doit être utilisée par le flux secondaire ou l'action associée à cette définition d'activité (Consulter le plan d'automatisation) pour capturer les données de temps d'exécution.

Définitions d'activités



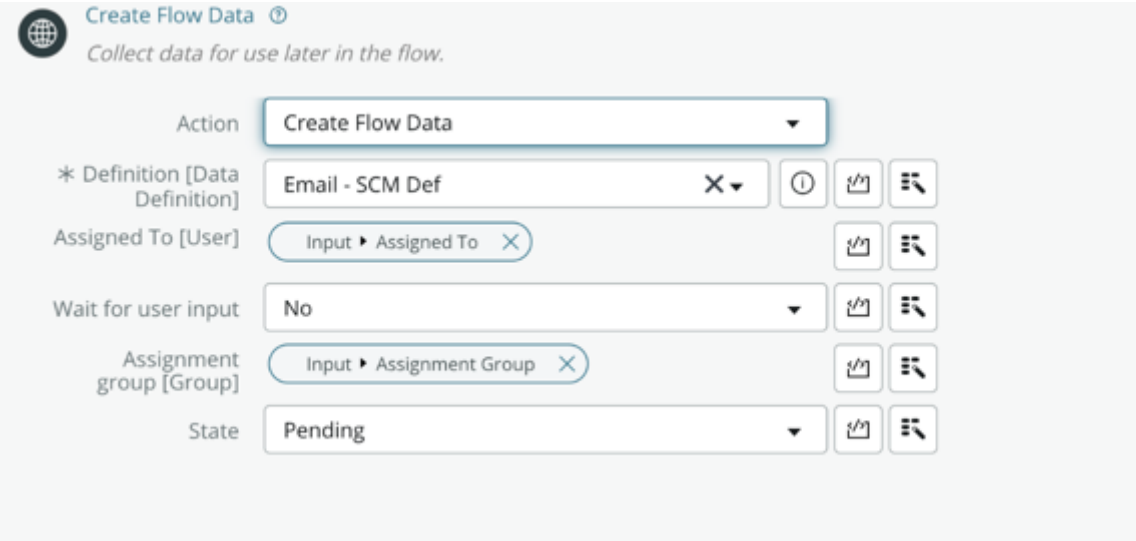
3. Dans cet exemple, ouvrez le flux secondaire : **Envoyer un e-mail - Activité ESCM**. À l'étape **Créer des données de flux** , la définition des données de flux que vous avez créée est mappée par rapport au champ **Définition** . Cet enregistrement de données de flux est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

utilisé dans le flux secondaire. Dans cet exemple, l'état de la carte d'activité (état de l'expérience) est capturé dans la table de données de flux.

Envoyer un e-mail : activité ESCM



Remarque : Si vous souhaitez capturer les données d'exécution dans un enregistrement de table autre que la table de données de flux, par exemple dans une tâche de réponse. Vous pouvez sélectionner la table associée en tant que table de tâche de réponse. L'enregistrement associé doit être défini sur l'enregistrement de tâche de réponse créé par le flux secondaire.

De même, la table de l'état de l'expérience capture l'état de la carte d'activité. Dans le système de base, le champ d'état de la table de données de flux est mappé à l'état de la carte d'activité. Ainsi, lorsque la table de données de flux est utilisée pour capturer l'état de l'expérience, elle met automatiquement à jour l'état de la carte d'activité. Vous pouvez également utiliser une autre table que la table de données de flux pour capturer l'état de l'expérience.

Par exemple, si vous souhaitez mapper l'état de la tâche de réponse à l'état de la carte d'activité, c'est possible. Pour ce faire, procédez comme suit :

1. Accédez à la **Tout** > **Expériences Playbook**.

Expériences Playbook

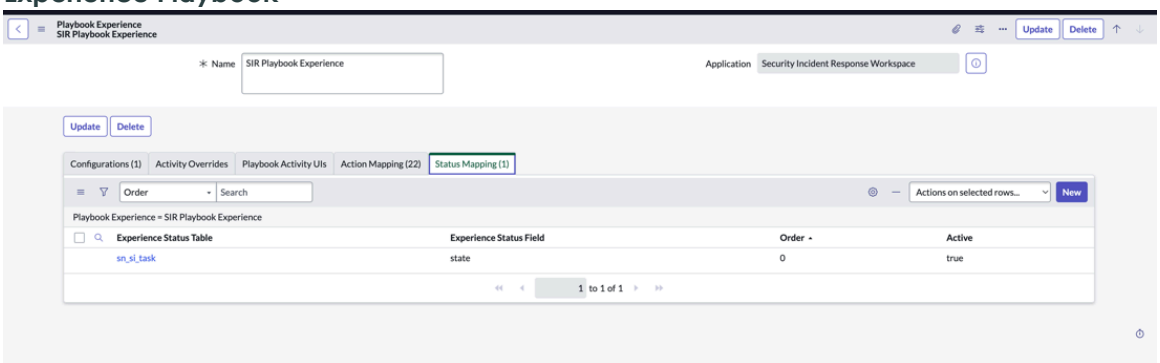


2. Ouvrez **l'expérience Playbook SIR**.
3. Ouvrez la liste connexe **Mappage de statut** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Expérience Playbook



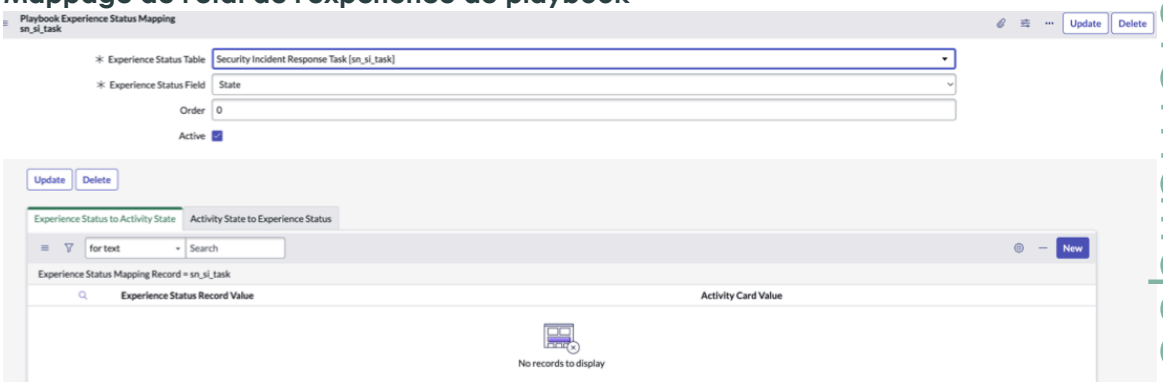
4. Saisissez le champ **Tâche de réponse** par rapport à la table de l'état de l'expérience.
5. Saisissez le champ **État** par rapport à l'état de l'expérience.

État de l'expérience



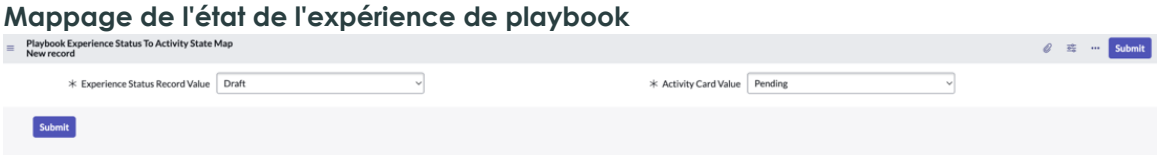
6. Cliquez sur **Envoyer**. L'enregistrement est créé.

Mappage de l'état de l'expérience de playbook



7. Sous État de l'expérience à l'état d'activité, mappez les états de la tâche de réponse à l'état de la carte d'activité.
8. Le côté gauche affiche les états de la tâche de réponse et le côté droit affiche l'état de la carte d'activité.

Mappage de l'état de l'expérience de playbook



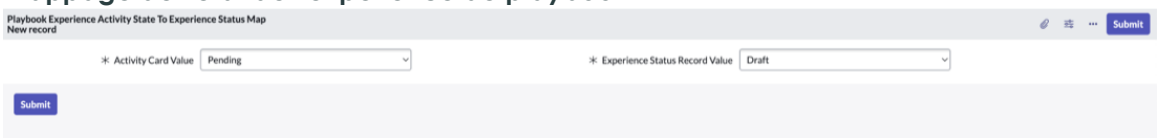
9. Le mappage peut être bidirectionnel. Dans la liste connexe État d'activité sur expérience également, mappez correctement les états. Cette étape est l'inverse de l'étape

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

précédente. Dans ce cas, le côté gauche affiche l'état de la carte d'activité et le côté droit affiche l'état de la tâche de réponse.

Mappage de l'état de l'expérience de playbook



Détails

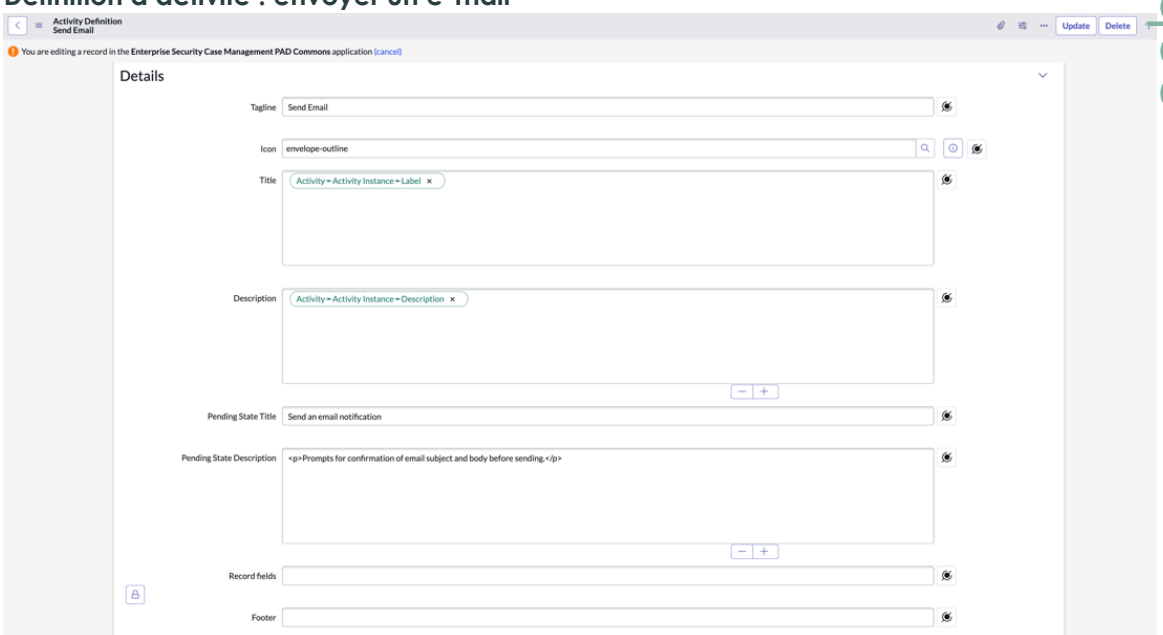
- Ligne de balise : Envoyer un e-mail
- Icône : contour de l'enveloppe (non affiché dans l'interface utilisateur)
- Titre: **Activité** > **Instance d'activité** > **Étiquette**. Ici, nous avons sélectionné l'étiquette de l'instance d'activité. Cette remontée pas à pas remplacera dynamiquement la valeur d'étiquette en tant que titre lors de l'exécution.
- Description : **Activité** > **Instance d'activité** > **Description**. Ici, nous avons sélectionné la description de l'instance d'activité. Cette remontée pas à pas remplacera dynamiquement la valeur d'étiquette en tant que titre lors de l'exécution.
- Titre de l'état en attente : envoyer une notification par e-mail. Il s'agit du titre lorsque l'activité est dans l'état En attente.
- Description de l'état en attente : invite à confirmer l'objet et le corps de l'e-mail avant l'envoi. Il s'agit de la description de la carte d'activité lorsque l'état est En attente Champs d'enregistrement : des champs d'enregistrement sont sélectionnés dans cet exemple.

  Les champs d'enregistrement sont des listes de noms de champs séparés par des virgules à afficher pour l'enregistrement associé dans une liste de paires nom-valeur. Les données sont pré-extraites sur le serveur, la remontée pas à pas est prise en charge et les permissions **canRead()** sont évaluées sur chaque champ.

- Pied de page : aucun pied de page n'est défini pour cet exemple.

  Le pied de page est un texte dans une zone grise du pied de page de la carte. Vous pouvez ajouter n'importe quelle information significative à afficher.

Définition d'activité : envoyer un e-mail



Traduction automatique

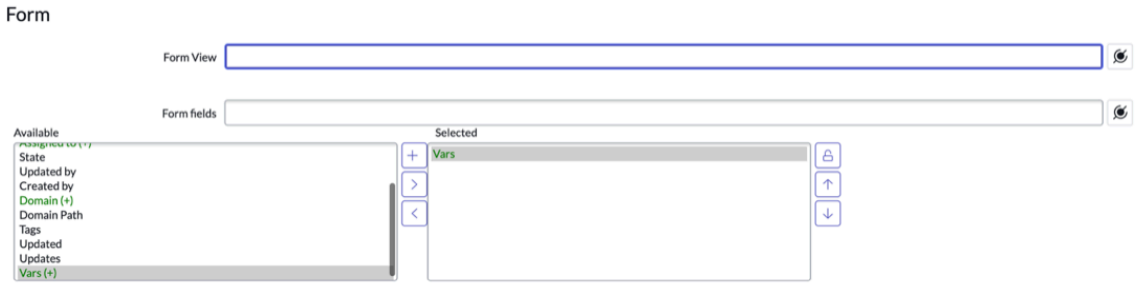
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire

- Vue du formulaire : collect_data
- Champs de formulaire :

Cet exemple utilise collect_data vue pour afficher les champs qui doivent être présentés à l'utilisateur pour entrer des entrées. Collect_data vue est une vue fournie par la plateforme correspondant à la table de données de flux. Vous pouvez également laisser la vue de formulaire vide et sélectionner des variables dans la liste des valeurs disponibles par rapport aux champs de formulaire. (cliquez sur l'icône de verrou pour ouvrir la liste des valeurs disponibles). (cliquez sur l'icône de verrou pour ouvrir la liste des valeurs disponibles).

Vue du formulaire



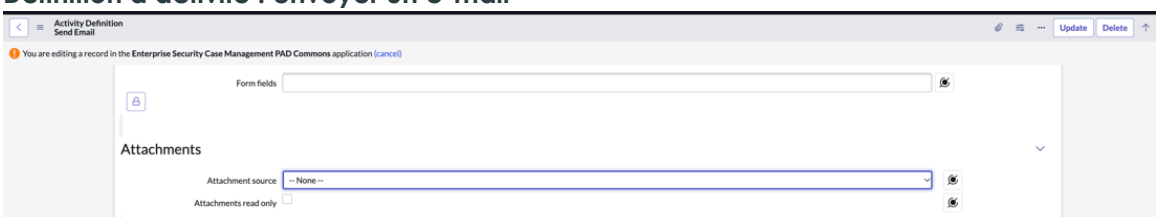
Pièces jointes

Dans cet exemple :

- La source de la pièce jointe est vide.
- Pièce jointe en lecture seule non sélectionnée.

1. Source de la pièce jointe : déroulante. Les pièces jointes à afficher sur la carte : celles jointes à l'enregistrement parent, à l'enregistrement associé ou aucune.
2. Pièce jointe en lecture seule : vrai ou faux. Empêchez l'utilisateur de renommer ou de supprimer les pièces jointes existantes.

Définition d'activité : envoyer un e-mail



Fonctionnalités

Dans cet exemple,

- Afficher le SLA : effacé
- Afficher la liste de vérification : effacée
- Est automatisé : effacé

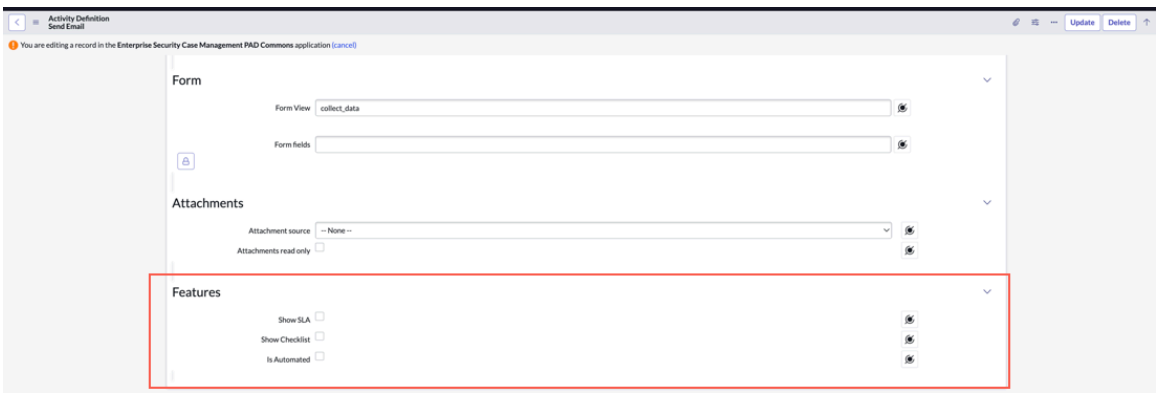
Afficher le SLA : Vrai/Faux. Affiche un minuteur SLA dans l'en-tête de la carte pour l'enregistrement associé. Le SLA est choisi en fonction de l'enregistrement de configuration SLA spécifié dans la configuration Playbook.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Afficher la liste de vérification : Vrai ou Faux. Affiche toute liste de vérification jointe à l'enregistrement associé. La liste de vérification est modifiable et les changements sont enregistrés sans nécessiter d'action déclarative.
2. Est automatisé : vrai ou faux. Si vrai, la **ligne de base** et **l'icône** seront remplacées par le texte **Tâche automatisée** et une icône automatisée.

Définition d'activité : formulaire d'envoi d'e-mail

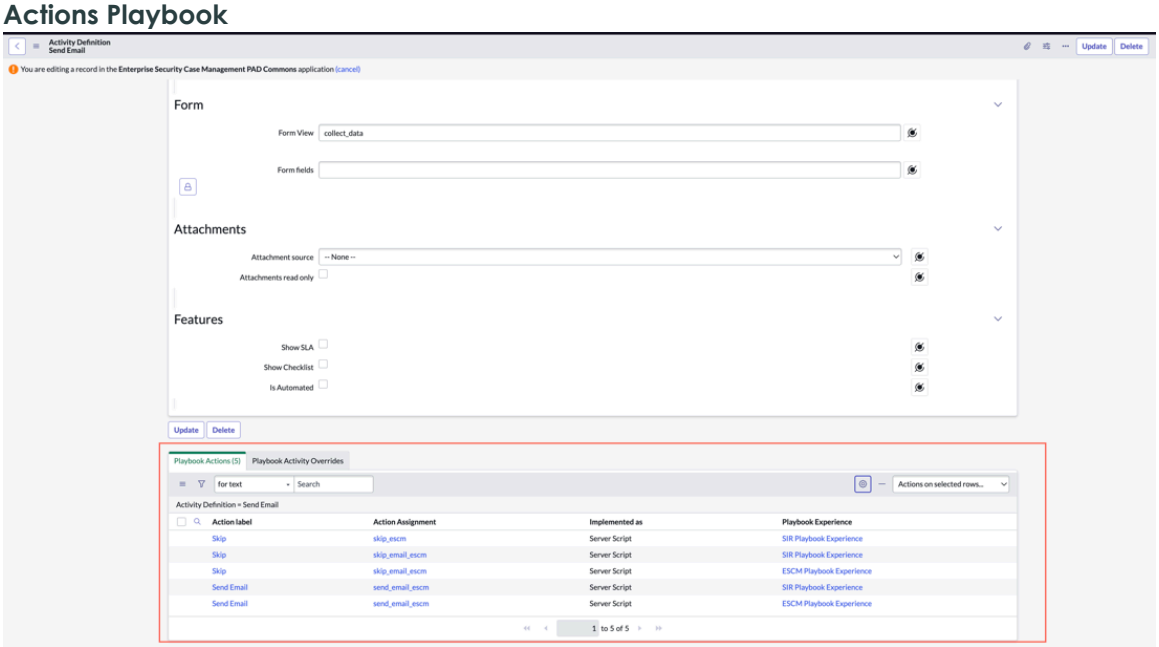


Actions Playbook dans la définition d'activité

Cette section contient les actions qui seront affichées sur la carte d'activité. Dans cet exemple, les actions Ignorer et **Envoyer un e-mail** sont **Ignorer**.

Pour ajouter une nouvelle action à la carte d'activité, vous devez créer un enregistrement dans la liste connexe **Actions Playbook** présente en bas de la page.

Actions Playbook



1. Cliquez sur **Nouveau**.
2. Sélectionnez l'action d'activité existante par rapport au champ Affectation d'action.
3. Sélectionner **Expérience de playbook SIR** en regard du champ Expérience de playbook.

Créer une action d'activité

Voici la procédure pour créer une action d'activité.

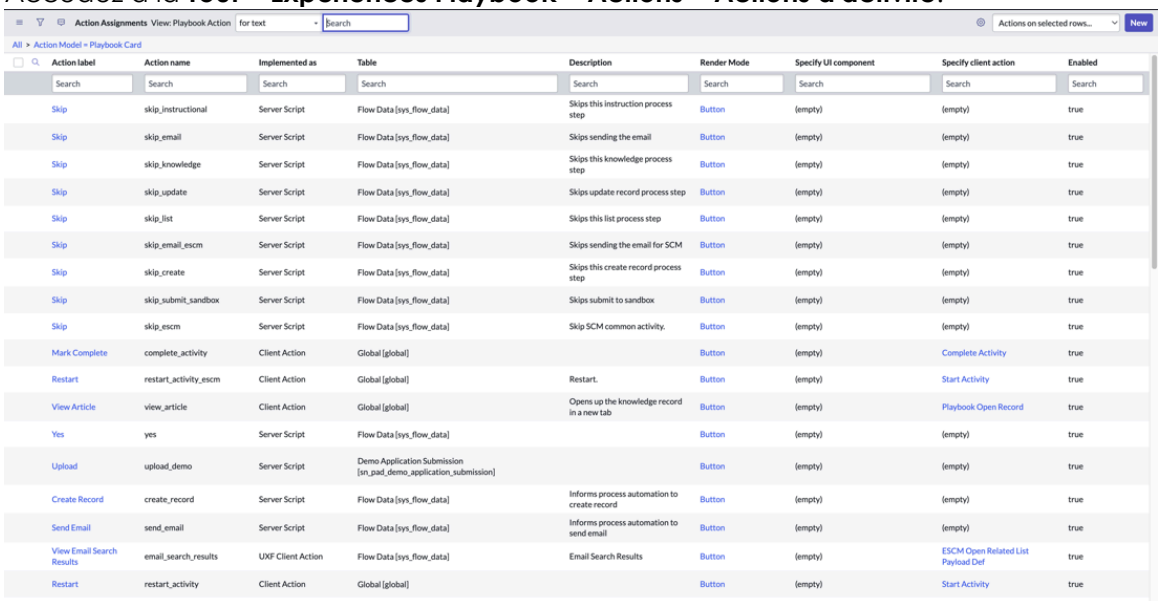
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Expériences Playbook** > **Actions** > **Actions d'activité**.



Action Assignments View: Playbook Action | for text | Search | Actions on selected rows... | New

All > Action Model = Playbook Card

Action label	Action name	Implemented as	Table	Description	Render Mode	Specify UI component	Specify client action	Enabled
Search	Search	Search	Search	Search	Search	Search	Search	Search
Skip	skip_instructional	Server Script	Flow Data [sys_flow_data]	Skips this instruction process step	Button	(empty)	(empty)	true
Skip	skip_email	Server Script	Flow Data [sys_flow_data]	Skips sending the email	Button	(empty)	(empty)	true
Skip	skip_knowledge	Server Script	Flow Data [sys_flow_data]	Skips this knowledge process step	Button	(empty)	(empty)	true
Skip	skip_update	Server Script	Flow Data [sys_flow_data]	Skips update record process step	Button	(empty)	(empty)	true
Skip	skip_list	Server Script	Flow Data [sys_flow_data]	Skips this list process step	Button	(empty)	(empty)	true
Skip	skip_email_escm	Server Script	Flow Data [sys_flow_data]	Skips sending the email for SCM	Button	(empty)	(empty)	true
Skip	skip_create	Server Script	Flow Data [sys_flow_data]	Skips this create record process step	Button	(empty)	(empty)	true
Skip	skip_submit_sandbox	Server Script	Flow Data [sys_flow_data]	Skips submit to sandbox	Button	(empty)	(empty)	true
Skip	skip_escm	Server Script	Flow Data [sys_flow_data]	Skip SCM common activity.	Button	(empty)	(empty)	true
Mark Complete	complete_activity	Client Action	Global [global]		Button	(empty)	Complete Activity	true
Restart	restart_activity_escm	Client Action	Global [global]	Restart.	Button	(empty)	Start Activity	true
View Article	view_article	Client Action	Global [global]	Opens up the knowledge record in a new tab	Button	(empty)	Playbook Open Record	true
Yes	yes	Server Script	Flow Data [sys_flow_data]		Button	(empty)	(empty)	true
Upload	upload_demo	Server Script	Demo Application Submission [sn_pad_demo_application_submission]		Button	(empty)	(empty)	true
Create Record	create_record	Server Script	Flow Data [sys_flow_data]	Informs process automation to create record	Button	(empty)	(empty)	true
Send Email	send_email	Server Script	Flow Data [sys_flow_data]	Informs process automation to send email	Button	(empty)	(empty)	true
View Email Search Results	email_search_results	UXF Client Action	Flow Data [sys_flow_data]	Email Search Results	Button	(empty)	ESCM Open Related List Payload Def	true
Restart	restart_activity	Client Action	Global [global]		Button	(empty)	Start Activity	true

2. Cliquez sur **Nouveau**.

   Consultez la documentation Now Platform pour savoir comment créer ces actions. Dans cet exemple, Skip est implémenté en tant que script serveur.

3. **Remplacement Playbook :**

   C'est possible si vous souhaitez remplacer le type d'expérience d'activité existant. Pour plus d'informations, consultez la documentation Now Platform. Aucun remplacement Playbook pour cet exemple.

Soumettre au bac à sable CSF X

Soumettre au bac à sable CSF X est un exemple de processus de définition d'activité.

Élémentaire

Les détails de base capturent le nom (étiquette), l'application, la description, la table et toutes les applications à partir desquelles elle est accessible.

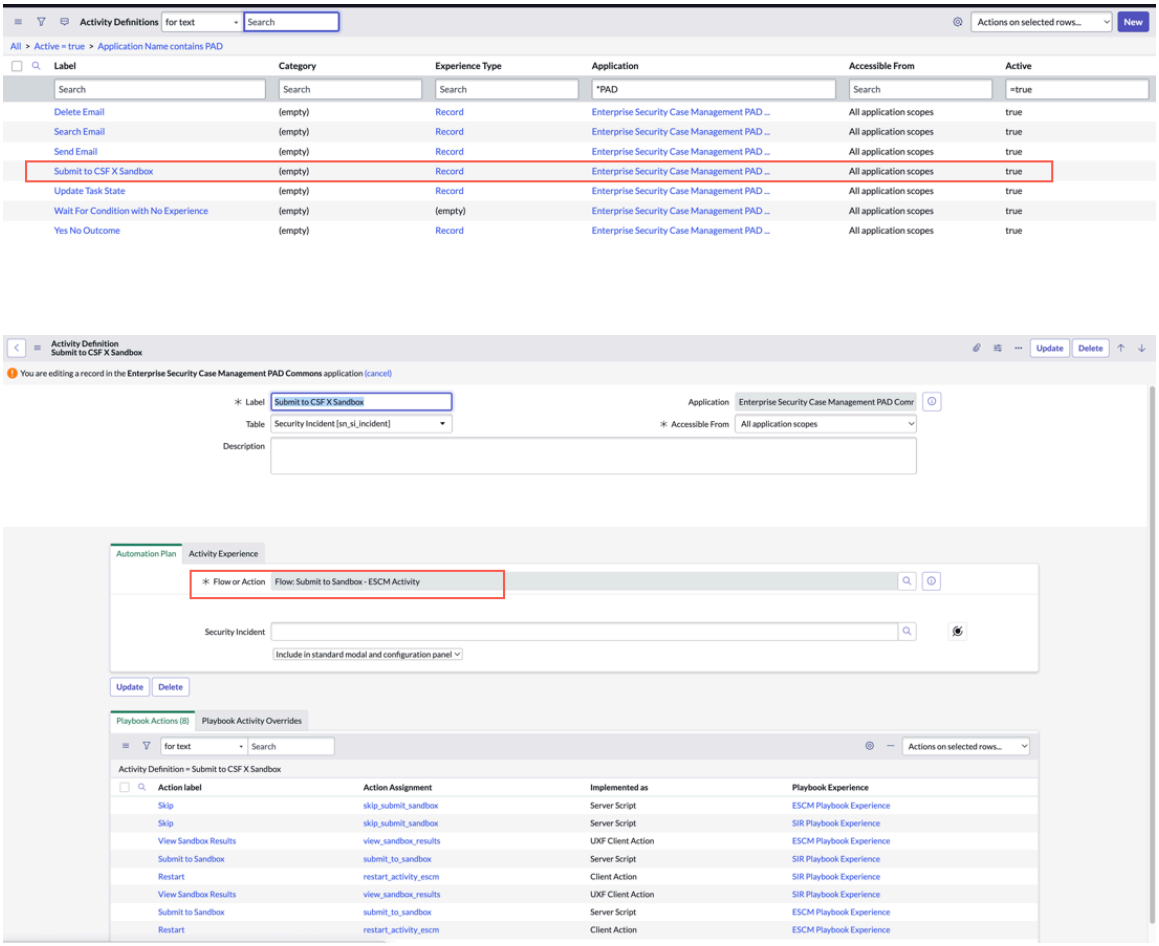
Ajoutez le plan d'automatisation, l'expérience d'activité et soumettez. Une fois soumis, modifiez le document pour ajouter plus de détails à chaque onglet.

Plan d'automatisation

Le plan d'automatisation associe l'action/le flux secondaire back-end créé à l'aide du Flow Designer. Cet exemple utilise le sous-flux **d'activité Soumettre au bac à sable : ESCM**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Ce sous-flux permet de soumettre les observables malveillants au bac à sable. Tous les champs d'entrée et de sortie sont définis.

L'incident de sécurité est le champ d'entrée.

Expérience de l'activité

Dans cet exemple, **le type d'enregistrement** est sélectionné.

Enregistrement associé

L'enregistrement associé sert à stocker les données associées relatives à l'activité actuelle. Cela capturerait les données de temps d'exécution, ainsi que l'état de l'expérience.

- Table associée : données de flux
- Enregistrement associé : VL
- Table de l'état de l'expérience : données de flux
- Enregistrement de l'état de l'expérience : VL

Détails

- Ligne de balise : Envoyer un e-mail
- Icône : contour de l'enveloppe
- Titre: **Activité** > **Instance d'activité** > **Étiquette**. Ici, nous avons sélectionné l'étiquette de l'instance d'activité. Cette remontée pas à pas remplacera dynamiquement la valeur d'étiquette en tant que titre au moment de l'exécution.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Description : VL (la sortie du flux secondaire est mappée)
- Titre de l'état en attente : blanc
- Description d'état en attente : vide
- Champs d'enregistrement
- Pied de page

Formulaire

- Vue du formulaire : vide
- Champs de formulaire : vides

Pièces jointes

Dans cet exemple :

- Source de la pièce jointe : aucune
- Pièce jointe en lecture seule : non vérifiée

1. Source de la pièce jointe : il s'agit d'une liste déroulante. Les pièces jointes à afficher sur la carte : celles jointes à l'enregistrement parent, à l'enregistrement associé ou aucune.
2. Pièce jointe en lecture seule : il s'agit d'un vrai/faux. Empêchez l'utilisateur de renommer ou de supprimer les pièces jointes existantes.

Fonctionnalités

Dans cet exemple,

- Afficher le SLA : non coché
- Afficher la liste de vérification : non vérifiée
- Est automatisé : non vérifié

Actions Playbook dans la définition d'activité

Cette section contient les actions qui seront affichées sur la carte d'activité.

Cet exemple comporte les actions Ignorer, Afficher les résultats du bac à sable, Soumettre au bac à sable et Redémarrer.

Pour ajouter une nouvelle action à la carte d'activité, vous devez créer un nouvel enregistrement dans la liste connexe Actions Playbook présente en bas de la page.

Remplacement Playbook

Aucun remplacement Playbook pour cet exemple.

Exemples de playbooks pour l'espace de travail SIR

Vous pouvez créer ou configurer des playbooks pour l'espace de travail SIR rapidement et facilement sans écrire de code compliqué. Vous pouvez utiliser ces playbooks pour résoudre les menaces de sécurité étape par étape. Vous pouvez invoquer le flux du playbook d'incident de sécurité automatiquement ou manuellement.

Security Incident Response fournit les playbooks suivants avec le système de base :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Playbook pour l'hameçonnage manuel
- Playbook pour l'hameçonnage automatisé
- Playbook pour les programmes malveillants manuels
- Playbook pour les programmes malveillants automatisés
- Playbook pour Échec de connexion manuelle

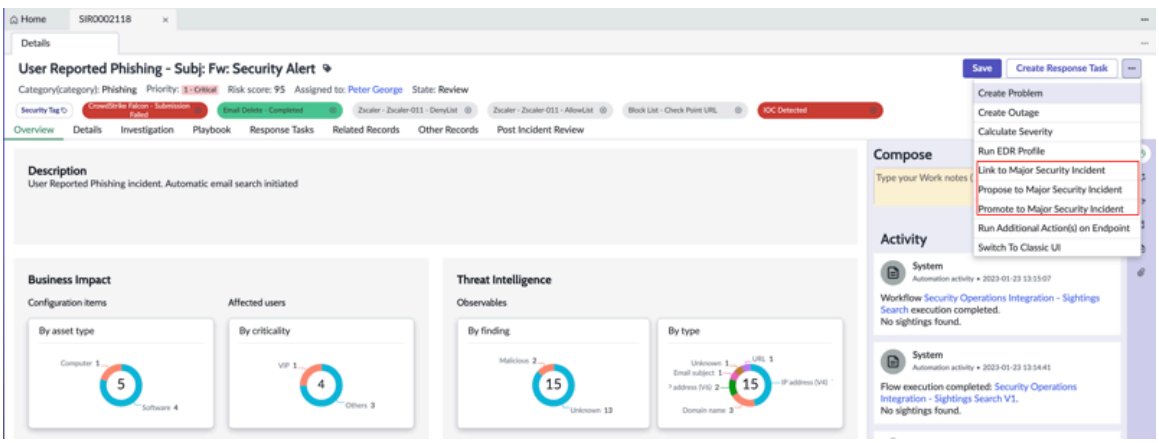
Utilisation des enregistrements MSI

À l'aide de l'espace de travail Réponse aux incidents de sécurité, vous pouvez proposer, promouvoir ou lier des incidents de sécurité en tant qu'incidents de sécurité majeurs lorsque les incidents sont identifiés comme une menace critique pour l'organisation.

Après l'installation Gestion des incidents de sécurité majeurs de MSIM sur votre Now Platform instance, vous pouvez gérer la transition des incidents de sécurité vers les incidents majeurs.

Les Gestion des incidents de sécurité majeurs actions d'interface utilisateur (MSIM) s'affichent en haut à droite de la bannière du formulaire d'incident de sécurité de l'espace de travail SIR. Sélectionnez l'action d'interface utilisateur le cas échéant.

Remarque : Certaines actions sont contextuelles. Par exemple, l'action Dissocier n'est disponible que lorsque l'incident de sécurité est déjà proposé, promu ou lié à un incident de sécurité majeur.



Proposer comme incident de sécurité majeur

Proposer un incident de sécurité en tant qu'incident de sécurité majeur (MSI).

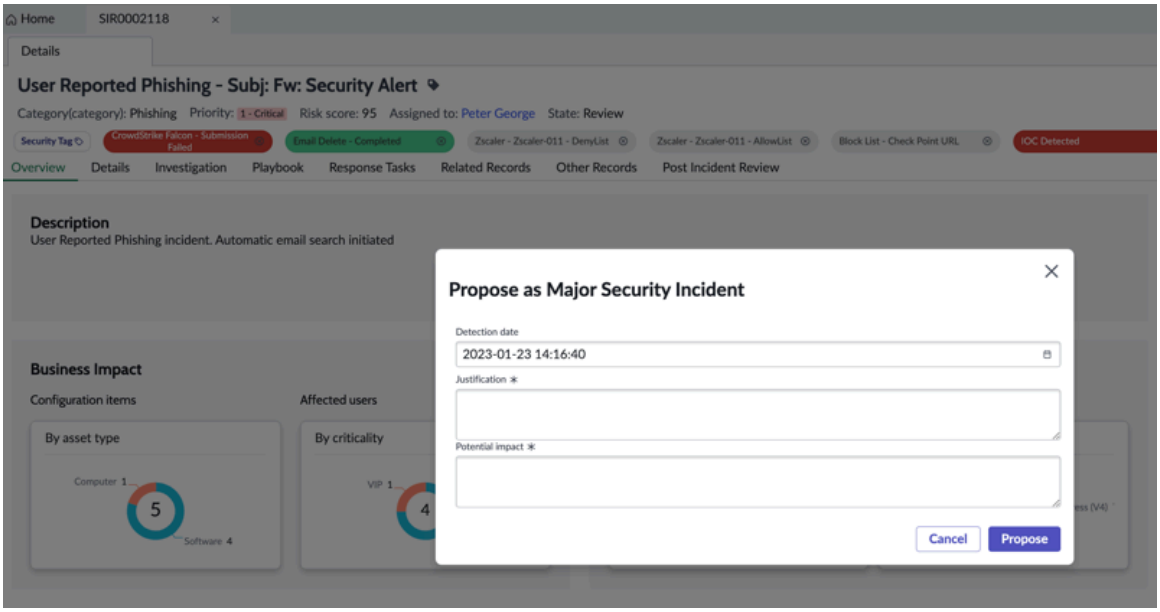
Avant de commencer

Rôle requis : sn_si.analyst.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Cliquez sur **Proposer en incident de sécurité majeur**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Renseignez les champs tels que Date de détection, Justification et Impact potentiel.
5. Cliquez sur **Proposer**.
   L'enregistrement d'incident est proposé en tant que candidat à l'incident de sécurité majeur.
   Une fois que l'enregistrement d'incident est proposé en tant que candidat à l'incident de sécurité majeur, la balise **Candidat à l'incident de sécurité majeur** est appliquée et affichée sur la bannière du formulaire d'incident de sécurité.

> **Remarque :** Cliquez sur **Dissocier de l'incident de sécurité majeur** pour dissocier l'incident si vous ne souhaitez pas le proposer ou s'il n'a pas d'impact critique. L'incident sera dissocié et répertorié sous la vue de liste vers l'analyste de sécurité pour le rattrapage.

Promouvoir en incident de sécurité majeur

Promouvoir un incident de sécurité en incident de sécurité majeur.

Avant de commencer

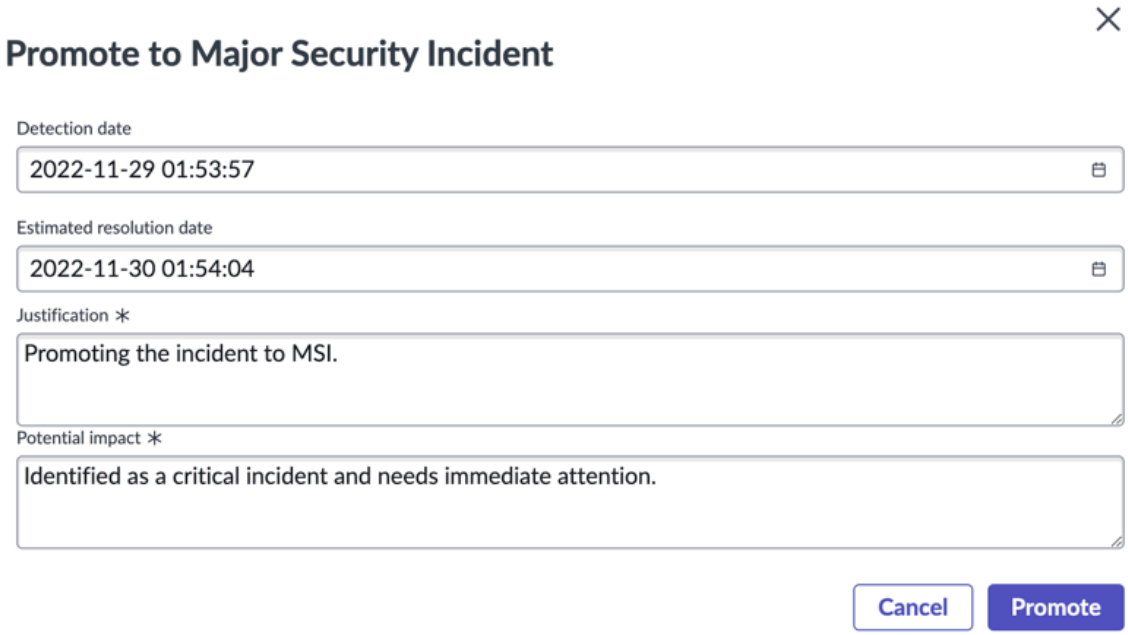
Rôle requis : sn_si.analyst.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Cliquez sur **Promouvoir en incident de sécurité majeur**.
4. Renseignez les champs tels que Date de détection, Date de résolution estimée, Justification et Impact potentiel.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Promouvoir**.
   L'enregistrement d'incident est promu en tant qu'incident de sécurité majeur.
   Une fois que l'enregistrement d'incident est promu en tant qu'incident de sécurité majeur, la balise **d'incident de sécurité majeur** est appliquée et affichée sur la bannière du formulaire.

   Remarque : Vous pouvez également dissocier l'incident de sécurité majeur s'il n'est pas critique, l'incident sera alors dissocié et répertorié sous la vue de liste pour le rattrapage de l'analyste de sécurité.

Lier à l'incident de sécurité majeur

Lier un incident de sécurité à un incident de sécurité majeur en tant qu'incident de sécurité enfant.

Avant de commencer

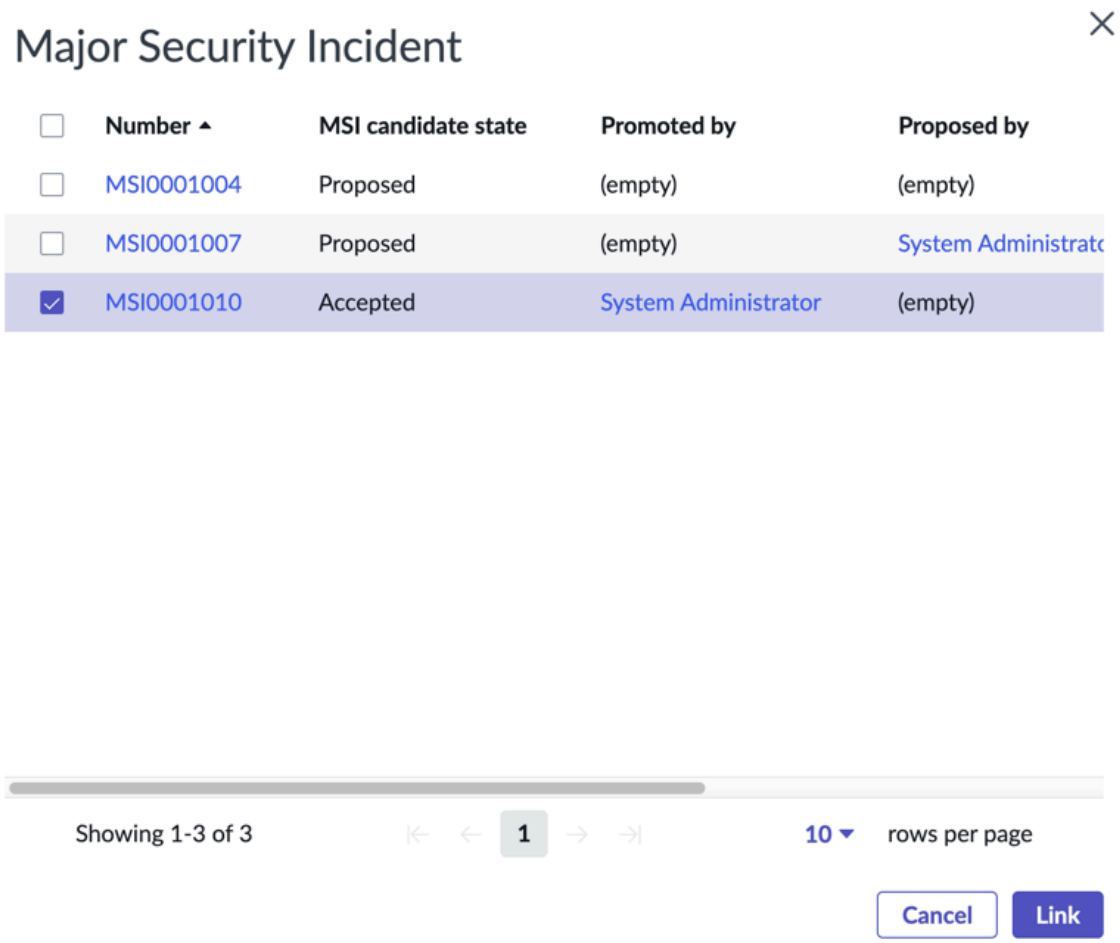
Rôle requis : sn_si.analyst.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. **Cliquez sur Lier à l'incident de sécurité majeur**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez le ou les incidents à associer à un incident de sécurité majeur.
5. Cliquez sur **Lier**.
6. L'enregistrement d'incident est lié en tant qu'incident enfant de l'incident de sécurité majeur.
   Une fois que l'incident est lié en tant qu'incident enfant à un incident de sécurité majeur, la balise **d'incident de sécurité majeur** est appliquée et affichée sur la bannière du formulaire.

Utiliser les actions d'interface utilisateur de formulaire

Voici les actions d'interface utilisateur qui s'affichent sur le formulaire d'incident de sécurité.

Pour accéder aux actions d'interface utilisateur du formulaire :

1. Accéder à **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez un incident de sécurité dans la vue de liste.
3. Toutes les actions d'interface utilisateur sont présentes dans le coin supérieur droit du formulaire d'incident de sécurité.

Actions d'interface utilisateur du formulaire d'espace de travail

Nom de champ	Description
Discuter	Créez ou démarrez une discussion dans la barre latérale pour l'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description
Enregistrer	Enregistrez ou mettez à jour l'enregistrement Réponse aux incidents de sécurité après avoir apporté des modifications.
Créer une tâche de réponse	Créez une tâche de réponse pour l'incident de sécurité.
Composer des e-mails	Composez des e-mails pour l'incident de sécurité.
Ajouter un Playbook	Ajoutez manuellement le playbook pour l'incident de sécurité.
Créer un incident	Créez un incident au sein de l'incident de sécurité.
Créer un ticket du service clientèle	Créez un ticket du service clientèle pour l'incident de sécurité qui sera suivi par l'équipe Gestion du service clientèle (CSM). **Remarque :** Cette option n'est disponible que lorsque Customer Service Management (CSM) est installé.
Ouvrir le(s) flux(s) associé(s)	Ouvrez n'importe quel contexte de workflow associé à l'incident de sécurité. Cette option n'est visible que s'il existe des workflows.
Créer une demande de changement	Créez une demande de changement dans le cadre de l'incident de sécurité.
Créer un problème	Créer un problème au sein de l'incident de sécurité.
Créer une panne	Créer une panne au sein de l'incident de sécurité.
Calculer la gravité	Calculez la gravité d'un incident de sécurité à l'aide de calculateurs prédéfinis. La gravité est calculée en fonction des règles prédéfinies dans les calculateurs. La gravité d'un incident est basée sur le score de risque, l'impact sur l'entreprise et la priorité.
Exécuter le profil PEPT	Sélectionnez et exécutez le profil EDR pour l'intégration requise. **Remarque :** Cette option n'est disponible que lorsque des intégrations sont installées.
Lier à l'incident de sécurité majeur	Lier un incident de sécurité à un incident de sécurité majeur.
Signaler un événement à risque	Signalez cet incident de sécurité comme événement à risque à l'équipe de gestion des risques. L'équipe de gestion des risques analyse l'événement et veille à ce que de tels événements et les pertes associées ne se reproduisent pas. **Remarque :** Cette option n'est disponible que lorsque Gestion des risques est installée.
Dissocier d'un incident de sécurité majeur	Dissocier d'un incident de sécurité majeur.
Proposer comme incident de sécurité majeur	Proposer un incident de sécurité en tant qu'incident de sécurité majeur.

Traduction automatique

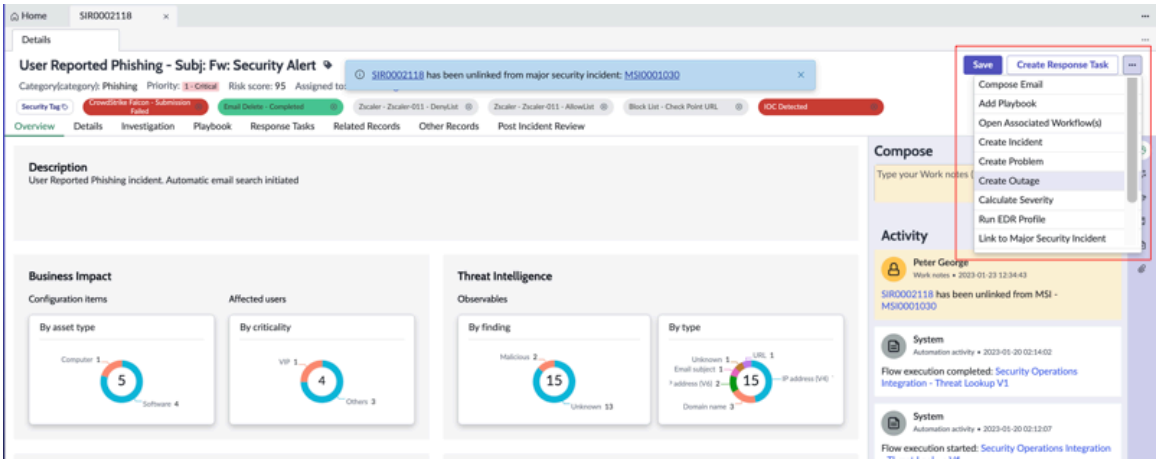
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description
Promouvoir en incident de sécurité majeur	Promouvoir un incident de sécurité en tant qu'incident de sécurité majeur.
Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison	Exécuter des actions supplémentaires sur le point de terminaison. **Remarque :** Cette option n'est disponible que lorsque les intégrations de point de terminaison sont installées. Par exemple : FireEye HX
Créer un nouvel événement dans MISP	Créez et modifiez automatiquement ou manuellement des événements dans MISP. **Remarque :** Cette option n'est disponible que lorsque l'intégration MISP est installée.
Associer la technique MITRE ATT&K	Associez les techniques MITRE ATT&K à l'incident de sécurité. **Remarque :** Cette option est disponible lorsque MITRE ATT&K est installé.
Afficher les informations MITRE ATT&K	Affiche les informations MITRE ATT&K associées à l'incident de sécurité. **Remarque :** Cette option est disponible lorsque MITRE ATT&K est installé.
Ajouter au ticket de sécurité	Ajoutez l'incident de sécurité à un ticket de sécurité existant ou nouveau. **Remarque :** Cette option est disponible lorsque Threat Intelligence est installé.
Basculer vers l'interface utilisateur classique	Permettez à l'analyste de basculer entre l'interface utilisateur classique et la nouvelle interface utilisateur afin qu'il puisse également travailler sur les fonctionnalités existantes qui ne sont pas encore disponibles dans le nouvel espace de travail.
Abolir	Annulez un incident de sécurité. Une fois que vous avez sélectionné **Annuler** tous les enregistrements connexes tels que les tâches de réponse, les incidents de sécurité enfants sont également annulés.
Supprimer	Supprimer un enregistrement d'incident de sécurité.

4. Cliquez sur un numéro d'incident de sécurité pour afficher l'enregistrement de l'incident de sécurité. Vous pouvez voir les actions d'interface utilisateur en haut de la page.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Workflow de fermeture de l'incident de sécurité

Fermez l'incident de sécurité en mettant à jour l'état de l'incident.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

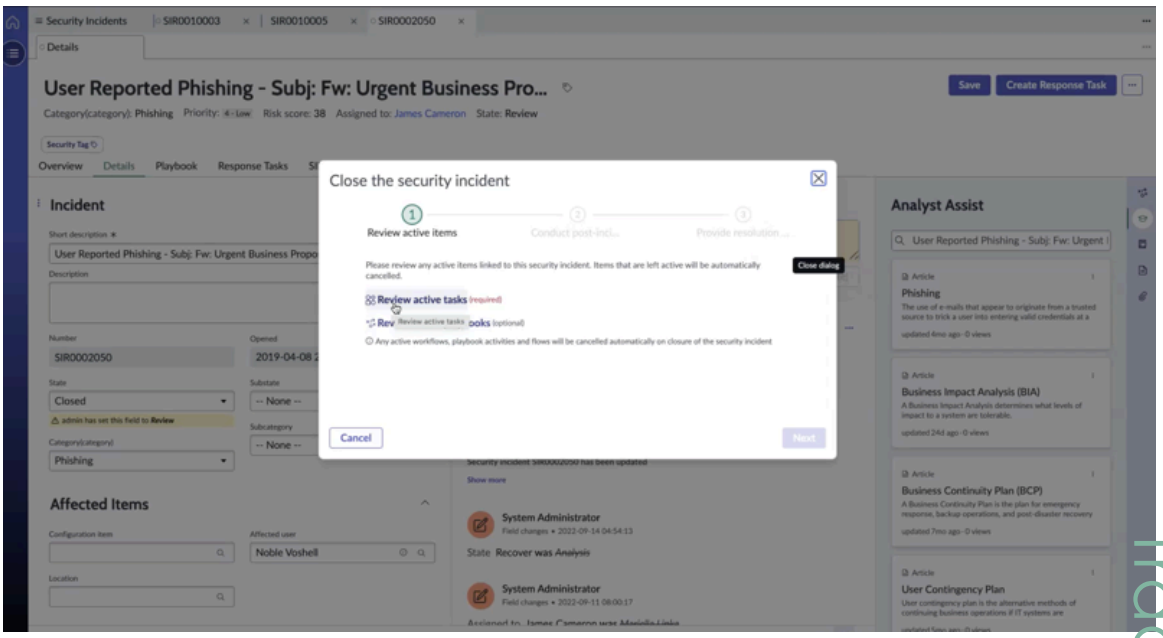
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Par exemple, accédez à **Listes** > **Incidents de sécurité** > **Incidents ouverts**.
3. Ouvrez un incident que vous souhaitez fermer.
4. Accédez à l'onglet **Détails** .
5. Explorez l'état de l'incident et sélectionnez **Fermer**.
6. Effectuez les activités de fermeture.

   - Il s'agit d'une étape obligatoire pour examiner n'importe quelle tâche avant de fermer un incident de sécurité. Toute tâche de réponse doit être examinée par l'analyste et fermée ou annulée avant d'être fermée en tant qu'incident de sécurité. Lorsque l'analyste clique sur **Examiner les tâches actives**, il redirige l'utilisateur vers l'onglet **Tâches de réponse** . Un message de session s'affiche pour vous informer que vous êtes sur le point de fermer un incident de sécurité. Cliquez sur **Continuer**.
   - Cliquez sur **Continuer**. La première étape – examiner les tâches actives lors de la fermeture de l'incident de sécurité – est terminée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

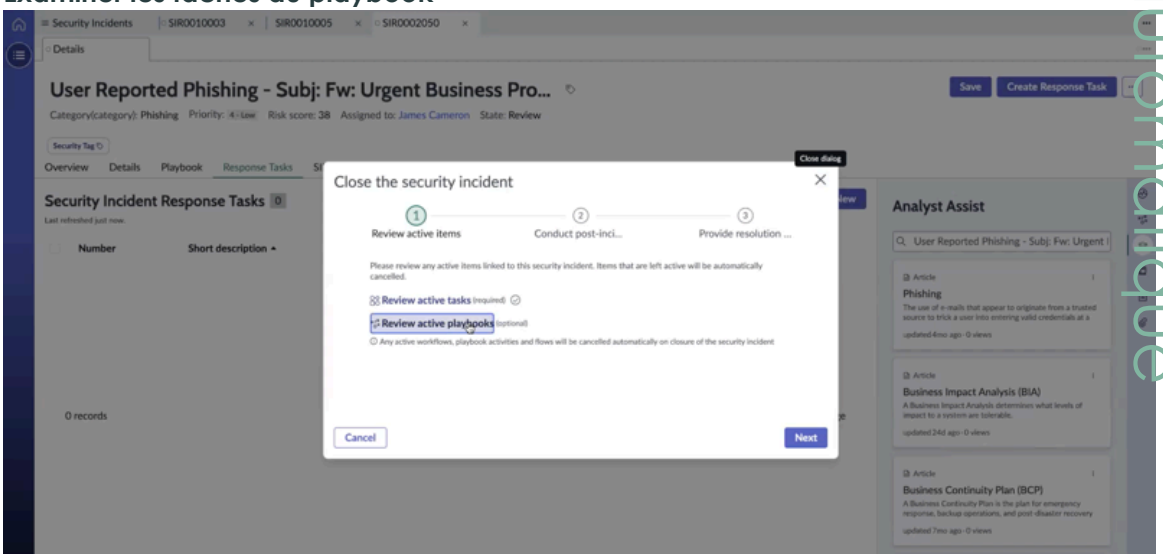
Examen des tâches de fermeture



- Passez à l'étape suivante pour examiner les playbooks actifs que l'analyste doit examiner, qui est une étape facultative. Vous pouvez cliquer sur le lien pour examiner la tâche Playbook active et la fermer au besoin.

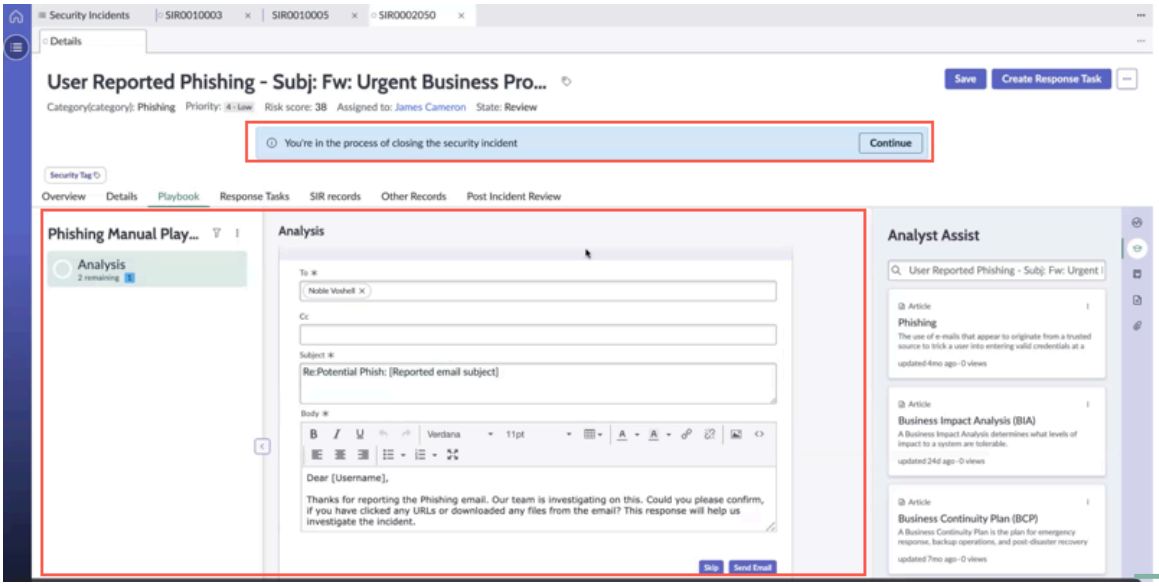
> **Remarque :** Tous les workflows, activités de playbook et flux actifs seront automatiquement annulés lors de la fermeture de l'incident de sécurité.

Examiner les tâches du playbook



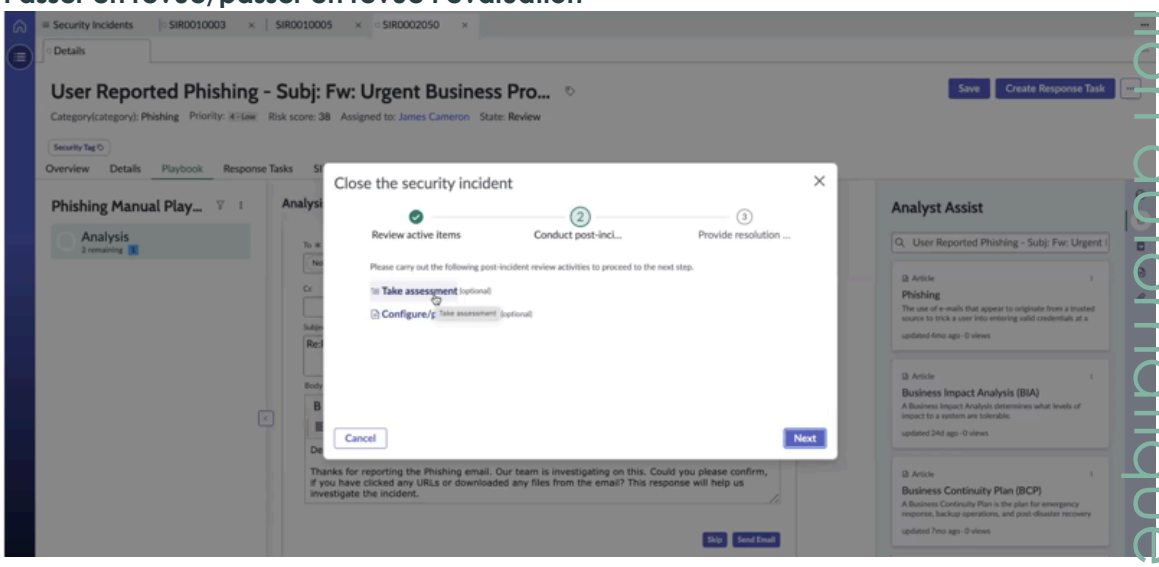
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



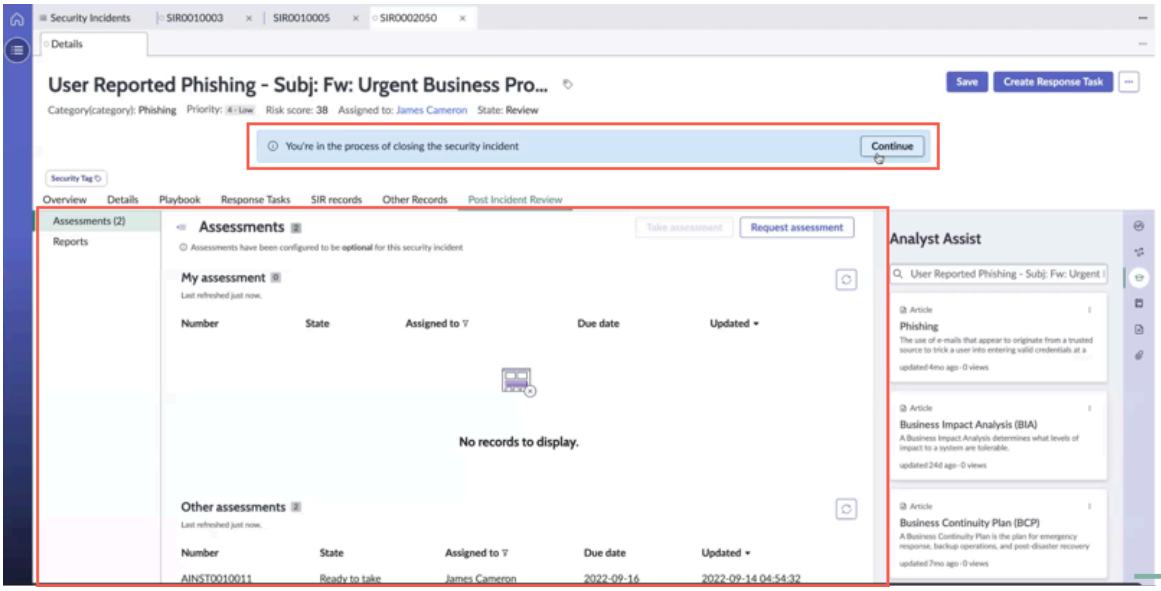
◦ Rapport d'examen post-incident : vous allez maintenant être déplacé pour examiner les activités post-incident afin de poursuivre la fermeture. Si l'évaluation est facultative, ignorez l'étape ou si l'évaluation est obligatoire, passez l'évaluation et terminez-la.

Passer en revue/passer en revue l'évaluation

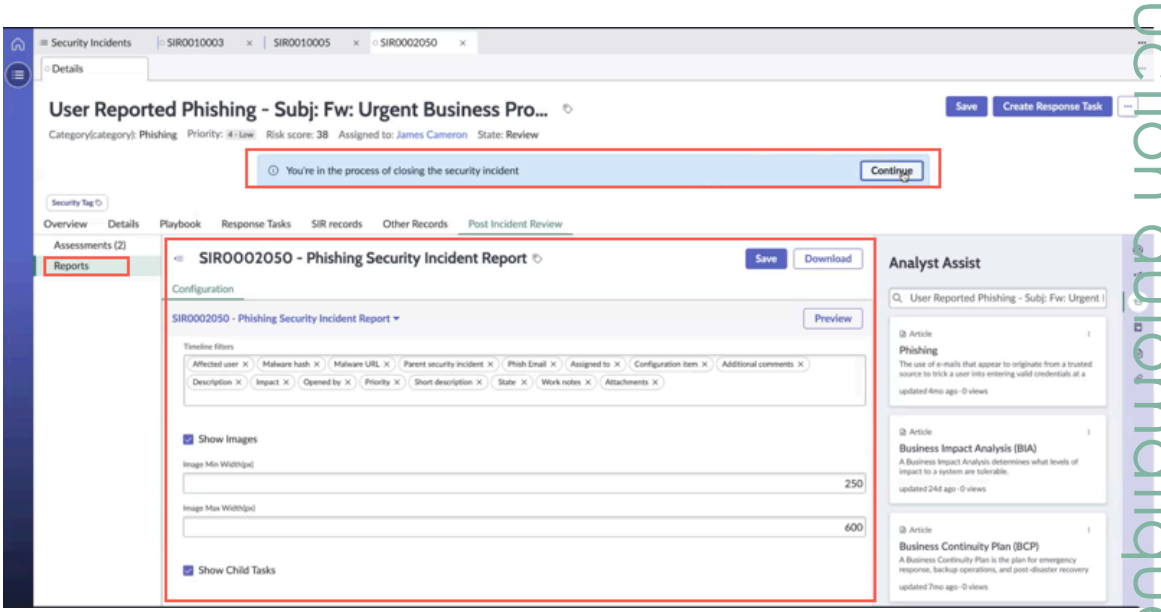


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



◦ Configurer/prévisualiser le rapport : il s'agit là encore d'une étape facultative, cliquez sur le lien pour examiner le rapport et passer à l'étape **suivante** .

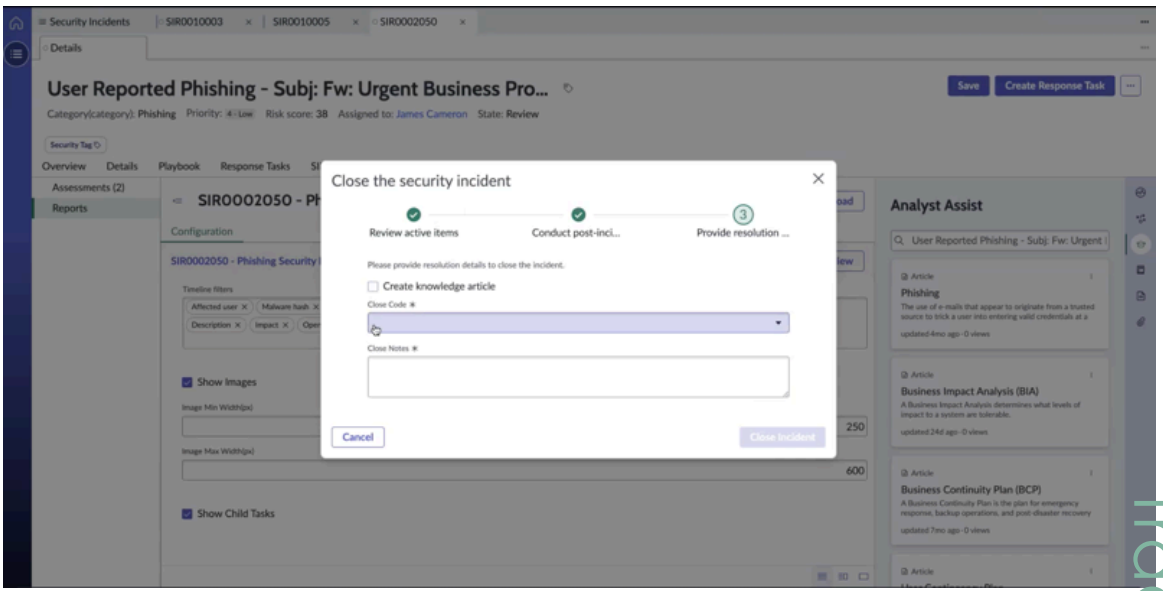


◦ Fournir les détails de la résolution : l'analyste peut cocher la case pour créer automatiquement des articles de la base de connaissances.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

◦ Fournissez le code de fermeture, les notes de fermeture, puis cliquez sur **Fermer l'incident**.



Remarque : Si l'analyste annule la boîte de dialogue **Fermer l'incident de sécurité** , il peut accéder à l'onglet **Détails** et basculer l'état de l'incident sur **Fermer** pour poursuivre la fermeture.

Affichage des tableaux de bord de l'espace de travail SIR

Cette section présente les mesures importantes pour analyser votre Réponse aux incidents de sécurité processus, telles que les nouveaux incidents de sécurité ou l'âge moyen des incidents de sécurité ouverts.

Dans l'interface utilisateur classique, quelques tableaux de bord standard sont disponibles sous la page d'accueil et Analyse des performances les tableaux de bord sont disponibles lorsque Analyse des performances le Réponse aux incidents de sécurité module d'extension est installé. Tous ces éléments seront désormais disponibles dans le nouvel espace de travail, sous la section **Tableaux de bord SIR** .

Tableaux de bord standard sous la page d'accueil :

- Aperçu de Security Incident Response
  - Vue d'ensemble des analystes
  - Vue d'ensemble du gestionnaire (prise en charge dans les versions futures)
  - Vue d'ensemble du CISO (prise en charge dans les versions futures)
- **Analyse de la plateforme pour** *Réponse aux incidents de sécurité*
  - Explorateur des incidents de sécurité
  - Tableau de bord des CISO (version ultérieure)
  - Sécurité – Gestion des incidents
  - KPI de gestion des incidents de sécurité de premier plan
  - Efficience de Opérations de sécurité
  - Analyse contextuelle : tableau de bord SI

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Il peut y avoir une certaine répétition des tableaux de bord dans les analyses standard et de plateforme pour les tableaux de bord Security Incident Response tels que le tableau de bord CISO. Lorsque le module d'extension est installé, il y a du contenu supplémentaire dans ces tableaux de bord et il n'est pas disponible en double.

Les utilisateurs doivent installer le module d'extension pour que les tableaux de bord répertoriés sous Analyse de la plateforme pour les tableaux de bord Security Incident Response soient présents dans l'espace de travail. Dans le cas contraire, seuls les tableaux de bord standard seront disponibles.

Dans la version actuelle du , les tableaux de SIR Workspacebord suivants sont disponibles dans la section **Tableaux de bord SIR** . Les autres tableaux de bord manquants seront disponibles dans les versions ultérieures.

Tableaux de bord Security Incident Response

Tableau de bord	Description
Tableau de bord standard	
Vue d'ensemble des analyses de sécurité	Grâce à ce tableau de bord, les analystes de sécurité peuvent afficher les incidents de sécurité résumés en fonction des tâches de priorité critique, des tâches de priorité élevée de l'analyste, des incidents de sécurité affectés à l'analyste, des tâches affectées aux analystes et du nombre d'incidents.
Analyse des performances (PA) pour les tableaux de bord Security Incident Response	
Explorateur des incidents de sécurité	Grâce à ce tableau de bord, les gestionnaires et analystes de sécurité peuvent afficher les incidents de sécurité résumés et regroupés par catégorie, sous-catégorie, emplacement, priorité et impact sur l'entreprise. Ces vues permettent aux gestionnaires et aux analystes d'avoir rapidement une idée de la fréquence à laquelle les attaques se produisent et des services aux entreprises qui sont affectés.
Sécurité – Gestion des incidents	Grâce à ce tableau de bord, les gestionnaires de sécurité peuvent facilement suivre le volume, les performances et la progression des incidents de sécurité, de l'analyse/détection initiale au confinement, à l'éradication et à la récupération.
Tableau de bord des CISO	Proposé pour la prise en charge dans une version future.
Efficience de Opérations de sécurité	Grâce à ce tableau de bord, les gestionnaires et les analystes peuvent consulter les mesures d'efficacité globales et mesurer les performances du SOC.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableaux de bord Security Incident Response (suite)

Tableau de bord	Description
KPI de gestion des incidents de sécurité de premier plan	Grâce à ce tableau de bord, les gestionnaires de sécurité peuvent suivre et visualiser le volume, les performances et la progression des incidents de sécurité, depuis l'analyse/détection initiale jusqu'au confinement, à l'éradication et à la récupération.
Analyse contextuelle : S	Grâce à ce tableau de bord, les gestionnaires et les analystes peuvent afficher les incidents de sécurité ouverts, l'âge moyen des incidents de sécurité ouverts, le délai moyen de clôture des incidents de sécurité, le pourcentage d'incidents de sécurité qui ont été ouverts et fermés le même jour et le pourcentage des incidents qui n'ont pas été mis à jour au cours des 5 derniers jours et 30 jours.

Accéder aux tableaux de bord SIR et PA

L'icône **Tableaux de bord SIR** affichée sur le côté gauche de la page d'accueil de l'espace de travail.

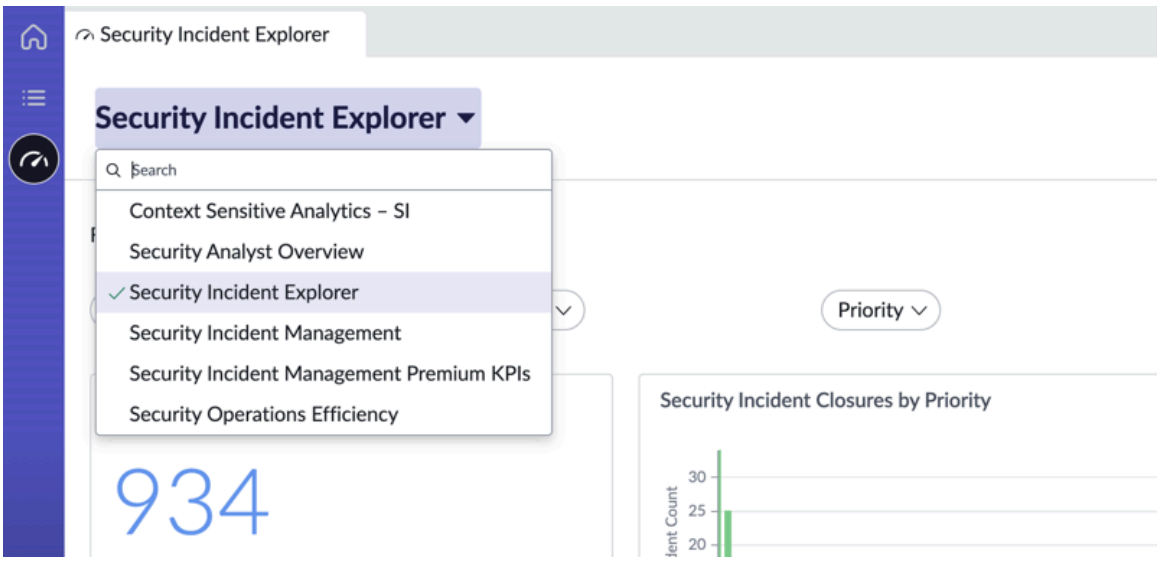
Remarque : Les utilisateurs disposant d'un accès sn_si.manager ou sn_si.admin peuvent modifier les tableaux de bord. Les utilisateurs doivent se trouver dans le même champ d'application des tableaux de bord que celui qu'il essaie de modifier. Par exemple, le tableau de bord de vue d'ensemble de l'analyste de sécurité est disponible dans l'espace de travail SIR, puis l'utilisateur doit également se trouver dans le même champ d'application de l'espace de travail SIR pour apporter les modifications au tableau de bord.

1. Accédez à la **Espaces de travail** > **Espace de travail Security Incident Management**.
2. Cliquez sur **des tableaux de bord SIR**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez le tableau de bord souhaité dans la liste déroulante.



Vous pouvez modifier les tableaux de bord, ajouter de nouveaux éléments aux tableaux de bord et créer vos propres tableaux de bord. Pour plus d'informations sur l'utilisation des tableaux de bord, consultez Utilisation de tableaux de bord réactifs

Afficher le tableau de bord de vue d'ensemble des analystes de sécurité

Grâce à ce tableau de bord, les analystes de sécurité peuvent afficher les incidents de sécurité résumés en fonction des tâches de priorité critique, des tâches de priorité élevée, des incidents de sécurité affectés à l'analyste, des tâches affectées aux analystes et du nombre d'incidents.

Avant de commencer

Par défaut, le tableau de bord Vue d'ensemble de l'analyste de la sécurité s'affiche pour les utilisateurs disposant de l'accès sn_si.analyst.

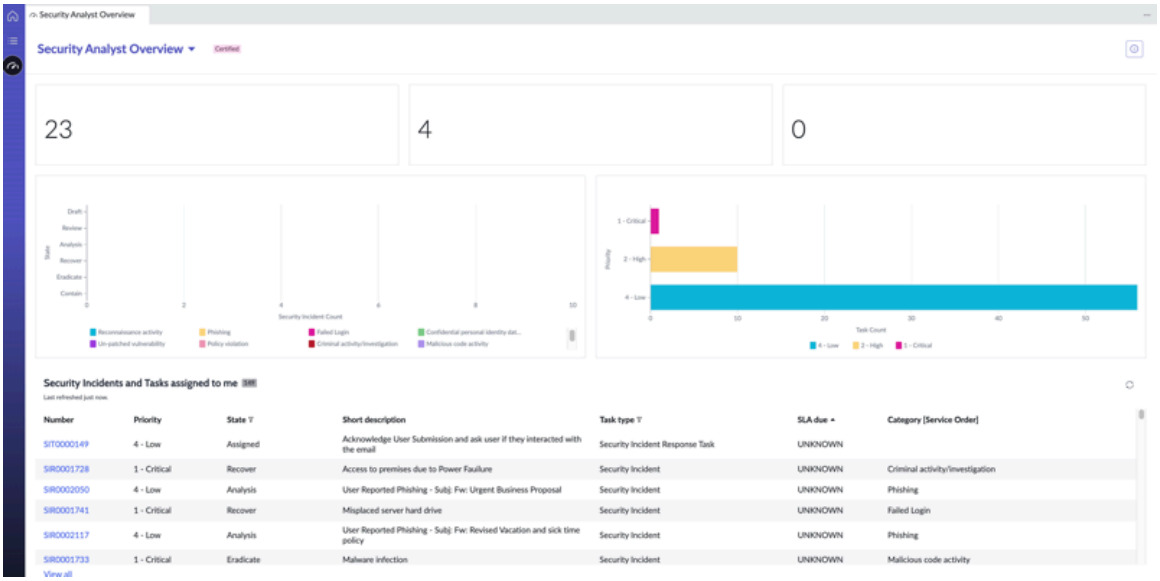
Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Espaces de travail** > **Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , affichée sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Vue d'ensemble de l'analyste de sécurité** dans la liste déroulante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Consultez le tableau de bord de vue d'ensemble de l'analyste de sécurité pour connaître les actions suivantes. Pour en savoir plus sur le tableau de bord Vue d'ensemble des analystes de la sécurité, reportez-vous à la section Réponse aux incidents de sécurité Solutions Analyse de la plateforme et Reporting.

Afficher le tableau de bord de l'Explorateur des incidents de sécurité

Grâce à ce tableau de bord, les gestionnaires de sécurité peuvent visualiser les incidents de sécurité résumés et regroupés par catégorie, sous-catégorie, emplacement, priorité et impact sur l'entreprise.

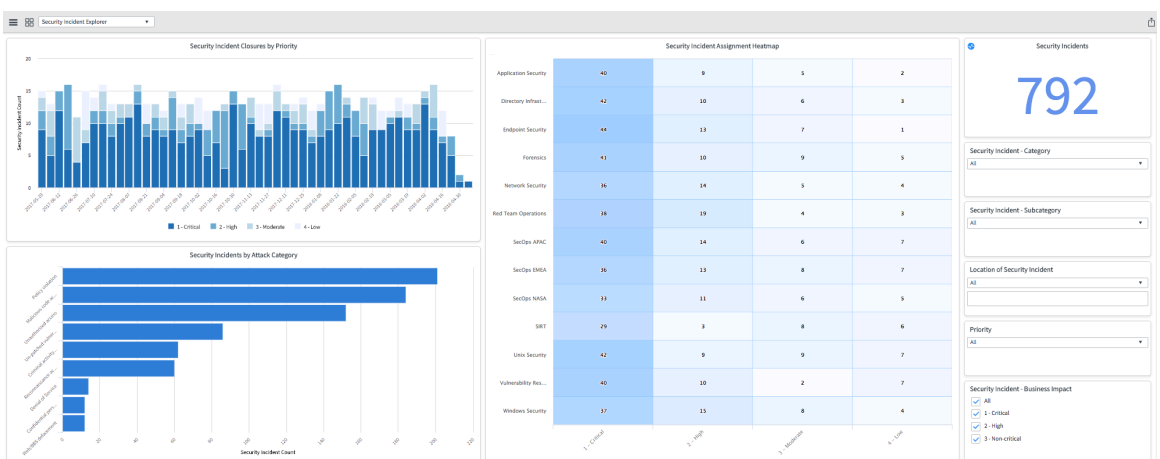
Avant de commencer

Par défaut, le tableau de bord de l'Explorateur des incidents de sécurité s'affiche pour les utilisateurs disposant de l'accès sn_si.manager.

Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Espaces de travail** > **Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , affichée sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Explorateur des incidents de sécurité** dans la liste déroulante.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consultez le tableau de bord de l'Explorateur des incidents de sécurité pour connaître les actions suivantes. Pour en savoir plus sur le tableau de bord de l'Explorateur des incidents de sécurité, consultez le tableau de bord de l'Explorateur des incidents de sécurité

Dans la version actuelle, la liste suivante des rapports n'est pas prise en charge dans le tableau de bord de l'Explorateur des incidents de sécurité :

- Carte thermique d'affectation des incidents de sécurité : la visualisation de la carte thermique n'est pas disponible.
- Carte des incidents de sécurité : la visualisation de carte n'est pas disponible.

Afficher le tableau de bord Gestion des incidents de sécurité

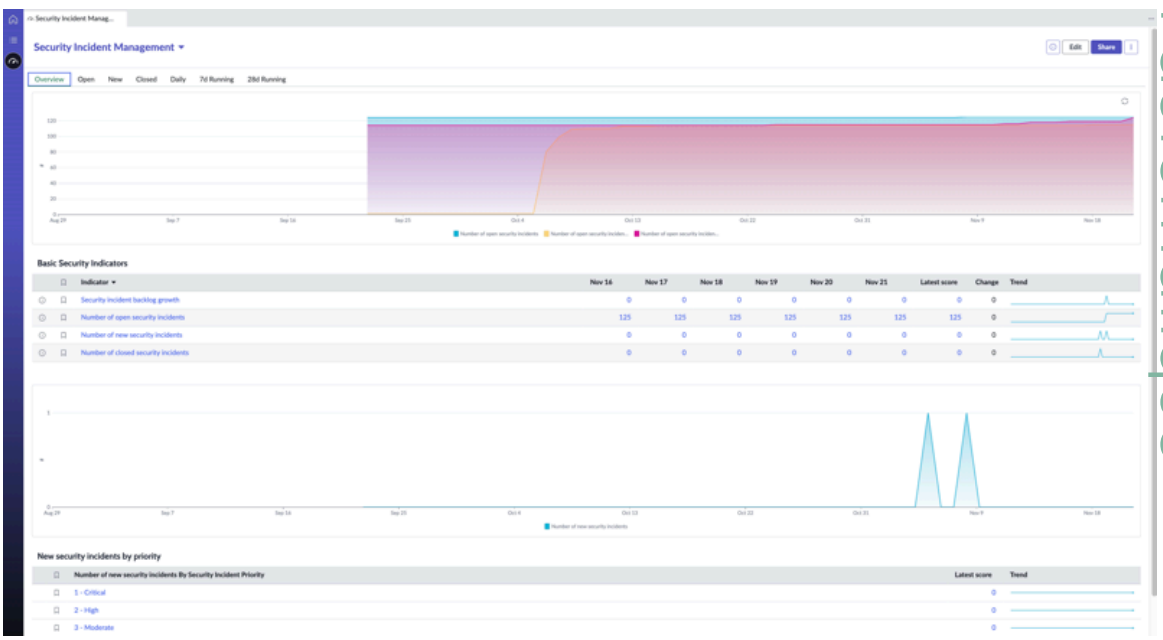
Grâce à ce tableau de bord, les responsables de la sécurité peuvent facilement suivre le volume, les performances et la progression des incidents de sécurité, de l'analyse/détection initiale au confinement, à l'éradication et à la récupération.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , affichée sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Gestion des incidents de sécurité** dans la liste déroulante.



Consultez le tableau de bord Gestion des incidents de sécurité pour connaître les actions suivantes. Pour en savoir plus sur le tableau de bord Gestion des incidents de sécurité, consultez Tableau de bord Gestion des incidents de sécurité

Afficher le tableau de bord Efficience des opérations de sécurité

Les responsables des centres des opérations de sécurité (SOC) peuvent consulter les mesures d'efficacité globales et mesurer les performances individuelles des membres de l'équipe SOC au sein de l'organisation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

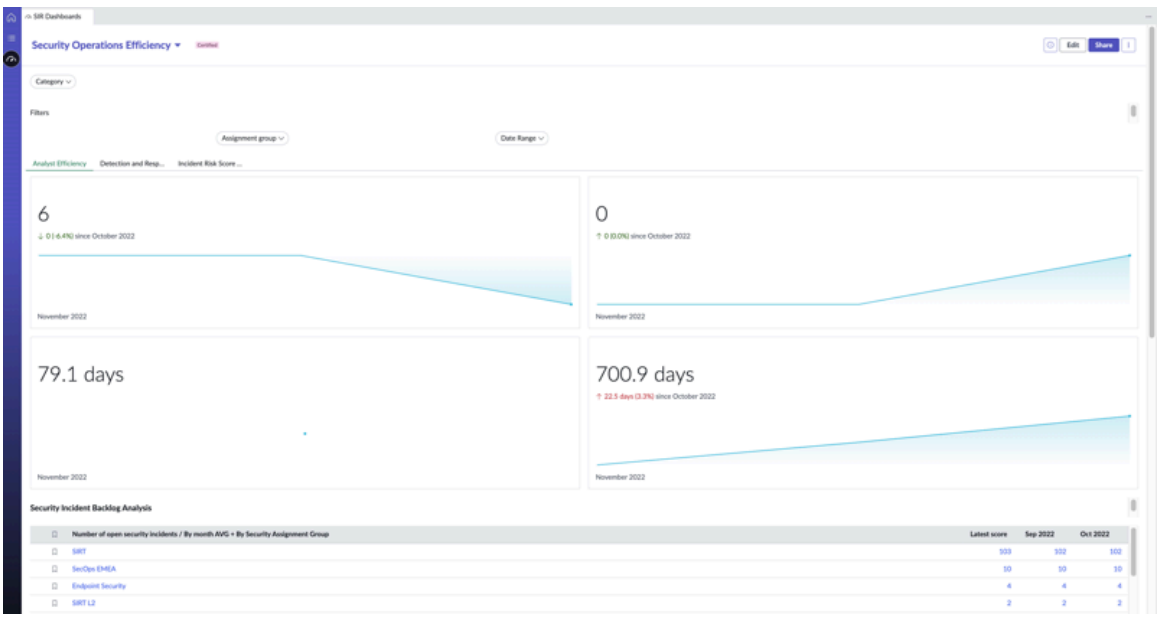
Dans la version actuelle, le rapport suivant n'est pas pris en charge dans le tableau de bord Security Operations Efficiency :

- Analyse de l'étape de l'incident de sécurité : la console n'est pas disponible

Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Espaces de travail** > **Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , affichée sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Efficacité de Security Operations** dans la liste déroulante.



Consultez le tableau de bord Efficacité des opérations de sécurité pour connaître les actions à suivre. Pour obtenir des informations détaillées sur le tableau de bord Efficacité de Security Operations, consultez Tableau de bord Efficience de Security Operations

Afficher le tableau de bord des KPI de premier plan de Security Incident Response

Grâce à ce tableau de bord, les gestionnaires de sécurité peuvent suivre et visualiser le volume, les performances et la progression des incidents de sécurité, depuis l'analyse/détection initiale jusqu'au confinement, à l'éradication et à la récupération.

Avant de commencer

Dans la version actuelle, la liste suivante des rapports n'est pas prise en charge dans le tableau de bord des KPI de Security Incident Response Premium :

- Processus par état : la console n'est pas disponible
- Processus par âge : la console n'est pas disponible
- Incidents de sécurité ouverts pendant plus de 30 jours par groupe d'affectation et par état : la visualisation de la carte thermique n'est pas disponible.
- Incidents de sécurité non mis à jour pendant plus de 30 jours par groupe d'affectation et par état : la visualisation de la carte thermique n'est pas disponible.
- Incidents de sécurité avec un délégataire qui n'est pas actif - La visualisation de la carte thermique n'est pas disponible.

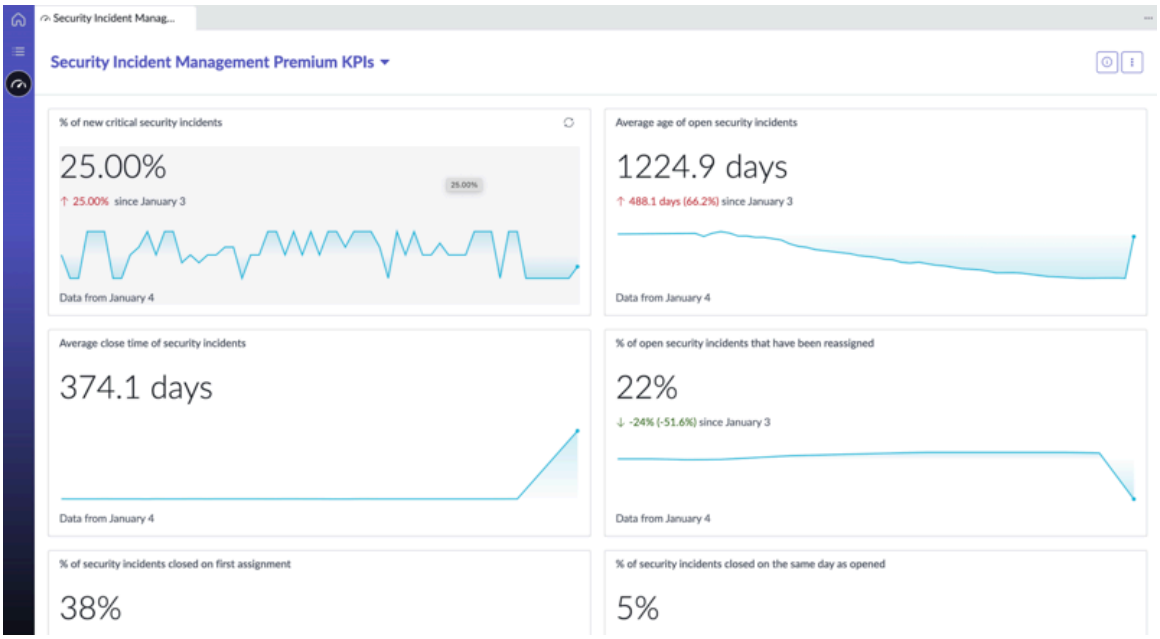
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , affichée sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **les KPI Premium de Réponse aux incidents de sécurité** dans la liste déroulante.



4. Consultez le tableau de bord des KPI de Réponse aux incidents de sécurité Premium pour connaître les actions ultérieures.
   Pour obtenir des informations détaillées sur le tableau de bord des KPI de Security Incident Response Premium, consultez le tableau de bord de Security Incident Management Premium

Afficher le tableau de bord Analyse contextuelle - SI

Grâce à ce tableau de bord, les gestionnaires et les analystes peuvent afficher les incidents de sécurité ouverts, l'âge moyen des incidents de sécurité ouverts, le délai moyen de clôture des incidents de sécurité, le pourcentage d'incidents de sécurité qui ont été ouverts et fermés le même jour et le pourcentage des incidents qui n'ont pas été mis à jour au cours des 5 derniers jours et 30 jours.

Avant de commencer

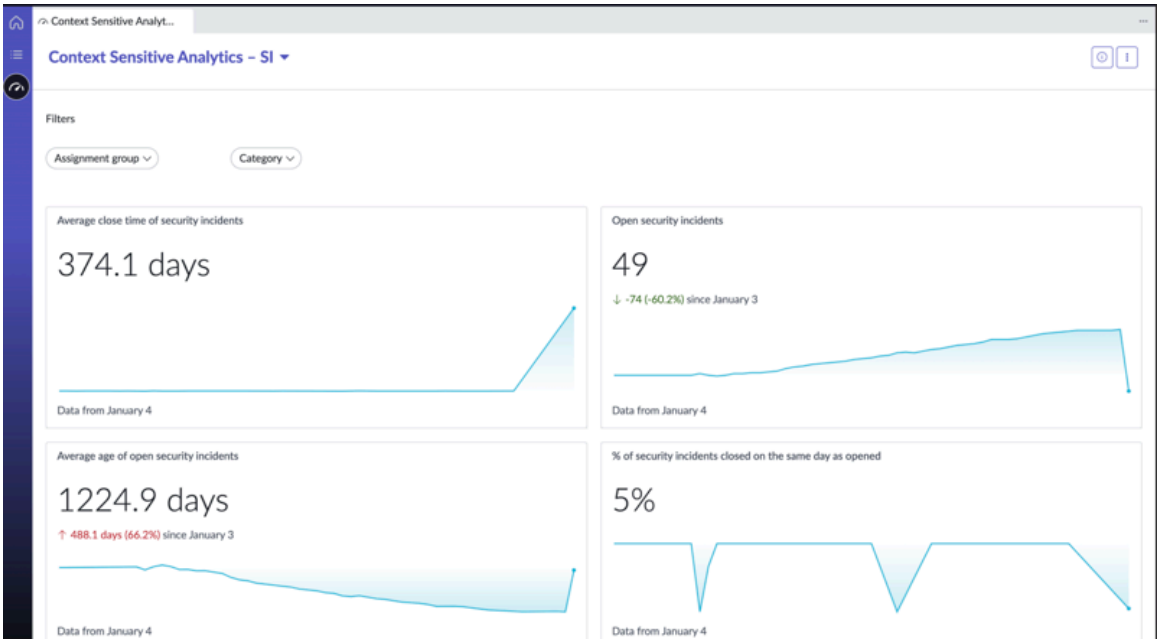
Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , affichée sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Analyse contextuelle : SI** dans la liste déroulante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Consultez le tableau de bord Analyse contextuelle : SI pour connaître les actions à suivre.

Afficher le tableau de bord des CISO

Ce tableau de bord fournit aux responsables de la sécurité de l'information (CISO) une vue d'ensemble approfondie des incidents de sécurité et des tendances des incidents hebdomadaires sur l'instance sous la forme de graphiques graphiques. Ces graphiques vous aident à visualiser et analyser efficacement les performances du centre des opérations de sécurité (SOC).

Avant de commencer

- Rôle requis : sn_si.admin et sn_si.ciso : modifier et afficher les incidents.
- Assurez-vous que l'application Analyse des performances pour Réponse aux incidents de sécurité est installée.

Pourquoi et quand exécuter cette tâche

Remarque : Le tableau de bord du CISO et le tableau de bord de vue d'ensemble du CISO étaient deux éléments différents dans l'interface utilisateur classique. Mais maintenant, les capacités des deux tableaux de bord ont été fusionnées sous le tableau de bord CISO.

Le tableau de bord CISO fournit chaque semaine des informations clés sur vos incidents de sécurité. Vous pouvez configurer des indicateurs et collecter des instantanés de données des incidents correspondant aux conditions dans les propriétés de l'indicateur. Les données collectées sont ensuite visualisées à l'aide de widgets dans le tableau de bord.

Vous pouvez visualiser les tendances hebdomadaires à l'aide des widgets du tableau de bord CISO. Les données ou statistiques relatives aux tendances de vos incidents de sécurité sont collectées à partir des propriétés de l'indicateur d'incidents hebdomadaires définies par l'organisation. Vous pouvez obtenir des aperçus clés à l'aide des graphiques suivants :

- **Durée moyenne pour l'identification (hebdomadaire)** : ce graphique illustre la durée hebdomadaire moyenne nécessaire pour identifier un incident de sécurité.
- **Temps moyen pour contenir (hebdomadaire)** : ce graphique illustre le temps hebdomadaire moyen nécessaire pour contenir un incident de sécurité.

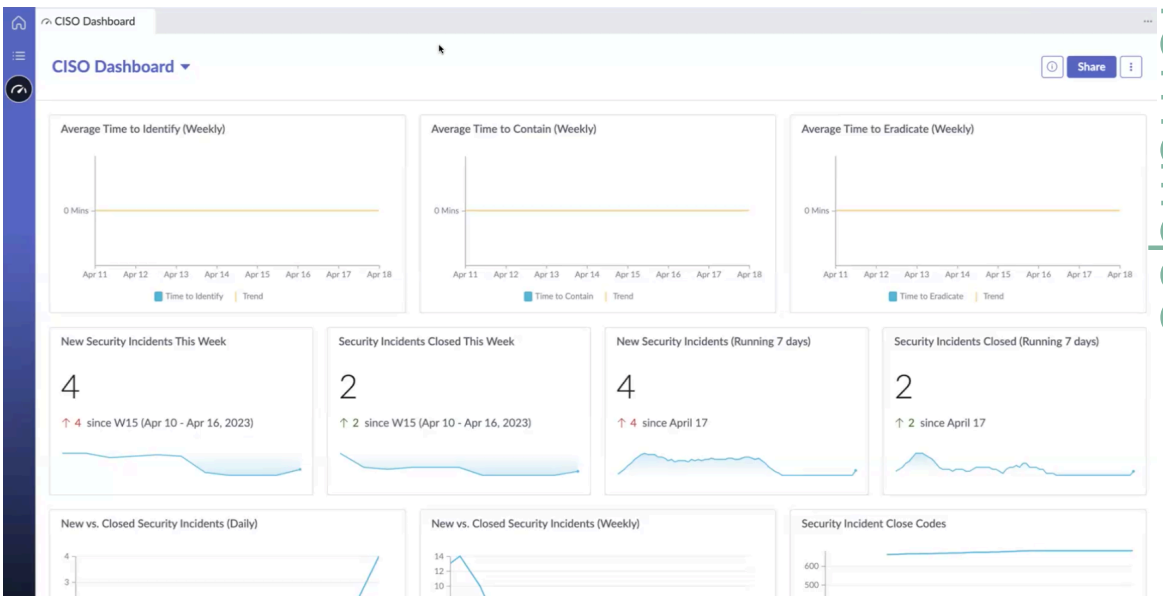
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Durée moyenne pour l'élimination (hebdomadaire)** : ce graphique illustre la durée hebdomadaire moyenne nécessaire pour supprimer un incident de sécurité.
- **Nouveaux incidents de sécurité cette semaine** : ce graphique illustre le nombre de nouveaux incidents de sécurité cette semaine.
- **Incidents de sécurité fermés cette semaine** : ce graphique illustre le nombre d'incidents de sécurité fermés cette semaine.
- **Nouveaux incidents de sécurité (sur 7 jours)** : ce graphique illustre le nombre de nouveaux incidents de sécurité qui s'exécutent pendant une semaine.
- **Incidents de sécurité clôturés (sur 7 jours)** : ce graphique illustre le nombre de nouveaux incidents de sécurité qui sont fermés mais en cours d'exécution pendant une semaine.
- **Incidents nouveaux par rapport aux incidents fermés (quotidien)** : ce graphique illustre la comparaison entre les nouveaux incidents de sécurité quotidiens et les incidents de sécurité fermés quotidiens.
- **Incidents nouveaux par rapport aux incidents fermés (hebdomadaire)** : ce graphique illustre la comparaison entre les nouveaux incidents de sécurité hebdomadaires et les incidents de sécurité fermés hebdomadaires.
- **Codes fermés des incidents de sécurité** : ce graphique illustre les codes fermés des incidents de sécurité.

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône **Tableaux de bord SIR** sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Tableau de bord du CISO** dans la liste déroulante.



4. Affichez le tableau de bord CISO pour les actions suivantes.

Afficher le tableau de bord Vue d'ensemble de la génération de rapports CISO

Ce tableau de bord fournit aux responsables de la sécurité de l'information (CISO) une vue d'ensemble des rapports de haut niveau sur les incidents de sécurité et les tendances des incidents hebdomadaires sur l'instance sous la forme de graphiques graphiques. Ces

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

graphiques vous aident à visualiser et analyser efficacement les performances du centre des opérations de sécurité (SOC).

Avant de commencer

Rôle requis : sn_si.admin et sn_si.ciso : modifier et afficher les incidents.

Pourquoi et quand exécuter cette tâche

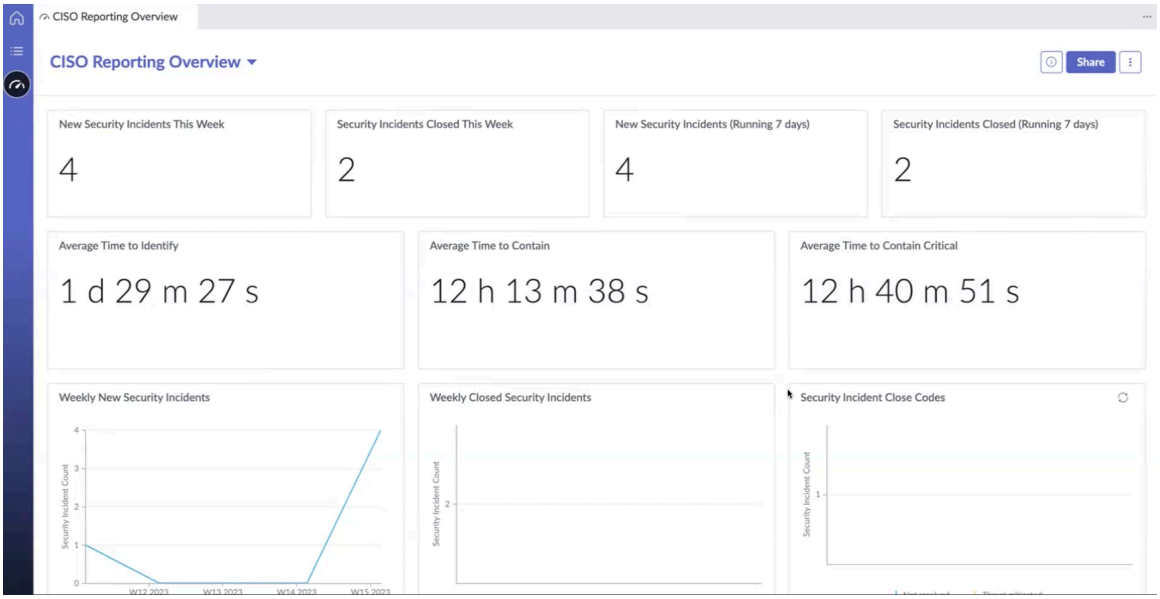
Le tableau de bord Vue d'ensemble de la génération de rapports CISO fournit des informations clés sur les incidents de sécurité sur une base hebdomadaire, et vous pouvez visualiser les tendances hebdomadaires à l'aide de widgets. Vous pouvez obtenir des informations clés sur la génération de rapports CISO à l'aide des graphiques suivants :

- **Nouveaux incidents de sécurité de cette semaine** : cette vignette affiche le rapport sur le nombre de nouveaux incidents de sécurité de cette semaine.
- **Incidents de sécurité fermés cette semaine** : cette vignette affiche le rapport sur le nombre d'incidents de sécurité fermés cette semaine.
- **Nouveaux incidents de sécurité (sur 7 jours)** : cette mosaïque affiche le rapport du nombre de nouveaux incidents de sécurité en cours d'exécution pendant une semaine.
- **Incidents de sécurité clôturés (sur 7 jours)** : cette mosaïque affiche le rapport sur le nombre de nouveaux incidents de sécurité fermés, mais en cours d'exécution pendant une semaine.
- **Délai moyen d'identification** : cette mosaïque affiche le rapport sur le temps hebdomadaire moyen nécessaire pour identifier les incidents de sécurité.
- **Durée moyenne de confinement** : cette mosaïque affiche le rapport sur le temps hebdomadaire moyen nécessaire pour contenir les incidents de sécurité.
- **Délai moyen pour contenir critique** : cette mosaïque affiche le rapport sur le temps hebdomadaire moyen nécessaire pour contenir les incidents de sécurité critiques.
- **Nouveaux incidents de sécurité hebdomadaires** : ce graphique illustre le rapport des nouveaux incidents de sécurité hebdomadaires.
- **Incidents de sécurité fermés chaque semaine** : ce graphique illustre le rapport des incidents de sécurité fermés chaque semaine.
- **Codes fermés des incidents de sécurité** : ce graphique illustre le rapport des codes fermés des incidents de sécurité.

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône **Tableaux de bord SIR** sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Vue d'ensemble de la génération de rapports CISO** dans la liste déroulante.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Affichez le tableau de bord Reporting CISO pour connaître les actions à suivre.

Afficher le tableau de bord de vue d'ensemble du gestionnaire d'incidents de sécurité

Ce tableau de bord fournit aux gestionnaires une vue d'ensemble des incidents de sécurité critiques ou haute priorité au niveau de l'équipe, des SLA qui arrivent à expiration dans 24 heures et des tendances des incidents hebdomadaires sur l'instance sous la forme de rapports et de graphiques graphiques.

Avant de commencer

Rôle requis :

- sn_si.admin : modifier et afficher le tableau de bord.
- sn_si.manager : afficher le tableau de bord.

Pourquoi et quand exécuter cette tâche

Vous pouvez analyser les incidents de sécurité critiques ou haute priorité, ou SLA qui requièrent une attention immédiate. Vous pouvez également visualiser les tendances hebdomadaires à l'aide des widgets du tableau de bord Vue d'ensemble du gestionnaire d'incidents de sécurité. Les données ou statistiques relatives aux tendances hebdomadaires ou mensuelles de vos incidents de sécurité sont collectées à partir des tables d'incidents définies par l'organisation. Vous pouvez obtenir des aperçus clés à l'aide des graphiques suivants :

- **Incidents de sécurité critique de l'équipe** : cette vignette affiche le nombre d'incidents de sécurité critiques pour l'équipe cette semaine.
- **Incidents de sécurité élevée de l'équipe** : cette vignette affiche le nombre d'incidents de sécurité élevée pour l'équipe cette semaine.
- **SLA arrivant à expiration dans les 24 heures** : cette mosaïque affiche le nombre de SLA qui arriveront à expiration dans les 24 heures.
- **Délai moyen d'identification** : cette mosaïque affiche le temps hebdomadaire moyen nécessaire pour identifier les incidents de sécurité.
- **Durée moyenne de confinement** : cette mosaïque affiche le temps hebdomadaire moyen nécessaire pour contenir les incidents de sécurité.

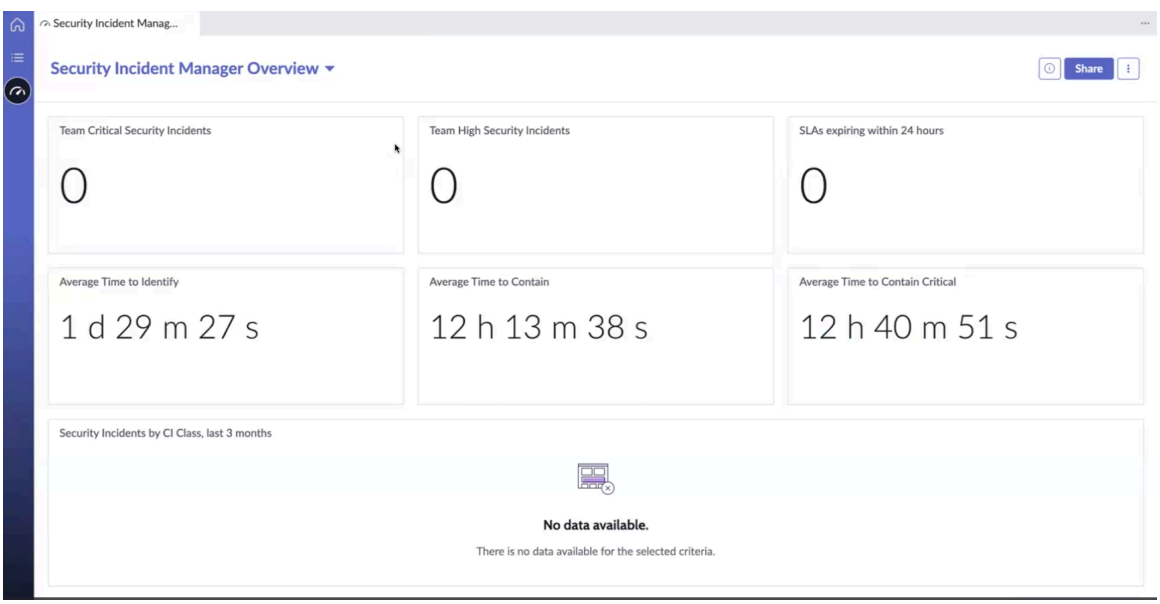
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Délai moyen pour contenir critique** : cette mosaïque affiche le temps hebdomadaire moyen nécessaire pour contenir les incidents de sécurité critiques.
- **Incident de sécurité par classe CI, 3 derniers mois** : ce graphique illustre les tendances de tous les incidents de sécurité basés sur la classe CI pour les trois derniers mois.
- **Tendance de tous les incidents de sécurité par catégorie** : ce graphique illustre les tendances de tous les incidents de sécurité par catégorie.
- **Tendance de tous les incidents de sécurité par priorité** : ce graphique illustre les tendances de tous les incidents de sécurité en fonction de la priorité.

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône **Tableaux de bord SIR** sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Vue d'ensemble du gestionnaire d'incidents de sécurité** dans la liste déroulante.



4. Consultez la vue d'ensemble du gestionnaire d'incidents de sécurité pour les actions à suivre.

Traduction automatique

Afficher le tableau de bord d'intégrité de Security Incident Response

La fonctionnalité de tableau de bord d'intégrité de Security Incident Response fournit une vue centralisée des aspects critiques liés à l'implémentation du processus de réponse aux incidents, aux problèmes/erreurs rencontrés et aux mesures des performances. Il s'agit d'un outil essentiel pour surveiller et optimiser l'efficacité des capacités de réponse aux incidents de sécurité d'une organisation.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.analyst ou sn_si.analytics_read : afficher le tableau de bord.

Pourquoi et quand exécuter cette tâche

Vous pouvez surveiller l'intégrité des incidents de sécurité à l'aide des widgets et des graphiques de tendance de chaque application. Ces statistiques présentent un score d'intégrité complet détaillant l'état de configuration et l'efficacité du rattrapage au sein

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

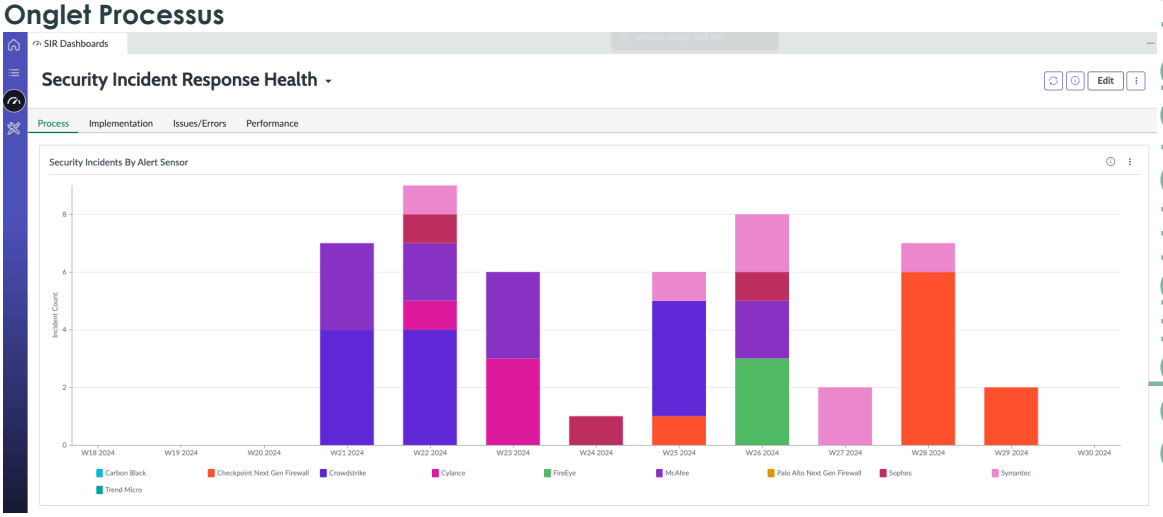
des applications SIR. Le tableau de bord Intégrité de Security Incident Response prend en charge les quatre onglets suivants :

- **Processus** : cet onglet affiche un résumé de tous les incidents provenant de différents capteurs d'alerte regroupés chaque semaine.
- **Implémentation** : cet onglet affiche les personnalisations que les clients effectuent dans leurs instances (includes de script, règles métier, flux et mises à niveau).
- **Problèmes/Erreurs** : cet onglet affiche des widgets mettant en évidence les erreurs dans les processus d'intégration, les discordances lors de l'ingestion des données d'incident brutes, les erreurs HTTP sortantes dans les applications SIR et tout problème survenant lors de l'exécution des playbooks.
- **Performance** : cet onglet affiche les problèmes de performances dans les applications SIR, notamment la lenteur des requêtes de performance, des règles métier et des scripts.

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez l'icône **Tableaux de bord SIR** sur la page d'accueil de l'espace de travail SIR.
3. Sélectionnez **le tableau de bord Intégrité de Security Incident Response** dans la liste déroulante.
4. Sélectionnez l'onglet **Processus** pour afficher le nombre d'incidents de sécurité qui ont été déclenchés chaque semaine pour chaque capteur d'alerte du graphique.

Onglet Processus



Vous pouvez effectuer les tâches suivantes :

a. Sélectionnez un capteur d'alerte sur le graphique pour afficher les détails KPI du nombre d'incidents de sécurité déclenchés par les capteurs d'alerte en une semaine.

b. Pour obtenir les détails des KPI d'une semaine particulière, utilisez l'option **Calendrier** .

c. Pour comparer les incidents de sécurité déclenchés par le capteur d'alerte, sélectionnez l'option **Comparer les enregistrements** .

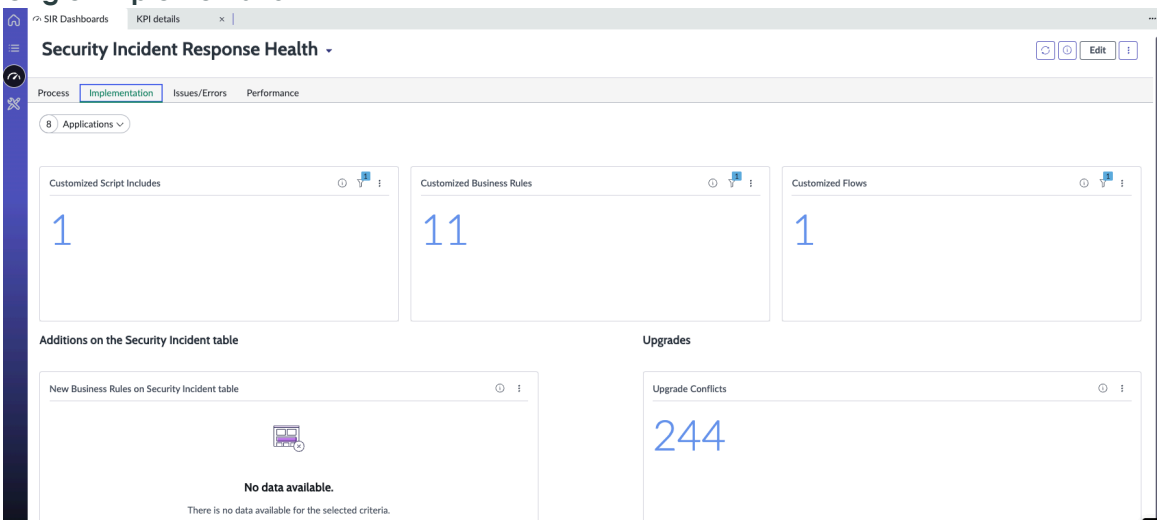
d. Pour utiliser le type de graphique, les séries chronologiques ou l'analyse, sélectionnez les **options de graphique**.

5. Sélectionnez l'onglet **Implémentation** pour afficher le nombre de personnalisations qui ont été créées pour les incidents de sécurité dans les applications Réponse aux incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Implémentation



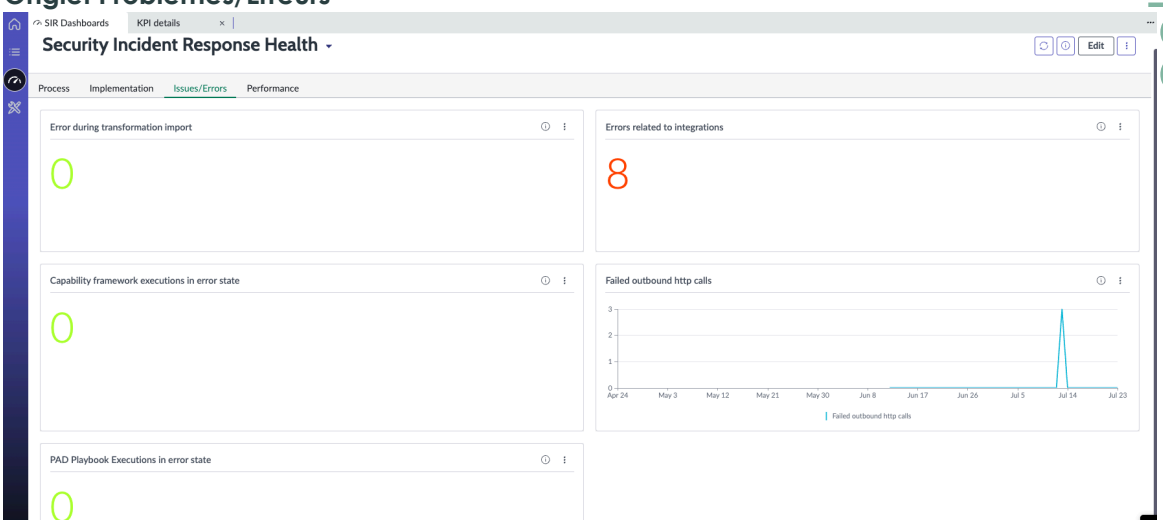
Onglet Implémentation :

Vous pouvez afficher le tableau de bord agrégé correspondant au nombre de personnalisations créées pour chaque application Incident Response.

- **Includes de script personnalisés** : ce widget affiche le nombre de scripts personnalisés qui ont été ajoutés en fonction de vos besoins dans les applications SIR.
- **Règles métier personnalisées** : ce widget affiche le nombre de règles métier personnalisées qui ont été ajoutées en fonction de vos besoins dans les applications SIR.
- **Flux personnalisés** : ce widget affiche le nombre de flux personnalisés qui ont été ajoutés en fonction de vos besoins dans les applications SIR.
- **Nouvelle règle métier sur la table Incident de sécurité** : ce widget affiche le nombre de règles métier qui ont été créées dans la table Incident de sécurité.
- **Conflits de mise à niveau** : ce widget affiche le nombre de conflits qui ont été déclenchés pendant les mises à niveau dans les applications SIR.

6. Sélectionnez l'onglet **Problèmes/Erreurs** pour afficher le nombre de problèmes ou d'erreurs qui ont été déclenchés dans les applications Réponse aux incidents de sécurité.

Onglet Problèmes/Erreurs



Onglet Problèmes/Erreurs :

Traduction automatique

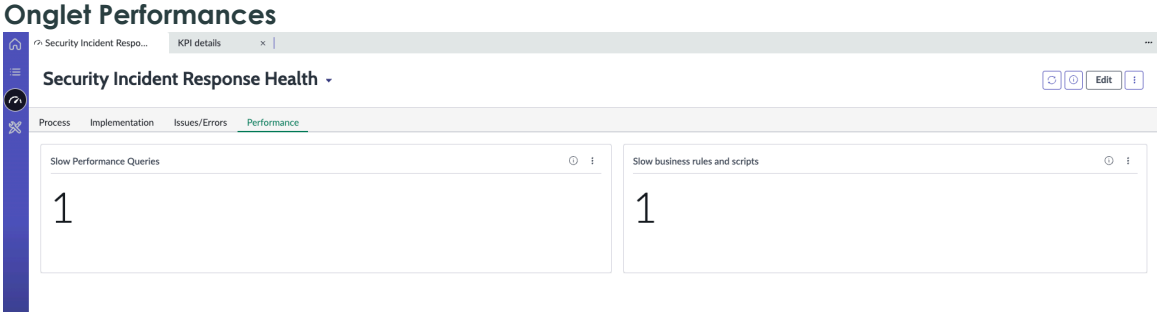
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez afficher le tableau de bord agrégé pour les problèmes ou les erreurs dans les applications Réponse aux incidents de sécurité.

- **Erreurs lors de l'importation** de transformation : ce widget affiche le nombre d'erreurs qui ont été déclenchées pendant l'importation de transformation dans les applications SIR.
- **Erreurs liées aux intégrations** : ce widget affiche le nombre d'erreurs qui ont été déclenchées au cours des intégrations SIR.
- **Exécutions du cadre de travail d'aptitude en état d'erreur** : ce widget affiche le nombre d'erreurs qui ont été déclenchées pendant les exécutions du cadre de travail d'aptitude dans les applications SIR.
- **Échec des appels HTTP sortants** : ce widget affiche le nombre d'échecs des appels HTTP sortants qui ont été déclenchés dans les applications SIR.
- **Exécutions de playbook PAD en état d'erreur** : ce widget affiche le nombre d'erreurs d'exécution de playbook PAD qui ont été déclenchées dans les applications SIR.

7. Sélectionnez l'onglet **Performance** pour afficher le nombre de problèmes de performance qui ont été déclenchés dans les applications Security Incident Response.

Onglet Performances



Onglet Performance :

Vous pouvez afficher le tableau de bord agrégé pour les problèmes de performances dans les applications Réponse aux incidents de sécurité.

- **Requêtes de performances lentes** : ce widget affiche le nombre de requêtes de performances dans les applications SIR dont le temps d'exécution moyen est supérieur à 10 ms et dont la moyenne est calculée sur 1 000 exécutions ou plus.
- **Règles métier et scripts lents** : ce widget affiche le nombre de règles métier et de scripts dans les applications SIR dont le temps d'exécution moyen est supérieur à 10 ms et dont la moyenne est calculée sur 1 000 exécutions ou plus.

8. Vous pouvez utiliser l'icône **Actualiser** pour actualiser les données dans le tableau de bord d'intégrité de Security Incident Response.
9. Vous pouvez utiliser l'icône **Afficher les détails du tableau de bord** pour afficher les détails du tableau de bord d'intégrité de Security Incident Response.
10. Vous pouvez utiliser l'option **Modifier** pour modifier les détails du tableau de bord d'intégrité de Security Incident Response.
11. Vous pouvez utiliser l'option **Plus** pour effectuer des actions supplémentaires sur le tableau de bord d'intégrité de Security Incident Response.

Création d'un incident de sécurité

Les incidents de sécurité peuvent être créés manuellement à partir du formulaire ou automatiquement via des événements de sécurité reçus d'outils de surveillance des alertes tiers intégrés, tels que Splunk.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Les dernières fonctionnalités de sont Réponse aux incidents de sécurité exclusivement disponibles dans le Espace de travail de la Réponse aux incidents de sécurité. Veuillez installer ou mettre à niveau vers la dernière Réponse aux incidents de sécurité version pour Espace de travail de la Réponse aux incidents de sécurité accéder et exploiter des fonctionnalités telles que Transfert d'équipe, Calculateur de score de risque, etc.

Si vous disposez d'un rôle de sécurité, vous pouvez utiliser l'une des méthodes suivantes pour créer manuellement des incidents de sécurité.

Méthodes de création manuelle d'incidents de sécurité

Méthode	Description
Créé manuellement à partir de la liste d'incidents de sécurité	Dans la liste des incidents de sécurité, cliquez sur **Nouveau** pour créer un incident de sécurité.
Créé manuellement à partir du catalogue des incidents de sécurité	Vous pouvez créer des incidents de sécurité en sélectionnant l'une des catégories de menaces de sécurité définies dans le catalogue des incidents de sécurité.
Gestion des incidents	Sur le formulaire d'incident dans Gestion des incidents, cliquez sur **Créer un incident de sécurité** pour créer un nouvel incident de sécurité.
Converti manuellement à partir d'une demande de sécurité	Sur le formulaire de demande de sécurité, cliquez sur **Convertir en incident de sécurité** pour créer un nouvel incident de sécurité.
Créé manuellement à partir d'une alerte Event Management	Dans le formulaire Alertes de Gestion des événements, cliquez sur **Créer un incident de sécurité** pour créer un nouvel incident de sécurité à partir d'une alerte.
Créé manuellement à partir d'une alerte	Sur le formulaire Alerte de Gestion des événements, cliquez sur **Créer un incident de sécurité** pour créer un nouvel incident de sécurité.
Converti manuellement à partir d'un enregistrement de vulnérabilité (si le module d'extension Vulnerability Response est activé)	Sur le formulaire Éléments de vulnérabilité, cliquez sur **Créer un incident de sécurité** pour créer un nouvel incident de sécurité.

Création automatique d'incidents de sécurité

En règle générale, les administrateurs de sécurité sont responsables de la configuration des règles d'alerte utilisées pour générer automatiquement des incidents de sécurité.

Méthode d'administration de sécurité pour la création des incidents de sécurité

Méthode	Description
Créé automatiquement à l'aide de règles d'alerte	Les incidents de sécurité peuvent être créés en fonction des règles d'alerte définies dans la gestion des événements de votre application de centre de données .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Création manuelle de l'incident de sécurité

Vous pouvez créer un incident de sécurité à partir du formulaire d'incident de sécurité, ainsi que de plusieurs autres formulaires.

Vous pouvez créer des incidents de sécurité basés sur un enregistrement existant à partir des formulaires suivants :

- À partir de n'importe quelle liste d'incidents de sécurité
- Formulaire d'incident
- Gestion des événements Formulaire Alerte
- Formulaire des éléments vulnérables
- Formulaire de demande de sécurité

Créer un incident de sécurité à partir de la liste Incident de sécurité

Outre les méthodes automatiques de création des incidents de sécurité, vous pouvez les créer manuellement, selon les besoins.

Cette vidéo montre une vue d'ensemble visuelle de la création d'un incident de sécurité à partir de la liste Incidents de sécurité.

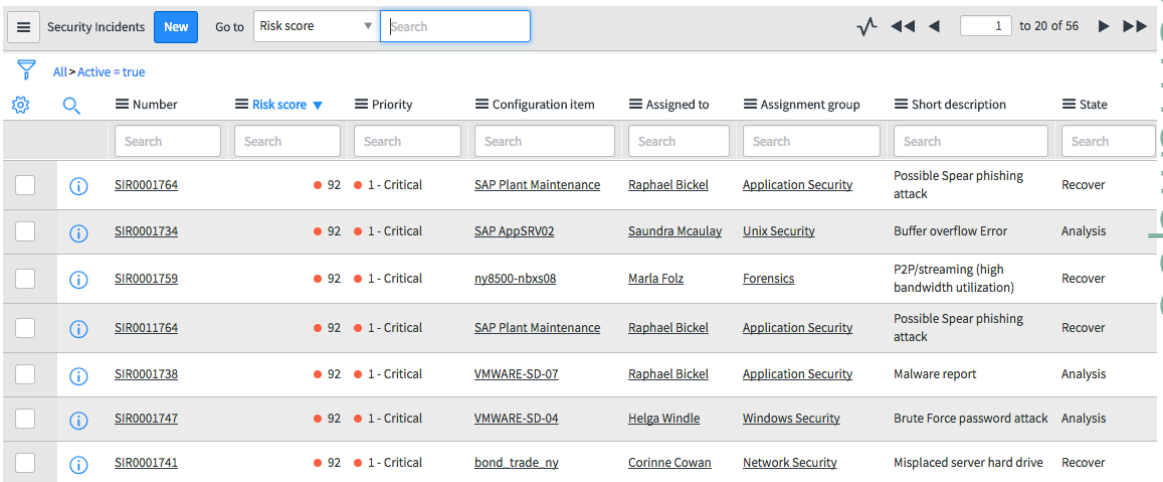
Créer un incident de sécurité à partir de la liste Incident de sécurité

Avant de commencer

Rôle requis : sn_si.basic

Procédure

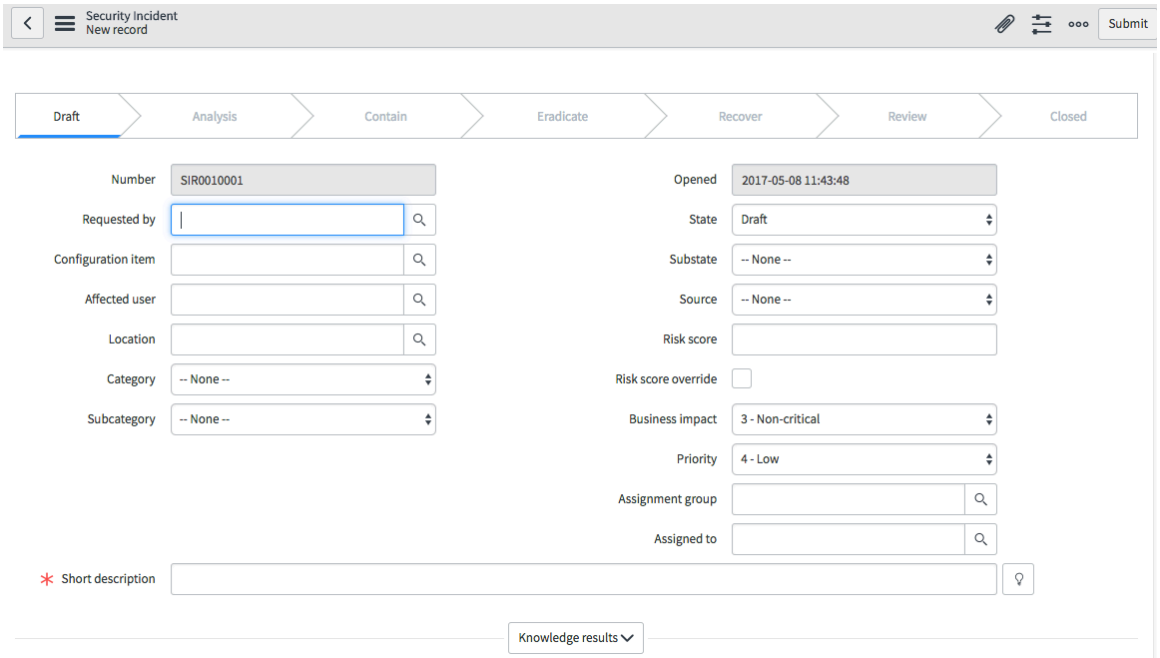
1. Accédez à n'importe quelle liste d'incidents de sécurité (par exemple, **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**).



2. Cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Renseignez les champs du formulaire.

Champ	Description
Sélectionner une balise de sécurité	Si nécessaire, sélectionnez une balise de sécurité pour ajouter des métadonnées à l'enregistrement ou identifier qui doit avoir accès à cet enregistrement d'incident de sécurité. Ce champ s'affiche uniquement une fois que l'incident de sécurité a été enregistré.
Numéro	[Lecture seule] Le numéro d'incident de sécurité.
Demandés par	La personne demandant l'exécution du travail.
ID d'élément de configuration	Serveur, ordinateur, routeur ou autre élément de configuration affecté par le problème de sécurité.
Utilisateur affecté	La personne affectée par le problème de sécurité.
Emplacement	L'emplacement du demandeur ou de la ressource. Si aucun **élément de configuration** n'est sélectionné, ce champ est pré-rempli avec l'emplacement du demandeur.
Catégorie	Catégorie qui identifie le type de problème de sécurité. Si une catégorie est sélectionnée, un workflow d'analyse de ce problème est exécuté lorsque l'enregistrement est enregistré. Par exemple, si vous sélectionnez **Déni de service**, le workflow Incident de sécurité - Déni de service - Modèle est exécuté. Pour plus d'informations, consultez Modèles de workflow Security Incident Response.
Sous-catégorie	Sous-catégorie qui précise le problème.
Ouverts	[Lecture seule] Affiche la date et l'heure d'ouverture de l'incident.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
État	État actuel de l'incident de sécurité. Lors de la création d'un incident de sécurité, ce champ est défini par défaut sur **Brouillon**.
Sous-état	Identifie si l'incident de sécurité inclut un problème ou un changement en attente.
Source	Identifie la source de l'incident de sécurité, par exemple un e-mail, un appel téléphonique ou une surveillance du réseau.
Capteur d'alerte	Intégration de sécurité via laquelle vous ingérez les données d'alerte ou d'événement telles que CarbonBlack, CrowdStrike, McAfee, etc.
Règle d'alerte	Règle du produit de sécurité qui a déclenché la création de cet incident de sécurité.
Score du risque	Affiche le score de risque calculé pour cet incident de sécurité. La valeur est basée sur la priorité de l'incident de sécurité, le type d'incident de sécurité (déni de service, harponnage ou activité de code malveillant) et le nombre de sources qui ont déclenché un score de réputation échoué sur un indicateur. Le score de risque aide à hiérarchiser le travail des analystes sur les incidents de sécurité. Trois propriétés d'incident de sécurité vous permettent de désigner un point à code couleur à afficher à côté du score de risque dans la vue de liste afin de les rendre plus facilement identifiables. Si vous apportez des modifications à certains champs de l'incident de sécurité, tels que **l'impact sur l'entreprise** ou la **priorité**, et que vous sauvegardez l'enregistrement, le **score de risque** est automatiquement recalculé et affiché. Le changement est également reflété dans les notes de travail et sur la liste connexe des audits de score de risque. **Remarque :** Le score de risque est également recalculé lorsque les utilisateurs affectés sont associés à un incident de sécurité, à des services affectés ou à des éléments vulnérables. Vous pouvez également saisir manuellement un nouveau **score de risque**. Cela peut être utile si vous souhaitez qu'un incident de sécurité particulier reste en tête de la liste des incidents de sécurité que vous analysez. Si vous saisissez un nouveau **score de risque**, la case **Remplacer le score de risque** est automatiquement cochée. Quels que soient les changements apportés à l'incident de sécurité, un score de risque saisi manuellement n'est pas automatiquement recalculé. **Remarque :** Si vous avez mis à niveau votre instance à partir d'une version antérieure, les scores de risque ont été calculés pour tous vos incidents de sécurité ouverts. Pour plus d'informations, consultez Comprendre les calculateurs d'incidents de sécurité.
Remplacement du score des risques	Cochez cette case pour remplacer la mise à jour automatique du score de risque. Le remplacement sera reflété dans les notes de travail.
Impact sur l'activité	Sélectionnez l'importance de cet incident de sécurité pour votre entreprise. La valeur par défaut est Non critique. Si, après l'enregistrement de l'incident de sécurité, vous modifiez la valeur dans les champs **Priorité / ou Risque**, **l'impact sur l'entreprise** est recalculé.

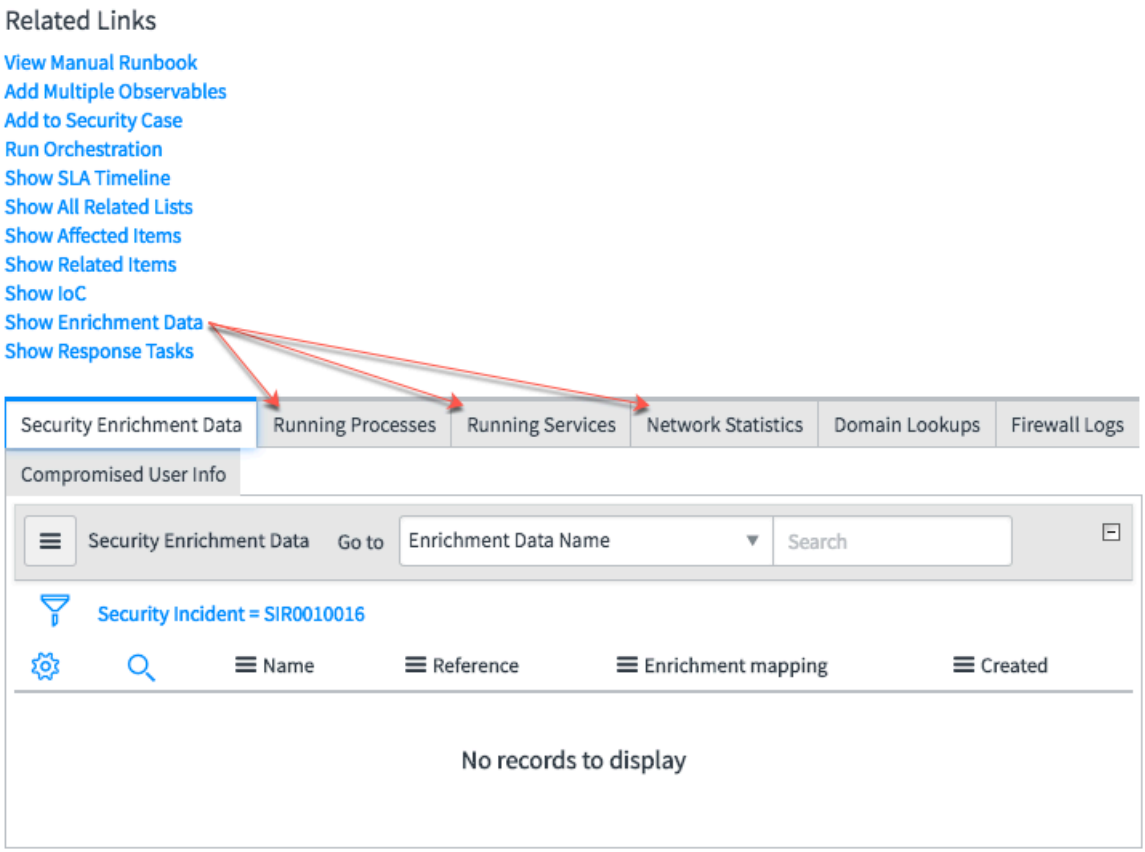
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Priorité	Sélectionnez l'ordre dans lequel traiter cet incident de sécurité, en fonction de l'urgence. Si cette valeur est modifiée après la sauvegarde de l'enregistrement, cela peut affecter le calcul de **l'impact sur l'entreprise** .
Groupe d'affectation	Groupe auquel cet incident de sécurité est affecté.
Affecté à	Personne affectée à l'analyse de cet incident de sécurité. Les affectations peuvent être effectuées manuellement ou automatiquement. Pour plus d'informations, consultez Affectation des analystes de sécurité.
Description brève	Brève description de l'incident de sécurité.
Résultats de recherche dans la base de connaissances	Au fur et à mesure que vous saisissez la brève description, des liens vers des articles connexes de la base de connaissances s'affichent. L'analyse des informations pourrait résoudre votre problème.

4. Cliquez avec le bouton droit dans l'en-tête de l'enregistrement et sélectionnez **Enregistrer**. Si vous avez ajouté un nouveau CI à l'incident de sécurité, les workflows d'intégration suivants sont automatiquement exécutés :
   - Security Operations : workflow Obtenir les processus en cours d'exécution. Ce workflow récupère une liste des processus en cours d'exécution sur un élément de configuration (CI) à partir d'un hôte ou d'un point de terminaison.
   - Réponse aux incidents de sécurité : workflow Obtenir les services d'exécution. Ce workflow récupère une liste des services en cours d'exécution à partir des CI Windows.
   - Workflow Security Operations Integrations - Obtenir les statistiques réseau. Ce workflow récupère une liste de connexions réseau actives à partir d'un hôte ou d'un point de terminaison.
5. Pour afficher les informations récupérées par ces workflows, cliquez sur le lien connexe **Afficher les données d'enrichissement** , puis cliquez sur l'un des onglets indiqués.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Des workflows supplémentaires sont exécutés en fonction des intégrations tierces que vous avez activées comme suit Intégration de Security Operations Carbon Black : workflow Obtenir les processus en cours d'exécution

Information associée

Configurer Réponse aux incidents de sécurité

Créer un incident de sécurité à partir du catalogue des incidents de sécurité

Les utilisateurs de votre entreprise peuvent utiliser le catalogue des incidents de sécurité pour demander différents types d'analyses liées à la sécurité.

Avant de commencer

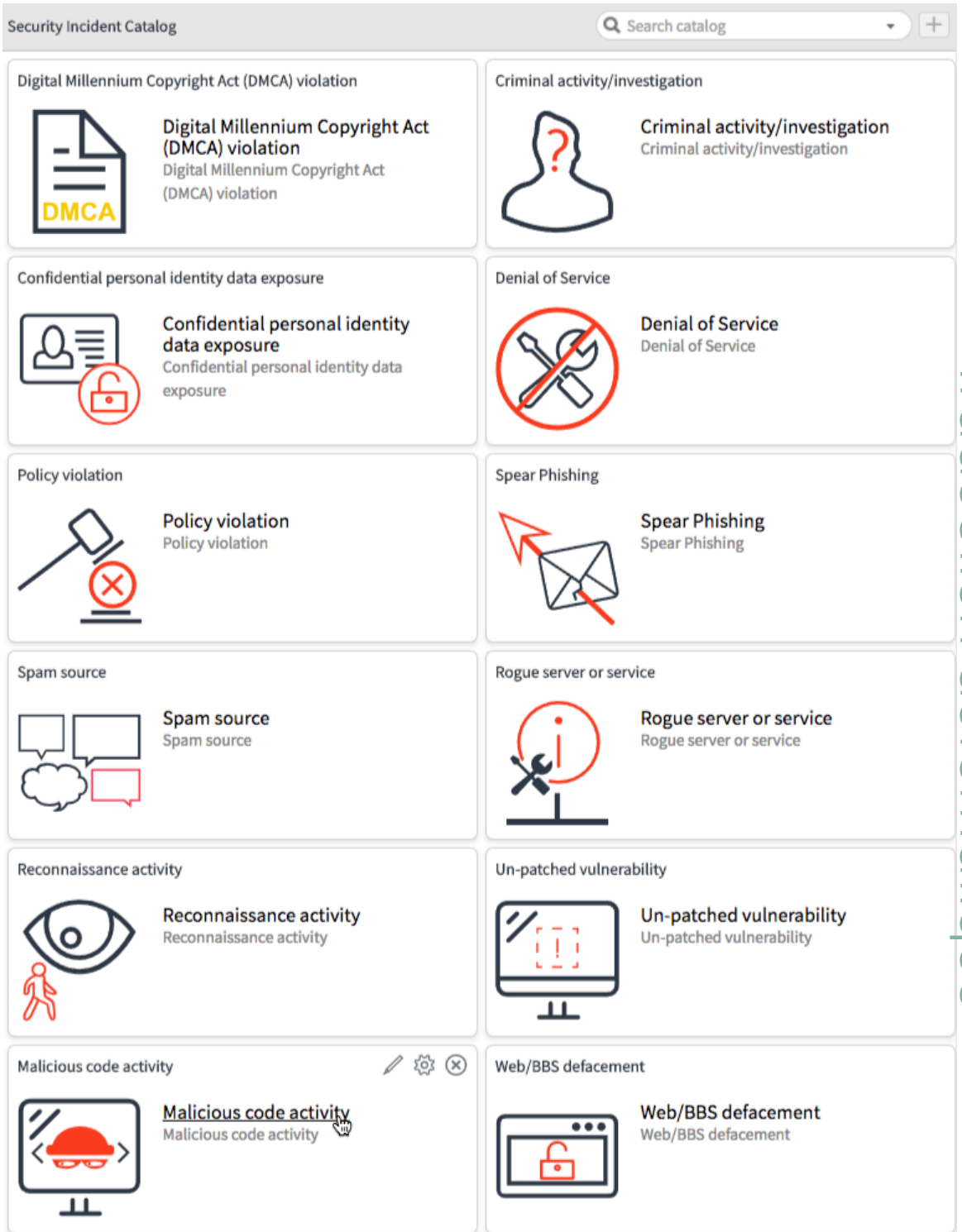
Rôle requis : aucun

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

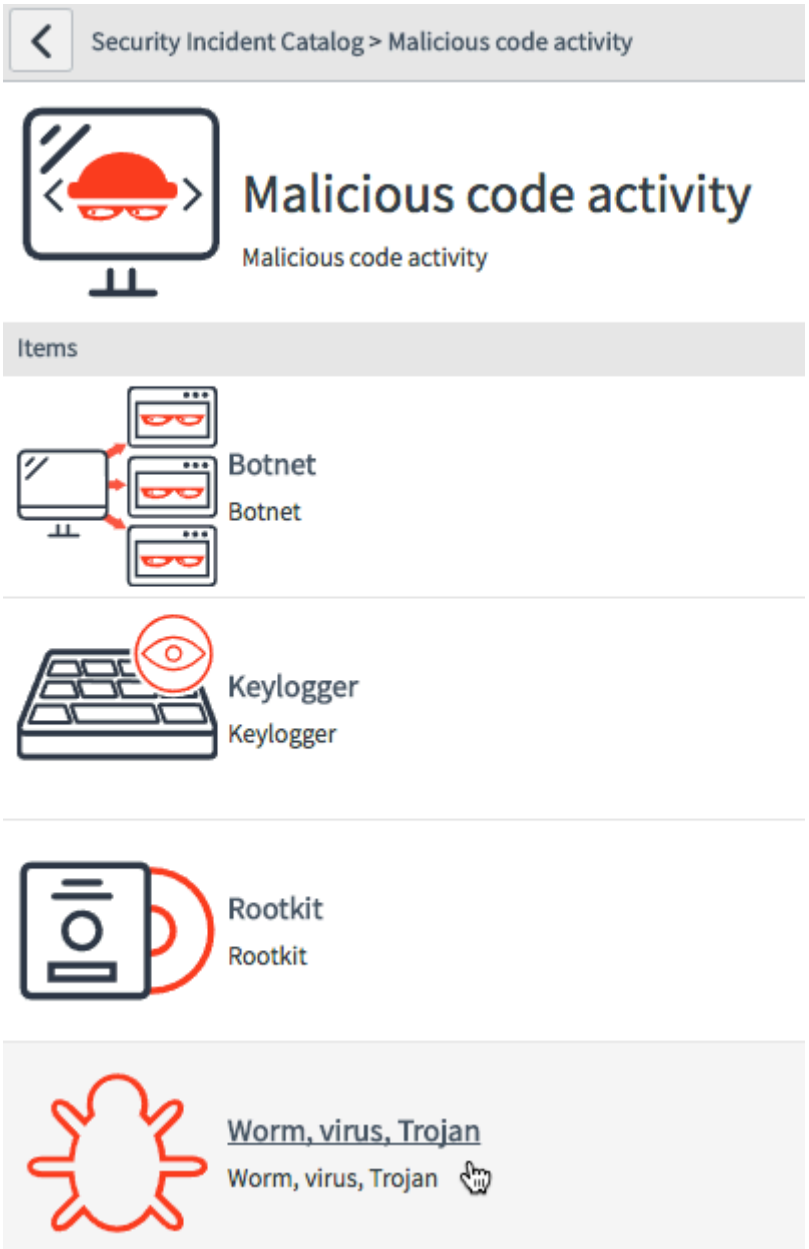
1. Accédez à la **Tout** > **Libre-service** > **Catalogue des incidents de sécurité**.



2. Cliquez sur l'élément de catalogue pour lequel vous souhaitez effectuer une demande. Si l'élément que vous avez sélectionné dans le catalogue principal contient des sous-catégories, la liste s'affiche. Dans l'exemple suivant, **Activité de code malveillant** a été sélectionnée.

Traduction automatique

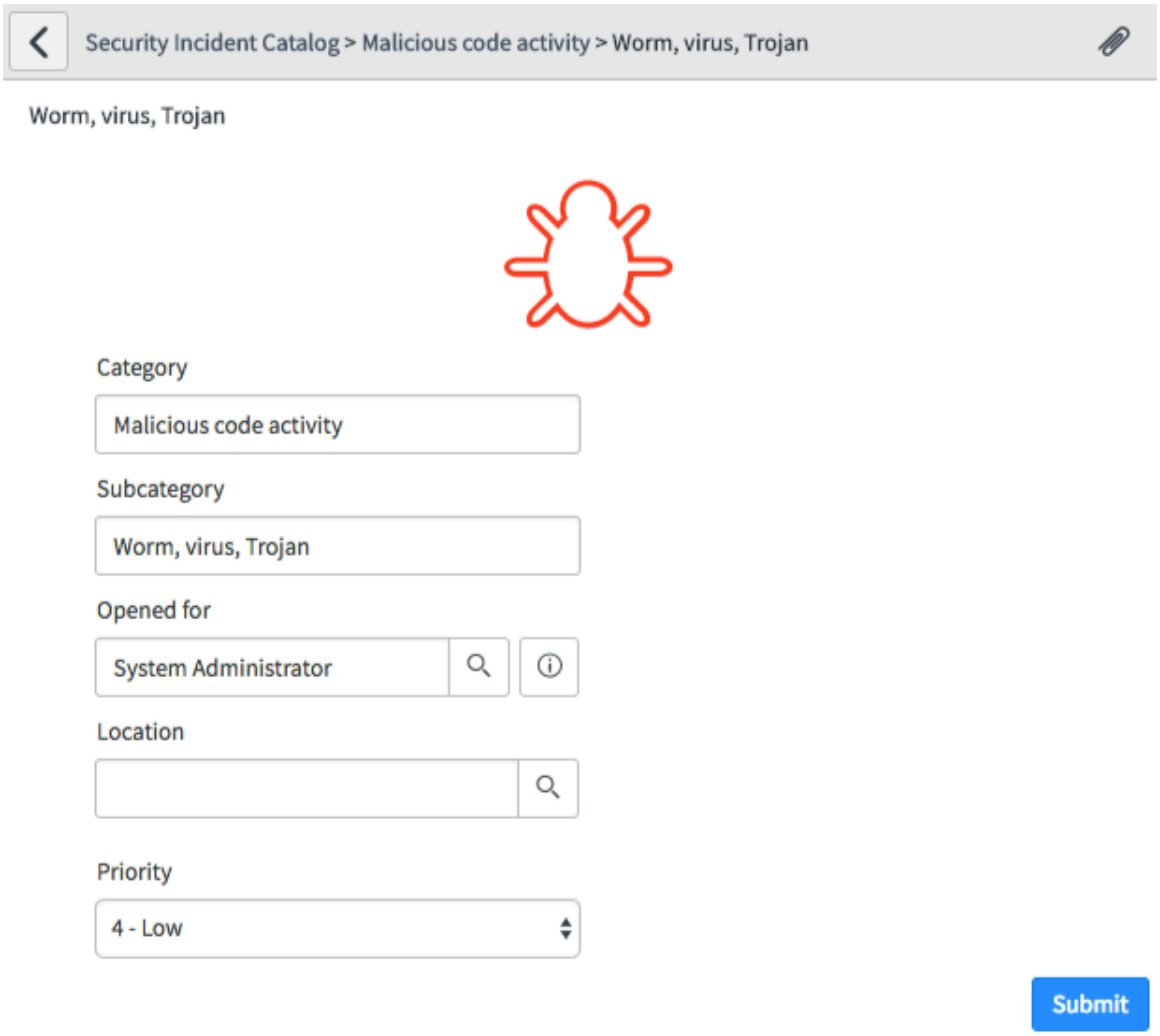
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur la sous-catégorie qui correspond le mieux au type de demande que vous souhaitez effectuer.
Dans cet exemple, la sous-catégorie **Ver, virus, cheval de Troie** a été sélectionnée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Saisissez les informations de la demande, puis cliquez sur **Soumettre**.
   La demande est envoyée à votre service des incidents de sécurité.
5. Une fois que vous avez soumis la demande, vous pouvez suivre sa progression en accédant à **Libre-service** > **Mes demandes**et en saisissant le numéro de demande.

Créer un incident de sécurité à partir d'une alerte de gestion des événements

Lorsque la gestion des événements est activée, vous pouvez créer manuellement des incidents de sécurité à partir du formulaire Alerte.

Avant de commencer

Le module d'extension Gestion des événements nécessite un abonnement séparé et doit être activé par le personnel ServiceNow. Ce module d'extension inclut des données de démonstration et active les modules d'extension connexes s'ils ne sont pas déjà activés. L'analyse de service est activée automatiquement lorsque la gestion des événements est activée.
Rôle requis : evt_mgmt_admin, evt_mgmt_operator ou evt_mgmt_user

Procédure

1. Accédez à la **Tout** > **Gestion des événements** > **Toutes les alertes**.
2. Cliquez sur le **numéro** d'alerte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Créer un incident de sécurité**.
4. Cliquez sur **Mettre à jour**.

Création automatique d'incidents de sécurité

Il est possible d'intégrer Réponse aux incidents de sécurité des outils de surveillance tiers, tels que Splunk, afin que les événements de sécurité importés à partir de ces outils génèrent automatiquement des incidents de sécurité. Vous pouvez également importer des données à partir d'outils tiers dans les alertes de sécurité.

Pour intégrer des outils de surveillance des alertes à Réponse aux incidents de sécurité, vous devez utiliser l'API REST pour écrire dans la table d'importation d'incidents de sécurité [sn_si_incident_import]. Ensuite, à l'aide des cartes de transformation **Incident de sécurité**, la table source des ensembles de données à importer est mappée aux champs de la table Incident de sécurité [sn_si.incident] cible.

Si vous tentez d'importer des enregistrements de CI qui ne sont pas reconnus par la carte de transformation, le script de carte de transformation vérifie l'enregistrement pour les éléments suivants (dans cet ordre) afin d'établir une correspondance :

- sys_id
- Nom CI :
- nom de domaine pleinement qualifié
- Adresse IP

Remarque : Si vous trouvez que la carte de **transformation de l'incident de sécurité** n'est pas adaptée à l'outil de surveillance des alertes tiers que vous utilisez, dupliquez-la, créez-en une nouvelle et modifiez les champs si nécessaire.

Incidents de sécurité créés à partir d'événements et d'alertes

Au fur et à mesure que les événements sont importés à partir d'outils de surveillance des alertes, ils sont d'abord traités et Event Management regroupés en alertes. Ces alertes peuvent être utilisées pour créer des incidents de sécurité basés sur des règles d'alerte personnalisables ou examinées manuellement pour sélectionner ces alertes à examiner en tant qu'incident de sécurité.

Vous trouverez un exemple de règle **d'alerte appelée Créer des incidents de sécurité à partir d'alertes critiques** dans le Règles d'alerte module de l'application Event Management . Cette règle d'alerte crée automatiquement des incidents de sécurité lorsque des événements critiques liés à la sécurité sont reçus depuis ou depuis ServiceNow des applications de surveillance tierces. Une fois l'incident de sécurité créé, il est mis à jour à mesure que de nouveaux événements sont reçus. Vous pouvez modifier le modèle de tâche dans la règle d'alerte pour changer les valeurs initiales de l'incident de sécurité créé par cette règle d'alerte. Pour gérer chaque variété distincte d'incidents de sécurité que vous souhaitez créer, vous pouvez définir d'autres règles d'alerte avec des conditions différentes.

Si vous êtes un utilisateur disposant du rôle d'administrateur de sécurité, vous pouvez également créer manuellement un incident de sécurité en cliquant sur le bouton **Créer un incident de sécurité** à partir d'une alerte suspecte.

Il est important que les événements reçus d'outils externes incluent les informations suivantes :

- Le nœud défini sur le nom, l'adresse IP ou l'sys_id du CI qui devient la ressource affectée.
- La classification des événements est définie sur Sécurité pour les distinguer des autres événements informatiques.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Description de l'événement, qui remplit la description de l'incident de sécurité.
- Les informations supplémentaires peuvent inclure toutes les informations supplémentaires qui ne rentrent pas dans les champs répertoriés précédemment ou d'autres champs d'événement, tels que la catégorie, les vecteurs d'attaque, l'URL de retour ou l'ID de corrélation. Le format est une chaîne qui répertorie les noms de champs ainsi que leurs valeurs, à l'aide du format JSON suivant :

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Remarque : Pour chaque paire de champ et de valeur, si le champ dans l'incident de sécurité où le nom de colonne correspond au fieldName est vide, il est défini sur fieldValue. Si le champ de l'incident de sécurité n'est pas vide, il n'est pas modifié. Dans les deux cas, l'événement et tous les champs et valeurs codés dans les informations supplémentaires sont enregistrés dans une entrée de notes de travail décrivant l'événement. Si rien ne change dans l'incident de sécurité, une entrée de note de travail n'est pas créée. Tous les champs d'un incident de sécurité, y compris les champs personnalisés que vous ajoutez à la table, peuvent être définis.

Données importées dans les alertes de sécurité

Lorsqu'un événement est créé avec davantage de données codées JSON, ces données sont importées dans n'importe quel champ dont le nom correspond au fieldName de cette valeur dans les données JSON.

Si votre logiciel de surveillance tiers (par exemple, Splunk) contient des données qui ne sont pas communes au système de base, vous pouvez ajouter de nouveaux champs à la table Alerte pour faciliter l'importation des données. Le format JSON pour l'importation de données dans les alertes est le même que celui utilisé pour créer des incidents de sécurité à partir d'événements et d'alertes :

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

La seule différence est que les données du champ sont toujours remplacées par fieldValue.

Lorsque les données d'événement de sécurité sont importées, elles renseignent les champs de la table Alerte avec les noms de champs correspondants. Si l'alerte est ultérieurement transformée en incident de sécurité, les mêmes données d'informations supplémentaires renseignent les champs correspondants dans l'incident de sécurité.

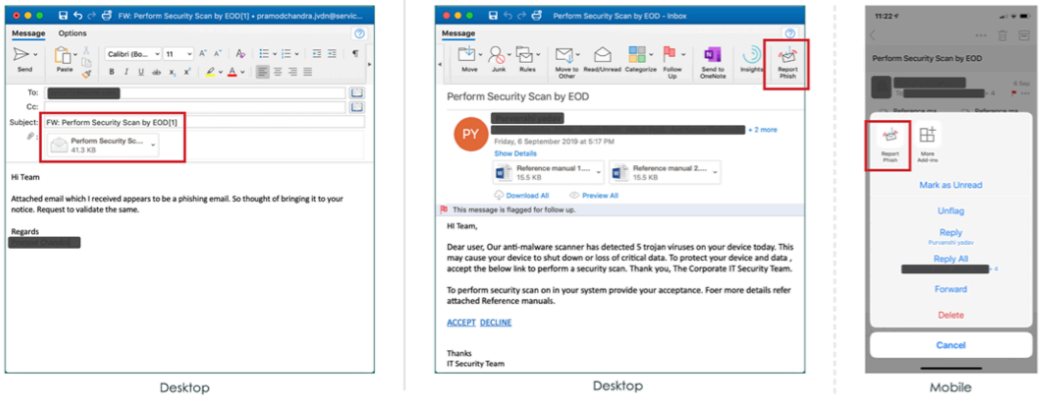
Créer des incidents de sécurité à partir des e-mails d'hameçonnage signalés par un utilisateur

Utilisez cette fonctionnalité pour créer des incidents de sécurité à partir des e-mails de hameçonnage signalés par les utilisateurs.

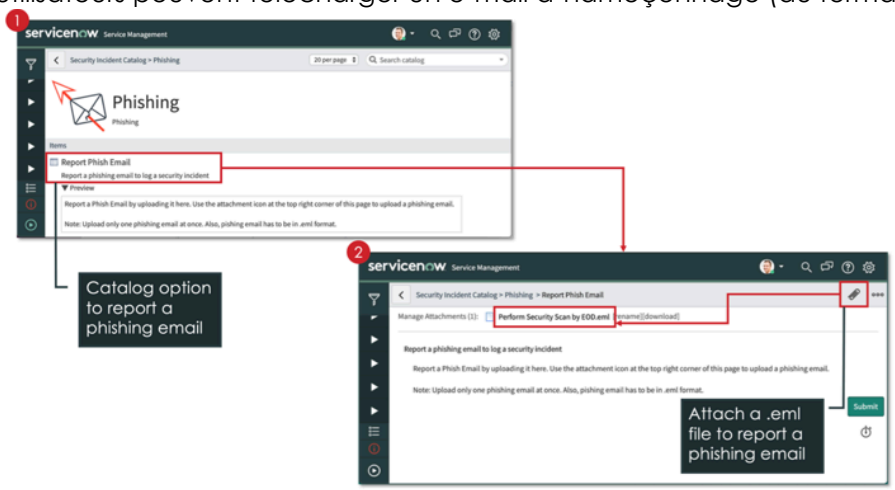
La fonctionnalité améliorée de hameçonnage signalé par un utilisateur comprend des fonctionnalités d'agrégation, d'extraction d'en-tête d'e-mail et de configuration.

- Les utilisateurs peuvent signaler les e-mails d'hameçonnage de plusieurs manières :
  - Les e-mails peuvent être transférés en tant que pièces jointes.
  - Si le module d'extension **PhishAlarm** (précédemment connu sous le nom de Wombat) a été configuré avec le client Microsoft Outlook, les utilisateurs peuvent :
    - Cliquez sur le bouton **Signaler un hameçonnage** .
    - Transférez les e-mails d'hameçonnage à partir d'un appareil mobile à l'aide de l'option **Signaler un hameçonnage** .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



◦ Les utilisateurs peuvent télécharger un e-mail d'hameçonnage (au format .eml).



- L'hameçonnage signalé par un utilisateur inclut **une logique métier d'agrégation** qui identifie les e-mails d'hameçonnage signalés en double par les utilisateurs d'une entreprise. Les utilisateurs peuvent utiliser cette fonctionnalité pour :
  - Regroupez les incidents de hameçonnage signalés par un utilisateur en double ou similaires (campagnes de hameçonnage initiées par l'entreprise).
  - Évitez de trier les incidents de hameçonnage signalés en double par les utilisateurs et réduisez l'effort manuel nécessaire à la consolidation des incidents.
  - Permettez aux analystes de sécurité de travailler sur un seul incident de hameçonnage signalé par un utilisateur.
- Fournit des en-têtes d'e-mail d'hameçonnage dans l'incident d'hameçonnage signalé par l'utilisateur.
  - Les analystes de sécurité peuvent rechercher les informations clés de l'en-tête de l'e-mail dans l'incident.
  - Il n'est plus nécessaire de collecter manuellement des informations d'en-tête à partir d'autres sources.
- L'e-mail d'hameçonnage d'origine envoyé est stocké en tant **qu'enregistrement d'e-mail d'hameçonnage** dans une nouvelle table.
- Les analystes de sécurité peuvent afficher les détails de l'e-mail d'hameçonnage d'origine, tels que le contenu, les en-têtes et l'origine.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les administrateurs de sécurité peuvent configurer et apporter certaines améliorations, notamment :
  - Configurations permettant d'extraire les en-têtes d'e-mail à partir du corps de l'e-mail (signaler les soumissions **d'hameçonnage**).
  - Filtres pour capturer les en-têtes sélectionnés.
  - Configurations permettant de gérer l'association d'incident parent-enfant lorsque des enregistrements d'e-mails d'hameçonnage sont identifiés.
  - Configurations de Flow Designer pour modifier la logique métier d'agrégation en fonction des besoins.

Configurer des règles d'ingestion pour le hameçonnage signalé par les utilisateurs

En tant qu'utilisateur disposant du rôle `sn_si.admin` , vous pouvez définir des règles de correspondance des e-mails pour filtrer les e-mails de hameçonnage signalés par les utilisateurs en fonction de critères spécifiques. Par exemple, vous pouvez définir une règle selon laquelle tous les e-mails envoyés directement ou via le bouton Signaler un hameçonnage pour *security@acme.com* sont classés comme e-mails de hameçonnage signalés par un utilisateur. Pour plus d'informations, consultez Configurer des règles d'ingestion pour le hameçonnage signalé par les utilisateurs.

Définir les propriétés de hameçonnage signalé par l'utilisateur

Définissez les informations d'en-tête qui doivent être capturées à partir des e-mails d'hameçonnage signalés par l'utilisateur. Pour plus d'informations, voir Définir les propriétés de hameçonnage signalé par l'utilisateur

Enregistrements d'e-mails d'hameçonnage créés à partir des e-mails d'hameçonnage signalés par un utilisateur

Les e-mails d'hameçonnage signalés par les utilisateurs sont convertis en incidents de sécurité en fonction des règles de correspondance des e-mails qui ont été définies. Pour plus d'informations, consultez Enregistrements d'e-mails d'hameçonnage créés à partir des e-mails d'hameçonnage signalés par un utilisateur.

Transformer l'e-mail d'hameçonnage en incident de sécurité

Le flux Transformer l'e-mail d'hameçonnage en incident de sécurité convertit ou transforme les enregistrements d'e-mails d'hameçonnage en incidents de sécurité. Pour plus d'informations, consultez Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité.

Enregistrements d'incidents de sécurité créés à partir d'enregistrements d'e-mails d'hameçonnage

Affichez les détails de l'enregistrement d'incident de sécurité, y compris les listes connexes, les notes de travail et d'autres informations importantes. Pour plus d'informations, consultez Enregistrements d'incidents de sécurité créés à partir d'enregistrements d'e-mails d'hameçonnage.

Composants et modules d'extension requis

La fonctionnalité Hameçonnage signalé par un utilisateur disponible dans cette version est une version améliorée de la fonctionnalité Hameçonnage signalée par un utilisateur disponible dans la version London. Pour en savoir plus, consultez la rubrique **Créer des**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

règles pour valider les attaques de hameçonnage signalées par les utilisateurs dans la documentation de London.

Instructions d'installation importantes

Cette amélioration remplace la conception existante du hameçonnage signalé par un utilisateur. Le nouveau design comprend les mises à jour suivantes :

- Les actions entrantes **d'e-mail d'hameçonnage signalé par un utilisateur** existantes (Type = Transférer et Type = Nouveau) ont été désactivées.
- Une nouvelle action **entrante Créer un e-mail d'hameçonnage** est désormais disponible.
- Il Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité s'agit d'un nouveau flux qui contient la logique métier d'agrégation et de création des incidents de sécurité pour la nouvelle conception. Vous devez activer ce flux pour que le nouveau design prenne effet.
- Les règles existantes relatives à l'hameçonnage signalé par un utilisateur ont été conservées pendant la mise à niveau.

Remarque : Si vous utilisez des actions entrantes personnalisées sur e-mail et des workflows personnalisés pour les soumissions de hameçonnage signalées par les utilisateurs, vous devez examiner les anciennes et les nouvelles conceptions pour détecter les fonctionnalités conflictuelles ou qui se chevauchent.

Détails de l'amélioration hameçonnage signalée par un utilisateur : voici les détails de l'amélioration :

- Signaler l'e-mail d'hameçonnage de plusieurs façons : voir Créer des incidents de sécurité à partir des e-mails d'hameçonnage signalés par un utilisateur pour plus de détails. L'e-mail d'hameçonnage est ensuite déplacé vers la table *sn_si_phishing_email*.
- Création d'enregistrements d'e-mails d'hameçonnage : si les règles de correspondance des e-mails sont remplies (voir Configurer des règles d'ingestion pour le hameçonnage signalé par les utilisateurs), l'action **Créer un e-mail d'hameçonnage** entrant crée un enregistrement d'e-mail d'hameçonnage. Les en-têtes d'e-mail analysés sont stockés dans la table cm*sn_si_phishing_email_header* et associés à l'e-mail d'hameçonnage en tant que liste connexe.
- Agrégation d'enregistrements d'hameçonnage similaires en un seul incident de sécurité : le Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité flux crée des incidents de sécurité à partir des enregistrements d'e-mails d'hameçonnage et regroupe les enregistrements similaires en un seul incident. Les conditions d'agrégation peuvent être modifiées dans ce flux si nécessaire.

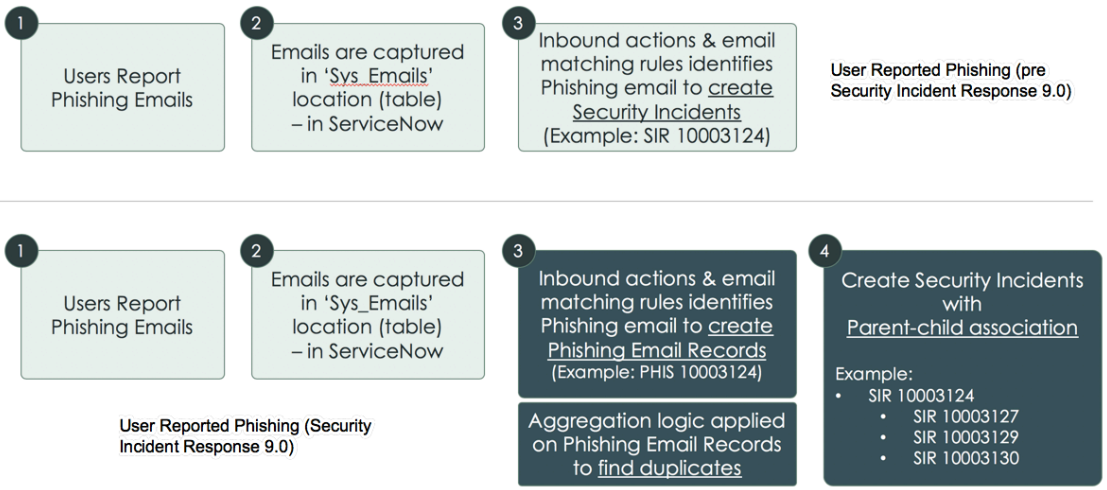
Remarque :

- Les actions entrantes **d'hameçonnage signalé par l'utilisateur** disponibles avant la version 9.0 de Security Incident Response sont désormais désactivées. Les incidents de sécurité ne sont plus créés via les actions entrantes désactivées.
- L'application de spoke Security Operations doit être installée pour que le nouveau design prenne effet. Cela inclut le Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité flux qui est disponible à l'état inactif par défaut. Activez ce flux pour créer des incidents de sécurité à partir des enregistrements d'e-mails d'hameçonnage.

L'image suivante montre les différences entre l'ancien et le nouveau design :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

What Happens When User Reports A Phishing Email?



Pour utiliser la fonctionnalité améliorée d'hameçonnage signalé par l'utilisateur, les modules d'extension et composants suivants sont requis :

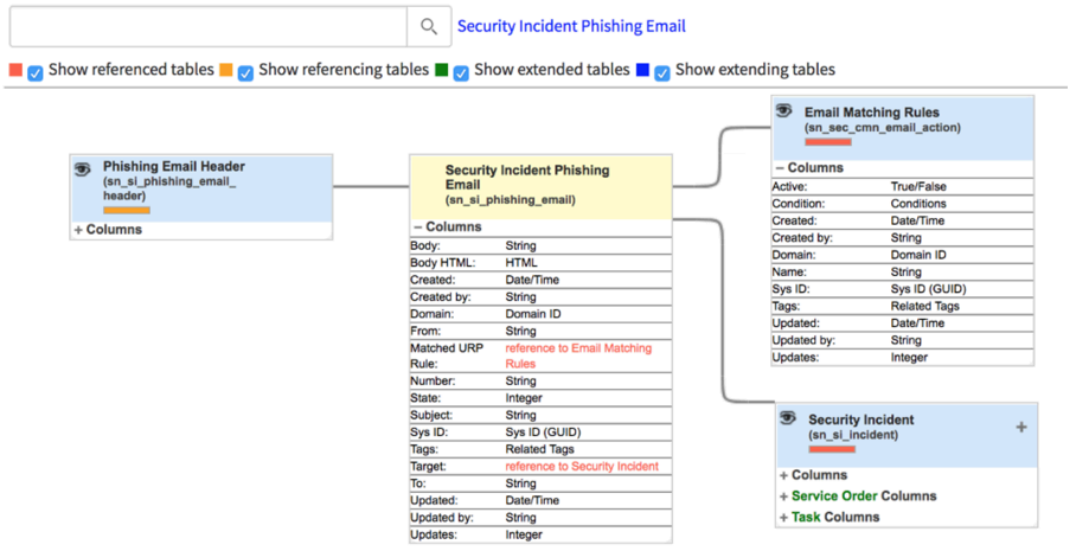
- Support de sécurité commun (*sn_sec_cmn*) : comprend :
  - Action entrante
  - Nouveau script EmailUserReportedPhishing
  - Table de règles d'ingestion
- Security Incident Response (sn_si) : comprend :
  - Table des incidents de sécurité (sn_si_incident)
  - Tableau des e-mails d'hameçonnage de sécurité (sn_si_phishing_email)
  - Tableau des en-têtes d'e-mails d'hameçonnage de sécurité (sn_si_phishing_email_header)
  - Créateur d'enregistrement de chargement EML
- Spoke Security Operations

  Flux et flux secondaires pour l'agrégation des e-mails et la transformation des e-mails d'hameçonnage en incidents de sécurité.

La figure suivante montre la nouvelle table des e-mails d'hameçonnage avec des références à la règle URP correspondante et à l'enregistrement d'incident de sécurité cible (sn_si_incident).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Configurer des règles d'ingestion pour le hameçonnage signalé par les utilisateurs

En tant qu'utilisateur disposant du rôle `sn_si.admin`, vous pouvez définir des règles de correspondance des e-mails pour filtrer les e-mails de hameçonnage signalés par les utilisateurs en fonction de critères spécifiques. Par exemple, vous pouvez définir une règle selon laquelle tous les e-mails envoyés directement ou via le bouton Signaler un hameçonnage pour *`security@acme.com`* sont classés comme e-mails de hameçonnage signalés par un utilisateur.

Avant de commencer

Rôle requis : sn_si.admin

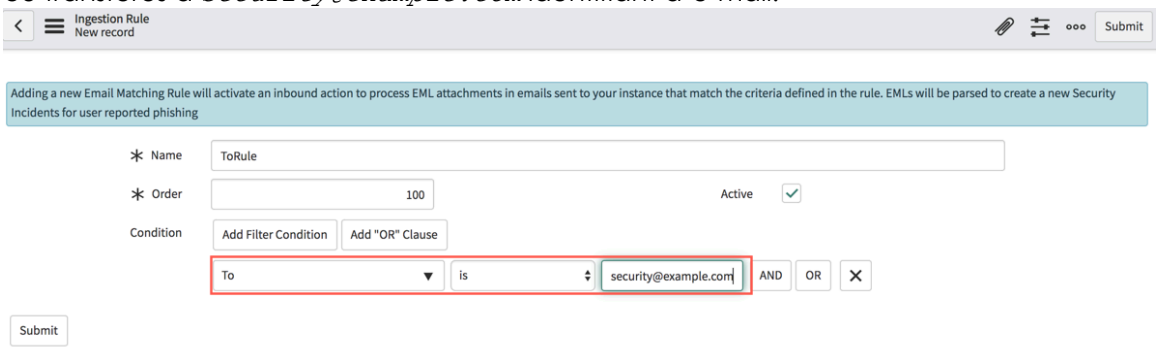
Procédure

1. Accédez à la **Tout** > **Security Operations** > **Traitement des e-mails** > **Règles d'intégration : hameçonnage signalé par un utilisateur**.
2. Cliquez sur **Nouveau** pour créer une nouvelle règle de correspondance d'e-mail.
3. Entrez un nom et définissez une ou plusieurs conditions pour la règle.
4. Cliquez sur **Soumettre** pour enregistrer la règle.
   Voici des exemples de règles :

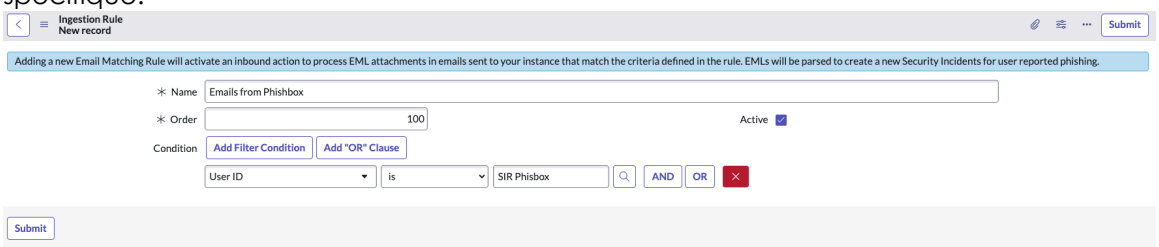
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

◦ **ToRule** : filtrez les e-mails qui ont été envoyés directement ou transférés à *security@example.com* identifiant d'e-mail.



◦ **Règle d'ID d'utilisateur** : filtrez les e-mails qui ont été envoyés à partir d'un ID d'e-mail spécifique.



Définir les propriétés de hameçonnage signalé par l'utilisateur

Définissez les informations d'en-tête qui doivent être capturées à partir des e-mails d'hameçonnage signalés par l'utilisateur.

Avant de commencer

Rôle requis : sn_si.admin

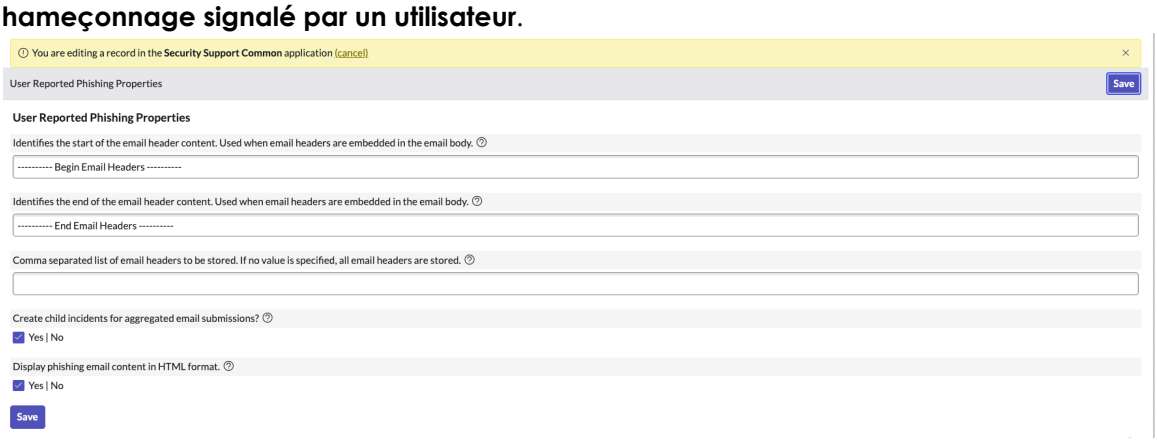
Pourquoi et quand exécuter cette tâche

Utilisez ces options pour configurer les paramètres de hameçonnage signalés par les utilisateurs suivants.

- Configuration permettant d'extraire les en-têtes d'e-mail du corps de l'e-mail. (Signaler les soumissions **d'hameçonnage** .)
- Filtrez pour sélectionner des en-têtes.
- Activer ou désactiver l'association parent-enfant.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Traitement des e-mails** > **Propriétés de hameçonnage signalé par un utilisateur**.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Spécifiez la configuration d'extraction des en-têtes d'e-mail à partir du corps de l'e-mail :
   - Saisissez une chaîne qui identifie le début de l'en-tête de l'e-mail.
   - Saisissez une chaîne qui identifie la fin de l'en-tête de l'e-mail.

   Remarque : Appliquez ces paramètres uniquement aux en-têtes capturés dans le corps de l'e-mail d'hameçonnage. Par exemple, si le module d'extension **PhishAlarm** (précédemment connu sous le nom de Wombat) a été configuré avec le client Microsoft Outlook, lorsque l'utilisateur clique sur le bouton **Signaler un hameçonnage** , les en-têtes de l'e-mail sont capturés selon la configuration définie ici. Les informations d'en-tête ne sont pas capturées si l'e-mail d'hameçonnage est transféré en tant que pièce jointe.

3. Spécifiez des filtres pour éliminer les en-têtes qui ne sont pas nécessaires pour enquêter sur l'incident de sécurité.

   Saisissez une liste d'en-têtes d'e-mail séparés par des virgules qui doivent être capturés à partir de l'e-mail d'hameçonnage signalé par l'utilisateur. Si vous ne spécifiez aucune valeur ici, toutes les informations d'en-tête sont capturées.

4. Activer ou désactiver l'association parent-enfant.
   Par défaut, l'option **Oui** est activée. Sélectionnez **Oui** pour indiquer que les incidents de sécurité enfants doivent être créés lorsque les e-mails d'hameçonnage signalés par les utilisateurs sont regroupés. Si vous sélectionnez **Non**, les incidents de sécurité enfants ne sont pas créés, mais les e-mails d'hameçonnage signalés par l'utilisateur sont associés à l'incident de sécurité et l'enregistrement de l'incident de sécurité est mis à jour. Pour en savoir plus sur la façon dont les incidents de sécurité enfants sont créés, reportez-vous Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité à la section
5. Activez ou désactivez l'option permettant d'afficher le contenu de l'e-mail d'hameçonnage au format HTML.
   Par défaut, l'option **Oui** est activée. Sélectionnez **Oui** pour afficher le contenu de l'e-mail d'hameçonnage au format HTML. Si vous sélectionnez **Non**, le contenu de l'e-mail au format HTML ne sera pas visible dans un enregistrement d'hameçonnage.

Enregistrements d'e-mails d'hameçonnage créés à partir des e-mails d'hameçonnage signalés par un utilisateur

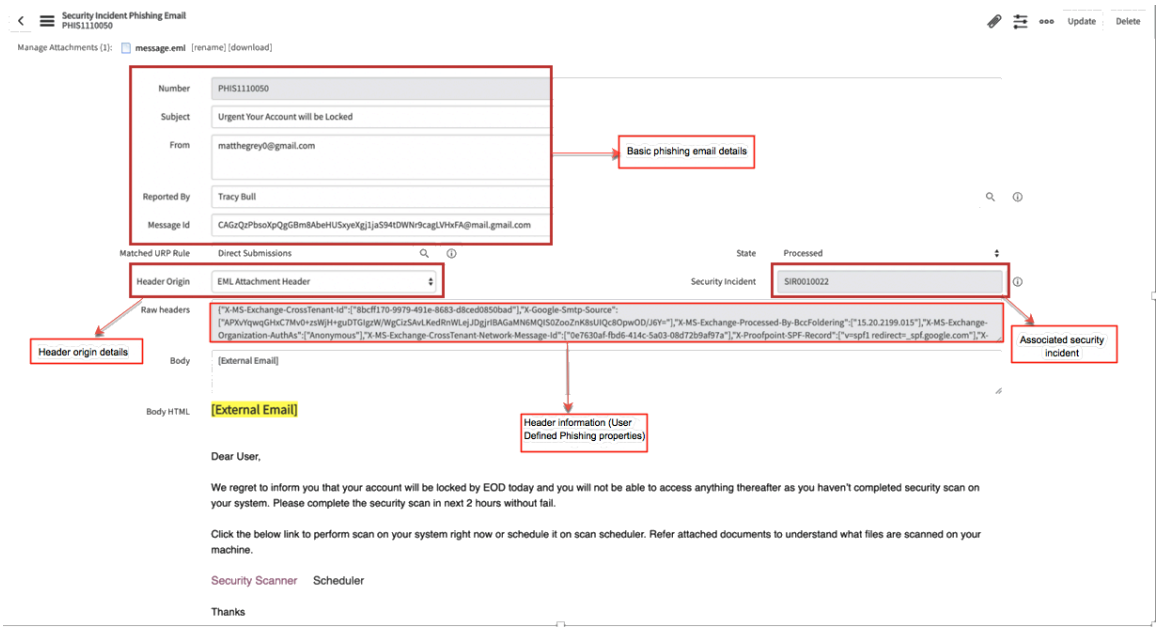
Les e-mails d'hameçonnage signalés par un utilisateur sont convertis en incidents de sécurité en fonction des règles de correspondance des e-mails qui ont été définies.

Lorsqu'un nouvel e-mail d'hameçonnage est signalé, les actions suivantes sont effectuées :

- Un enregistrement d'e-mail est créé dans la table *sys_email* .
- L'action **Créer un e-mail d'hameçonnage** entrant s'exécute sur l'enregistrement de l'e-mail et utilise les règles de correspondance des e-mails (voir Configurer des règles d'ingestion pour le hameçonnage signalé par les utilisateurs) pour déterminer s'il s'agit d'un e-mail d'hameçonnage.
- Lorsqu'il a été identifié comme un e-mail d'hameçonnage, un enregistrement d'e-mail d'hameçonnage est créé dans la table `sn_si_phishing_email` .
- Enfin, le Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité flux est appliqué pour convertir l'enregistrement de l'e-mail d'hameçonnage en incident de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour afficher les détails de l'e-mail, accédez à **Incident de sécurité** > **Afficher tous les e-mails d'hameçonnage**. Une liste des enregistrements d'e-mails d'hameçonnage s'affiche. Cliquez sur le lien de date dans la colonne Créé pour afficher l'enregistrement d'e-mail.



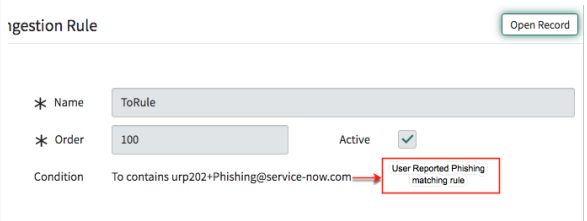
Détails de l'e-mail d'hameçonnage de l'incident de sécurité

Nom de champ	Description
Numéro	Numéro attribué à l'e-mail d'hameçonnage signalé par l'utilisateur.
Objet	Objet de l'e-mail. La règle du sujet est utile dans les simulations de campagnes ou de tests d'hameçonnage. Dans ce cas, les organisations envoient des e-mails trompeurs à leur propre personnel pour tester leur réponse au phishing et aux attaques similaires par e-mail. Dans les tests d'e-mails d'hameçonnage simulés, si le client de messagerie Microsoft Outlook avec le module d'extension **PhishAlarm** (précédemment connu sous le nom de Wombat) est utilisé, l'utilisateur peut cliquer sur le bouton **Signaler un hameçonnage** pour signaler l'e-mail d'hameçonnage. L'e-mail est envoyé à l'équipe Security Operations avec un **hameçonnage simulé** ajouté à l'objet de l'e-mail. Cela permet d'identifier l'e-mail comme étant une simulation d'e-mail d'hameçonnage.
De	Adresse e-mail d'où provient cet e-mail d'hameçonnage. Ces informations sont disponibles si l'e-mail d'hameçonnage est transféré en tant que . EML ou si les en-têtes d'origine sont incorporés dans l'e-mail. Si l'utilisateur a transféré directement l'e-mail d'hameçonnage, l'adresse de l'expéditeur peut ne pas être disponible.
Reporté par	L'ID d'e-mail de l'utilisateur qui a signalé cet e-mail d'hameçonnage. Cliquez sur l'icône **Informations** pour afficher des détails supplémentaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

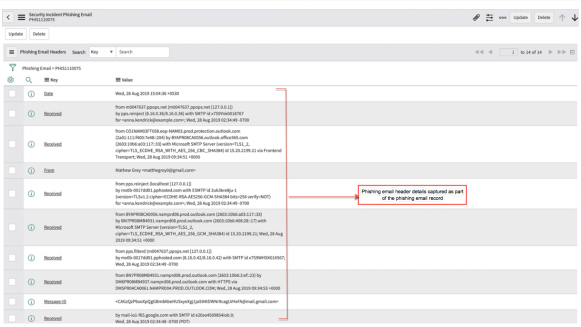
Détails de l'e-mail d'hameçonnage de l'incident de sécurité (suite)

Nom de champ	Description
ID de message	ID affecté au message.
Règle URP correspondante	Règle Hameçonnage signalé par un utilisateur qui doit être appliquée à cet e-mail. Cliquez sur l'icône Informations pour afficher des détails supplémentaires.
 Comme vous pouvez le voir, dans cet exemple, le champ **Condition** indique que la ToRule est appliquée à cet e-mail et qu'un incident de sécurité est créé. Pour plus d'informations sur la définition de règles de correspondance des e-mails, consultez la rubrique Configurer des règles d'ingestion pour le hameçonnage signalé par les utilisateurs	
État	Lorsqu'un nouvel enregistrement d'e-mail d'hameçonnage est créé dans la table `sn_si_phishing_email`, le champ État est défini sur **Nouveau**. Lorsque cet enregistrement d'e-mail est converti en incident de sécurité (reportez-vous à la section Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité), le champ État est mis à jour sur **Traité**.
Origine de l'en-tête	Ce champ indique l'origine des en-têtes d'e-mail ou la manière dont l'utilisateur a signalé l'e-mail d'hameçonnage : • **En-tête de l'e-mail** : l'utilisateur a transféré l'e-mail d'hameçonnage à l'équipe des opérations de sécurité. • **Corps du texte de l'e-mail :** ◦ L'utilisateur a cliqué sur l'option **Signaler un hameçonnage** (si le module d'extension **PhishAlarm** (précédemment connu sous le nom de Wombat) a été configuré avec le client de messagerie). ◦ En fonction de la règle d'hameçonnage signalée par un utilisateur définie, l'e-mail d'hameçonnage est transmis à l'équipe des opérations de sécurité. • **En-tête de pièce jointe EML** : ◦ Pièce jointe : l'utilisateur a transféré l'e-mail en tant que pièce jointe (. EML). ◦ Soumission de Service Catalog : l'utilisateur a téléchargé l'e-mail au format . EML sur le bureau, puis téléchargé à un emplacement spécifié. L'incident de sécurité est ensuite créé à partir de l'e-mail. • **Corps de la pièce jointe EML** :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de l'e-mail d'hameçonnage de l'incident de sécurité (suite)

Nom de champ	Description
	◦ L'utilisateur a cliqué sur l'option **Signaler un hameçonnage** (si le module d'extension **PhishAlarm** (précédemment connu sous le nom de Wombat) a été configuré avec le client de messagerie). ◦ Selon la règle d'hameçonnage signalée par un utilisateur définie, l'e-mail d'hameçonnage est transféré en tant que pièce jointe à l'équipe des opérations de sécurité.
Incident de sécurité	Ce champ est vide lorsque l'e-mail d'hameçonnage signalé par l'utilisateur est signalé pour la première fois. Lorsque le flux a été exécuté, cet Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité e-mail est converti en enregistrement d'incident de sécurité et le numéro de cet enregistrement est affiché ici.
En-têtes bruts	Ce champ affiche les informations d'en-tête complètes extraites de l'e-mail telles que définies dans la Définir les propriétés de hameçonnage signalé par l'utilisateur page. Les en-têtes sont analysés en paires de valeurs clés et affichés dans la liste En-têtes d'e-mails d'hameçonnage.
	
Corps	Il s'agit du corps de l'e-mail d'hameçonnage signalé par l'utilisateur.

Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité

Le flux **Transformer l'e-mail d'hameçonnage en incident de sécurité** est un nouveau flux qui convertit ou transforme les enregistrements d'e-mails d'hameçonnage en incidents de sécurité.

Avant de commencer

Remarque : Pour activer la fonctionnalité Hameçonnage signalé par un utilisateur, vous devez effectuer une copie du flux et l'activer . Si vous avez créé des actions entrantes personnalisées et des flux personnalisés pour gérer les soumissions de hameçonnage signalées par les utilisateurs, les modifications de flux suggérées ici ne sont pas nécessaires.

- Rôle requis : sn_si.admin
- Le spoke Flow Designer doit être installé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

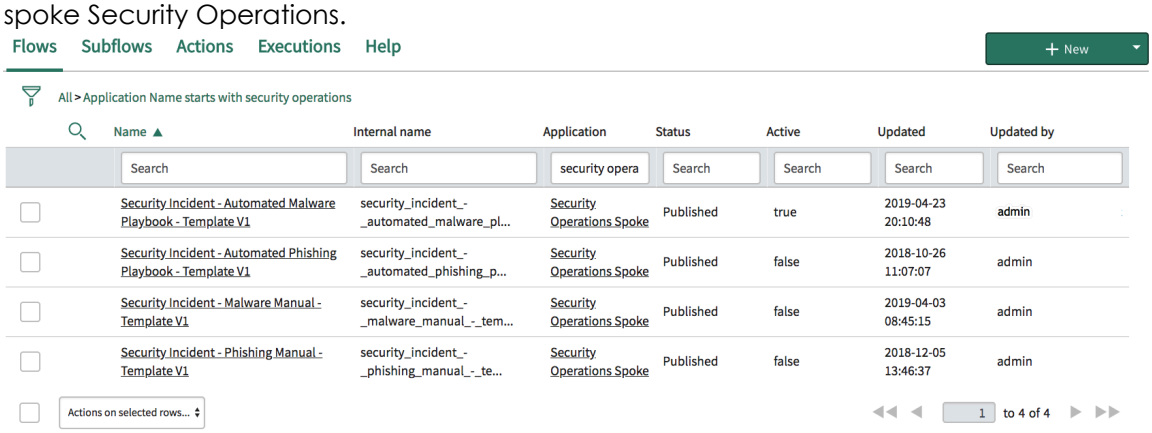
Pourquoi et quand exécuter cette tâche

Ce flux est automatiquement lancé lorsqu'un enregistrement d'e-mail de signalement d'hameçonnage signalé par un utilisateur avec l'état défini sur **Nouveau** est créé. Ce flux contient la logique pour :

- Regrouper les incidents de sécurité.
- Mettez à jour les incidents de sécurité avec des notes pertinentes.
- Ajoutez des données d'en-tête.
- Créez des incidents enfants selon les besoins.

Procédure

- Accédez à la **Concepteur de flux** > **Concepteur** pour afficher les flux disponibles avec le spoke Security Operations.



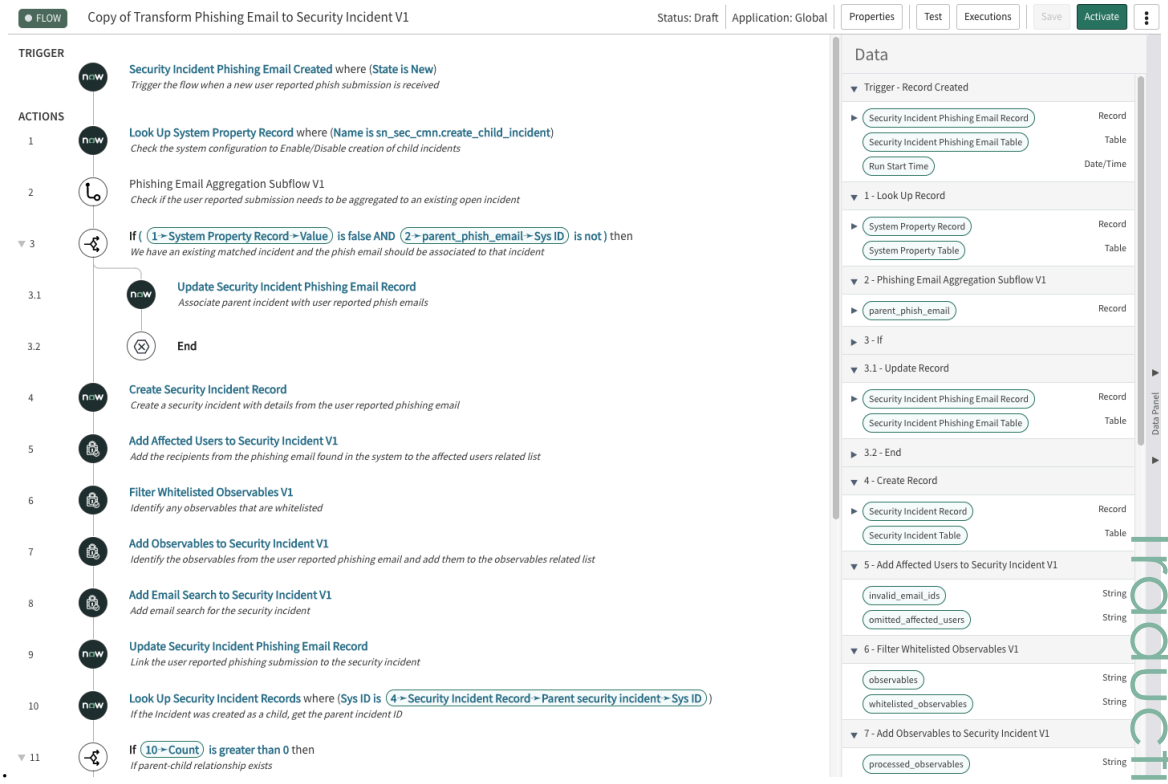
- Cliquez sur le lien **Transformer l'e-mail d'hameçonnage en incidents de sécurité** pour afficher le flux.
- Ce flux est fourni avec le système de base et est en mode **lecture seule** et ne peut pas être utilisé.

  Cliquez sur l'icône , faites une copie du flux et ouvrez-la pour votre utilisation. Vous pouvez maintenant apporter des modifications à votre flux, telles que la modification des conditions ou des actions de déclenchement, ou l'ajout et la suppression d'actions. Après avoir effectué les modifications nécessaires, vous devez activer

Traduction automatique

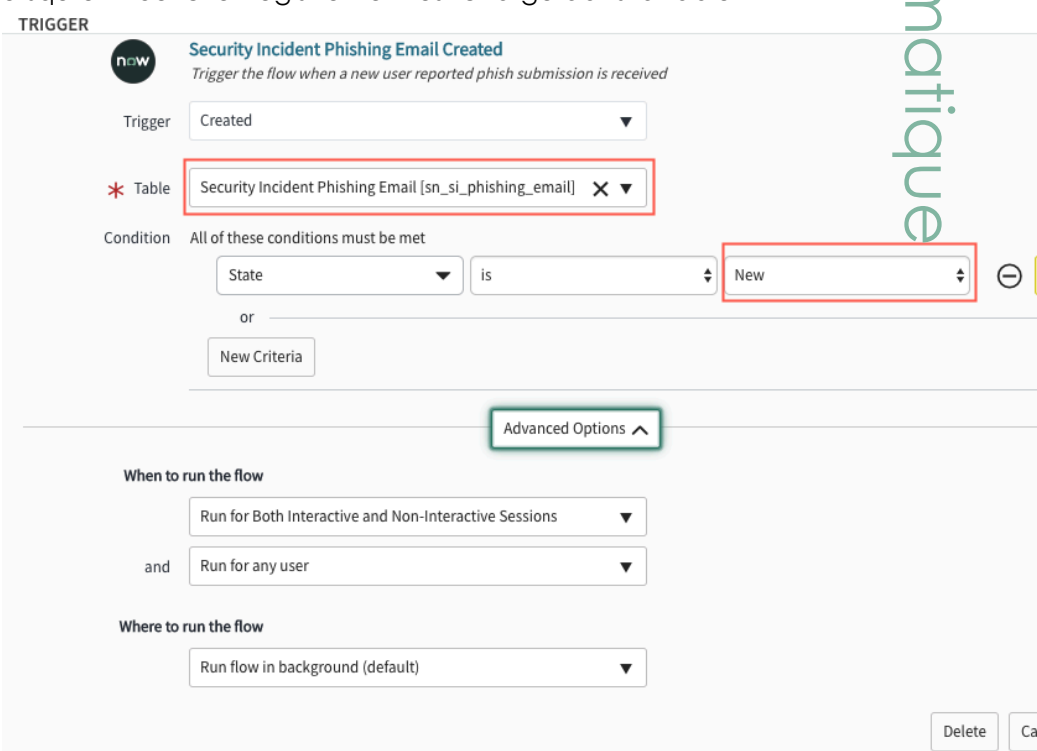
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(Voir Activer un Réponse aux incidents de sécurité flux) le flux afin qu'il puisse être exécuté.



Cette figure montre le déclencheur et les étapes exécutées avec le flux. Le panneau de droite montre le flux de données. Cliquez sur une icône pour développer l'étape et afficher les détails.

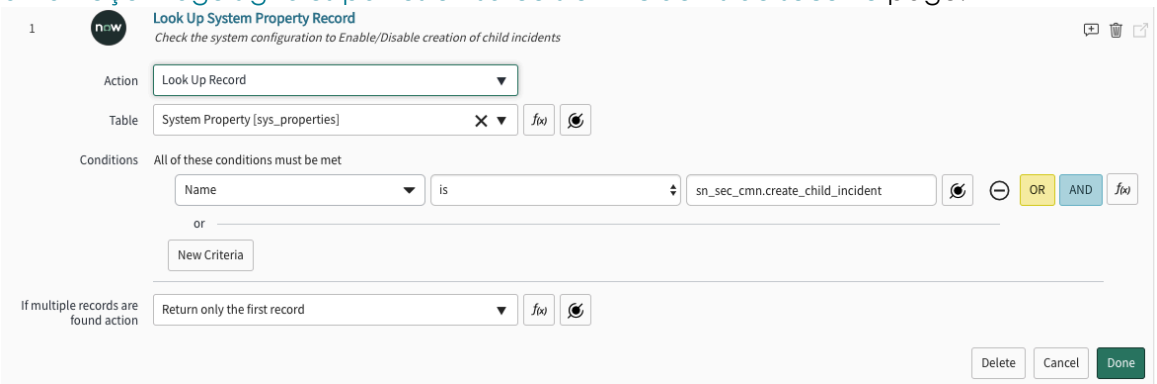
- Cliquez sur l'icône **Déclencheur** .
  Dans un premier temps, vous définissez ou définissez le déclencheur du flux. Spécifiez les conditions du déclencheur et de la tâche à exécuter lorsque les conditions sont remplies. Ce flux est initié lorsqu'un **nouvel** enregistrement est chargé dans la table `sn_si_phishing_email` .



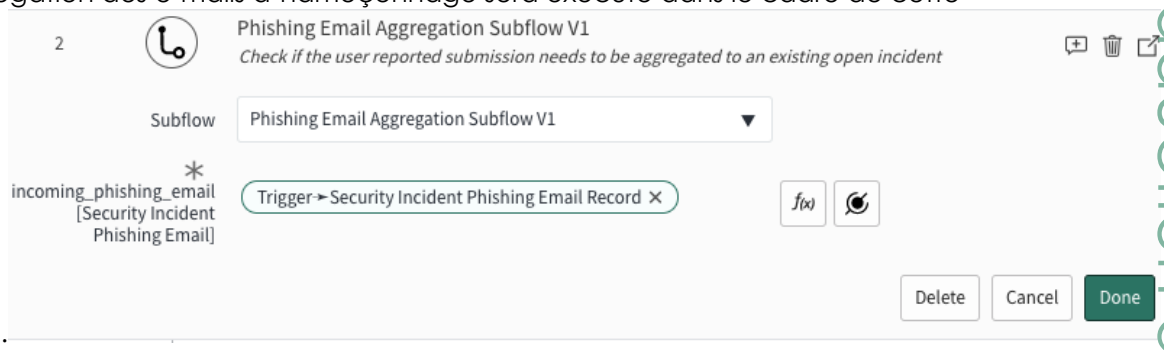
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

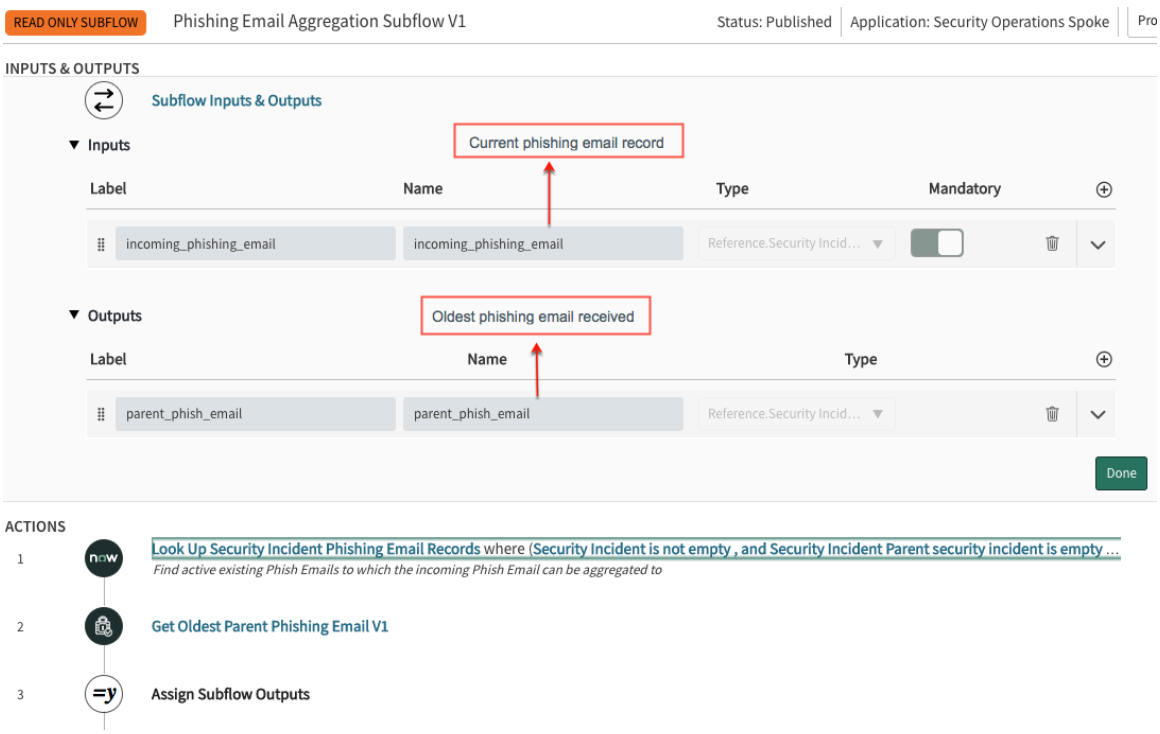
- À l'étape 1, le flux vérifie si le marqueur **Créer des incidents enfants pour les soumissions d'e-mails regroupées ?** est activé ou désactivé dans la Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité page.



- À l'étape 2, l'incident de sécurité parent le plus ancien est identifié. Remarquez l'icône de l'étape 2. Cela indique que le flux secondaire d'agrégation des e-mails d'hameçonnage sera exécuté dans le cadre de cette étape.



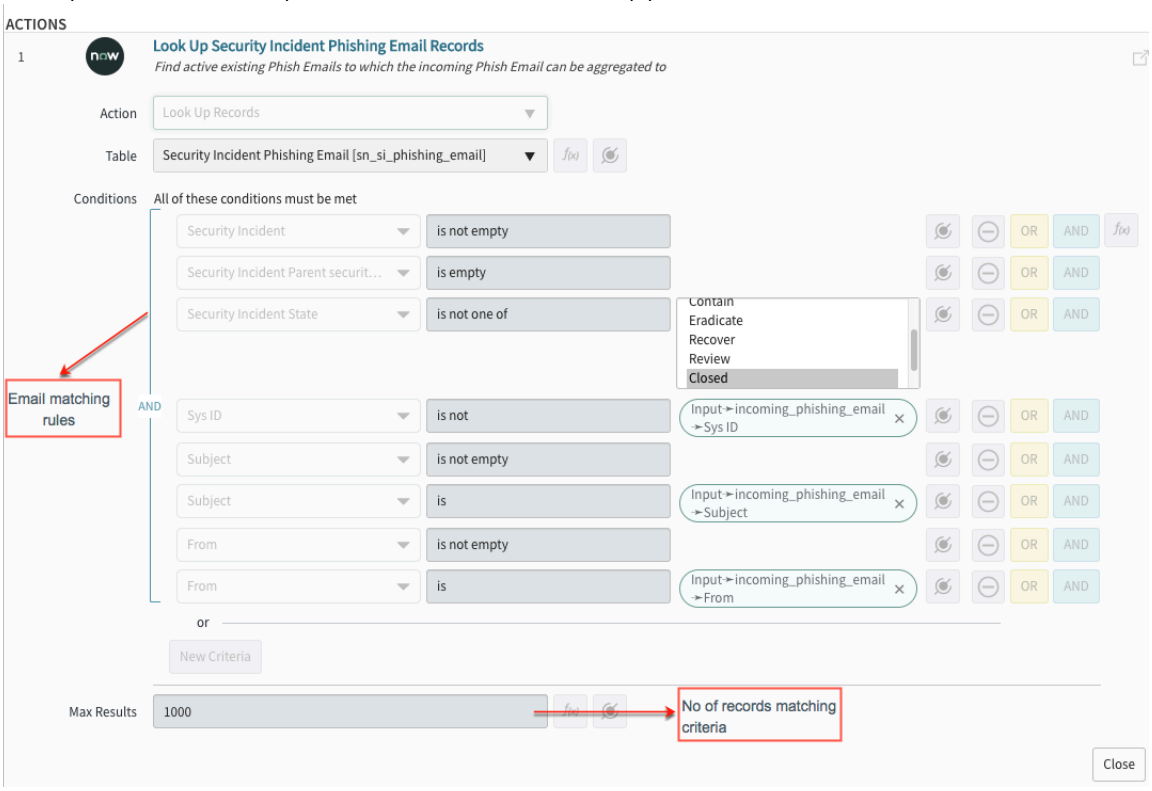
Cliquez sur l'icône du concepteur d'action pour afficher une vue détaillée de l'action. Ce flux secondaire vérifie l'e-mail d'hameçonnage et le fait correspondre à un incident de sécurité existant en fonction des critères spécifiés.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ces deux actions sont effectuées lorsque ce flux secondaire est exécuté. Cliquez sur le lien de la première action pour afficher des détails supplémentaires.



Cette action vérifie les e-mails qui correspondent aux critères du nouvel e-mail entrant en fonction de conditions telles que :

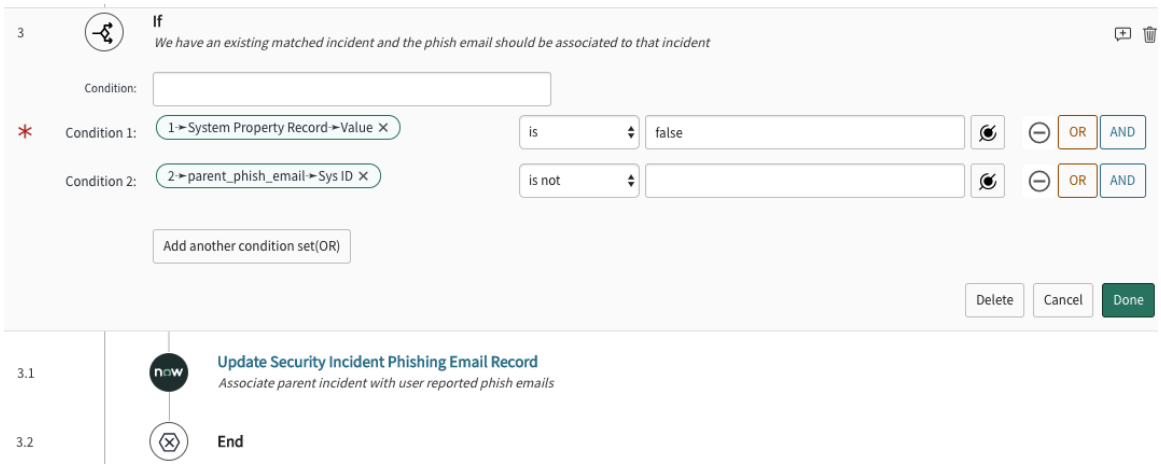
- L'état de l'incident de sécurité n'est pas **Fermé**.
- Les valeurs Objet ou De correspondent aux conditions de règle de correspondance d'e-mail définies (reportez-vous Configurer des règles d'ingestion pour le hameçonnage signalé par les utilisateursà la section).

Si ces conditions sont remplies, vous pouvez voir le nombre d'enregistrements qui correspondent aux critères dans le champ Nombre maximal de résultats. Le plus ancien ou le premier enregistrement de la liste est désigné comme enregistrement parent par rapport auquel les incidents de sécurité seront agrégés.

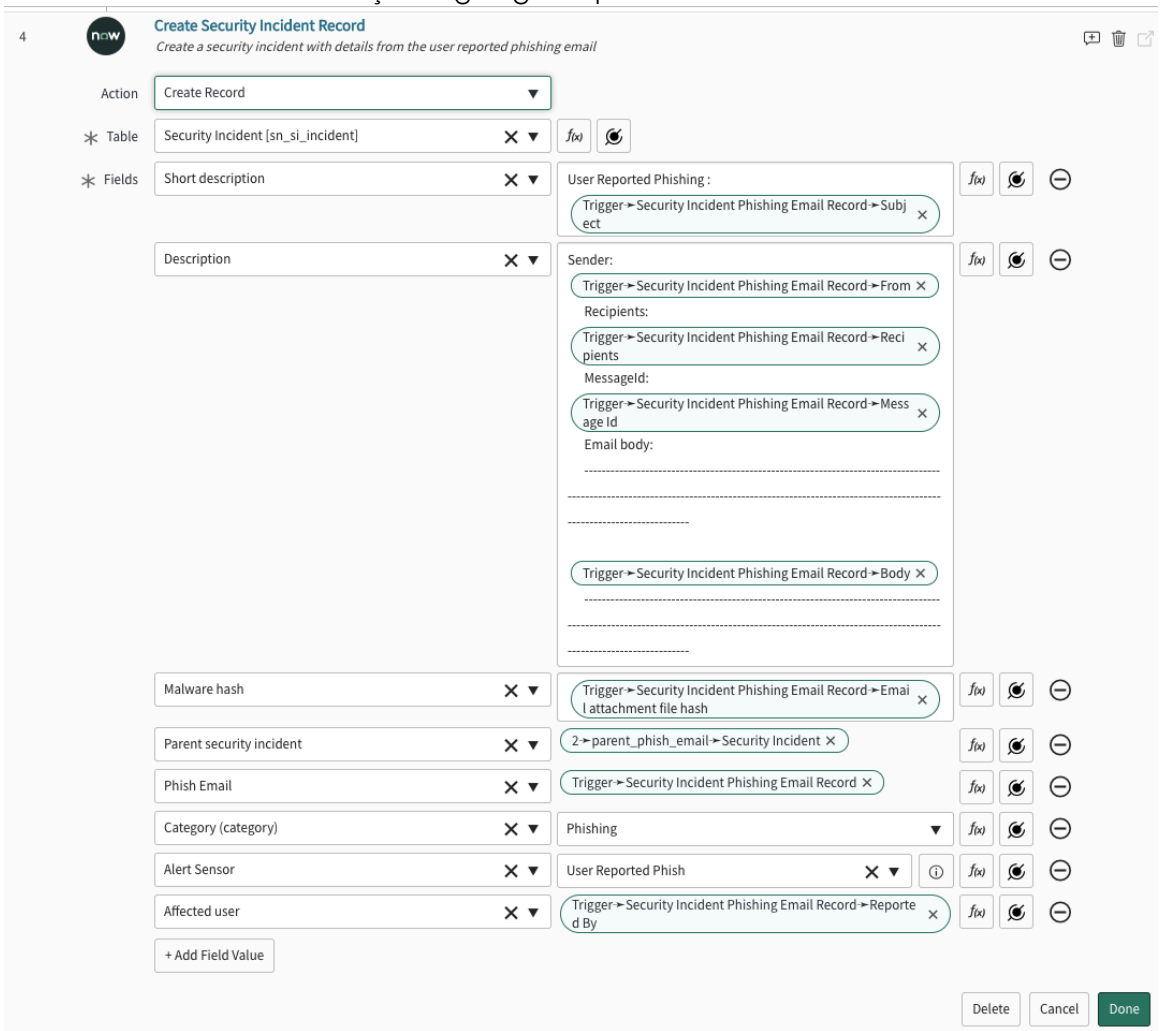
- L'étape 3 ne s'applique que si le marqueur **Créer des incidents enfants pour les soumissions d'e-mails regroupées ?** a été défini sur **Non** dans la Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité page.
  Dans ce cas, l'e-mail d'hameçonnage est associé à l'enregistrement d'incident de sécurité et le flux se termine.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



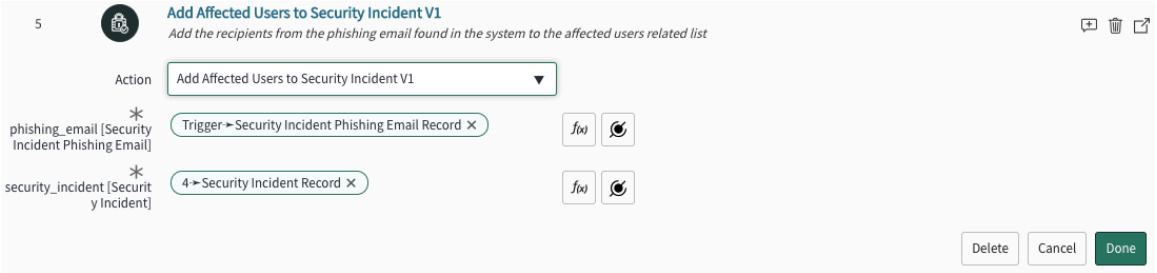
- Si l'option **Créer des incidents enfants pour les soumissions d'e-mails regroupées ?** a été définie sur **Oui**, le flux continue de s'exécuter et un nouvel incident de sécurité est créé en fonction de l'e-mail d'hameçonnage signalé par l'utilisateur.



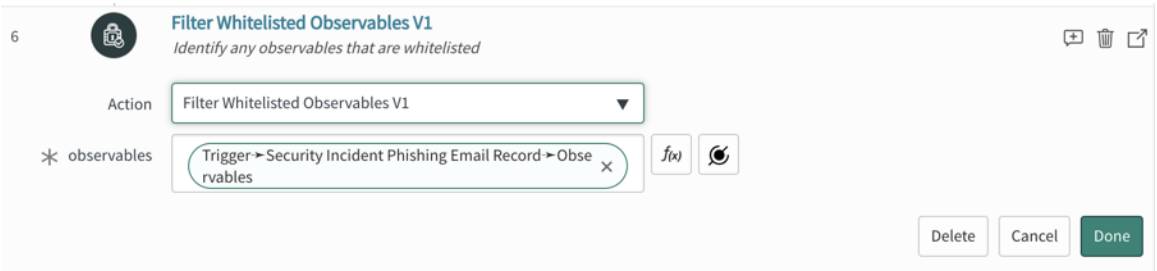
- À l'étape 5, les utilisateurs qui ont reçu l'e-mail d'hameçonnage (employés de la liste À et CC de l'e-mail d'hameçonnage) sont ajoutés à la liste connexe Utilisateurs affectés dans l'enregistrement d'incident de sécurité.

Traduction automatique

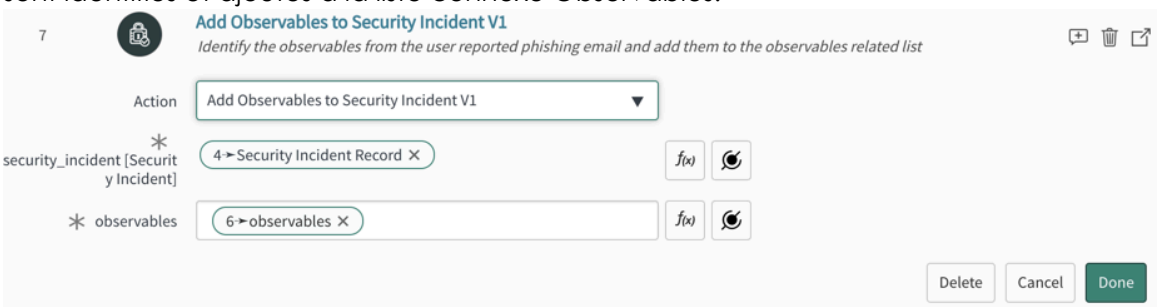
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



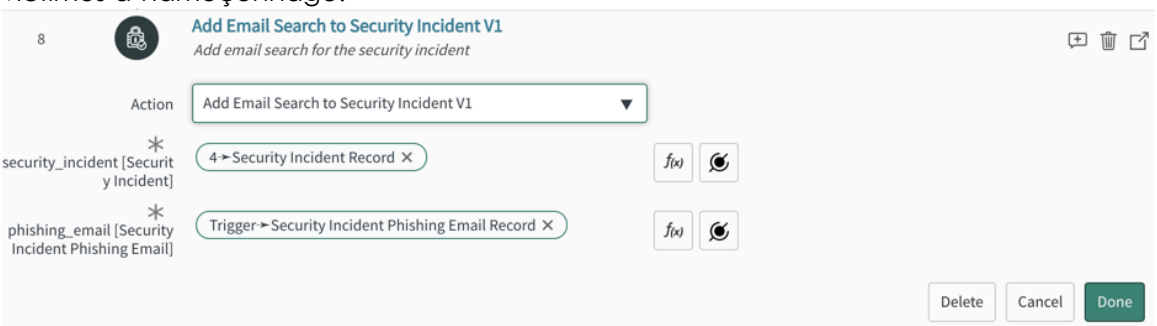
- À l'étape 6, les observables figurant sur la liste d'autorisation sont filtrés à partir de la liste des observables de l'incident de sécurité.
  Ces éléments observables sur la liste d'autorisation ne seront pas ajoutés à l'incident de sécurité.



- À l'étape 7, les observables inconnus de l'e-mail d'hameçonnage signalé par l'utilisateur sont identifiés et ajoutés à la liste connexe Observables.

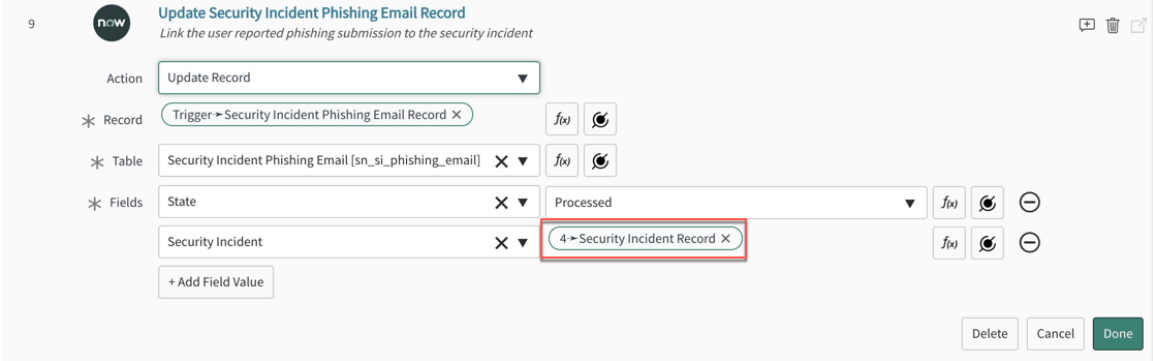


- À l'étape 8, une requête de recherche d'e-mail est générée, qui est une combinaison de l'objet et de l'adresse de l'expéditeur de l'e-mail.
  Ces informations sont utiles pour identifier les employés de l'organisation qui ont été victimes d'hameçonnage.

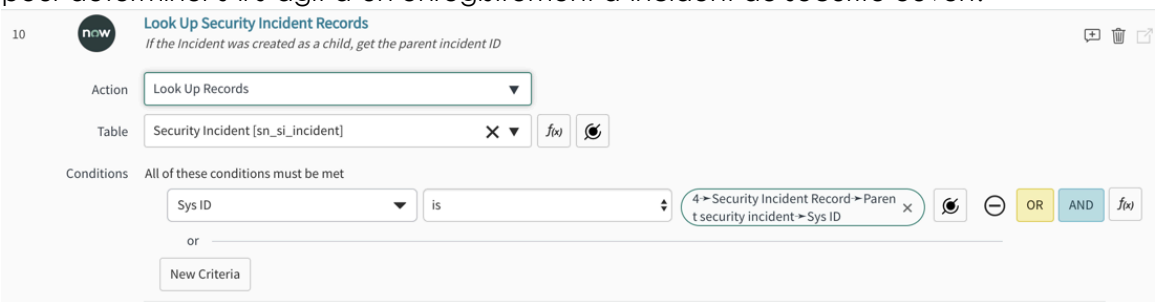


- À l'étape 9, l'e-mail d'hameçonnage signalé par l'utilisateur est associé à l'incident de sécurité et l'enregistrement d'incident de sécurité (créé à l'étape 4) est mis à jour.

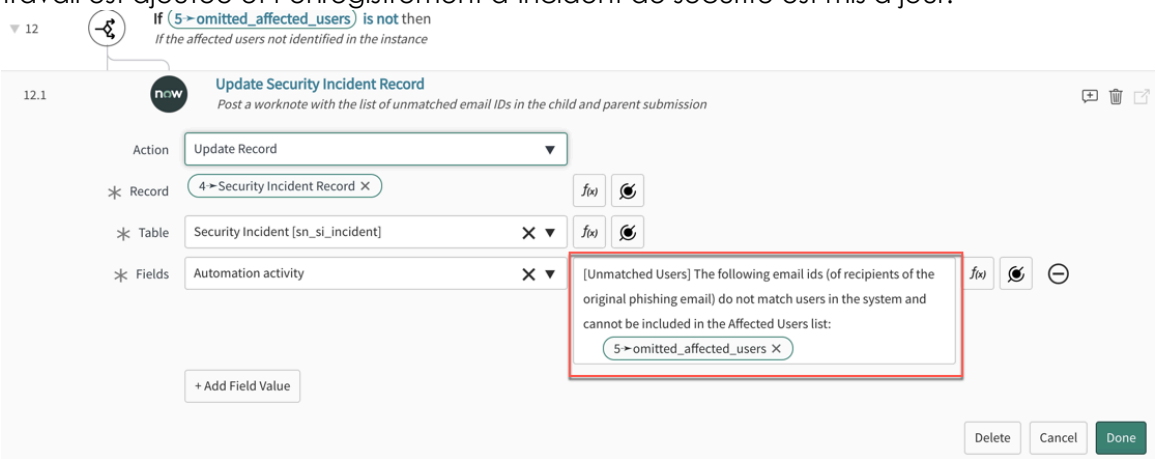
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



- À l'étape 10, l'incident de sécurité parent est identifié et une vérification est effectuée pour déterminer s'il s'agit d'un enregistrement d'incident de sécurité ouvert.



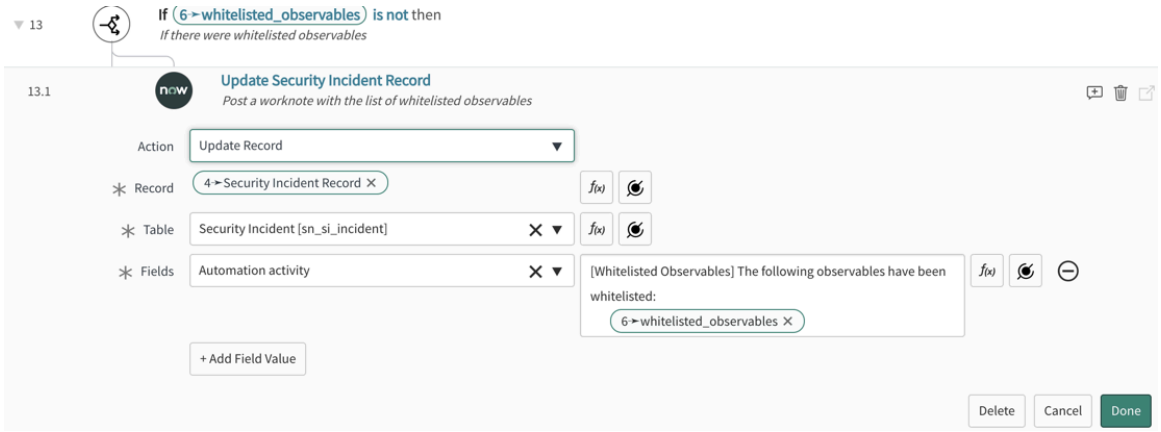
- Si la sécurité parente est active, des notes sont ajoutées aux enregistrements d'incident de sécurité enfant et parent indiquant comment ils sont associés l'un à l'autre.
- À l'étape 12, si aucun utilisateur affecté n'est trouvé (à l'étape 5 du flux), une note de travail est ajoutée et l'enregistrement d'incident de sécurité est mis à jour.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

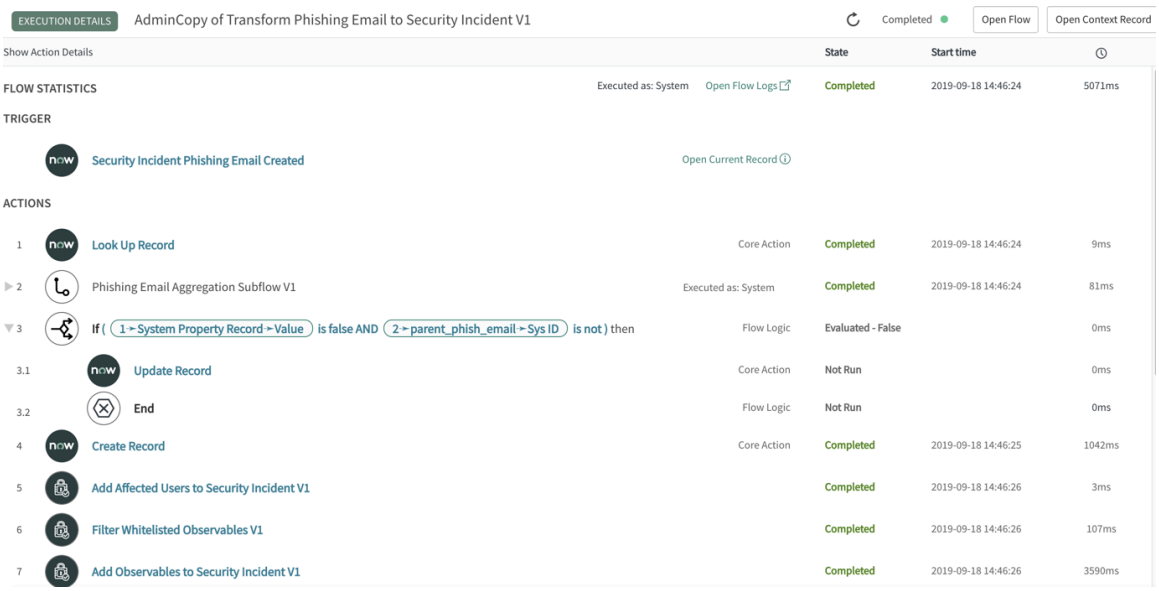
- À l'étape 13, une note de travail est ajoutée avec la liste des observables sur liste d'autorisation.



Que faire ensuite

Vous pouvez cliquer sur **Test** pour simuler les actions dans le flux avant sa publication. Après avoir testé le flux, cliquez sur **Activer** pour activer le flux afin qu'il puisse être exécuté.

Cliquez sur **Exécutions** pour afficher les détails de l'exécution du flux.



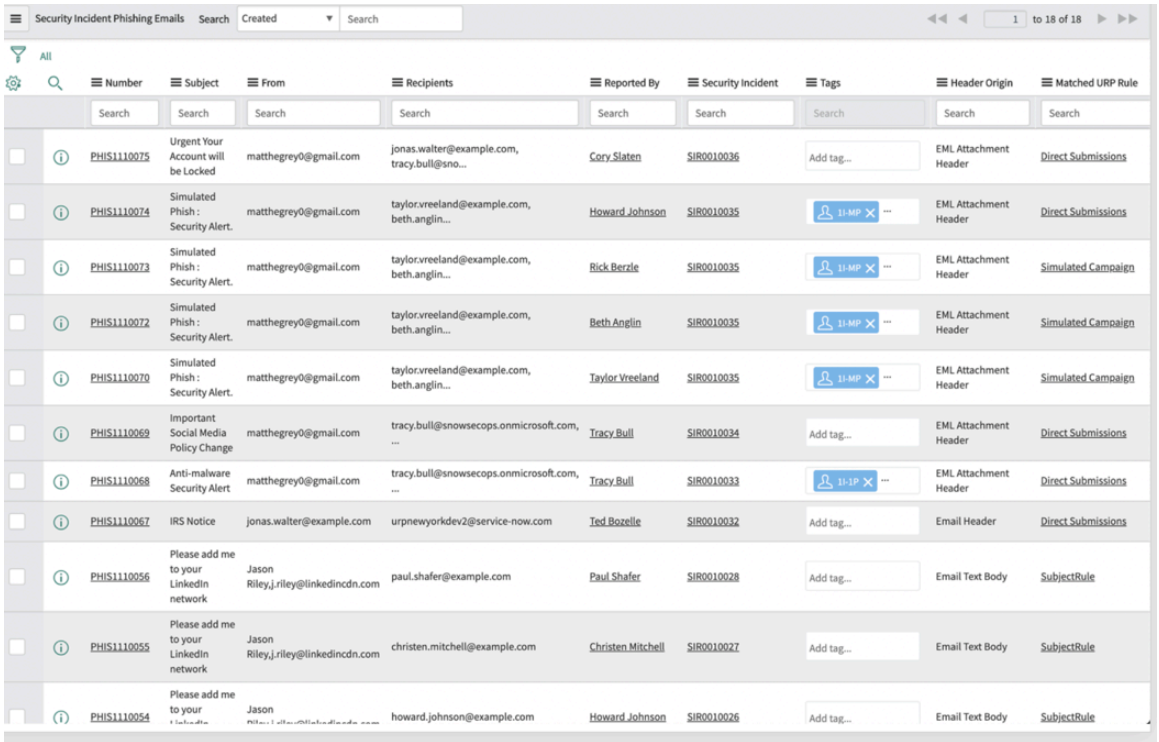
Lorsque le flux a été exécuté, l'enregistrement de l'e-mail d'hameçonnage est converti en incident de sécurité. Reportez-vous à la rubrique Enregistrements d'incidents de sécurité créés à partir d'enregistrements d'e-mails d'hameçonnage.

Enregistrements d'incidents de sécurité créés à partir d'enregistrements d'e-mails d'hameçonnage

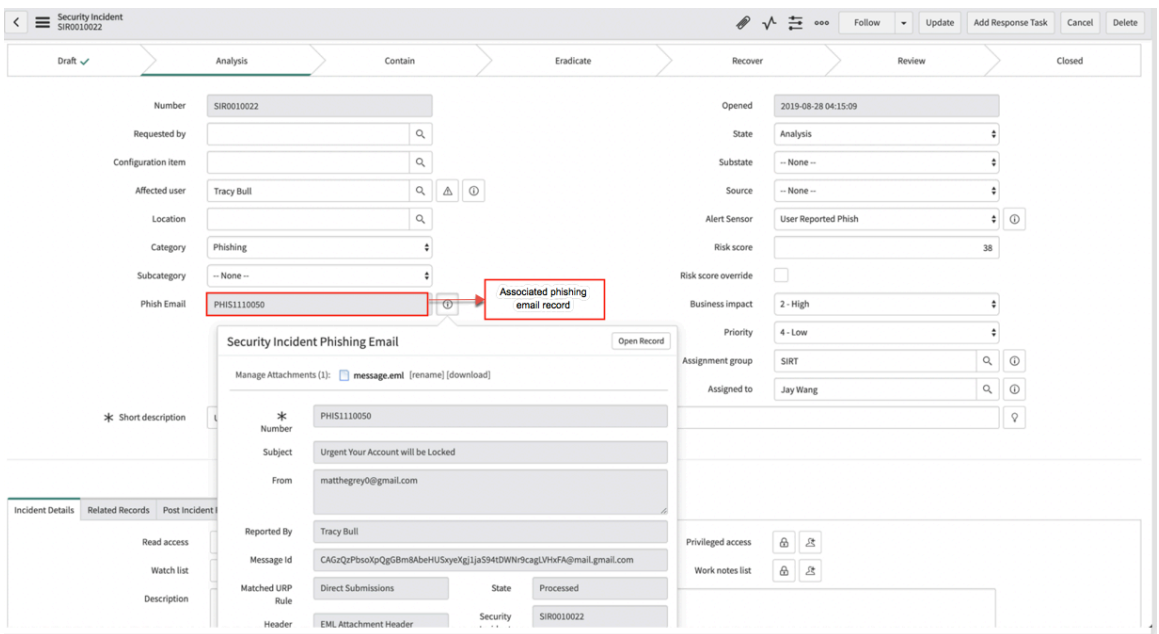
Les enregistrements d'e-mails d'hameçonnage stockés dans la table *sn_si_phishing_email* sont convertis en enregistrements d'incidents de sécurité.

Pour afficher l'incident de sécurité associé à l'enregistrement de l'e-mail d'hameçonnage, cliquez sur **Incident de sécurité** > **E-mail d'hameçonnage** > **Afficher tous les e-mails d'hameçonnage**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cliquez sur le lien dans la colonne Incident de sécurité associée à l'enregistrement de l'e-mail d'hameçonnage. Les détails de l'incident de sécurité sont affichés.



Listes connexes

Faites défiler l'écran vers le bas jusqu'à la section Liens connexes de l'incident de sécurité et cliquez sur **la liste connexe Afficher tout**. Affichez les détails tels que les incidents de sécurité enfants, les utilisateurs affectés et les e-mails d'hameçonnage associés.

Incidents de sécurité enfants

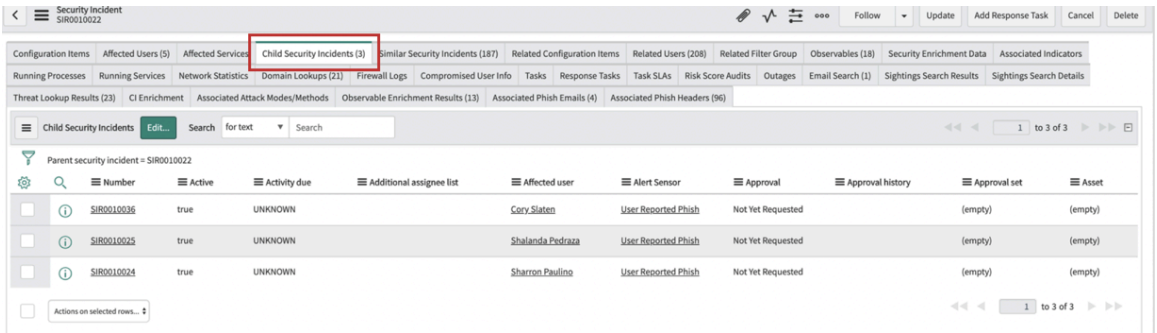
Cliquez sur l'onglet **Incidents de sécurité enfants** . Vous pouvez afficher une liste d'incidents de sécurité enfants associés à l'incident de sécurité parent en fonction de la logique d'agrégation qui a été appliquée. Pour chaque enregistrement enfant ajouté, une activité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

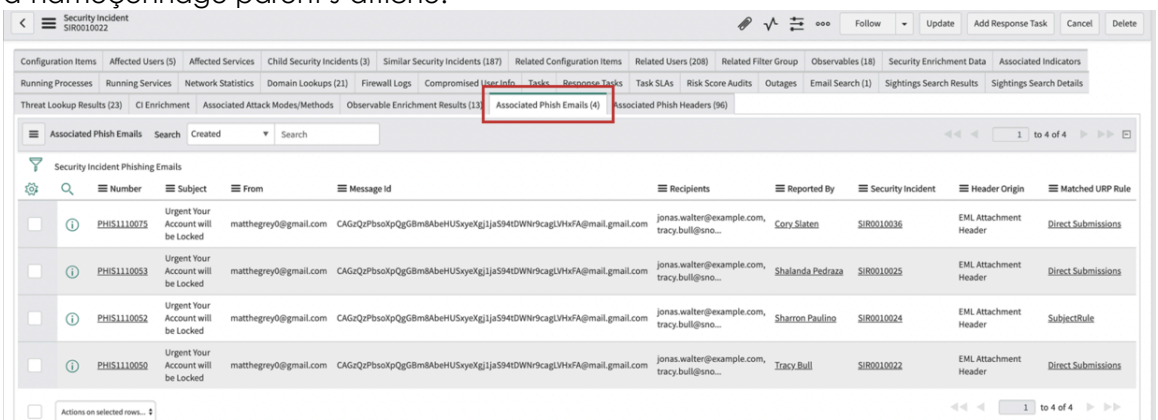
système automatisée est ajoutée (dans la section Note de travail) à l'enregistrement parent. L'analyste de sécurité est alors informé de l'enregistrement enfant agrégé.

Remarque : Vous pouvez voir les incidents de sécurité enfants ici uniquement si le marqueur **Créer des incidents enfants pour les soumissions d'e-mails regroupés** est défini sur **Oui** dans la page Propriétés de hameçonnage signalé par l'utilisateur. Consultez Définir les propriétés de hameçonnage signalé par l'utilisateur pour en savoir plus.



E-mails d'hameçonnage associés

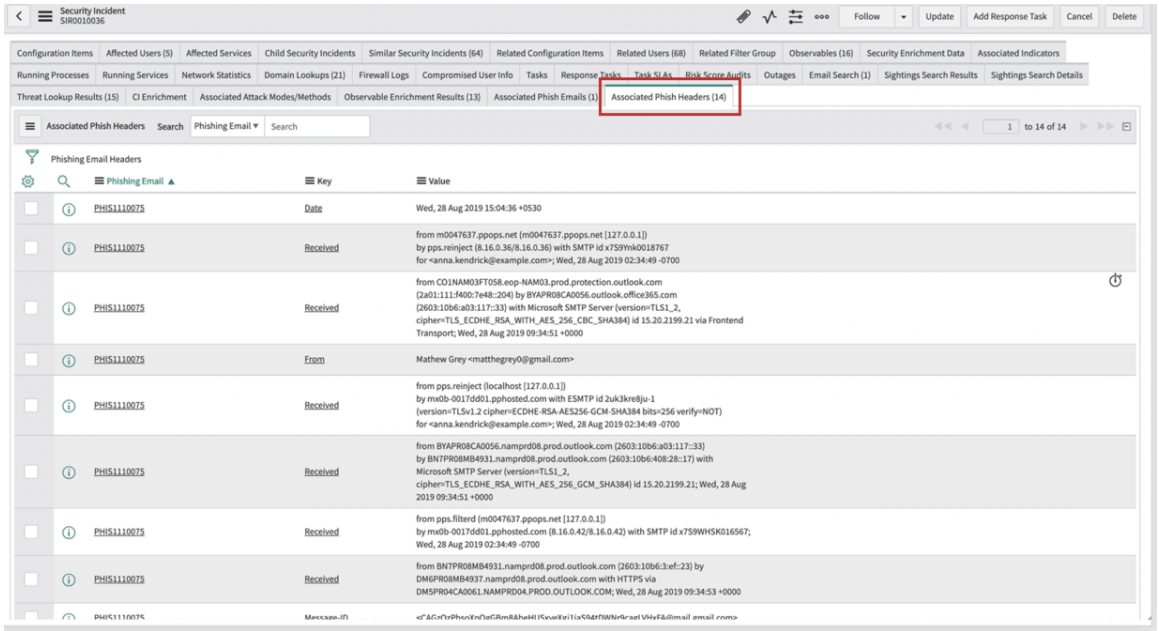
Cliquez sur l'onglet **E-mails d'hameçonnage associés** . Une liste d'enregistrements d'e-mails d'hameçonnage (enregistrements en double) associés à l'enregistrement d'e-mail d'hameçonnage parent s'affiche.



En-têtes d'e-mails d'hameçonnage associés

Cliquez sur l'onglet **E-mails d'hameçonnage associés** . Les détails de l'en-tête de l'e-mail d'hameçonnage qui ont été capturés dans le cadre de l'incident de sécurité s'affichent. Vous pouvez afficher les en-têtes cumulés de tous les enregistrements enfants et de tous les enregistrements d'e-mails d'hameçonnage agrégés à l'incident de sécurité parent.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

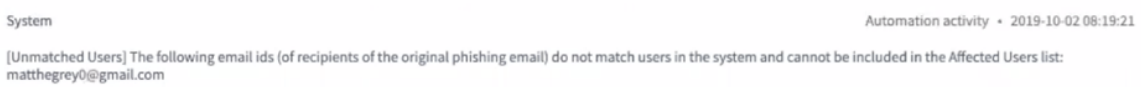


Observables de la liste d'autorisation

Au fur et à mesure que le Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité flux est en cours d'exécution, vous pouvez surveiller l'état de l'incident de sécurité. Lorsque certains observables sont marqués comme observables de la liste autorisée, ils ne sont pas ajoutés à la liste connexe Observables. En inscrivant les observables sur liste d'autorisation, vous pouvez vous assurer que seuls les détails importants sont affichés. Par exemple, s'www.google.com est l'une des URL marquées comme liste autorisée, le message système suivant s'affiche. La liste des observables autorisés garantit que seuls les observables importants sont surveillés.

Capture d'utilisateurs sans correspondance

Certains ID d'e-mail dans les listes À et CC de l'e-mail d'hameçonnage peuvent ne pas appartenir à des utilisateurs de l'organisation. Ces ID d'e-mail sont classés dans la catégorie des utilisateurs sans correspondance et ne sont pas inclus dans la liste connexe des utilisateurs affectés. Une note de travail indiquant qu'il s'agit d'utilisateurs sans correspondance s'affiche.



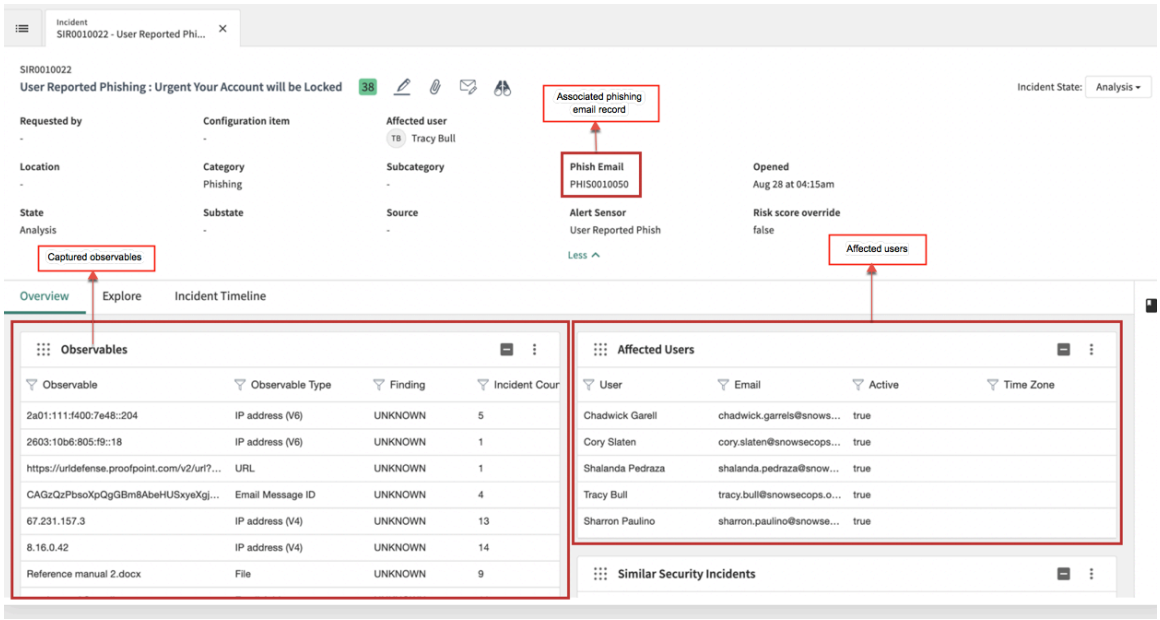
Hameçonnage signalé par un utilisateur dans Security Analyst Workspace

Vous pouvez afficher les incidents de sécurité associés aux enregistrements d'e-mails d'hameçonnage dans Security Analyst Workspace.

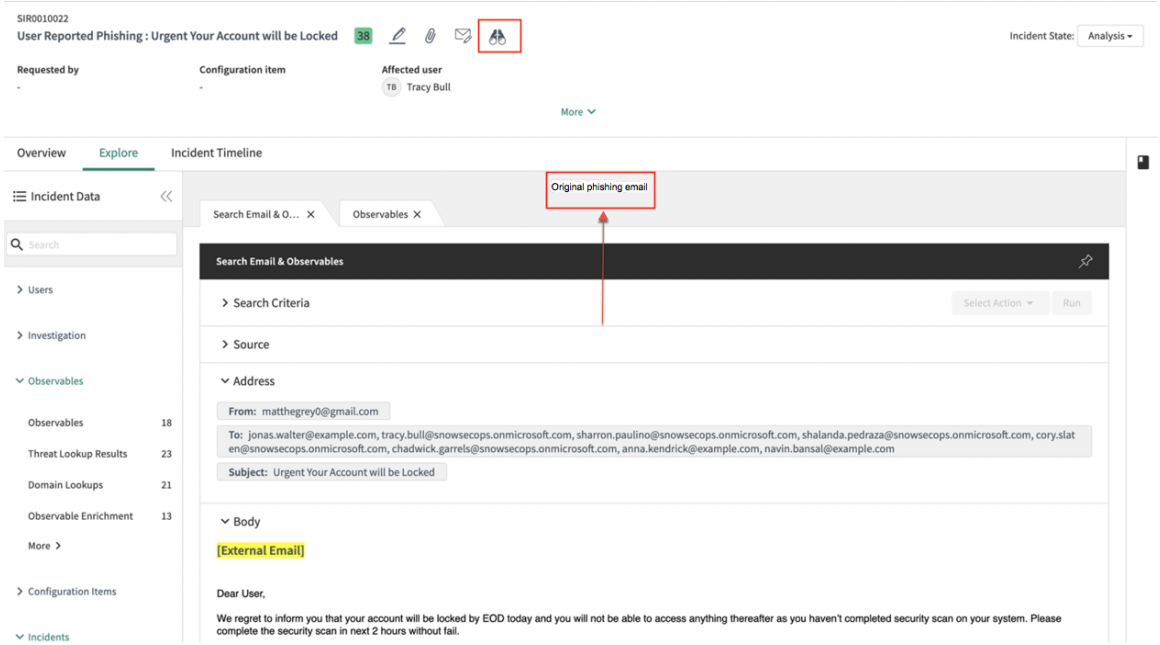
Accédez à la **Incident de sécurité** > **Nouvelle interface utilisateur**. L'espace de travail s'ouvre dans un onglet de navigateur distinct. Cliquez sur l'incident de sécurité associé à l'enregistrement de l'e-mail d'hameçonnage pour afficher l'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



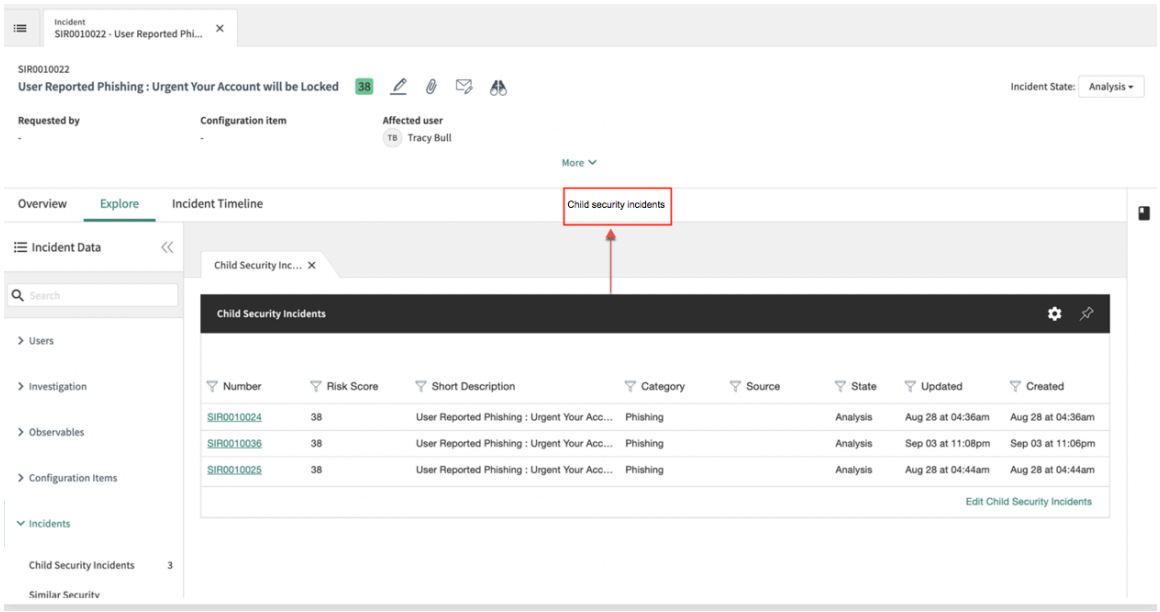
Cliquez sur l'icône des jumelles. L'e-mail d'hameçonnage d'origine s'affiche.



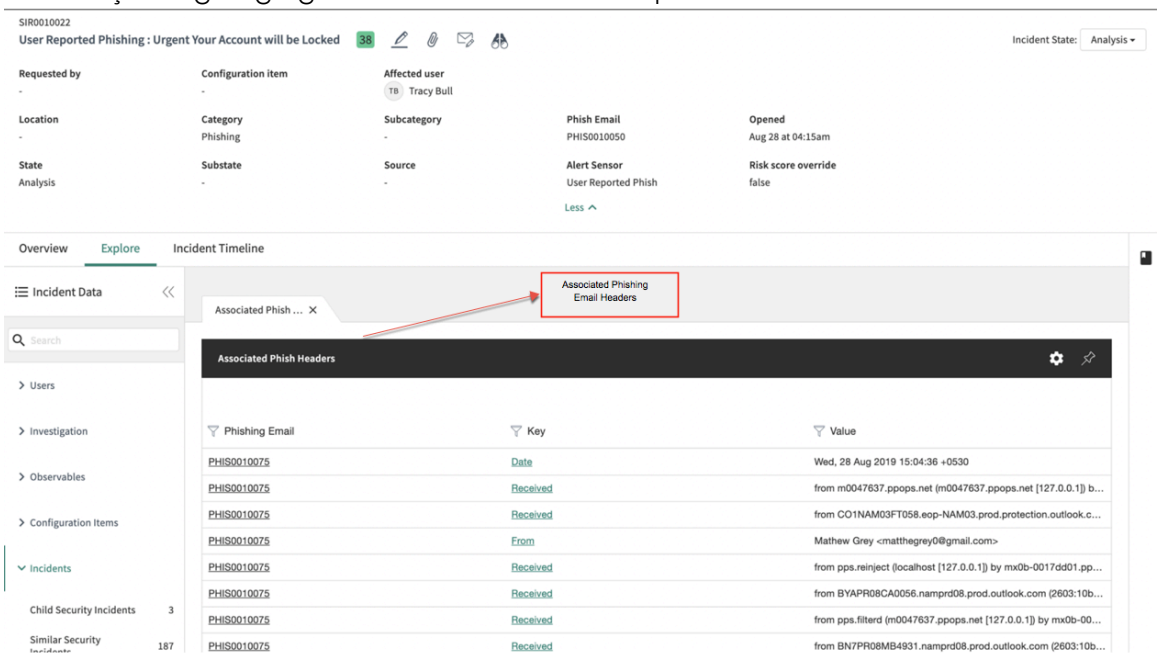
Dans l'onglet **Explorer** , cliquez sur **Incidents** > **Incidents de sécurité enfants**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



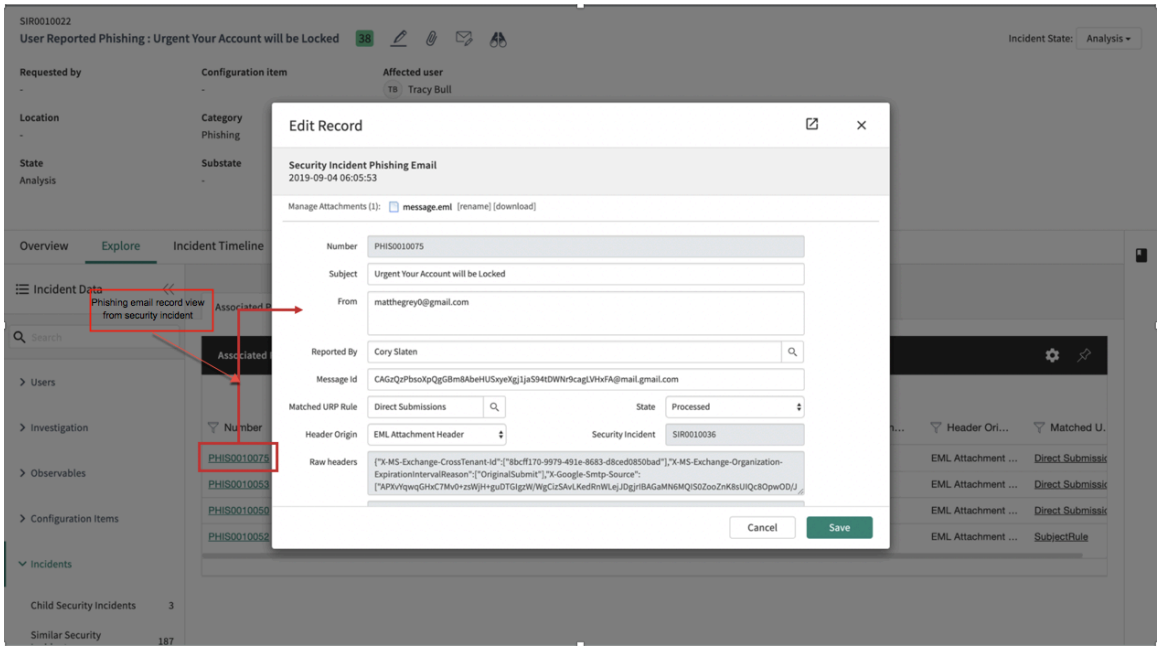
Cliquer sur **Incidents** > **En-têtes d'hameçonnage associés** > . Vous pouvez afficher les en-têtes cumulés de tous les enregistrements enfants et de tous les enregistrements d'e-mails d'hameçonnage agrégés à l'incident de sécurité parent.



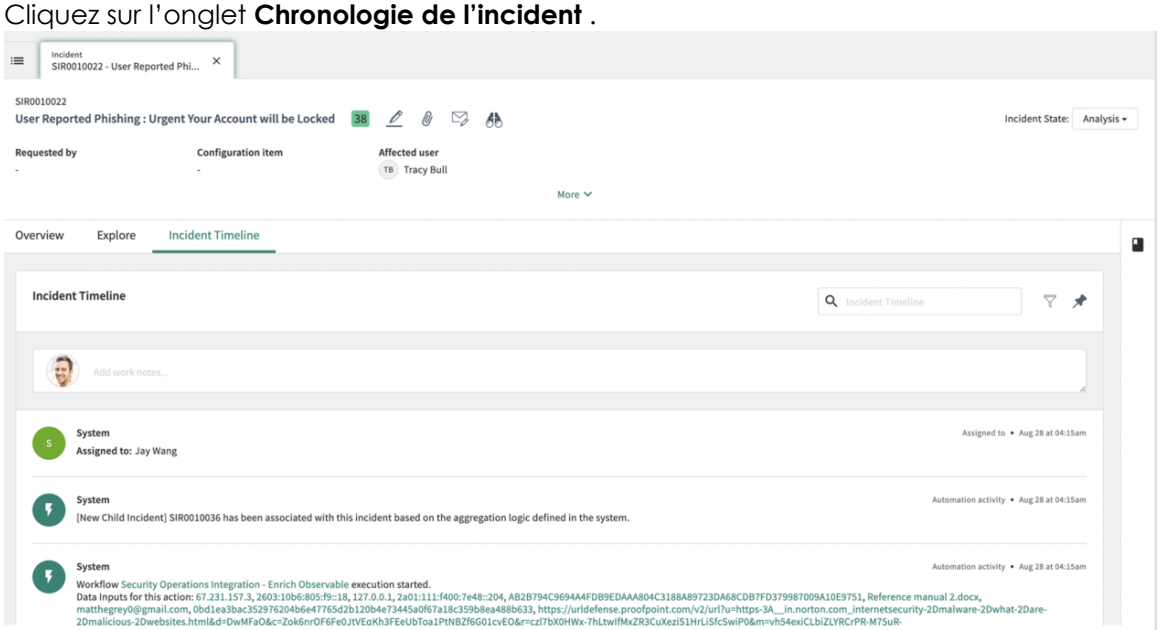
Cliquez sur le lien de l'e-mail d'hameçonnage pour afficher l'enregistrement de l'e-mail d'hameçonnage associé à l'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cliquez sur l'onglet **Chronologie de l'incident** .



Vous pouvez afficher les mises à jour système qui mettent en évidence :

- Enregistrements enfants en double identifiés.
- Liste des éléments observables autorisés.
- Utilisateurs sans correspondance qui ont reçu l'e-mail d'hameçonnage mais qui n'appartiennent pas à la liste des utilisateurs affectés.

Forum aux questions

Cette section recense certaines des questions fréquemment posées sur la fonctionnalité améliorée d'hameçonnage signalé par un utilisateur.

1. J'ai installé le nouveau spoke Security Incident Response, mais je ne peux afficher aucun incident de hameçonnage signalé par un utilisateur.

   Par défaut, la fonctionnalité Hameçonnage signalé par un utilisateur a été désactivée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour activer cette fonctionnalité, vous devez effectuer une copie du flux en lecture seule Transformer les e-mails d'hameçonnage signalés par les utilisateurs en incidents de sécurité et l'activer avant de l'utiliser.

2. Lors de l'ingestion des e-mails d'hameçonnage et de leur conversion en incidents de sécurité, quelles mesures de précaution sont utilisées pour gérer les liens et pièces jointes malveillants contenus dans les e-mails d'hameçonnage ?

L'analyseur ServiceNow antivirus analyse ces pièces jointes et liens malveillants. Toutefois, pour que les analystes de sécurité puissent enquêter sur les incidents avec précision, l'application Réponse aux incidents de sécurité capture tous les artefacts qui font partie d'un e-mail d'hameçonnage. Cependant, la fonctionnalité Hameçonnage signalé par un utilisateur désactive les liens malveillants contenus dans l'e-mail d'hameçonnage afin que les analystes de sécurité ne cliquent pas accidentellement sur ces liens. En ce qui concerne les pièces jointes malveillantes, les analystes de sécurité doivent être prudents lorsqu'ils les téléchargent.

3. Enregistrons-nous tous les fichiers malveillants qui font partie des e-mails d'hameçonnage à des fins d'enrichissement des incidents de sécurité ?

Oui, nous récupérons tous les fichiers des e-mails d'hameçonnage. Vous pouvez afficher ces détails disponibles dans le cadre des observables d'incident de sécurité sous la forme d'un hachage de fichier.

4. Envoyons-nous des fichiers et des liens malveillants à partir d'e-mails d'hameçonnage à une instance de bac à sable pour enquête ?

Actuellement, nous ne prenons pas en charge les intégrations de bac à sable prêtes à l'emploi pour enquêter sur les fichiers et les liens malveillants.

5. Existe-t-il une fenêtre de temps ou un déclencheur qui définit la durée pendant laquelle les enregistrements d'e-mails d'hameçonnage en double entrants sont associés à un incident de sécurité parent ?

Les enregistrements d'e-mails d'hameçonnage en double ne sont agrégés qu'à un incident de sécurité parent actif. Si l'incident parent est fermé ou annulé, le nouvel e-mail d'hameçonnage en double entrant est créé en tant que nouvel incident de sécurité. Toutefois, dans ce scénario, dans le nouvel incident de sécurité, vous pouvez afficher l'incident de sécurité parent fermé ou annulé dans la liste connexe **Incidents de sécurité similaires** .

Remarque : Ce comportement peut être configuré à l'aide du concepteur de flux.

6. La fonctionnalité User Report Phishing prend-elle en charge l'utilisation uniquement du module d'extension **Microsoft Outlook PhishAlarm** (précédemment connu sous le nom de Wombat) pour capturer les détails de l'en-tête des e-mails ?

La fonctionnalité Signalé par l'utilisateur a été conçue pour analyser les en-têtes des e-mails et est conforme aux normes RFC 822. Ainsi, à l'instar du module d'extension **PhishAlarm** (précédemment connu sous le nom de Wombat), tous les autres modules d'extension Microsoft Outlook qui capturent les en-têtes d'e-mail selon les normes RFC822 sont pris en charge.

Création d'enregistrements à partir d'incidents de sécurité

Une fois que vous avez créé et enregistré un incident de sécurité, vous pouvez créer un enregistrement de demande de changement (CHG), d'incident (INC) ou de problème (PRB)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à partir de celui-ci. Vous pouvez également créer un ticket de service clientèle à partir de n'importe quel incident de sécurité.

Créer un changement, un incident ou un problème à partir d'un incident de sécurité

Une fois que vous avez créé et enregistré un incident de sécurité, vous pouvez créer un enregistrement de demande de changement (CHG), d'incident (INC) ou de problème (PRB) à partir de celui-ci.

Avant de commencer

Rôle requis : sn.si_basic ou supérieur

Procédure

1. Ouvrez un incident de sécurité à l'aide de l'une de ces méthodes.
   - Ouvrez un incident de sécurité existant en accédant à **Incident de sécurité** > **Non affecté** > **Incidents**et en cliquant sur un incident de sécurité.
   - Créez un incident de sécurité en accédant à **Incident de sécurité** > **Non affecté** > **Incidents**, cliquez sur **Nouveau**, remplissez le formulaire et enregistrez l'enregistrement.
2. Cliquez avec le bouton droit dans la barre d'en-tête de l'incident de sécurité, puis cliquez sur l'un des onglets suivants :
   - **Créer un changement**
   - **Créer un incident**
   - **Créer un problème**

   Remarque : Ce choix s'applique uniquement si la propriété de fenêtre contextuelle (sn_vul.popup) est activée. Lorsque vous cliquez sur l'un de ces boutons, une fenêtre d'aperçu s'ouvre pour vous montrer les informations de l'incident de sécurité qui est utilisé pour créer le changement, l'incident ou le problème. C'est-à-dire l'élément de configuration, son emplacement, sa priorité et les descriptions courte et longue. Si vous créez une demande de changement, vous pouvez modifier les champs **Priorité**, **Description brève** et **Description** . Si vous créez un incident, vous pouvez modifier les champs **Impact**, **Urgence**, **Description brève** et **Description** . Les champs de l'écran d'incident de sécurité associé ne sont pas affectés.
3. Cliquez sur **Envoyer** pour créer le changement, l'incident ou le problème.

Créer un ticket du service clientèle à partir d'un incident de sécurité

Réponse aux incidents de sécurité est livré avec un mappage de champ par défaut qui mappe un incident de sécurité à un Service clientèle ticket (CS). Vous pouvez créer un ticket CS à partir de n'importe quel incident de sécurité, modifier la **priorité** et ajouter **des notes facultatives**.

Avant de commencer

Rôle requis : sn_si.basic et sn_customerservice_agent

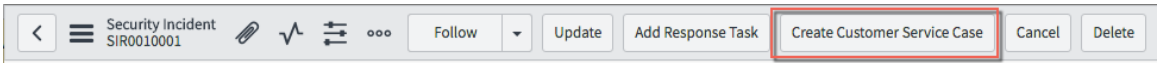
Remarque : Le Service clientèle module d'extension doit être activé pour effectuer cette tâche.

Procédure

1. Accédez à **l'incident de sécurité**.
2. Ouvrez l'incident de sécurité auquel vous souhaitez ajouter un ticket CS.
3. Cliquez sur **Créer un ticket du service clientèle** dans l'en-tête supérieur.

Traduction automatique

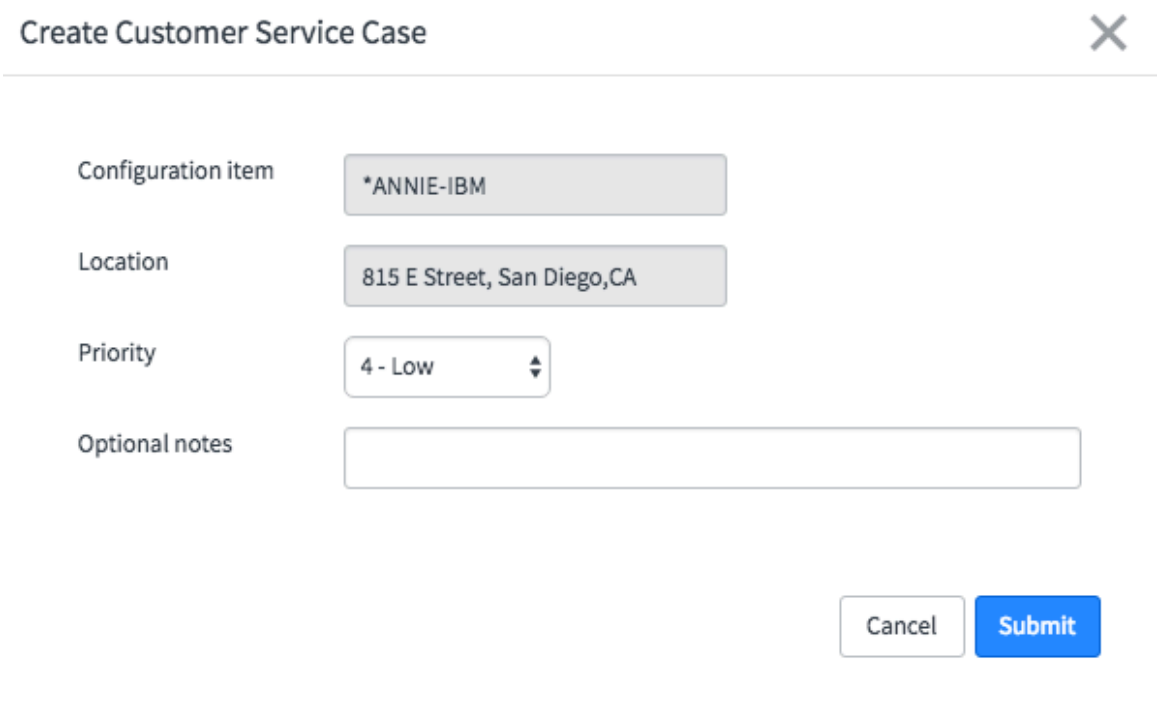
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La fenêtre contextuelle est préremplie avec les informations de l'incident de sécurité en fonction du mappage de vos champs.

4. Vous pouvez sélectionner une nouvelle **priorité** et ajouter des **notes facultatives**.

Remarque : Le champ **Priorité** remplace le paramètre par défaut. Les **notes facultatives** sont annexées à l'incident.



5. Cliquez sur **Envoyer**.
   Un ticket CS est créé et affiché dans la liste connexe Tickets du service clientèle de l'incident de sécurité.
6. Vous pouvez cliquer sur le lien du ticket CS pour suivre le ticket.

Information associée

Customer Service Case Management

Ajouter un incident de sécurité à un ticket de sécurité

Si vous déterminez qu'un incident de sécurité nécessite un niveau d'analyse plus élevé, ajoutez-le à un nouveau ticket ou à un ticket existant.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

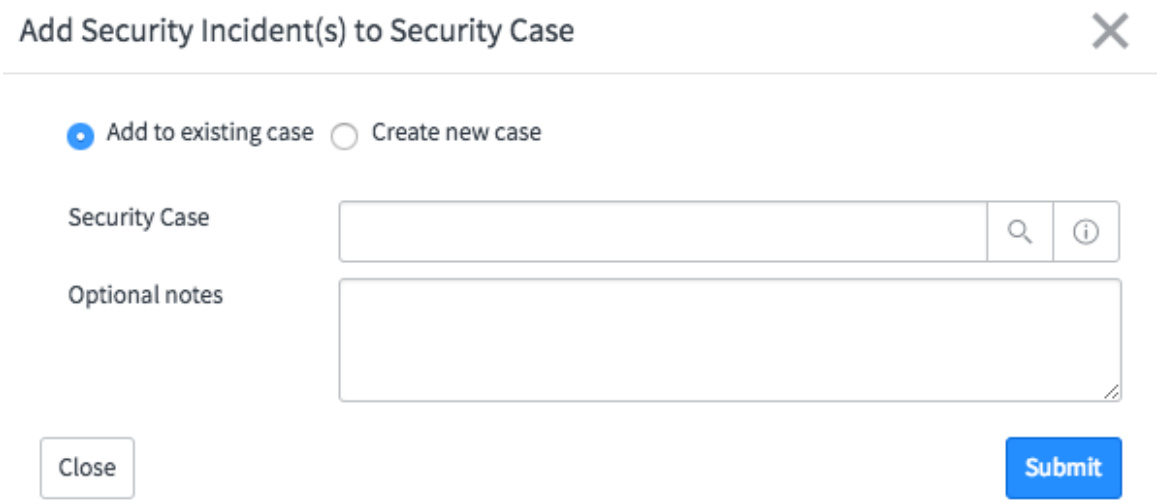
Rôle requis : sn_si.admin, sn_ti.case_user_write

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à l'incident de sécurité qui requiert une escalade en cliquant sur **Incident de sécurité** > **Incidents** > **Me l'affecter**et ouvrez l'incident de sécurité.
2. Cliquez sur le lien connexe **Ajouter au ticket de sécurité** .
   La boîte **de dialogue Ajouter un ou plusieurs incidents de sécurité au ticket de sécurité s'ouvre** .



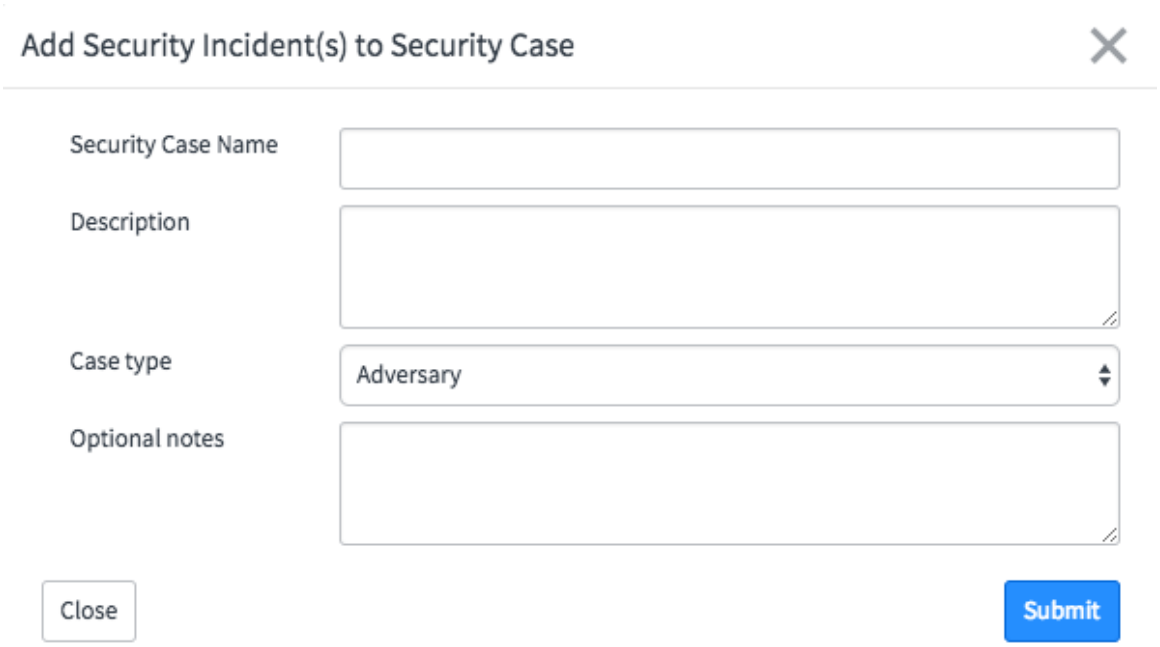
3. Si vous avez un ticket qui vous est affecté et auquel vous souhaitez ajouter cet incident de sécurité, renseignez les champs comme il convient, puis cliquez sur **Soumettre**.

Champ	Description
Ticket de sécurité	Sélectionnez le ticket de sécurité.
Notes facultatives	Au besoin, saisissez des notes supplémentaires qui pourraient être utiles à l'analyste de ticket.

4. Si un ou plusieurs tickets vous sont affectés, mais que vous souhaitez créer un nouveau ticket et lui affecter l'incident de sécurité, cliquez sur **Créer un ticket** pour afficher des champs supplémentaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Si aucun ticket ne vous a été affecté, l'écran ci-dessus s'ouvre en premier.

5. Renseignez les champs comme il convient.

Champ	Description
Nom du ticket de sécurité	Saisissez le nom du nouveau ticket de sécurité.
Description	Entrez une description pour le ticket.
Type de ticket	Sélectionnez le type de ticket faisant l'objet de l'enquête.
Notes facultatives	Au besoin, saisissez des notes supplémentaires qui pourraient être utiles à l'analyste de ticket.

6. Cliquez sur **Envoyer**.
Un message apparaît en haut de l'incident de sécurité, ainsi qu'un lien vers le nouveau ticket.

Information associée

Security Case Management

Créer des tâches de réponse

Une fois qu'un incident de sécurité a été créé, vous pouvez créer des tâches de réponse pour suivre les actions distinctes à effectuer pour répondre au problème de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à l'emplacement approprié pour ouvrir l'incident de sécurité pour lequel vous souhaitez créer des tâches.
   Par exemple :
   - Pour créer une tâche de réponse basée sur un incident de sécurité qui vous est affecté, sélectionnez **Incident de sécurité** > **Incidents** > **Me l'affecter**.
   - Pour créer une tâche de réponse basée sur un incident de sécurité affecté à votre équipe, sélectionnez **Incident de sécurité** > **Incidents** > **Affecté à une équipe** > **Incidents**.
   - Pour créer une tâche de réponse basée sur un incident de sécurité non affecté, sélectionnez **Incident de sécurité** > **Incidents** > **Incidents non affectés**.
2. Ouvrez l'incident de sécurité auquel vous souhaitez ajouter des tâches de réponse.
3. Cliquez sur le bouton **Ajouter une tâche de réponse** dans l'en-tête du formulaire.

   Remarque : Pour créer d'autres tâches, cliquez sur l'onglet **Tâches** dans la liste connexe des incidents. Pour plus d'informations sur la création d'autres types de tâches, voir Créez une tâche .

4. Renseignez les champs du formulaire comme il convient.

Incident de sécurité

Champ	Description
Sélectionner une balise de sécurité	Si vous configurez et activez des balises de sécurité, vous pouvez sélectionner une ou plusieurs balises pour ajouter des métadonnées à l'enregistrement ou spécifier le degré de sensibilité de la tâche de réponse. Si vous n'avez pas configuré ou activé les balises de sécurité, cette liste déroulante ne s'affiche pas.
Numéro	[Lecture seule] Numéro généré Réponse aux incidents de sécurité automatiquement.
Parent	[Lecture seule] Numéro de l'incident de sécurité associé.
Élément de configuration	Élément de configuration (ressource) affecté par le problème de sécurité.
Utilisateur affecté	La personne affectée par le problème de sécurité.
Priorité	Priorité utilisée pour déterminer le moment d'exécution de cette tâche.
État	État actuel de la tâche de réponse de sécurité. Lors de la création de la tâche, ce champ est défini par défaut sur **Brouillon**.
Compétences	Compétence requise pour effectuer cette tâche. Cliquez sur l'icône de verrouillage et sélectionnez la compétence requise. Une fois que vous avez terminé vos sélections, cliquez à nouveau sur l'icône de verrouillage.
Groupe d'affectation	Groupe d'affectation à partir duquel l'agent affecté est sélectionné.
Affecté à	Personne affectée à l'exécution de la tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description brève	Description de la Réponse aux incidents de sécurité tâche.
Description	Description de la tâche sélectionnée.
Notes sécurisées	Les notes de travail qui sont chiffrées et invisibles pour le client.
Notes de travail	Notes de travail qui ne sont pas visibles par le client.
Commentaires supplémentaires	Commentaires que vous souhaitez rendre visibles pour le client.

5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Remarque : Une fois les tâches créées Réponse aux incidents de sécurité , vous pouvez les afficher à l'aide de l'une des applications suivantes sous le module **Tâches de réponse** :

- **qui m'a été assignée**.
- **Affecté à l'équipe**.
- **Afficher les tâches ouvertes**
- **Afficher toutes les tâches**
- **Tâches non affectées**.

Gérer Intelligence prédictive pour le hameçonnage signalé par les utilisateurs

La fonctionnalité Intelligence prédictive pour le hameçonnage signalé par les utilisateurs offre une solution importante pour trier et classer par ordre de priorité les e-mails d'hameçonnage signalés par les utilisateurs.

Cette section décrit les points suivants :

- Intelligence prédictive pour le hameçonnage signalé par les utilisateurs
- Composants et modules d'extension requis
- Génération d'un verdict final pour le hameçonnage signalé par les utilisateurs
- Dépanner Predictive Intelligence pour le hameçonnage signalé par les utilisateurs

Intelligence prédictive pour le hameçonnage signalé par les utilisateurs

Cette fonctionnalité aide les analystes de sécurité à trier et à classer par ordre de priorité les e-mails de hameçonnage signalés par les utilisateurs.

Le cadre de travail Intelligence prédictive fournit des solutions pour entraîner le système à prédire, recommander et organiser les résultats des données. Pour en savoir plus sur Intelligence prédictive, reportez-vous à Intelligence prédictive . À l'aide de ce cadre, vous pouvez créer des modèles pour prédire automatiquement si un e-mail d'hameçonnage signalé par un utilisateur est suspect ou légitime.

À l'aide des données historiques sur les incidents de sécurité de hameçonnage signalés par les utilisateurs (en-têtes des e-mails, corps des e-mails et résultats de triage capturés via les codes de fermeture des incidents de sécurité), les analystes de sécurité peuvent former le système à classer les soumissions de hameçonnage signalées par les utilisateurs entrantes

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

comme celles qui doivent être triées davantage (probablement suspectes) et celles qui sont légitimes.

En triant automatiquement les e-mails entrants, les analystes de sécurité peuvent facilement hiérarchiser la file d'attente des incidents et se concentrer sur les incidents qui sont susceptibles de représenter un risque pour l'organisation en premier lieu et consacrer moins d'efforts aux e-mails qui sont très susceptibles d'être des faux positifs. Le résultat de prédiction fournit également un score de confiance sur la classification pour permettre une hiérarchisation granulaire.

Composants et modules d'extension requis

Pour utiliser Intelligence prédictive pour le hameçonnage signalé par les utilisateurs, vous devez installer les applications suivantes

Nom du module d'extension	Version minimale
Réponse aux incidents de sécurité	9.0.1 ou 10.0.2
Intelligence prédictive	Version Orlando
Intelligence prédictive pour le hameçonnage signalé par les utilisateurs	10.0.2

Remarque : Les nouvelles améliorations suivantes sont disponibles avec Security Incident Response 10.4 :

- Possibilité de choisir des codes de fermeture dans les champs personnalisés pour la formation du modèle.
- Possibilité d'activer explicitement les prédictions après la création du modèle.
- Possibilité de générer un verdict final sur la soumission d'hameçonnage signalé par un utilisateur à l'aide d'une table de décision. (requiert le spoke Security Operations 10.3.0)

Pour utiliser les nouvelles améliorations, vous devez mettre à niveau les applications suivantes :

Nom du module d'extension	Effectuer une mise à niveau vers
Réponse aux incidents de sécurité	10.0.4
Intelligence prédictive pour le hameçonnage signalé par les utilisateurs	10.3.1

Tables nouvelles et mises à jour

- sn_sir_ml_urp_config (Nouveau) : contient la configuration de l'application URP ML.
- sn_sir_ml_urp_feature (Nouveau) : enregistrements extraits de la table d'e-mail sn_si_phishing.
- sn_sir_ml_urp_feature_import (Nouveau) : permet de charger des données d'historique des e-mails d'hameçonnage.
- sn_si_incident (mis à jour) : Les nouveaux champs suivants ont été ajoutés :
  - Prédiction acceptée
  - Résultat de prédiction
  - Score de confiance

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Includes de script**
  - URPMLUtil : récupère la configuration, exécute la tâche de prédiction et suit le processus de prédiction.
  - URPMLProcessor : Extrait et traite les données de la table sn_si_phishing_email.
  - URPMLAction : exécute le flux pour accepter le résultat de prédiction.

Génération d'un verdict final pour le hameçonnage signalé par les utilisateurs

Les équipes de Security Incident Response peuvent désormais générer le verdict final pour un enregistrement d'hameçonnage signalé par un utilisateur, en fonction des résultats des intégrations de Predictive Intelligence et d'enrichissement des menaces.

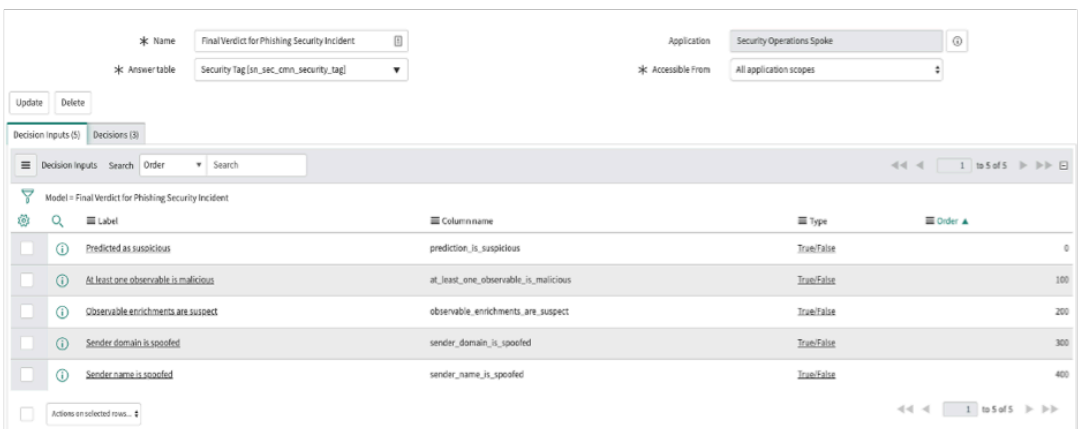
Cette génération de verdict final est activée par la construction d'une table de décision et exploitée dans un flux.

Prérequis

Assurez-vous que tous les modules d'extension répertoriés dans Composants et modules d'extension requis ont été installés.

Accédez à la **Intelligence prédictive pour l'hameçonnage** > **Verdict final** > **Verdict final pour l'incident de sécurité de hameçonnage**.

L'onglet Entrées de décision affiche les différentes conditions qui ont été évaluées pour arriver au verdict final.



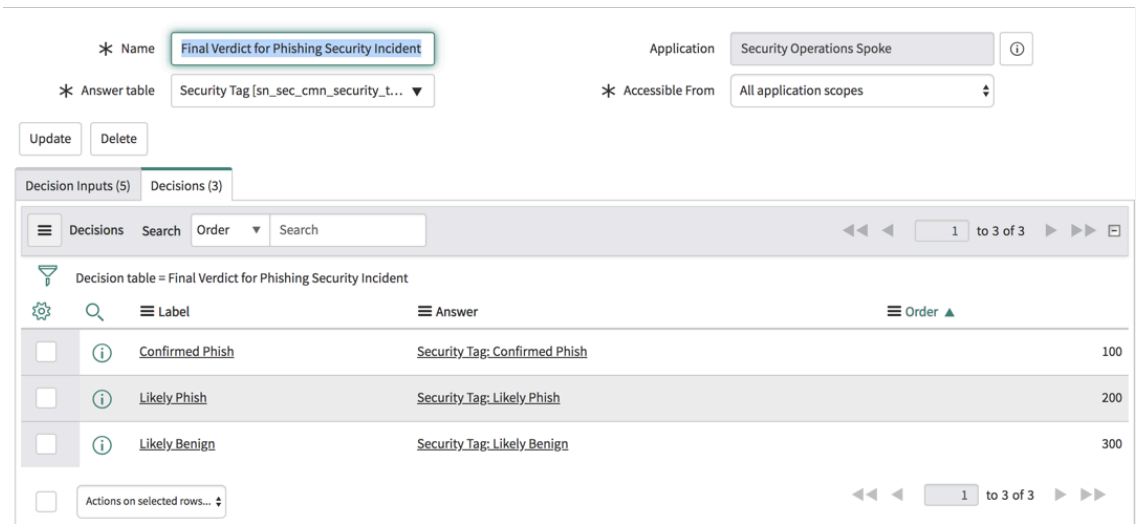
Les conditions suivantes sont disponibles avec le système de base :

- Prédit comme suspect : lorsque Predictive Intelligence a classé l'e-mail d'hameçonnage signalé par l'utilisateur comme **suspect.**
- Au moins un observable est malveillant : lorsqu'un observable impliqué dans l'incident de sécurité (par exemple, URL, domaine, adresse IP, hachage) a été classé comme **malveillant** par des sources de renseignements sur les menaces.
- L'enrichissement des observables est suspect : lorsque l'enrichissement des observables (par exemple, récence de l'enregistrement du domaine hameçonnage, pays de l'enregistrement du domaine hameçonnage) est considéré comme suspect.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le domaine de l'expéditeur est falsifié : lorsque le domaine de messagerie de l'hameçonneur est soupçonné d'usurper un domaine de confiance.
- Le nom de l'expéditeur est falsifié : lorsque l'adresse e-mail de l'hameçonneur est suspectée d'usurper un employé de confiance d'une organisation.

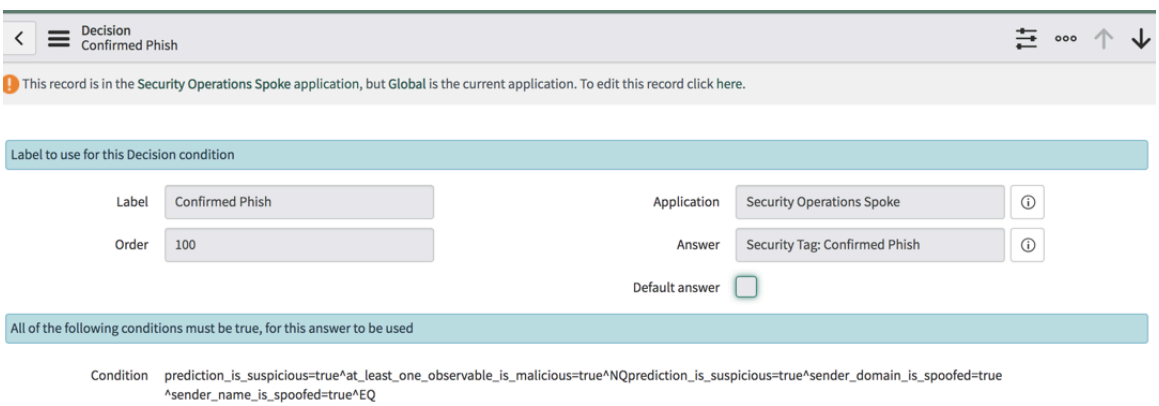
L'onglet **Décisions** affiche les options de verdict final qui peuvent être obtenues pour un incident de sécurité donné.



Les décisions suivantes sont disponibles avec le système de base :

- Hameçonnage confirmé : lorsque les conditions ont conduit au verdict final comme étant un e-mail d'hameçonnage confirmé.
- Hameçonnage probable : lorsque les conditions ont conduit au verdict final en tant que tentative d'hameçonnage potentielle.
- Probablement bénin : Lorsque les conditions ont conduit au verdict final en tant que soumission bénigne.

Vous pouvez voir les conditions qui ont été évaluées pour chacune des options de verdict final. Cliquez sur le lien Étiquette pour voir les conditions.



Vous pouvez personnaliser la table de décision fournie avec le système de base ou créer votre propre table de décision. Cette table de décision peut être exploitée dans les playbooks Security Incident Response. Le flux secondaire **Générer un verdict final pour les incidents de sécurité de hameçonnage** est disponible avec le système de base. Ce

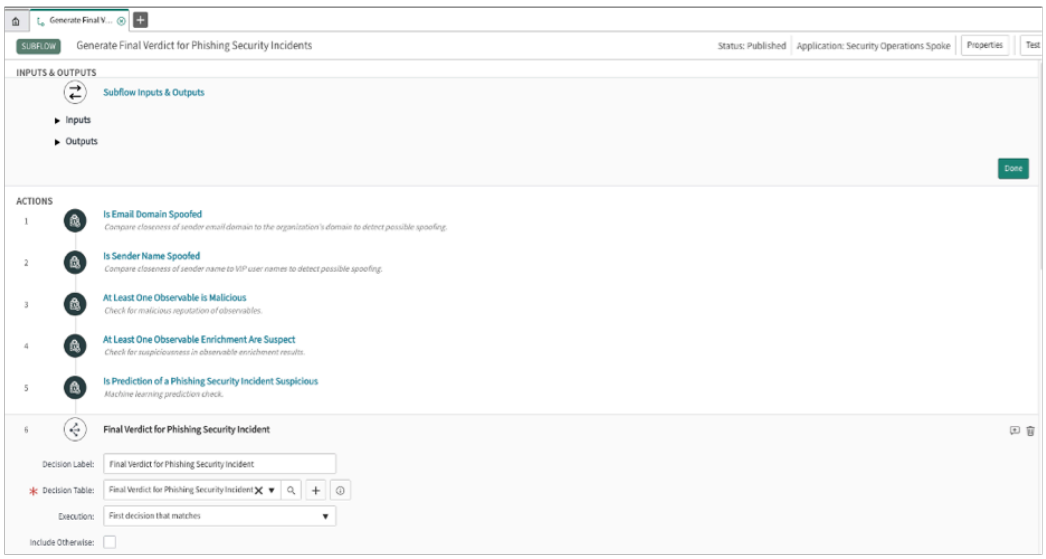
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

flux secondaire génère automatiquement le verdict final pour un incident de sécurité de hameçonnage et applique une balise de sécurité en fonction de cette décision. Vous pouvez inclure ce flux secondaire dans le cadre du playbook **Hameçonnage automatisé** .

Les entrées de ce flux secondaire sont les suivantes :

- incident_id : ID système de l'incident de sécurité de hameçonnage.
- c_level_names : liste de noms séparés par des virgules (par exemple, les noms des dirigeants de l'organisation) probablement falsifiés dans l'attaque d'hameçonnage.
- trusted_domains : liste séparée par des virgules de domaines de messagerie approuvés.
- enrichment_keywords : liste de mots clés séparés par des virgules qui indiquent le caractère malveillant de l'observable à partir des résultats d'enrichissement.
- sender_email (facultatif) : l'adresse e-mail de l'expéditeur de l'e-mail d'hameçonnage.

La sortie de ce flux peut être **Hameçonnage confirmé**, **Hameçonnage probable** ou **Probablement bénin**.



Dépanner Predictive Intelligence pour le hameçonnage signalé par les utilisateurs

Cette section couvre quelques scénarios de problèmes courants.

- Problème : je ne peux pas modifier la configuration d'Intelligence prédictive.

  Solution : vérifiez si vous disposez des autorisations nécessaires pour le faire. Vous devez vous connecter en tant qu'utilisateur disposant du rôle ml_admin pour modifier les seuils. Certains scénarios peuvent nécessiter des privilèges encore plus élevés, comme, par exemple, la nécessité de modifier la limite de données d'entraînement. Pour de tels scénarios, vous devez contacter le service client pour obtenir de l'aide.

- Problème : échec de la formation du modèle.

  Solution : vérifiez si les URL du planificateur ML ont été configurées. Accédez à la **Propriétés système** > **Toutes les propriétés** et vérifiez si la propriété *glide.shared_service_scheduler.url* a été configurée.

- Problème : les résultats de prédiction ne sont pas disponibles sur un incident de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Solution:

- Vérifiez si l'URL de prédiction a été configurée dans la propriété système *glide.prediction_service.url* et assurez-vous que le centre de données correspond à l'URL.
- Vérifiez si la tâche planifiée Prédire l'e-mail d'hameçonnage signalé par l'utilisateur est active.

Configurer Intelligence prédictive pour le hameçonnage signalé par les utilisateurs

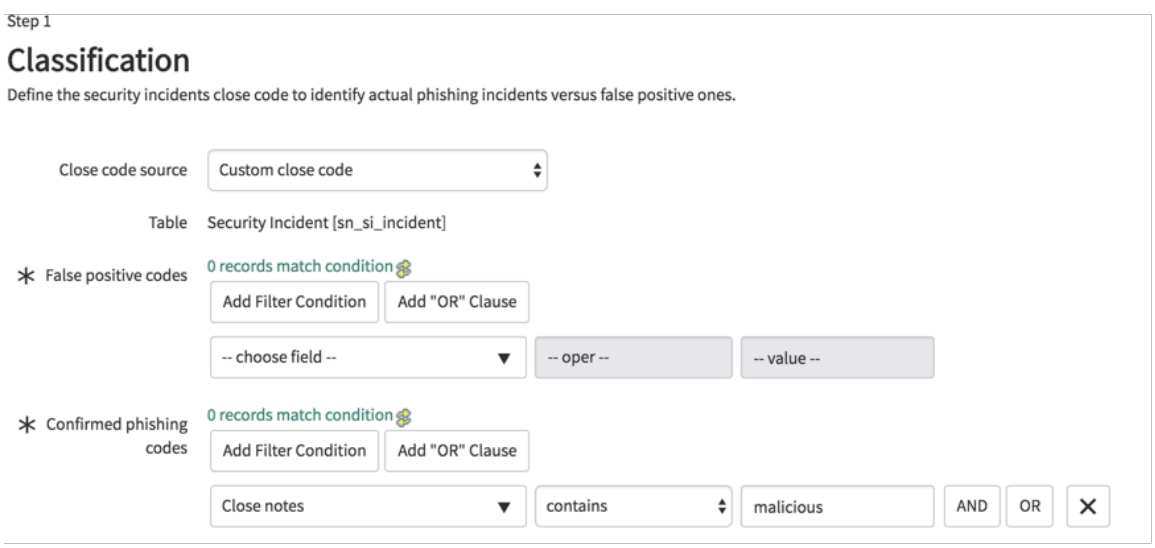
Configurez et préparez le modèle pour identifier les e-mails d'hameçonnage signalés par les utilisateurs.

Avant de commencer

Rôle requis : ml_admin

Procédure

1. Accédez à la **Tout** > **Intelligence prédictive pour l'hameçonnage** > **Configuration**.
2. À l'étape 1 de la configuration, sélectionnez l'une des options suivantes dans la liste Source du code de fermeture :
   - Code de fermeture par défaut : sélectionnez cette option pour spécifier les codes de fermeture d'incident de sécurité par défaut qui doivent être utilisés par le modèle de formation pour identifier les e-mails malveillants et les e-mails légitimes. Cliquez sur l'icône de verrouillage et sélectionnez un ou plusieurs codes de faux positif ou des codes de hameçonnage confirmés.
   - Code de fermeture personnalisé : sélectionnez l'option Code de fermeture personnalisé si vous souhaitez définir des codes de fermeture à partir de champs personnalisés qui peuvent être utilisés dans le cadre de vos procédures de réponse aux incidents existantes. Pour définir un code de fermeture, sélectionnez un champ dans la table d'incidents de sécurité et spécifiez une ou plusieurs conditions de filtre.



3. À l'étape 2, importez des données historiques qui peuvent être utilisées pour former le modèle.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sélectionnez la source de données pour importer les données historiques. Il peut s'agir de :

- Tableau des e-mails de hameçonnage signalés par un utilisateur : vous pouvez afficher le nombre d'enregistrements qui peuvent être importés en tant que données historiques. Sélectionnez cette option et cliquez sur **Importer**.
- Source de données personnalisée : vous pouvez joindre un seul fichier CSV formaté contenant des enregistrements de données historiques. Sélectionnez le fichier et cliquez sur **Importer**.

Remarque : Le fichier CSV que vous importez doit contenir les en-têtes suivants :

- Étiquette
- En-tête
- Corps de texte

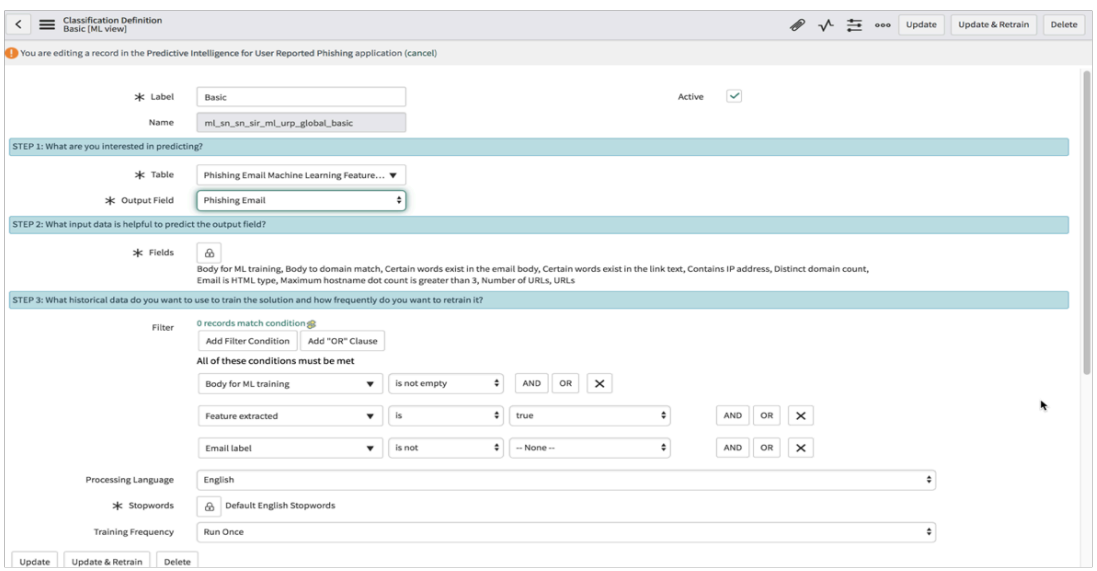
Chaque enregistrement doit contenir une balise malveillante ou légitime dans la colonne Étiquette du fichier CSV.

Cliquez sur **Annuler l'importation** pour arrêter l'importation des données. Le processus d'importation est annulé et tous les enregistrements importés jusqu'à présent sont supprimés.

4. Une fois que vous avez importé les données historiques, cliquez sur le lien pour actualiser la page.
   Vous pouvez ensuite importer d'autres données de formation ou passer à l'étape suivante.
5. À l'étape 3, vérifiez si le nombre d'enregistrements disponibles pour la formation répond aux exigences de seuil minimal.

Remarque : Les valeurs par défaut du nombre maximal et minimal d'enregistrements de formation s'affichent. Ces seuils peuvent être modifiés dans la page des propriétés d'apprentissage machine de la plateforme. Contactez le support client pour obtenir de l'aide.

6. Si les données d'entraînement sont suffisantes, cliquez sur **Former le modèle**.
   Vous pouvez mettre à jour les entrées de formation dans l'écran ci-dessous.



7. Les entrées de prédiction que vous pouvez modifier sont les suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Que souhaitez-vous prédire ?
- Quelles données d'entrée permettent de prédire le champ de sortie ?
- Quelles données historiques souhaitez-vous utiliser pour former la solution et à quelle fréquence souhaitez-vous la reformer ?

Les valeurs par défaut de ces entrées s'affichent. Vous pouvez les modifier et cliquer sur l'un des éléments suivants :

- **Mettre à jour** : met à jour la définition du modèle de formation.
- **Mettre à jour et reformer** : met à jour la définition du modèle de formation et reformate le modèle (déclenche la fonction **Former le modèle**).

8. Enfin, lorsque vous avez terminé l'entraînement du modèle, cochez la case **Activer la prédiction** .
   Les prédictions sont désormais fournies sur chaque enregistrement de hameçonnage signalé par un utilisateur à l'aide de ce modèle. Si vous souhaitez arrêter de fournir des prédictions sur les enregistrements de hameçonnage signalés par les utilisateurs, décochez la case **Activer la prédiction** et cliquez sur **Désactiver**.

Affectation des analystes de sécurité

En fonction des paramètres que vous avez définis dans l'écran Configuration de l'administration, vous pouvez affecter des analystes de sécurité aux incidents de sécurité manuellement, automatiquement à l'aide d'un workflow ou automatiquement à l'aide de l'affectation SIR automatique.

Affectation manuelle d'analyste

Vous pouvez configurer l'écran de configuration de l'administration Réponse aux incidents de sécurité pour exiger que les analystes de sécurité soient affectés manuellement chaque fois qu'une personne ou l'application SIR crée un incident de sécurité ou génère une tâche de réponse de sécurité.

Si un incident de sécurité ou une tâche de réponse ne peut pas être affecté automatiquement, vous pouvez configurer l'écran Configuration de l'administration SIR pour exiger l'affectation manuelle d'analystes de sécurité. Il s'agit d'un bon choix si vous disposez d'un nombre limité d'analystes de sécurité pour répondre aux demandes ou si vous ne souhaitez tout simplement pas les affecter automatiquement.

Affectation d'analyste de sécurité basée sur les workflows

Vous pouvez configurer l'écran de configuration de l'administration Réponse aux incidents de sécurité pour utiliser un workflow sélectionné afin d'affecter l'analyste de sécurité chaque fois qu'une personne ou l'application SIR crée un incident de sécurité ou une tâche de réponse de sécurité.

Dans l'écran de configuration de l'Administration des incidents de sécurité, vous pouvez choisir d'utiliser un workflow pour affecter un analyste à chaque tâche d'incident de sécurité ou de réponse de sécurité. Cette option est un bon choix pour les organisations qui utilisent un processus personnalisé pour résoudre les problèmes de sécurité ou qui disposent d'un processus qui peut être automatisé.

Affectation automatique d'analyste de sécurité

Vous pouvez configurer l'écran de configuration de l'administration Réponse aux incidents de sécurité afin d'affecter automatiquement l'analyste de sécurité chaque fois qu'une personne ou l'application SIR crée un incident de sécurité ou une tâche de réponse de sécurité. L'affectation automatique vous permet de définir, en fonction des besoins de votre

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

organisation, les critères selon lesquels les analystes sont affectés automatiquement aux incidents de sécurité.

Affectation automatique de l'agent en fonction des évaluations de l'agent

Si l'affectation automatique est activée et qu'un incident de sécurité ou une tâche de réponse est créé, les actions suivantes se produisent :

- Les analystes de sécurité disponibles sont évalués en fonction des critères définis dans la configuration.
- Un analyste de sécurité approprié est automatiquement affecté à la tâche.
- La tâche passe à l'état **Affecté**.

Si la configuration est configurée pour prendre en compte plusieurs ensembles de conditions, telles que les compétences, l'emplacement, le fuseau horaire ou la zone de couverture du groupe, les analystes de sécurité sont évalués en fonction des paramètres de propriété de pondération et d'autres critères. Ces paramètres de configuration vous permettent d'affecter automatiquement des agents en fonction de propriétés facultatives. Les évaluations calculées sont utilisées pour déterminer le meilleur agent pour l'incident de sécurité ou la tâche de réponse. Toute combinaison de méthodes basées sur l'évaluation peut être activée dans l'écran de configuration de l'application.

Lorsqu'une tâche est créée, une note pour chaque type de critères de sélection activé est calculée pour chaque agent disponible. L'agent dont la note totale est la plus élevée est pris en compte pour l'affectation automatique.

Les paramètres des propriétés de pondération d'affectation automatique, trouvés dans **Incident de sécurité** > **Administration** > **Propriétés**, sont inclus dans les calculs de cote.

Ces valeurs vous aident à classer par ordre de priorité les critères de sélection des affectations automatiques qui sont les plus importants pour votre organisation. Définissez les valeurs de priorité entre 1 (moins important) et 10 (important).

Pour un exemple de la façon dont les propriétés de pondération affectent les notes des agents, consultez Affectation automatique des agents à l'aide de plusieurs critères de sélection.

Affectation automatique d'agent à l'aide de l'emplacement

Les agents peuvent être affectés automatiquement en fonction de l'emplacement du domicile dans leur enregistrement utilisateur et de l'emplacement des tâches.

L'affectation automatique par emplacement s'effectue lorsque l'option **de configuration La sélection automatique d'agents tiendra compte de l'emplacement des agents** est activée.

Lorsqu'une tâche (incident de sécurité ou tâche de réponse) est créée, l'agent le plus proche de l'emplacement de la tâche est pris en compte pour la tâche. Si l'application est configurée de manière à ce que seul l'emplacement soit pris en compte, la tâche est automatiquement affectée à l'agent le plus proche.

Lorsqu'une tâche est créée, les emplacements des agents sont comparés aux plages suivantes pour déterminer la note de chaque emplacement d'agent.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calcul de la note d'emplacement

Distance (miles) entre l'agent et la tâche	Évaluation
0 à 0,1	1
0,11 à 0,5	0,9
0,51 à 5	0,7
5,1 à 10	0,5
10,1 à 20	0,4
20,1 à 30	0,3
30,1 à 40	0,2
40,1 à 100	0.1
>100	0

Si l'application est configurée pour utiliser d'autres critères de sélection, tels que les compétences, le fuseau horaire ou le calendrier, les évaluations de tous les critères de sélection sont pondérées et additionnées. L'agent ayant la note globale la plus élevée est automatiquement affecté à la tâche. Consultez Affectation automatique des agents à l'aide de plusieurs critères de sélection pour en savoir plus.

Affectation automatique de l'agent à l'aide des compétences

Les agents peuvent être affectés automatiquement en fonction de leurs compétences et des compétences requises pour effectuer la tâche. Affecter des compétences à leurs enregistrements utilisateur à l'aide de **Compétences** > **Utilisateurs**.

L'affectation automatique par compétences peut être effectuée lorsque l'option de configuration La **sélection automatique d'agents pour des tâches qui nécessite qu'ils aient des compétences** est définie sur **tout** ou **sur certains**.

Lorsqu'une tâche comprenant des compétences est affectée automatiquement, les compétences d'un agent sont comparées aux compétences requises pour effectuer la tâche. Une évaluation est calculée en fonction de l'option de configuration des compétences. Si l'option est définie sur **Certaines**, la tâche est automatiquement affectée à l'agent dont les compétences sont les plus proches. Si l'option est définie sur **Toutes**, seuls les agents qui possèdent toutes les compétences requises sont pris en compte. Si aucun agent ne possède toutes les compétences requises pour effectuer la tâche, aucun n'est affecté automatiquement.

L'évaluation des compétences est calculée comme suit :

Skills_agent/Skills_task

Où :

- Skills_agent est le nombre de compétences de l'agent qui correspondent aux compétences requises pour la tâche.
- Skills_task est le nombre total de compétences requises pour la tâche.

Par exemple, une tâche exige quatre compétences, l'agent A possède trois d'entre elles et l'agent B en possède deux :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cote de compétence de l'agent A = 3/4 ou 0,75
- Cote de compétence de l'agent B = 2/4 ou 0,5

Si l'application est configurée pour utiliser d'autres critères de sélection, tels que l'emplacement ou le fuseau horaire, les évaluations de tous les critères de sélection sont pondérées et additionnées. L'agent ayant la note globale la plus élevée est sélectionné pour la tâche. Consultez Affectation automatique des agents à l'aide de plusieurs critères de sélection pour en savoir plus.

Affectation automatique de l'agent à l'aide des fuseaux horaires

Les agents peuvent être affectés automatiquement en fonction du fuseau horaire défini dans leurs enregistrements utilisateur et du fuseau horaire des tâches.

Si l'option **de sélection automatique d'agents tiendra compte du fuseau horaire pour la configuration des tâches** est activée, l'affectation automatique par fuseau horaire peut être effectuée.

Lorsqu'une tâche est créée, les agents se trouvant dans le fuseau horaire le plus proche de celui de la tâche sont pris en compte pour la tâche. Si l'application est configurée de manière à ce que seul le fuseau horaire soit pris en compte, seul un agent se trouvant dans le même fuseau horaire peut être affecté automatiquement à la tâche.

Remarque : Il est important que les fuseaux horaires de l'agent et de la tâche soient définis correctement.

Lorsqu'une tâche est créée, les agents sont évalués en fonction du fuseau horaire de la tâche et du fuseau horaire de l'agent à l'aide de la formule suivante :

1 - [abs(Task_tz – Agent_tz) ÷ 12]

où :

- abs est la fonction mathématique de calcul de la valeur absolue.
- Task_tz est le décalage entre le fuseau horaire de la tâche et le fuseau GMT.
- Agent_tz le décalage entre le fuseau horaire de l'agent et le fuseau GMT.

Par exemple, une tâche est créée à New York (GMT-4) et deux agents sont disponibles pour effectuer la tâche, l'un à Los Angeles (GMT-7) et l'autre à Paris (GMT+1).

La note de l'agent à Los Angeles est calculée comme suit :

1 - abs((-4) - (-7)) ÷ 12 ou 0,75

La note de l'agent à Paris est calculée comme suit :

1 - abs((-4) - (+1)) ÷ 12 ou 0,58

Ainsi, si l'affectation automatique de la tâche est basée uniquement sur le fuseau horaire, elle est affectée à l'agent de Los Angeles.

Si l'application est configurée pour utiliser d'autres critères de sélection, tels que les compétences ou l'emplacement, les évaluations de tous les critères de sélection sont pondérées et additionnées. L'agent ayant la note globale la plus élevée est sélectionné pour la tâche. Consultez Affectation automatique des agents à l'aide de plusieurs critères de sélection pour en savoir plus.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affectation automatique de l'agent à l'aide des zones de couverture de groupe

Les agents peuvent être affectés automatiquement en fonction de la zone de couverture de groupe définie dans leurs enregistrements utilisateur.

Affectation automatique des agents à l'aide de plusieurs critères de sélection

Lorsqu'une tâche est créée, les évaluations des agents sont calculées. Pour en savoir plus, consultez :

- Affectation automatique d'agent à l'aide de l'emplacement
- Affectation automatique de l'agent à l'aide des compétences
- Affectation automatique de l'agent à l'aide des fuseaux horaires

L'affectation automatique est basée sur le calcul suivant :

(Note Criteria_1 x Pondération Criteria_1) + (Note Criteria_2 x Pondération Criteria_2) + (Note Criteria_3 x Pondération Criteria_3) / Nombre de types de critères utilisés où :

Nombre de types de critères utilisés = 1, 2 ou 3 selon les paramètres d'emplacement, de compétence et de fuseau horaire utilisés.

Cet exemple calcule l'affectation automatique de l'agent en fonction de l'emplacement et des compétences. L'exemple est basé sur les hypothèses suivantes.

- L'option de configuration **La sélection automatique d'agents tiendra compte de leur localisation** est activée pour l'application.
- L'option de configuration **La sélection automatique d'agents pour des tâches requiert qu'ils aient des compétences** est activée pour l'application.
- La propriété **Poids des compétences** est définie sur 10 pour l'application.
- La propriété **Poids de l'emplacement** est définie sur 5 pour l'application.
- Les agents A et B sont disponibles pour effectuer une tâche qui nécessite quatre compétences spécifiques.
- L'emplacement de l'agent A se trouve à 5 miles du site de la tâche et possède trois des quatre compétences requises.
- L'emplacement de l'agent B se trouve à un quart de mile du site et possède deux des compétences requises.

L'affectation automatique des agents utilise le calcul suivant : `[(Évaluation de l'emplacement x Poids de l'emplacement) + (Évaluation des compétences x Poids des compétences)]/ 2`

- Le calcul de l'affectation automatique pour l'agent A est le suivant : `[(0,7 x 0,5) + (0,75 x 1)]/ 2 = 0,55`
- Le calcul de l'affectation automatique pour l'agent B est le suivant : `[(0,9 x 0,5) + (0,5 x 1)]/ 2 = 0,475`

Dans cet exemple, la tâche est automatiquement affectée à l'agent A.

Gestion des incidents de sécurité et des demandes entrantes

Une fois qu'un incident de sécurité a été créé, de nombreux types d'informations peuvent être ajoutés et consultés au fur et à mesure que votre analyse du problème progresse vers sa résolution.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Les dernières fonctionnalités de sont Réponse aux incidents de sécurité exclusivement disponibles dans le Espace de travail de la Réponse aux incidents de sécurité. Veuillez installer ou mettre à niveau vers la dernière Réponse aux incidents de sécurité version pour Espace de travail de la Réponse aux incidents de sécurité accéder et exploiter des fonctionnalités telles que Transfert d'équipe, Calculateur de score de risque, etc.

Cette section décrit les points suivants :

- Créer une demande entrante
- Gérer les observables
- Gérer les recherches et les analyses
- Gérer l'orchestration àla demande
- Calculer la gravité d'un incident de sécurité
- Gérer les activités post-incident
- Fermer les incidents de sécurité

Créer une demande entrante

Contrairement aux incidents de sécurité, les demandes entrantes sont généralement moins prioritaires. Les demandes de recherche, d'analyse ou de nouveau badge sont des exemples de demandes entrantes.

Avant de commencer

Rôles requis : rôle sn_si.basic ou supérieur

Procédure

1. Accédez à l'un des formulaires de demandes.
   Par exemple : **Tout** > **Incident de sécurité** > **Demandes entrantes** > **Me l'affecter**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Demande de sécurité

Champ	Description
Numéro	[Lecture seule] Numéro de demande de sécurité généré automatiquement.
Société	Société demandeuse
Emplacement	L'emplacement du CI, le cas échéant. Ce champ est pré-rempli lorsque le CI est sélectionné.
Élément de configuration	Élément de configuration affecté par la demande.
Priorité	La priorité de la demande.
Ouverts	[Lecture seule] Date et heure d'ouverture de la demande.
État	État actuel de la demande de sécurité. Lors de la création de la demande de sécurité, ce champ est défini par défaut sur **Brouillon**.
Groupe d'affectation	Groupe d'affectation à partir duquel l'agent affecté est sélectionné.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Affecté à	Personne affectée à l'exécution du travail.
Description brève	Brève description de la demande de sécurité, visible par le demandeur.
Description	Description complète de la demande, visible par le demandeur.
Notes de travail	Notes de travail, qui sont visibles par le demandeur.

4. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.
5. Si vous devez escalader la demande en incident de sécurité, cliquez sur **Convertir en incident de sécurité**.

Gérer les observables

Les observables sont des artefacts présents sur un réseau ou un système d'exploitation susceptibles d'indiquer une intrusion. Les observables typiques sont les adresses IP, les hachages MD5 de fichiers ou d'URL de logiciels malveillants ou les noms de domaine. Renseignements sur les menaces Les données de la table des observables sont disponibles à partir d'un incident de sécurité.

Les informations sur les observables comprennent la valeur, le type, le contexte et l'horodatage.

Vous pouvez créer ou supprimer des observables manuellement ou automatiquement via des demandes de recherche.

Une nouvelle colonne **Résultats** a été ajoutée à l'onglet **Résultats de la recherche de menace** . Les valeurs possibles sont : Malveillant et Inconnu.

Si une demande de recherche IoC ne trouve pas d'incident de sécurité observable, elle est étiquetée Inconnu.

Si une demande de recherche IoC détecte un incident de sécurité observable, elle est étiquetée malveillant.

Lors d'une mise à niveau, la colonne **Résultat** des objets existants est définie sur malveillant.

Remarque : Bien que Renseignements sur les menaces les données de la table des observables fassent partie d'un incident de sécurité, aucune autre interaction avec le module n'est Renseignements sur les menaces incluse. Pour une fonctionnalité complète sur les menaces, le module d'extension Renseignements sur les menaces est disponible par abonnement.

Information associée

Créer un observable d'incident de sécurité

Afficher les informations IoC pour un incident de sécurité

Vous pouvez afficher des informations IoC telles que les observables et les résultats de recherche de perceptions associés à un incident de sécurité.

Avant de commencer
Rôle requis : sn_si.basic

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez afficher les informations relatives à IoC.
2. Cliquez sur le lien connexe **Afficher IoC** .
3. Cliquez sur l'une des listes connexes pour afficher ou ajouter des informations pour l'incident de sécurité.

Onglet	Description
Observables	Affichez ou ajoutez ou modifiez manuellement les observables associés à l'incident de sécurité. Pour plus d'informations, consultez Gérer les observables.
Indicateurs associés	Si Renseignements sur les menaces elle est activée, vous pouvez afficher tous les autres indicateurs associés à n'importe quel enregistrement de menace.
Résultats de recherche de perceptions	Contient les résultats de recherche de perceptions.
Détails de la recherche de perception	Contient les détails de l'enregistrement de recherche de perceptions.
Recherches de menace	Stocke les données d'enrichissement des systèmes de détection de programmes malveillants. Cet onglet n'apparaît que lorsque le module d'extension Renseignements sur les menaces est installé.
Modes/ méthodes d'attaque associés	Si Renseignements sur les menaces elle est activée, vous pouvez afficher tous les autres types d'attaques associés aux mêmes enregistrements de menaces.
Demandes d'analyses de sécurité	Si Renseignements sur les menaces elle est activée, vous pouvez afficher les demandes d'analyse et de recherche jointes à l'incident de sécurité.
Ressources avec IoC similaires	Si Renseignements sur les menaces elle est activée, vous pouvez afficher toutes les autres ressources avec des indicateurs similaires.
Utilisateurs avec IoC similaires	Si Renseignements sur les menaces elle est activée, vous pouvez afficher tous les autres utilisateurs ayant des indicateurs similaires.

4. Cliquez sur l'un des liens connexes suivants pour mettre à jour l'incident de sécurité :
   - Afficher les éléments affectés
   - Afficher les éléments connexes
   - Afficher les données d'enrichissement
   - Afficher les tâches de réponse
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un observable d'incident de sécurité

Vous pouvez créer et afficher un observable dans un incident de sécurité et prendre les mesures appropriées. Le fait d'avoir des observables disponibles dans l'incident de sécurité est évolutif et réduit le temps de réponse.

Avant de commencer

Rôle requis :

- sn_ti_observable.write (écriture)
- sn_ti_observable.read (lecture)
- sn_ti_observable.admin (supprimer)

Procédure

1. Accédez à **l'incident de sécurité**.
2. Choisissez un incident.
3. Cliquez sur **l'onglet de liste connexe Observables d'incident de sécurité** .
4. Cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire comme il convient.

Champ	Description
Sélectionner une balise de classification	Si vous avez configuré et activé des balises de sécurité pour ajouter des métadonnées à l'enregistrement, vous pouvez sélectionner une ou plusieurs balises pour spécifier le degré de sensibilité de l'observable. Si vous n'avez pas configuré ou activé les balises de sécurité, cette liste déroulante ne s'affiche pas.
Valeur	Valeur (par exemple, adresse IP ou hachage) associée à l'observable. **Remarque :** Si une analyse de menace porte sur une adresse IP ou un hachage, un programme malveillant renvoyé ou une autre défaillance, l'adresse IP ou la valeur de hachage est automatiquement ajoutée à la table Observable [sn_ti_observable]. En tant que tel, il peut être recherché à partir du formulaire Observables.
Type d'observable	Sélectionnez la classification de l'observable, telle qu'une adresse IP ou un hachage de fichier. Ces types d'observables sont définis dans le module **Types d'observables** .
Nombre d'incidents	Nombre de fois où la valeur observable a été rencontrée.
Est une composition	Ce champ s'affiche uniquement une fois l'enregistrement de l'observable enregistré. Si le **type d'observable** est défini sur autre chose que **la composition de l'observable** et que ce nouvel observable est une composition, cochez cette case. Si le **type d'observable** est déjà défini sur **Composition de l'observable**, la case est cochée et en lecture seule.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Une composition observable est un observable qui contient des observables enfants.
Résultat	Sélectionnez l'une des options suivantes : ◦ **malveillant** : indique que l'observable est préjudiciable à l'organisation. ◦ **Suspect** : indique que l'observable pourrait nuire à l'organisation. ◦ **Nettoyer** : indique que l'observable n'est pas nuisible pour l'organisation. ◦ **Inconnu** : indique que nous n'avons pas encore déterminé le résultat de l'observable. ◦ Valeur par défaut : inconnue. Pour plus d'informations, consultez Calculateurs de résultats de la recherche de menace. **Remarque :** Après une mise à niveau, les observables existants sont marqués malveillants.
Opérateur	Ce champ s'affiche uniquement lorsque la case **Est une composition** est cochée. En fonction du paramètre que vous avez défini dans ce champ, les observables et leurs enfants sont pris en compte pour décider si un indicateur associé est présent. Définissez ce champ sur **ET** si tous les observables enfants doivent être présents pour qu'un indicateur associé soit considéré comme présent. Affectez-lui la valeur **OU** si l'un des observables enfants est présent pour qu'un indicateur associé soit considéré comme présent.
Ne doit pas être présent	Ce champ s'affiche uniquement une fois l'enregistrement de l'observable enregistré. S'il est sélectionné, ce champ signifie que l'absence de l'observable est le problème potentiel (par exemple, une clé de registre manquante).
Emplacement	À l'aide des paramètres de deux propriétés et d'une définition de script include, vous pouvez effectuer un chargement Charger plus de données IoC dans ce champ.
Notes	Entrez toutes les notes supplémentaires sur l'observable.

6. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires.

Liste connexe	Description
Indicateurs connexes	Répertorie les indicateurs qui ont été identifiés par la source de menace.
Tâches associées	Répertorie les changements associés à l'observable.
Observables enfants	Répertorie les observables associés qui ont été identifiés par la source de menace.

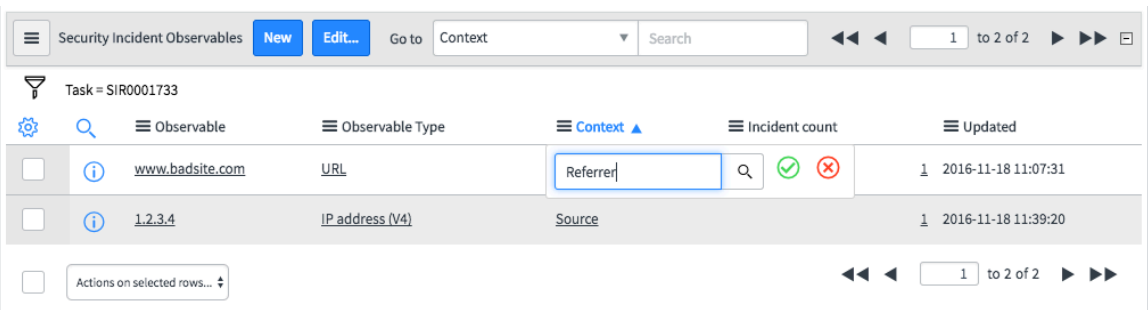
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Description
Ressources correspondantes pour IP	Si l'observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante.
Sources des observables	Répertorie les sources de cet observable, ainsi que le niveau de fiabilité de la source.
Annotations de sécurité	Répertorie les annotations de sécurité ajoutées à cet observable.

7. Pour en revenir à l'incident de sécurité, les informations suivantes sont disponibles.

Remarque : Lorsque vous ajoutez un observable à l'incident de sécurité, le système vérifie s'il existe d'autres éléments de configuration ou utilisateurs qui lui sont associés. Les onglets de liste connexe **Éléments de configuration connexes** et **Utilisateurs associés** sont mis à jour en conséquence.



Colonne	Définition
Observable	Valeur (par exemple, adresse IP ou hachage) associée à l'observable.
Type d'observable	Type spécifique de l'observable.
Contexte	Sélectionné par l'utilisateur. Les choix possibles sont les suivants : ◦ IP : source ou de destination **Remarque :** Si Renseignements sur les menaces et Palo Alto Networks - Firewall sont activés, la modification ou l'ajout d'une valeur à ce champ entraîne l'exécution du workflow Obtenir le workflow des données de journal Security Operations Palo Alto Networks - Obtenir les données de journal . Le workflow récupère les données enrichies du journal des menaces du pare-feu et les joint à l'incident de sécurité. Les informations sont également analysées et affichées dans la section Journaux de pare-feu sous l'onglet **Données d'enrichissage** . ◦ URL : référent **Remarque :** Lorsque l'utilisateur clique sur un lien dans un e-mail d'hameçonnage, un référent est l'URL du dernier saut avant l'accès à l'URL du programme malveillant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Définition
Nombre d'incidents	Nombre d'incidents dans lesquels cet observable apparaît. Cette valeur est automatiquement mise à jour lorsque l'observable est ajouté à un autre incident manuellement ou via un workflow.
Mis à jour	Données et heure de dernière mise à jour de la liste.

Remarque : Si le module d'extension Renseignements sur les menaces est installé, vous pouvez également afficher l'observable dans la liste **Observables** du **référentiel IoC**.

Information associée

Modifier un incident de sécurité Liste des observables

Ajouter plusieurs observablesd'incidents de sécurité

Gérer les observables de fichier

Gérer les observables de fichier fournit des mesures de sécurité strictes pour stocker les fichiers suspects et permet aux observables de type fichiers d'être intégrés dans le bac à sable.

Avant de commencer

Rôle requis : sn_ti_malicious_attachment_access (charger)

Chargez les observables de type de fichier :

- Automatiquement : lorsque les incidents de sécurité sont créés pour les e-mails d'hameçonnage, les pièces jointes de l'e-mail d'hameçonnage sont créées en tant qu'observables de type fichier.
- Manuellement : un analyste de sécurité peut également charger les fichiers suspects pour créer des observables de type fichier.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer et afficher des observables de type fichier pour un incident de sécurité. Les fichiers suspects qui font partie des observables sont stockés dans un emplacement spécifique, auquel l'analyste de sécurité peut accéder pour télécharger le fichier uniquement avec un rôle spécifique.

Procédure

1. Accédez à un incident de sécurité.
2. Sélectionnez **des observables** dans l'onglet **Afficher toutes les listes connexes** .

   Si l'e-mail d'hameçonnage contient des pièces jointes, ces pièces jointes sont créées par défaut en tant qu'observables de type fichier dans l'incident de sécurité correspondant. Chaque pièce jointe est créée en tant que deux observables, tels que l'observable de type de fichier et l'observable de hachage de fichier.

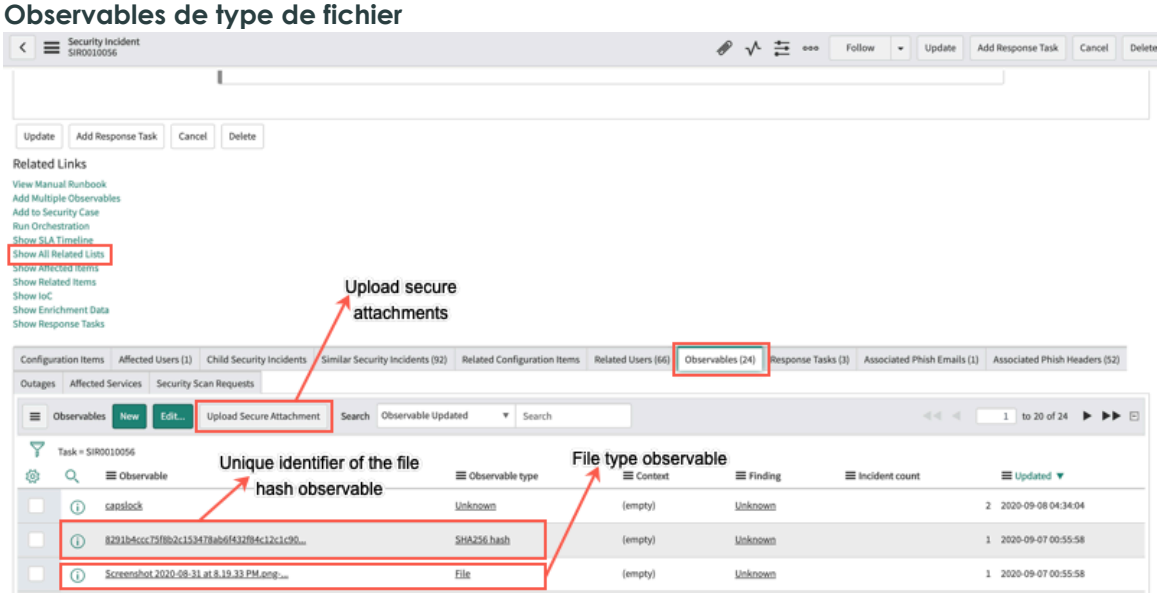
3. Pour charger manuellement les pièces jointes sécurisées :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cliquez sur **Télécharger la pièce jointe sécurisée**.
- Dans l'onglet Télécharger les pièces jointes sécurisées, cliquez sur **Choisir un fichier** pour charger un ou plusieurs fichiers. Chaque fichier est considéré comme un enregistrement observable unique.
- Cliquez sur **Créer un fichier Observables** pour créer les observables de type de fichier, tels que l'un est le type de fichier et l'autre est le hachage de fichier qui est un identificateur unique.

Observables de type de fichier



Sélectionnez l'observable de type de fichier à traiter pour d'autres intégrations telles que le bac à sable et la recherche de menace. En outre, vous pouvez également télécharger les pièces jointes à partir de l'observable de type de fichier.

Remarque :

La recherche de menace (VirusTotal) récupère le fichier à partir des pièces jointes sécurisées pour les nouveaux observables de type de fichier et les propriétés système ci-dessous ne sont pas applicables pour les nouveaux observables de type de fichier.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

Pour référence rapide, l'observable de type de fichier est mappé comme enfant à l'observable de hachage et l'observable de hachage est mappé comme enfant à l'observable de fichier.

Si les pièces jointes de l'e-mail d'hameçonnage dépassent la taille définie, les observables ne sont pas créés. Vous devez modifier les propriétés système pour prendre en charge les fichiers de plus grande taille.

Propriétés système de la taille du fichier

Propriété système	Description
glide.email.inbound.max_total_attachment_size_bytes	Si vous transférez directement l'e-mail d'hameçonnage, utilisez cette valeur de propriétés système pour augmenter la taille du fichier de 18 Mo à la taille souhaitée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété système	Description
com.glide.attachment.max_get_size	Si vous transférez l'e-mail d'hameçonnage en tant que pièce jointe, utilisez cette valeur de propriété système pour créer les propriétés système ci-dessous dans le champ d'application global afin d'augmenter la taille du fichier de 5 Mo à la taille souhaitée.

Vous pouvez également créer un observable de type de fichier comme suit :

a. Cliquez sur **Nouveau**.

b. Sélectionner le **type d'observable Catégorie : fichier**

c. Cliquez sur **Charger** pour joindre un fichier.

Modifier un incident de sécurité Liste des observables

Vous pouvez modifier les observables de la liste associés à un incident de sécurité à afficher.

Avant de commencer

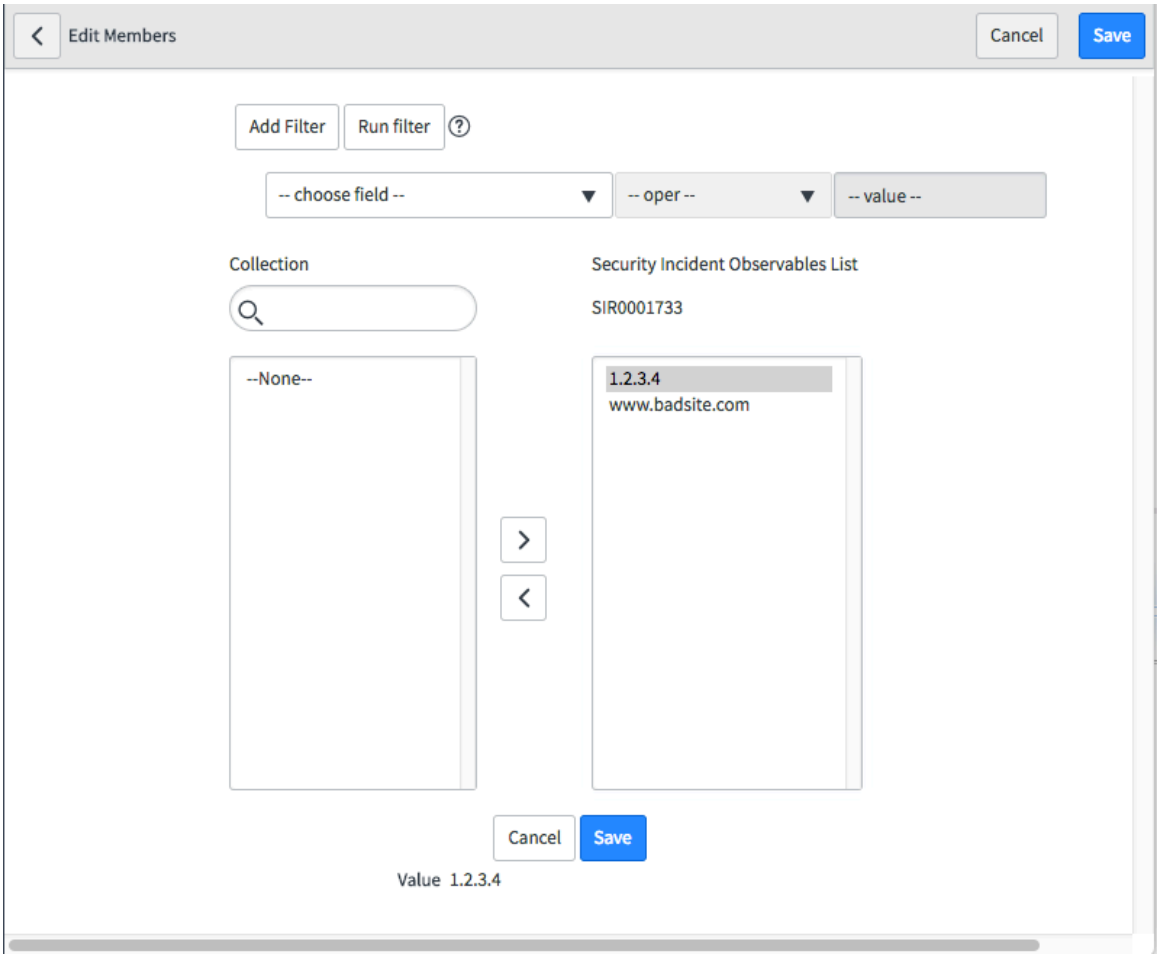
Rôle requis : sn_si.basic

Procédure

1. Accédez à **l'incident de sécurité**.
2. Choisissez un incident.
3. Cliquez sur **l'onglet de liste connexe Observables d'incident de sécurité** .
4. Cliquez sur **Modifier**.
5. Ajoutez ou supprimez des observables de la liste.
   Créez un filtre pour les longues listes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Enregistrer**.

Remarque : Lorsque vous ajoutez un observable à l'incident de sécurité, le système vérifie s'il existe d'autres éléments de configuration ou utilisateurs qui lui sont associés. Les onglets de liste connexe **Éléments de configuration connexes** et **Utilisateurs associés** sont mis à jour en conséquence. En outre, si le module d'extension Renseignements sur les menaces est activé et qu'au moins une implémentation d'intégrationIntégrations de Réponse aux incidents de sécurité est activée, un Security Operations Integration - Aptitude Recherche de menace ou plusieurs workflows sont exécutés et des recherches de sécurité des menaces sont effectuées sur les observables que vous avez ajoutés. Les résultats apparaissent dans l'onglet **Résultats de la recherche de menace** .

Information associée

Ajouter plusieurs observablesd'incidents de sécurité

Créer un observable d'incident de sécurité

Ajouter plusieurs observablesd'incidents de sécurité

Pour gagner du temps, vous pouvez ajouter plusieurs observables d'incident de sécurité à la liste des observables d'incident de sécurité.

Avant de commencer

Rôle requis : sn_ti_write

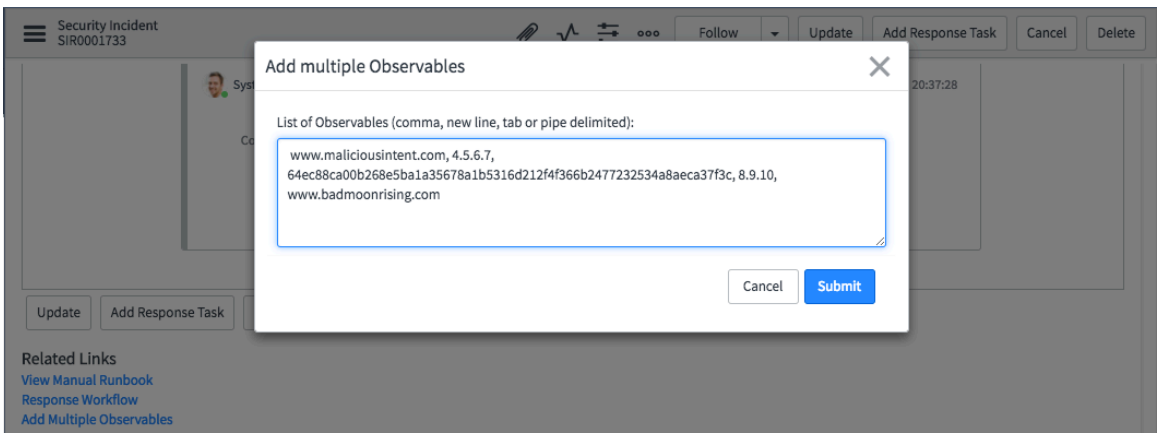
Remarque : Lors de l'ajout de plusieurs observables d'incident de sécurité, les doublons sont ignorés pendant le traitement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à **l'incident de sécurité**.
2. Choisissez un incident.
3. Cliquez sur le lien connexe **Ajouter plusieurs observables** .
4. Saisissez ou collez plusieurs observables.
   Les entrées peuvent être de n'importe quel type d'observable. Les formats acceptés sont : les séparateurs virgule, les nouvelles lignes, les onglets ou les séparateurs de barres verticales.



Remarque : Lorsque vous ajoutez un observable à l'incident de sécurité, le système vérifie s'il existe d'autres éléments de configuration ou utilisateurs qui lui sont associés. Les onglets de liste connexe **Éléments de configuration connexes** et **Utilisateurs associés** sont mis à jour en conséquence.

Remarque : les valeurs observables non détectées automatiquement sont affectées au type Inconnu.

5. Cliquez sur **Soumettre**.

Enrichissement automatique des données observables du journal des incidents de sécurité

Lors de la configuration de certaines applications et intégrations, y compris Renseignements sur les menaces l'intégration, les Palo Alto Networks - Firewall informations des observables dans un incident de sécurité peuvent être automatiquement enrichies avec les données du journal des menaces chaque fois que l'adresse IP source de ses observables est modifiée.

Lorsqu'une modification se produit, une règle métier lance un workflow qui récupère les données des journaux des menaces sur votre pare-feu et enrichit les informations observables dans l'incident de sécurité.

Avant que les observables puissent être enrichis, les étapes suivantes doivent être effectuées.

- Threat Intelligence doit être activé.
- L'intégration du pare-feu Palo Alto Networks doit être activée et configurée. Cela peut également inclure Configurer les informations d'identification SSH sur Serveur MID.

Une fois cette configuration terminée, le changement de l'adresse IP source des observables associés à un incident de sécurité entraîne l'exécution par une règle métier **du workflow Security Operations Palo Alto Networks - Obtenir les données de journal** . Les activités du workflow mettent en file d'attente une requête de recherche sur le pare-feu et renvoient un ID de tâche utilisé pour récupérer les données des journaux de menaces du pare-feu et les joindre sous forme de fichier XML à l'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

- Obtenir des informations sur la session AutoFocus Workflow d'enrichissement
- Workflow du lanceur de pare-feu Security Operations Integration Palo Alto Networks
- Security Operations Palo Alto Networks : workflow de vérification et de blocage de la valeur
- Obtenir le workflow des données de journal
- Obtenir le workflow d'enrichissement des données WildFire

Publier des observables dans une liste de surveillance tierce

Vous pouvez publier un ou plusieurs observables ou indicateurs associés dans une liste de surveillance tierce. Actuellement, la seule implémentation qui prend en charge cette fonctionnalité est CrowdStrike Falcon Host.

Avant de commencer

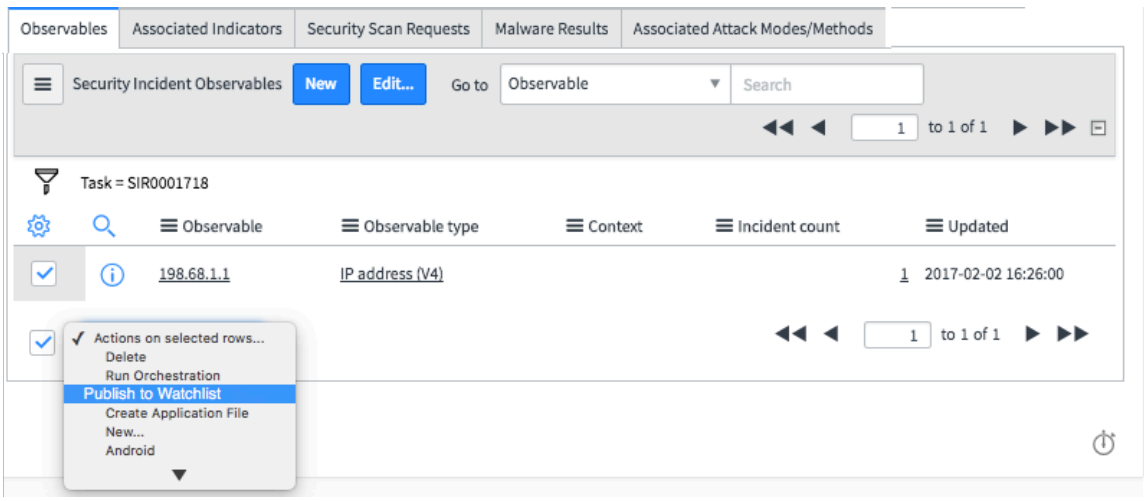
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Procédure

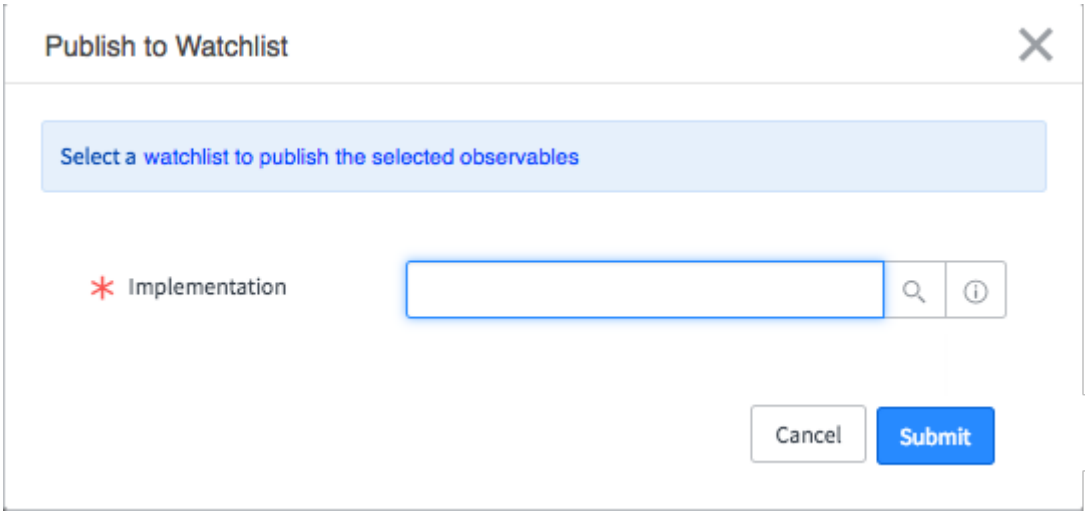
1. Accédez à un incident de sécurité.
2. Sélectionnez **des observables** dans l'onglet **Liste connexe** .
3. Cliquez sur **Publier dans la liste de surveillance** dans le menu déroulant **Actions sur les lignes sélectionnées.**



La boîte de dialogue s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Entrez ou choisissez l'implémentation.

   Remarque : Un workflow est déclenché par lorsque Intégration de Security Operations : aptitude Publier dans la liste de surveillance vous sélectionnez l'implémentation de CrowdStrike Falcon Host.

5. Cliquez sur **Envoyer**.

Gérer les recherches et les analyses

Vous pouvez effectuer des recherches et des analyses de vulnérabilité à partir des incidents de sécurité et du catalogue des incidents de sécurité pour identifier les menaces et vulnérabilités potentielles.

Soumettre une demande de recherche IoC à partir d'un incident de sécurité

Une recherche IoC s'exécute automatiquement chaque fois que des observables sont ajoutés à un incident de sécurité. De plus, si votre incident de sécurité possède des pièces jointes, il suffit d'appuyer sur un bouton pour les trouver.

Avant de commencer

Pour les recherches automatiques d'IoC, le module d'extension Renseignements sur les menaces doit être activé.

Rôle requis : sn_si.basic

Remarque : Par défaut, le **type de recherche** pour **le fichier** est inactif.

Procédure

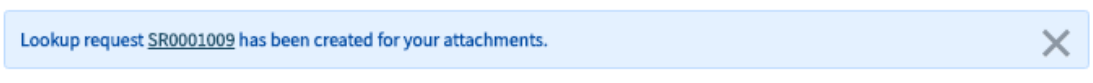
1. Créez un nouvel incident de sécurité ou ouvrez-en un existant si vous avez l'intention d'y joindre de nouveaux fichiers.
2. Cliquez sur l'icône du trombone dans l'en-tête du formulaire et joignez un ou plusieurs fichiers.
3. Lorsque vous avez terminé vos saisies sur le formulaire, cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un bouton **Rechercher des pièces jointes** s'affiche.
4. Cliquez sur **Rechercher des pièces jointes**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les notes de travail sous **Détails de l'incident** signalent la progression du processus de recherche.

5. Vous pouvez cliquer sur le numéro de recherche à la fin du message pour afficher l'enregistrement de recherche.
   Vous pouvez cliquer sur le lien Rechercher une référence pour afficher les résultats détaillés.



Soumettre une demande de recherche IoC à partir du Catalogue des incidents de sécurité

Si le module d'extension Réponse aux incidents de sécurité est activé, vous pouvez soumettre des recherches de menaces pour les fichiers, les valeurs de hachage, les URL et les adresses IP à partir du catalogue des incidents de sécurité. Les demandes sont soumises et vous pouvez afficher les résultats dans le module **Mes demandes** .

Avant de commencer
Rôle requis : aucun

Pourquoi et quand exécuter cette tâche
Les recherches sont automatiquement effectuées pour le type de recherche par défaut pour chaque source de recherche répertoriée dans l'enregistrement de recherche. Les résultats de la demande de recherche sont disponibles dans le module **Mes demandes** .

Procédure

1. Accédez à la **Tout** > **Libre-service** > **Catalogue des incidents de sécurité**.
2. Cliquez sur **Recherche d'IoC**.
3. Cliquez sur **Rechercher des fichiers, des valeurs de hachage, des URL ou des adresses IP**.
4. Entrez un ou plusieurs des éléments suivants :

Demande de recherche d'IoC

Élément à rechercher	Description
Fichiers	Cliquez sur l'icône en forme de trombone, puis localisez et joignez les fichiers que vous souhaitez rechercher. **Remarque :** Par défaut, le **type de recherche** pour **le fichier**est inactif. Les fichiers sont convertis et soumis sous forme de valeur de hachage.
URL	Dans le champ **URL** , saisissez les URL que vous souhaitez rechercher, séparées par des virgules. Par exemple : www.abc.com, www.xyz.net.
Adresses IP	Dans le champ **Adresses IP** , saisissez les adresses IP que vous souhaitez rechercher, séparées par des virgules.
Valeurs de hachage	Dans le champ **Valeurs de hachage** , entrez les valeurs de hachage que vous souhaitez rechercher, séparées par des virgules.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément à rechercher	Description
	Remarque : Lorsque le **type de recherche** pour **le fichier** est inactif, cette valeur est l'action par défaut pour les valeurs **de fichier** et **de hachage**.

5. Une fois que vous avez fait vos sélections, cliquez sur **Soumettre**.
6. Pour afficher l'état et/ou les résultats des recherches, accédez à **Libre-service** > **Mes demandes**.
7. Cliquez sur le numéro SR de la demande.
   Les notes de travail sous **Activité** répertorient les tâches effectuées au cours de la recherche, y compris la création de recherches individuelles pour chaque fichier, valeur de hachage, URL ou adresse IP, ainsi que les résultats de la recherche.

Soumettre une demande d'analyse de vulnérabilité à partir d'un incident de sécurité

Si votre incident de sécurité comporte un ou plusieurs éléments de configuration (serveurs, ordinateurs, etc.), ils peuvent être analysés à partir du formulaire pour détecter les Réponse aux incidents de sécurité vulnérabilités.

Avant de commencer

Le Réponse aux vulnérabilités module d'extension doit être activé.

Rôle requis : sn_si.write

Procédure

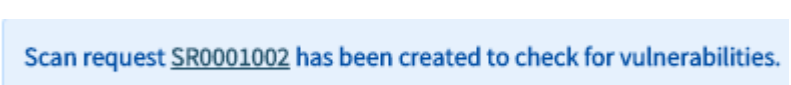
1. Créez un incident de sécurité et incluez au moins une ressource.
   Vous pouvez également ouvrir un incident existant qui possède des éléments de configuration.
2. Lorsque vous avez terminé vos saisies sur le formulaire, cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un lien connexe **Analyser les vulnérabilités** s'affiche.

   Remarque : Si la liste connexe **Rechercher des vulnérabilités** n'est pas affichée, vous devez accéder à **Vulnérabilité** > **Scanners**, configurez au moins un scanner et définissez sa valeur par défaut sur **vrai**.

3. Cliquez sur **Rechercher les vulnérabilités**.

   Remarque :

   Un message apparaît en haut du formulaire d'incident de sécurité, ainsi qu'un lien vers l'enregistrement d'analyse.

4. Vous pouvez cliquer sur le numéro de la demande d'analyse pour afficher l'enregistrement de l'analyse.
   Les détails de l'incident montrent les résultats de l'analyse dans l'enregistrement de demande d'analyse de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Soumettre une demande d'analyse de vulnérabilité à partir du catalogue Security Incident Response

Vous pouvez soumettre des analyses de vulnérabilité pour les CI et les adresses IP à partir du Réponse aux incidents de sécurité catalogue. Les demandes sont soumises et vous pouvez afficher les résultats dans le module **Mes demandes** .

Avant de commencer

Rôle requis : aucun

Procédure

1. Accédez à la **Tout** > **Libre-service** > **Catalogue des incidents de sécurité**.
2. Cliquez sur **Analyse de vulnérabilité**.
3. Cliquez sur **Analyser l'élément de configuration et les adresses IP.**
4. Entrez un ou plusieurs des éléments suivants à analyser.

Scanners de vulnérabilité

Élément à analyser	Description
Élément de configuration	Dans le champ **Élément de configuration à analyser** , sélectionnez le CI à analyser.
Adresses IP	Dans le champ **Adresses IP à analyser** , saisissez les adresses IP, séparées par des virgules.

5. Une fois que vous avez fait vos sélections, cliquez sur **Soumettre**.
   Si un observable est trouvé, un indicateur est créé, selon les standards STIXX.
6. Pour afficher l'état et/ou les résultats des analyses, accédez à **Libre-service** > **Mes demandes**.
7. Cliquez sur le numéro SR de la demande.
   Les notes de travail sous **Activités** répertorient les tâches effectuées pendant l'analyse, y compris la création d'analyses individuelles pour chaque CI ou adresse IP, ainsi que les résultats des analyses.

Gérer l'orchestration àla demande

Au cours Réponse aux incidents de sécurité de l'analyse, un analyste de sécurité peut vouloir effectuer une tâche qui est générée par un workflow d'incident de sécurité. Par exemple, exécutez un vidage de processus sur un CI particulier. Cela peut être accompli avec l'orchestration à la demande.

Chaque application Security Operations enregistrée inclut plusieurs orchestrations à la demande dans le système de base. Vous pouvez définir des orchestrations à la demande personnalisées, selon les besoins.

L'orchestration sur demande peut être invoquée à partir d'une liste de choix située au bas des listes et formulaires suivants dans Réponse aux incidents de sécurité:

- Formulaire d'incident de sécurité
- Liste des incidents de sécurité
- Liste connexe Observables d'incidents de sécurité
- Liste connexe Éléments de configuration

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Une propriété courante de Security Support appelée **sn_sec_cmn.use_on_demand_tbl_as_allowed** définit les workflows disponibles pour une exécution à la demande.
- Si la propriété est définie sur **true**, seuls les workflows spécifiés dans la table Orchestration à la demande [sn_sec_cmn_on_demand_orchestration] sont disponibles.
- Si la propriété est définie sur **faux** (valeur par défaut), tous les workflows des applications configurées dans le registre d'application SecOps sont disponibles.
- En fonction du paramètre de la propriété, la liste des workflows disponibles est adaptée au type d'informations analysées.

Effectuer une orchestration sur demande à partir du formulaire d'incident de sécurité

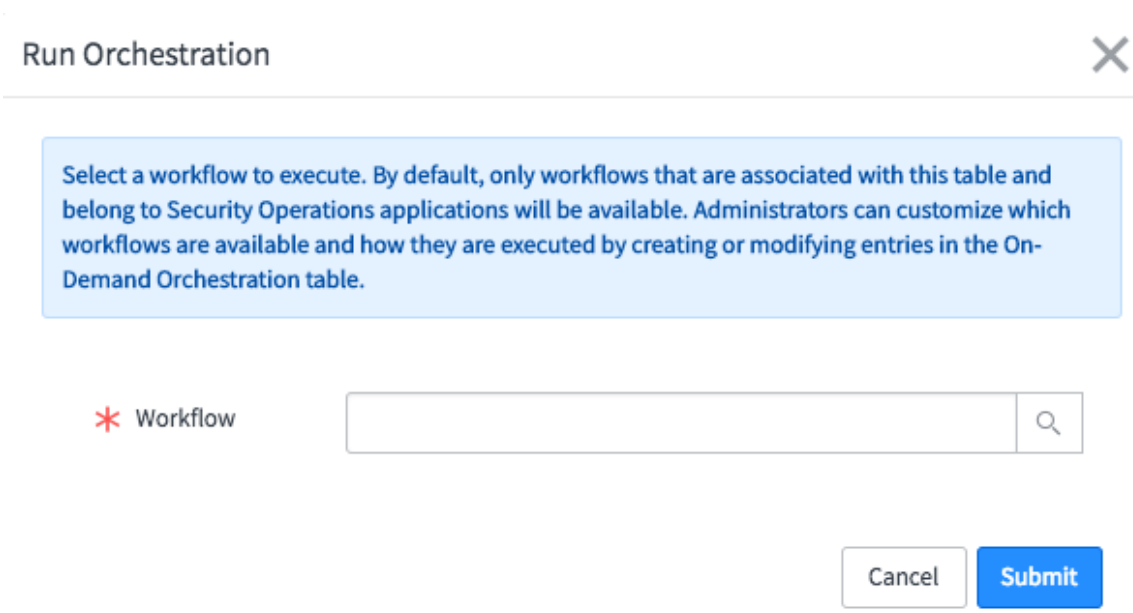
L'orchestration sur demande peut être invoquée à partir d'une liste de choix située en bas du formulaire d'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.write

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents ouverts**.
2. Sélectionnez l'enregistrement (incident de sécurité, observable ou CI) pour lequel vous souhaitez exécuter un workflow.
3. Cliquez sur le lien connexe **Exécuter l'orchestration** .
   La boîte de dialogue **Exécuter l'orchestration** s'ouvre. L'apparence de la boîte de dialogue dépend de la configuration de la propriété sn_sec_cmn.use_on_demand_tbl_as_whitelist dans Security Support Common.



4. Cliquez sur l'icône de recherche et sélectionnez le workflow que vous souhaitez exécuter.
   Le workflow sélectionné s'exécute. Pour plus de détails, voir Orchestration de la réponse aux incidents de sécurité Workflows et activités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Effectuer une orchestration sur demande à partir de la liste des incidents de sécurité

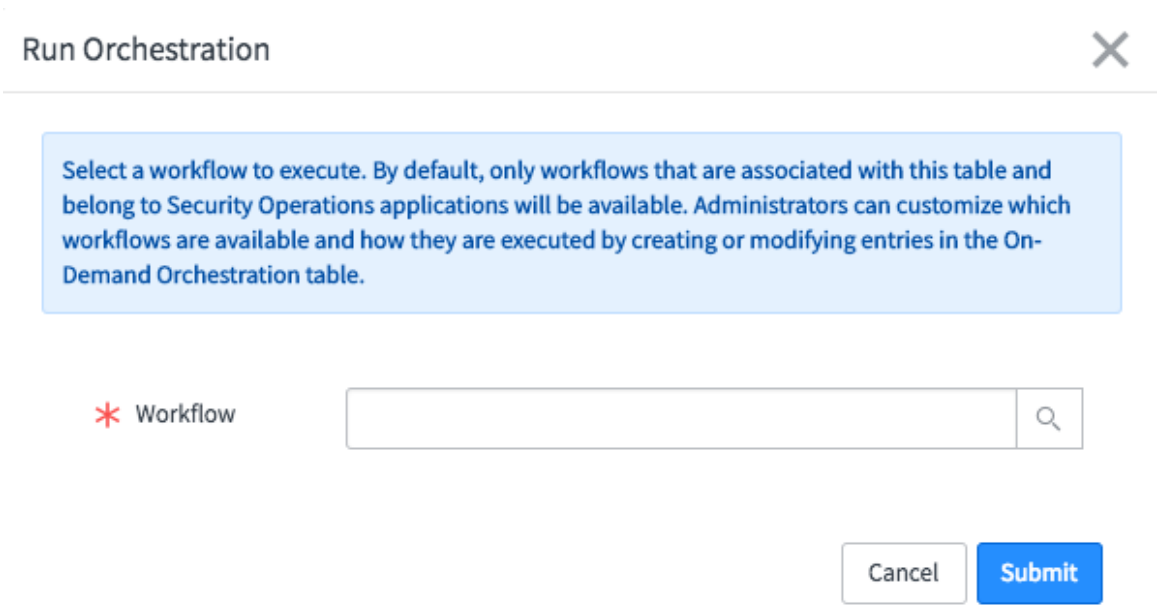
L'orchestration sur demande peut être invoquée à partir de la liste Incidents de sécurité, ainsi que des listes connexes dans Réponse aux incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.write

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents ouverts**.
2. Cochez la case en regard de l'incident de sécurité pour lequel vous souhaitez exécuter un workflow.
3. Cliquez sur la liste de choix **Actions sur les lignes sélectionnées** en bas de l'écran, puis cliquez sur **Exécuter l'orchestration**.
   La boîte de dialogue **Exécuter l'orchestration** s'ouvre. L'apparence de la boîte de dialogue dépend de la configuration de la propriété sn_sec_cmn.use_on_demand_tbl_as_whitelist dans Security Support Common.



4. Cliquez sur l'icône de recherche et sélectionnez le workflow que vous souhaitez exécuter.
   Le workflow sélectionné s'exécute. Pour plus de détails, voir Orchestration de la réponse aux incidents de sécurité Workflows et activités.

Définir de nouvelles orchestrations à la demande

Dans le système de base, vous pouvez sélectionner des orchestrations à la demande qui exécutent des workflows prédéfinis. Vous pouvez définir de nouvelles orchestrations à la demande pour personnaliser la manière dont les workflows sont appelés à partir des listes de choix **Exécuter l'orchestration** .

Avant de commencer

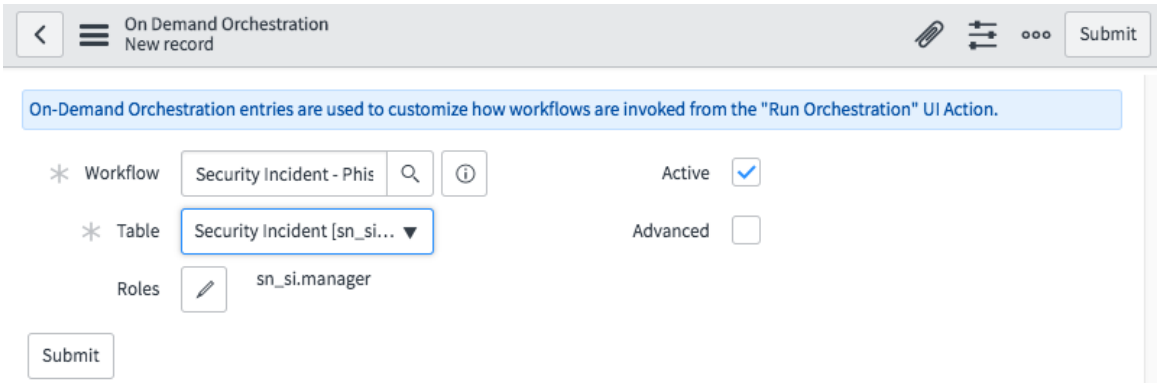
Rôle requis : sn_si.write

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Utilités** > **Orchestration sur demande**
2. Cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Renseignez les champs comme il convient.

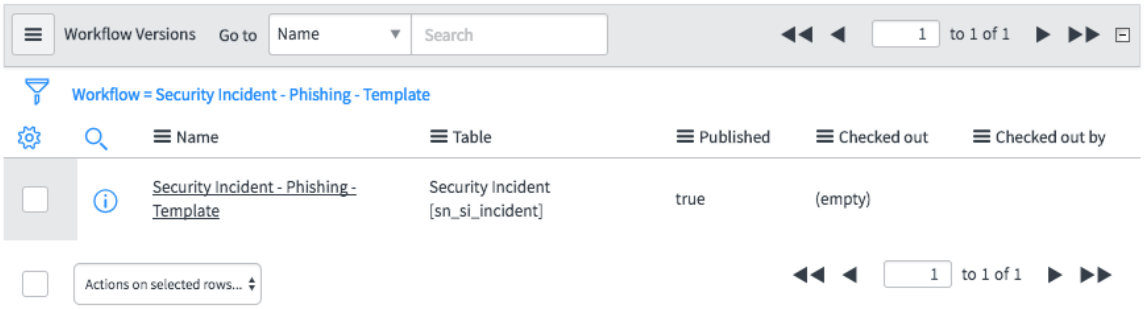
Orchestration à la demande

Champ	Description
Workflow	Sélectionnez le workflow à inclure dans la liste de choix **Exécuter Orchestration** .
Table	Sélectionnez la table sur laquelle le workflow sélectionné est exécuté. Si la table ne correspond pas à la table configurée pour le workflow sélectionné, vous devez cocher la case **Avancé** et modifier le **script d'exécution** pour transmettre le bon enregistrement au workflow lors de l'exécution.
Rôles	Si nécessaire, sélectionnez des rôles supplémentaires pour restreindre qui peut voir ce workflow dans la liste de choix **Exécuter Orchestration** .
Actif	Cochez cette case pour activer cet enregistrement d'orchestration sur demande.
Avancés	Cochez cette case pour modifier le script d'exécution afin qu'il transmette le bon enregistrement à la table sélectionnée pour ce workflow.
Script d'exécution	Modifiez le script d'exécution afin qu'il transmette l'enregistrement correct à la table sélectionnée pour ce workflow. Ce champ s'affiche uniquement si la case **Avancé** est cochée.

4. Cliquez avec le bouton droit dans l'en-tête de l'enregistrement, puis sélectionnez **Enregistrer**.
La liste connexe **Versions du workflow** s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Si vous devez apporter des modifications supplémentaires au workflow, vous devez les vérifier.

Information associée

Utiliser les versions de workflow

Enregistrer les nouvelles applications Security Operations pour l'orchestration sur demande

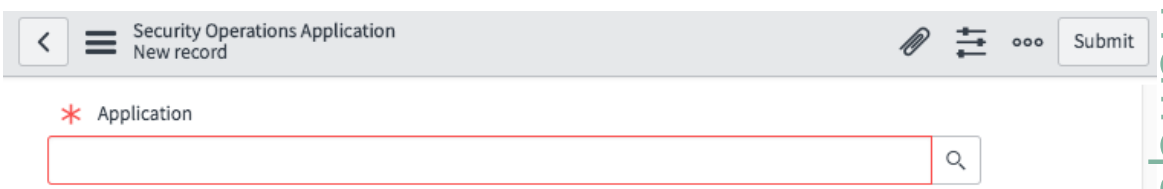
Dans le système de base, les applications Security Operations sont automatiquement enregistrées lorsqu'elles sont activées. L'inscription permet aux workflows associés aux applications d'être disponibles pour les demandes d'orchestration sur demande. Si nécessaire, vous pouvez définir de nouvelles applications et leur associer des workflows pour une orchestration à la demande.

Avant de commencer

Rôle requis : sn_si.write

Procédure

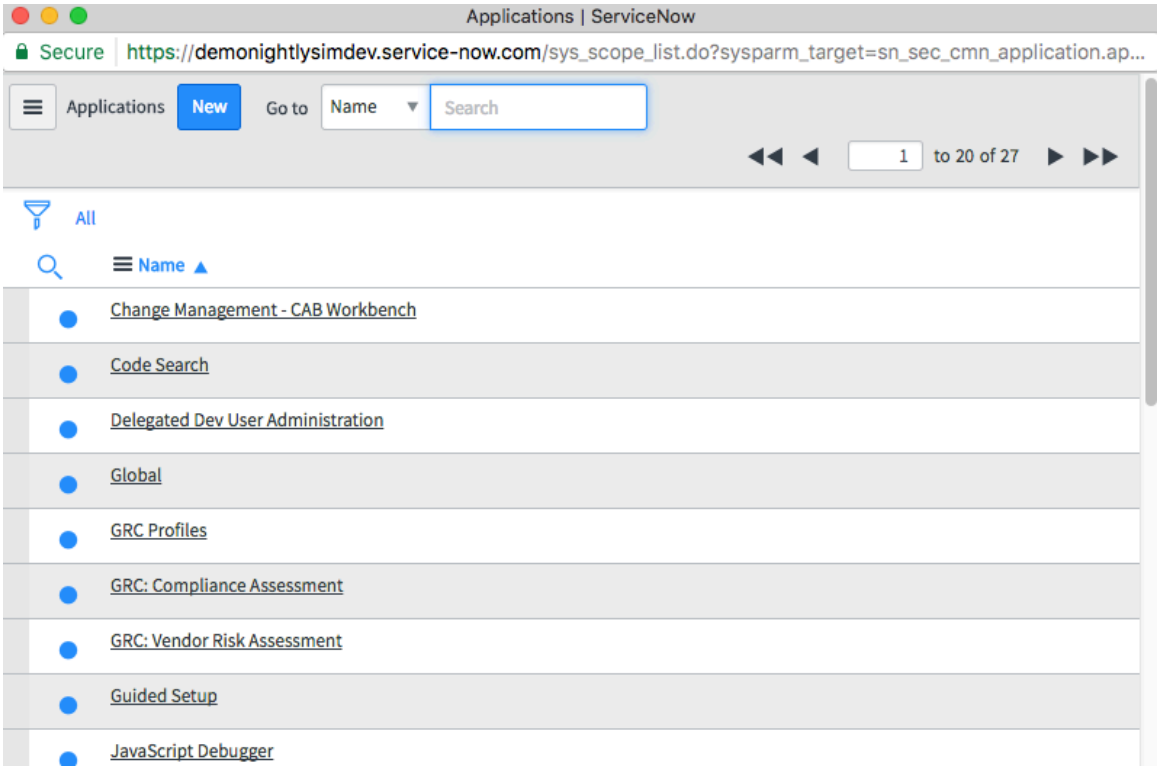
1. Accédez à la **Tout** > **Security Operations** > **Utilités** > **Registre des applications SecOps**, puis cliquez sur **Enregistrer l'application**.
   L'écran Application Security Operations s'affiche.



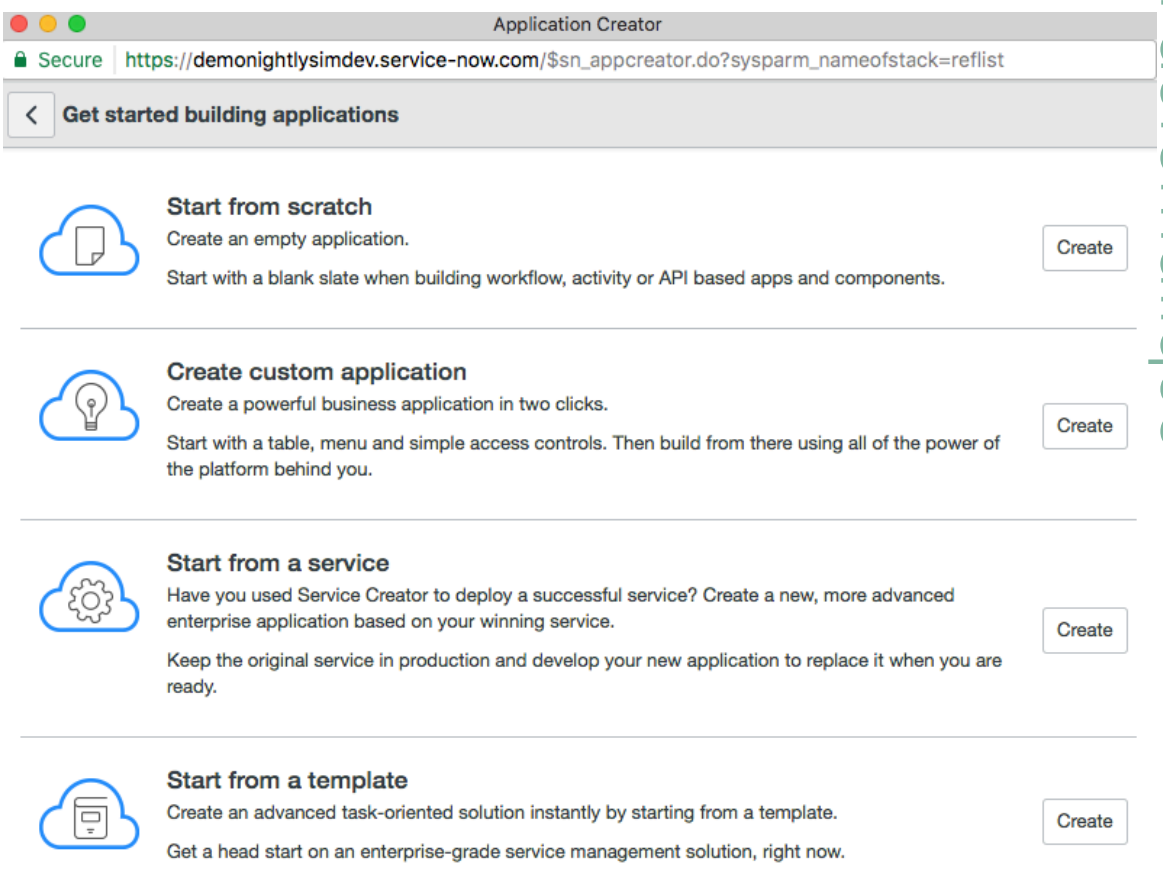
2. Dans le champ **Application** , cliquez sur l'icône Recherches (loupe).
   L'écran Applications s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur **Nouveau**.
L'écran Créateur d'application s'affiche.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les options qui s'affichent dépendent des applications que vous avez activées. Pour en savoir plus sur la création de nouvelles applications, consultez Applications de création .

4. Une fois l'application générée, vous pouvez créer des scripts pour configurer l'orchestration à la demande.

Remarque : La configuration de l'orchestration à la demande pour les nouvelles applications nécessite des connaissances techniques avancées en matière de scripting et de création de déclencheurs pour les scripts (règles métier, action d'interface utilisateur, workflows, etc.). Pour de plus amples renseignements, communiquez avec les ServiceNow Services professionnels.

Ajouter des informations à un incident de sécurité

Une fois qu'un incident de sécurité est créé, vous pouvez ajouter plus de détails pour faciliter l'analyse, tels que les rôles d'accès et les différents types de notes.

Avant de commencer

Rôle requis : sn_si.basic

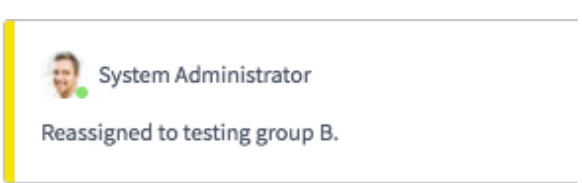
Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité que vous souhaitez mettre à jour.
2. Cliquez sur l'onglet **Détails de l'incident** .
3. Renseignez les champs nécessaires.

Champ	Description
Accès en lecture	Donne à un utilisateur disposant du rôle **d'accès spécial** un accès en lecture à l'incident de sécurité. L'utilisateur est capable de lire et d'écrire des notes de travail. **Remarque :** ◦ Si un utilisateur est ajouté à la fois aux listes **d'accès en lecture** et **d'accès privilégié,** seules les autorisations d'accès **privilégié** sont conservées. ◦ Seul l'utilisateur disposant du rôle sn_si.admin peut modifier à la fois l'accès en lecture et l'accès privilégié.
Liste de surveillance	Cliquez sur l'icône de verrou pour ajouter des utilisateurs qui sont notifiés lorsque des changements sont apportés à l'incident de sécurité. Une fois le champ déverrouillé, des options sont disponibles pour ajouter ou supprimer plusieurs utilisateurs ou saisir des adresses e-mail d'utilisateur. Lorsque vous avez terminé vos saisies, cliquez sur l'icône de verrou pour verrouiller le champ.
Accès privilégié	Donne à un utilisateur disposant du rôle **d'accès spécial** un accès en lecture et en écriture à tous les champs de l'incident de sécurité, à l'exception de **Affecté à**. Les utilisateurs disposant de rôles d'accès spéciaux disposent de leur propre module contenant tous les incidents de sécurité qui leur sont affectés. Aucun autre module n'est à leur disposition. Personne d'autre ne peut voir le module **Visible pour moi** .

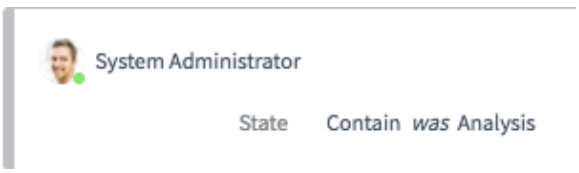
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

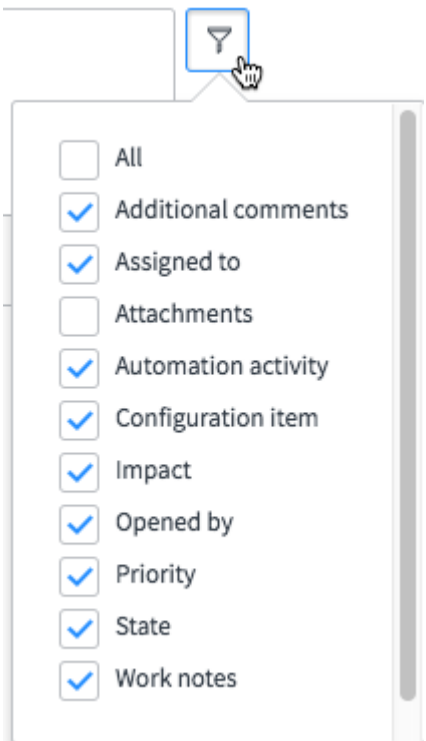
Champ	Description
	Remarque : Seul un utilisateur affecté ou une personne ayant un rôle de sécurité (par exemple, sn_si_analyst ou sn_si.admin) peut modifier le champ **Affecté à** . Si un utilisateur est ajouté à la fois aux listes **d'accès en lecture** et **d'accès privilégié,** seules les autorisations d'accès **privilégié** sont conservées.
Liste de notes de travail	Cliquez sur l'icône de verrouillage () pour ajouter des utilisateurs qui sont notifiés lorsque de nouvelles notes de travail sont ajoutées. Une fois le champ déverrouillé, des options sont disponibles pour ajouter ou supprimer plusieurs utilisateurs ou saisir des adresses e-mail d'utilisateur. Lorsque vous avez terminé vos saisies, cliquez sur l'icône de verrou pour verrouiller le champ.
Description	Saisissez une description complète de l'incident de sécurité, ainsi que toute information pouvant vous aider à trouver la cause ou à résoudre le problème.
Notes sécurisées	Seuls les rôles d'utilisateur avec sn_si.admin et sn_si.analyst peuvent afficher ou modifier les notes sécurisées.
Notes de travail	Saisissez des notes de travail qui ne sont pas visibles pour le client. Les notes de travail apparaissent dans la zone **Activité** .
Activité	Affiche les informations saisies manuellement dans les notes de travail et toutes les activités de tâche mises à jour dynamiquement (actions, commentaires, notes de travail, etc.) sur les enregistrements connexes pour cet incident de sécurité. Les notes de travail apparaissent avec une bande de couleur jaune. 

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Les notes générées automatiquement apparaissent avec une bande de couleur grise. 

4. Vous pouvez limiter les types d'informations affichées dans le champ **Activité** en cliquant sur l'icône de filtre ( ).



Remarque : La case à cocher **Activité d'automatisation** vous permet d'inclure tout enrichissement effectué par cet incident de sécurité, y compris les activités de workflow, les mises à jour du score de risque, etc.

5. Cliquez sur l'un des onglets suivants pour mettre à jour l'incident de sécurité :
   - Enregistrements connexes
   - Revue post-incident
   - Informations sur la fermeture
6. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Ajouter des problèmes, des changements et des incidents connexes à un incident de sécurité

Vous pouvez ajouter des enregistrements connexes, tels que des problèmes, des changements et des incidents, aux incidents de sécurité existants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.basic

Procédure
1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité que vous souhaitez mettre à jour.

2. Cliquez sur l'onglet **Enregistrements connexes** .

3. Renseignez les champs nécessaires.

Champ	Description
Problème	Sélectionnez un enregistrement de problème (PRB) qui résout le problème sous-jacent à l'origine de la création de cet incident de sécurité. Les PRB pour cet incident sont généralement créés en cliquant avec le bouton droit de la souris dans l'en-tête du formulaire d'incident de sécurité et en sélectionnant **Créer un problème**.
Parent	Sélectionnez un enregistrement de tâche lié au problème sous-jacent à l'origine de la création de cet incident de sécurité.
Incident de sécurité parent	Sélectionnez un enregistrement d'incident de sécurité lié au problème sous-jacent à l'origine de la création de cet incident de sécurité. Consultez Relations d'incidents de sécurité parents et enfants.
Incident	Sélectionnez un enregistrement d'incident (INC) qui résout le problème sous-jacent à l'origine de la création de cet incident de sécurité. L'incident est généralement créé en cliquant avec le bouton droit de la souris dans l'en-tête du formulaire d'incident de sécurité et en sélectionnant **Créer un incident**.
Demande de changement	Sélectionnez un enregistrement de demande de changement (CHG) qui résout le problème sous-jacent à l'origine de la création de cet incident de sécurité. La demande de changement est généralement créée en cliquant avec le bouton droit de la souris dans l'en-tête du formulaire d'incident de sécurité et en sélectionnant **Créer un changement**.

4. Cliquez sur l'un des onglets suivants pour mettre à jour l'incident de sécurité :
- Détails de l'incident
- Revue post-incident
- Informations sur la fermeture

5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Invoquer un vidage de processus pour un processus enrichi dans Windows

Un analyste de la sécurité peut exécuter un vidage de processus sur un processus spécifique, le vider dans un fichier et le publier sur un site partagé sur un réseau interne. Un analyste peut ensuite afficher un processus sur liste de refus, surligné en rouge dans un incident de sécurité, et effectuer une analyse supplémentaire.

Avant de commencer
Les éléments suivants sont requis :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Un client exécutant Windows Vista ou une version ultérieure, ou un serveur exécutant Windows Server 2008 ou une version ultérieure.
- L'utilitaire de ligne de commande ProcDump installé, avec une variable d'environnement système qui pointe vers le chemin d'accès au fichier exécutable procdump. Le nom de la variable doit être PROCDUMP. Ce nom est utilisé dans un script PowerShell.

Rôle requis : sn_si.analyst

Procédure

1. Accédez à l'incident de sécurité avec le processus enrichi sur lequel vous souhaitez invoquer un procdump en cliquant sur **Tout** > **Incident de sécurité** > **Afficher les incidents ouverts**et ouvrez un incident de sécurité.
2. Cliquez sur **l'onglet Données d'enrichissement** .
3. Cliquez sur l'enregistrement d'enrichissement **Récupérer les processus en cours d'exécution** .
4. Cochez les cases correspondant aux processus en cours pour lesquels vous souhaitez effectuer un procdump, cliquez sur la liste déroulante Actions sur les lignes sélectionnées en bas de la liste, puis cliquez sur **Exécuter le procdump**.
   Un **workflow de prodump initié pour le message du processus sélectionné** apparaît en haut de la liste et le workflow **Réponse aux incidents de sécurité - Exécuter le procdump** s'exécute.

Afficher les informations dans un incident de sécurité

Vous pouvez effectuer plusieurs autres actions sur un incident de sécurité existant à l'aide des liens connexes.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité que vous souhaitez mettre à jour.
2. Dans **les liens connexes**, vous pouvez effectuer les tâches suivantes :

Option	Description
Afficher le Runbook manuel	Consultez la liste des guides d'exploitation disponibles pour cet incident de sécurité.
Workflow de réponses	Affichez tout workflow associé à cet incident.
Ajouter plusieurs observables	Ajoute une liste d'observables délimités par des virgules, des retours à la ligne, des tabulations ou des barres verticales.
Ajouter au ticket de sécurité	Ajoute l'incident de sécurité à un ou plusieurs tickets de sécurité. Vous pouvez également créer un nouveau ticket de sécurité et y ajouter cet incident de sécurité.
Obtenir les résumés IP de QRadar	Si une intégration QRadar est disponible et contient des CI, des adresses IP sources et de destination valides, elle déclenche les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	flux de travail QRadar et affiche les résultats dans des notes de travail.
Exécuter l'orchestration	Choisissez et exécutez un workflow Security Operations.
Afficher la chronologie SLA	Vous pouvez afficher une chronologie SLA à partir d'un enregistrement SLA de tâche ou d'une définition de SLA.
Afficher toutes les listes connexes	Affiche toutes les listes connexes standard et toutes les listes ajoutées manuellement. **Remarque :** Les éléments ajoutés manuellement ne sont disponibles que dans cette vue.
Afficher les éléments affectés	Affiche les listes des CI, des utilisateurs et des services directement affectés par cet incident
Afficher les éléments connexes	Affiche les listes des incidents associés, des CI, des utilisateurs et des groupes affectés par cet incident.
Afficher IoC	Affiche les listes des observables, des indicateurs, des programmes malveillants, des modes et méthodes, ainsi que des demandes d'analyse de sécurité associées à cet incident.
Afficher les données d'enrichissement	Affiche les listes des données d'enrichissement, des processus, des services, des statistiques, des recherches, des journaux de pare-feu et des informations sur les utilisateurs compromis associés à cet incident.
Afficher les tâches de réponse	Affiche les listes des tâches, des SLA, des audits de score de risque, des pannes et des recherches Exchange associés à cet incident.
Afficher les détails dans le système externe	Si cet incident de sécurité a été généré à partir d'une application externe, directement ou par des événements, et qu'un lien vers les données d'origine a été fourni, l'action **Afficher les détails dans le système externe** ouvre l'URL. Vous pouvez afficher et rechercher dans les journaux qui ont généré cet incident.
Rechercher des vulnérabilités	Si Réponse aux vulnérabilités est activé et que vous avez sélectionné au moins un CI affecté pour l'incident de sécurité, vous pouvez soumettre une demande d'analyse pour déterminer quelles vulnérabilités existent sur le CI.

Traduction automatique

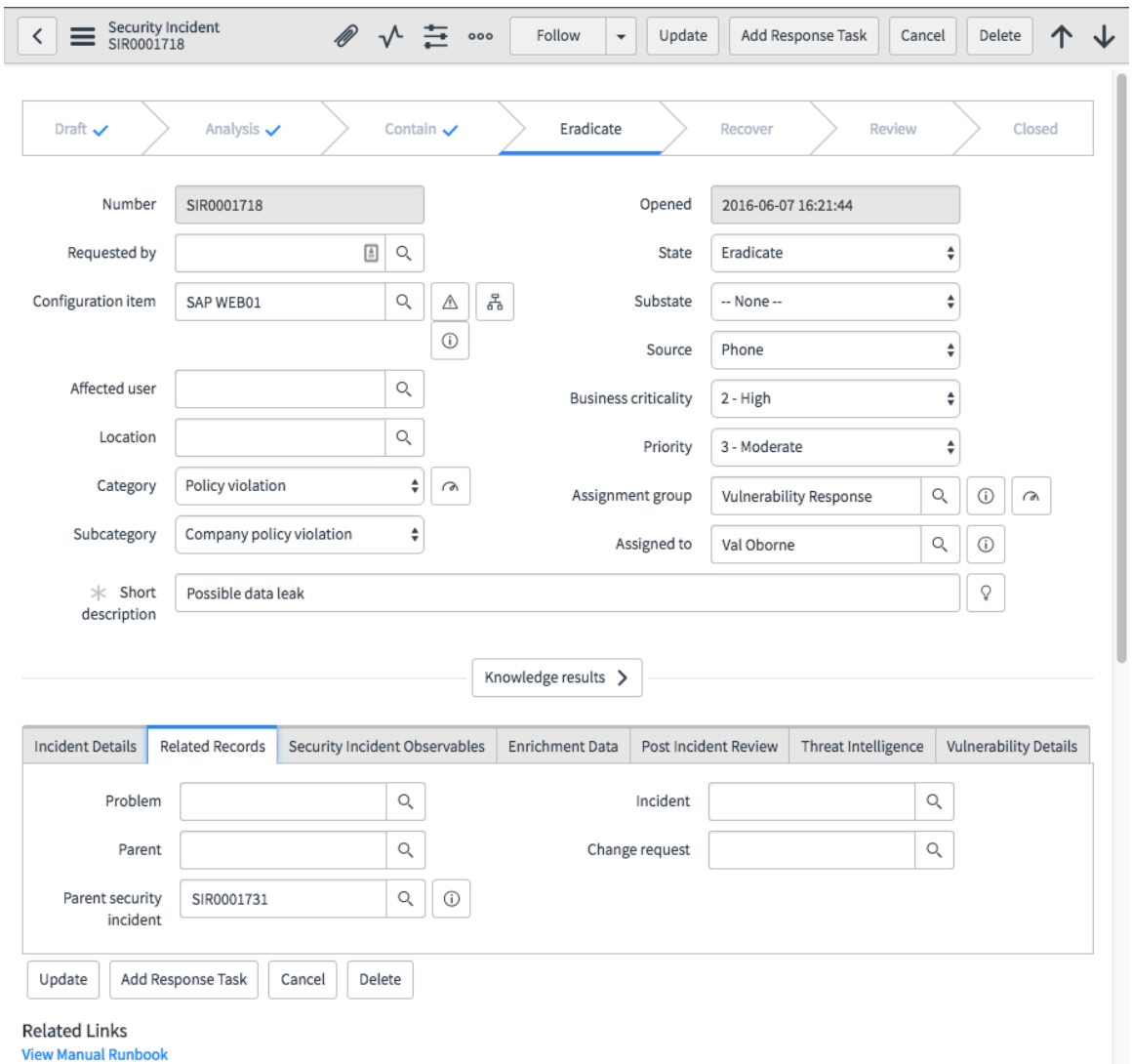
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Relations d'incidents de sécurité parents et enfants

Vous pouvez associer et suivre l'impact d'un problème donné à l'aide des relations d'incident de sécurité parent et enfant dans Réponse aux incidents de sécurité.

À l'aide de l'onglet **Enregistrements connexes** , vous pouvez ajouter un **problème d'incident de sécurité parent** à n'importe quel Réponse aux incidents de sécurité formulaire. Cette fonctionnalité fait automatiquement de l'incident un enfant qui apparaît dans l'onglet **Listes connexes - Incidents de sécurité enfants** du problème parent.

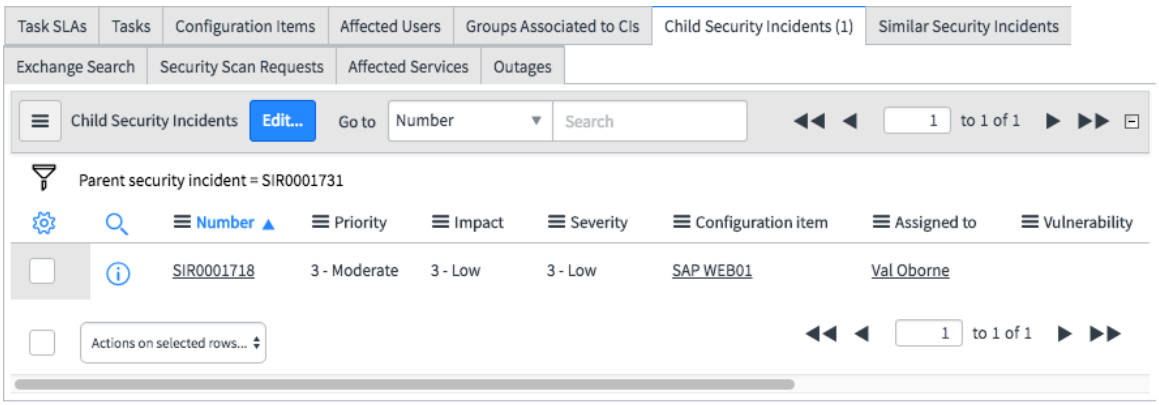
Remarque : Vous ne pouvez pas faire d'un incident de sécurité parent existant son propre enfant en utilisant le même numéro pour les deux incidents.



Traduction automatique

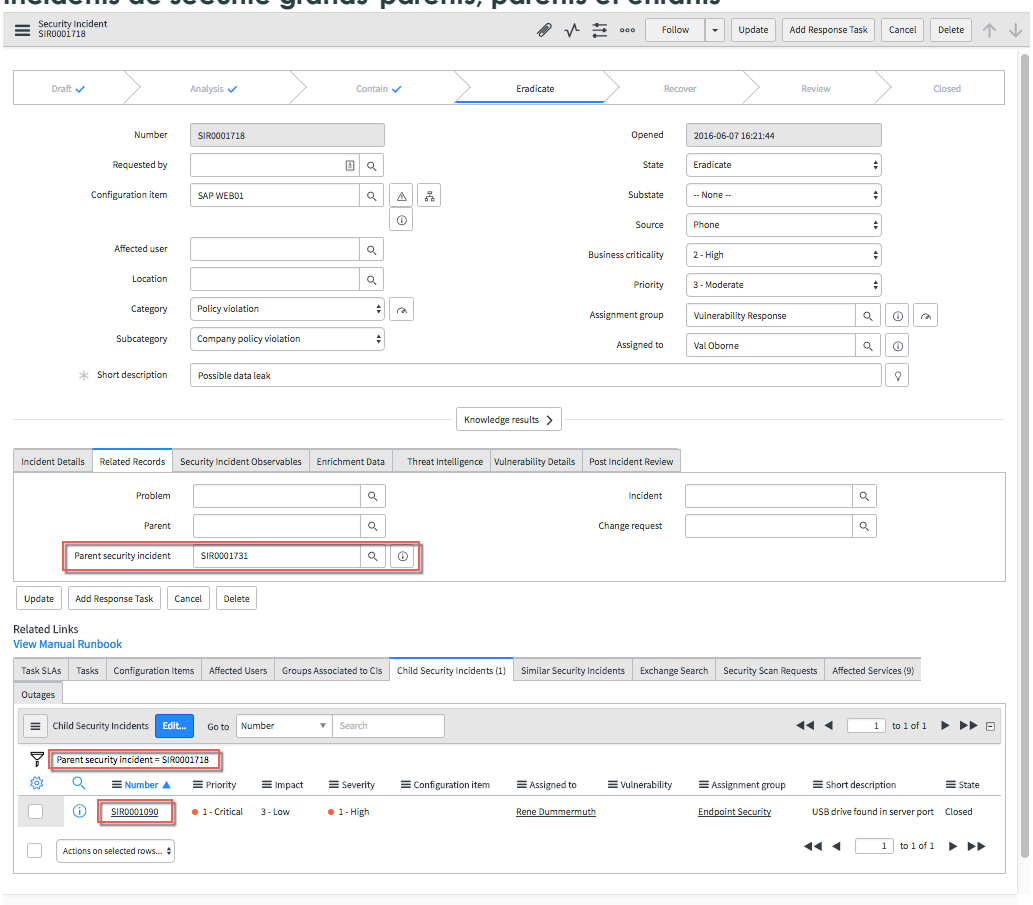
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incident de sécurité enfant



Vous pouvez également ajouter un ou plusieurs **incidents de sécurité enfants** à n'importe quel enregistrement d'incident de sécurité à l'aide du bouton **Modifier** de l'onglet **Incidents de sécurité enfants** . Dans l'exemple suivant, les trois enregistrements sont connectés.

Incidents de sécurité grands-parents, parents et enfants



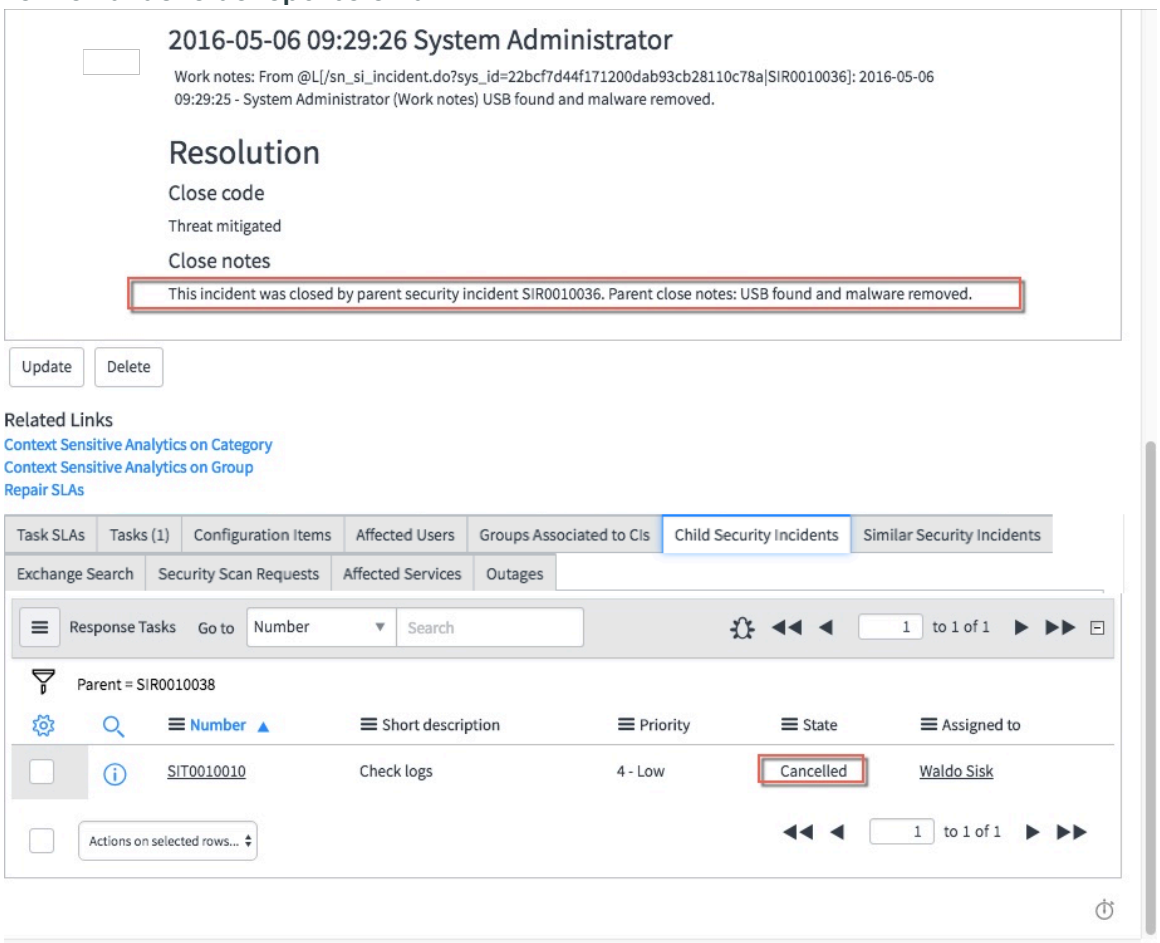
Remarque : toutes les notes de travail enregistrées dans le parent sont propagées à tous les enfants actifs dans les **activités** sous l'onglet **Détails de l'incident** .

Lorsqu'un parent est fermé ou annulé, tous les enfants actifs sont également fermés ou annulés. Toutes les **tâches de réponse** actives sur le ou les incidents enfants sont annulées. S'il n'y a pas d'autres **tâches ouvertes**, l'incident enfant est fermé. Lorsqu'il est fermé, **l'entretien post-incident** enregistre la fermeture et les informations disponibles dans l'onglet **Informations sur la fermeture** sont propagées du parent aux enfants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fermer la tâche de réponse enfant



Afficher les éléments affectés pour un incident de sécurité

Vous pouvez afficher les éléments affectés, tels que les CI, les utilisateurs affectés et les services affectés associés à un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez afficher les éléments affectés.
2. Cliquez sur le lien connexe **Afficher les éléments affectés** .
3. Cliquez sur l'une des listes connexes pour afficher ou ajouter des informations pour l'incident de sécurité.

Onglet	Description
Éléments de configuration	Éléments de configuration (CI) affectés. Une fois les CI affectés identifiés, vous pouvez ajouter manuellement les ressources affectées à partir de cette liste connexe.
Utilisateurs affectés	Une fois les utilisateurs affectés identifiés, vous pouvez ajouter manuellement les utilisateurs affectés à partir de cette liste connexe.
Services affectés	Affichez ou ajoutez les services aux entreprises associés à l'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet	Description
	Remarque : Si un CI affecté est ajouté après l'ouverture de l'incident de sécurité, il est conseillé de cliquer avec le bouton droit dans l'en-tête du formulaire et de sélectionner **Actualiser les services impactés**.

Remarque : Si l'option d'intégration Intégration des opérations de sécurité : obtenir les processus en cours d'exécution est active et que vous ajoutez un CI à un incident de sécurité, le workflow Obtenir les processus en cours d'exécution s'exécute et récupère une liste des processus en cours sur le CI.

Si l'option d'intégration Security Operations Integration - Isoler l'hôte est active, vous pouvez sélectionner un ou plusieurs CI et restreindre leurs connexions système à d'autres périphériques. Pour ce faire, cochez les cases des CI et cliquez sur **Isoler l'hôte** de la liste de choix **Actions sur les lignes sélectionnées** .

4. Cliquez sur l'un des liens connexes suivants pour mettre à jour l'incident de sécurité :
   - Afficher les éléments connexes
   - Afficher IoC
   - Afficher les données d'enrichissement
   - Afficher les tâches de réponse
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Afficher les éléments connexes pour un incident de sécurité

Vous pouvez afficher les éléments connexes, tels que les incidents de sécurité similaires et enfants, les utilisateurs associés, les groupes de vulnérabilité et les éléments vulnérables associés à un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez afficher les éléments connexes.
2. Cliquez sur le lien connexe **Afficher les éléments connexes** .
3. Cliquez sur l'une des listes connexes pour afficher ou ajouter des informations pour l'incident de sécurité.

Onglet	Description
Incidents de sécurité enfants	Sélectionnez un enregistrement de tâche lié au problème à l'origine de la création de cet incident de sécurité.
Incidents de sécurité similaires	Affichez tous les autres incidents de sécurité associés à l'un des mêmes enregistrements observables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet	Description
Éléments de configuration associés	Affiche une liste des incidents de sécurité contenant des éléments de configuration avec le même observable que cet incident de sécurité. Cette liste peut être filtrée à l'aide du groupe de filtres **d'exclusions de CI** . Lorsqu'un observable est ajouté à un incident de sécurité, cette liste est automatiquement mise à jour. Par défaut, les observables dont le type de contexte est Destination sont exclus.
Utilisateurs associés	Affiche une liste des incidents de sécurité contenant des utilisateurs ayant les mêmes observables que cet incident de sécurité. Cette liste peut être filtrée à l'aide du groupe de filtres **d'exclusion d'utilisateurs** . Lorsqu'un observable est ajouté à un incident de sécurité, cette liste est automatiquement mise à jour. Par défaut, les observables dont le type de contexte est Destination sont exclus.
Groupe de filtres connexes	Une fois les éléments de configuration identifiés, tout CI ou groupe de filtres correspondant est automatiquement ajouté.
Groupes de vulnérabilité	Si Réponse aux vulnérabilités elle est activée, vous pouvez afficher les groupes de vulnérabilité associés à cet incident de sécurité.
Éléments vulnérables	Si Réponse aux vulnérabilités elle est activée, vous pouvez afficher les éléments de vulnérabilité associés à cet incident de sécurité.
Risques	Si l'un des principaux modules d'extension de Gestion des risques (Gestion de la politique et de la conformité, Audit, Gestion ou Gestion des risques) est activé, vous pouvez afficher ou ajouter les risques associés à l'incident de sécurité. Vous pouvez ajouter cette liste connexe à partir du menu contextuel de l'en-tête du formulaire sous **Configurer** > **Listes connexes**.
Événements d'éléments de configuration	Si Gestion des événements elle est activée, vous pouvez afficher les événements.
Alertes d'éléments de configuration	Si Gestion des événements elle est activée, vous pouvez afficher les alertes.
Tickets du service clientèle	Si Service clientèle elle est activée, vous pouvez afficher Service clientèle les informations sur le ticket.

4. Cliquez sur l'un des liens connexes suivants pour mettre à jour l'incident de sécurité :
   - Afficher les éléments affectés
   - Afficher IoC
   - Afficher les données d'enrichissement
   - Afficher les tâches de réponse
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les données d'enrichissement pour un incident de sécurité

Vous pouvez afficher les données d'enrichissement, telles que les processus en cours, les services en cours et les statistiques réseau associées à un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez afficher les données d'enrichissement.
2. Cliquez sur le lien connexe **Afficher les données d'enrichissement** .
3. Cliquez sur l'une des listes connexes pour afficher ou ajouter des informations pour l'incident de sécurité.

   Remarque : Les détails des données brutes sont stockés dans une pièce jointe à l'enregistrement des données d'enrichissement. S'ils dépassent la limite de champ, les détails affichés sont tronqués.

Onglet	Description
Processus en cours	Stocke les enregistrements créés par le workflow Réponse aux incidents de sécurité **Obtenir l'exécution des processus** .
Services d'exécution	Stocke les enregistrements créés par le workflow Réponse aux incidents de sécurité **Obtenir les services d'exécution** .
Statistiques réseau	Stocke les enregistrements créés par le workflow Réponse aux incidents de sécurité **Obtenir les statistiques réseau** .
Recherches de domaine	Si le module d'extension est activé, stocke WhoisXML API Integration les enregistrements créés par une recherche Whois.
Journaux du pare-feu	Stocke les données d'enrichissement des journaux de pare-feu, tels que les journaux de pare-feu Palo Alto Network.
Info sur l'utilisateur compromis	Stocke les comptes identifiés comme étant compromis par le biais d'un Have I Been Pwned ? Recherche.

   Remarque : **L'onglet Données d'enrichissement de sécurité** affiche les données d'enrichissement brutes provenant des Réponse aux incidents de sécurité workflows, tels que la récupération des statistiques réseau ou des processus en cours d'exécution. Cet onglet peut être consulté en cliquant sur le lien connexe **Afficher toutes les listes connexes** .

4. Cliquez sur l'un des liens connexes suivants pour mettre à jour l'incident de sécurité :
   - Afficher les éléments affectés
   - Afficher les éléments connexes
   - Afficher IoC
   - Afficher les tâches de réponse
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les informations sur la tâche de réponse pour un incident de sécurité

Vous pouvez afficher des informations sur les tâches de réponse, telles que les SLA de tâche et les audits de score de risque. et les pannes associées à un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez afficher les tâches de réponse.
2. Cliquez sur le lien connexe **Afficher les tâches de réponse** .
3. Cliquez sur l'une des listes connexes pour afficher ou ajouter des informations pour l'incident de sécurité.

Onglet	Description
Tâches	Affiche les tâches déjà définies pour l'incident de sécurité. Vous pouvez créer manuellement une tâche de réponse ou et Créer une tâche à partir de cette liste connexe.
Tâches de réponse	Affiche les actions à effectuer en réponse à l'incident de sécurité.
SLA de tâche	Affichez ou ajoutez les SLA de tâche actifs qui ont été définis pour l'incident de sécurité.
Audits de score du risque	Un enregistrement d'audit pour chaque instance de modification d'un score de risque.
Pannes	Affichez ou ajoutez manuellement de nouveaux enregistrements de panne associés à l'incident de sécurité.
Recherche d'e-mail	Liste des enregistrements qui contient des critères de recherche pour exécuter des requêtes sur un serveur de messagerie, tel qu'un serveur Microsoft® Exchange (basé sur l'implémentation installée), et stocke les résultats reçus. **Remarque :** si l'option n'est pas active, le lien connexe **Recherche d'e-mail** ne s'affiche Security Operations Integration - Aptitude de recherche et de suppression d'e-mails pas.

4. Cliquez sur l'un des liens connexes suivants pour mettre à jour l'incident de sécurité :
   - Afficher les éléments affectés
   - Afficher les éléments connexes
   - Afficher IoC
   - Afficher les données d'enrichissement
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Afficher les événements et alertes associés dans les incidents de sécurité

Au fur et à mesure qu'un incident de sécurité est en cours de traitement, vous pouvez afficher les détails des événements. Pour les alertes, vous pouvez les afficher et les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

authentifier, et créer des incidents ou des incidents de sécurité à partir de celles-ci, selon les besoins.

Avant de commencer

Le module d'extension de prise en charge de la gestion des événements de réponse aux incidents de sécurité doit être activé.

Rôle requis : si.sn_agent

Procédure

1. Accédez à n'importe quelle liste d'incidents de sécurité (par exemple, **Tout** > **Incident de sécurité** > **Incidents** > **Incidents non affectés**).
2. Si les ressources affectées par l'incident de sécurité que vous consultez ont reçu des alertes ou des événements au cours des 24 heures précédentes, l'une ou les deux listes connexes suivantes s'affichent.
   - Alertes CI d'incident de sécurité
   - Événements CI d'incidents de sécurité
3. Cliquez sur la liste connexe que vous souhaitez afficher.

Liste connexe	Description
Alertes CI d'incident de sécurité	Vous pouvez afficher les détails des alertes reçues au cours des 24 heures précédentes. Vous pouvez cliquer sur **Authentifier** pour indiquer que vous êtes au courant de l'alerte et qu'elle est en cours de traitement. Utilisez **Fermer** pour indiquer que l'alerte n'est pas importante.
Événements CI d'incidents de sécurité	Vous pouvez afficher les détails des événements reçus au cours des 24 heures précédentes.

Afficher l'incident de sécurité sur le mappage des tickets du service clientèle

Réponse aux incidents de sécurité Livré avec un mappage de champ par défaut qui mappe un incident de sécurité à un Service clientèle ticket. Vous pouvez afficher la carte par défaut incident de sécurité vers ticket CS.

Avant de commencer

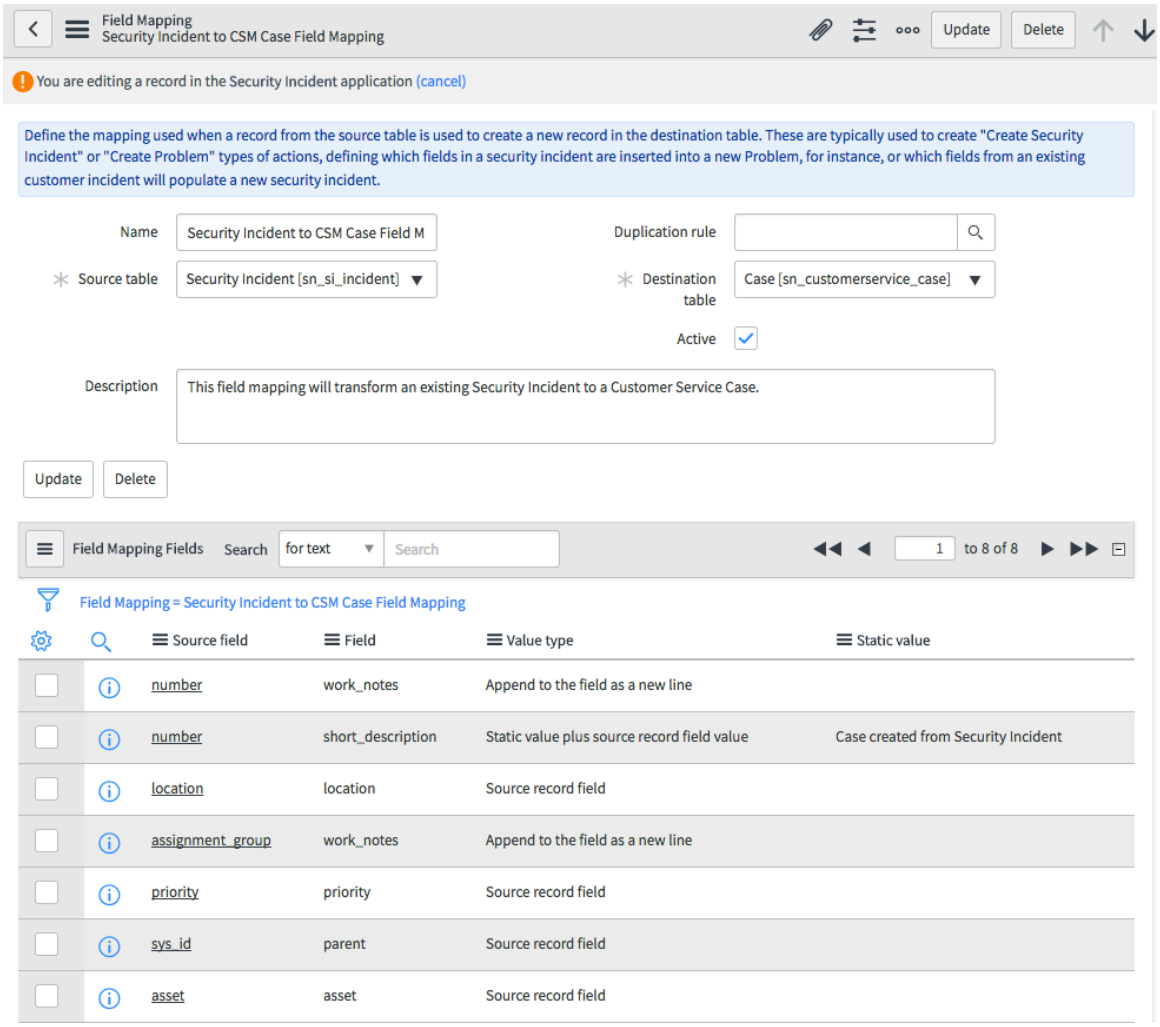
Rôle requis : sec_cmn.read

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Utilités** > **Mappage de champs**.
2. Cliquez sur **Mappage de champs Incident de sécurité sur ticket CSM** pour afficher la carte par défaut.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Vous pouvez modifier le mappage selon vos besoins.
4. Lorsque vous avez terminé vos changements, cliquez sur **Mettre à jour**.

Afficher un Runbook de Réponse aux incidents de sécurité

Les Runbooks vous donnent accès aux procédures liées aux tâches sur lesquelles vous travaillez.

Avant de commencer

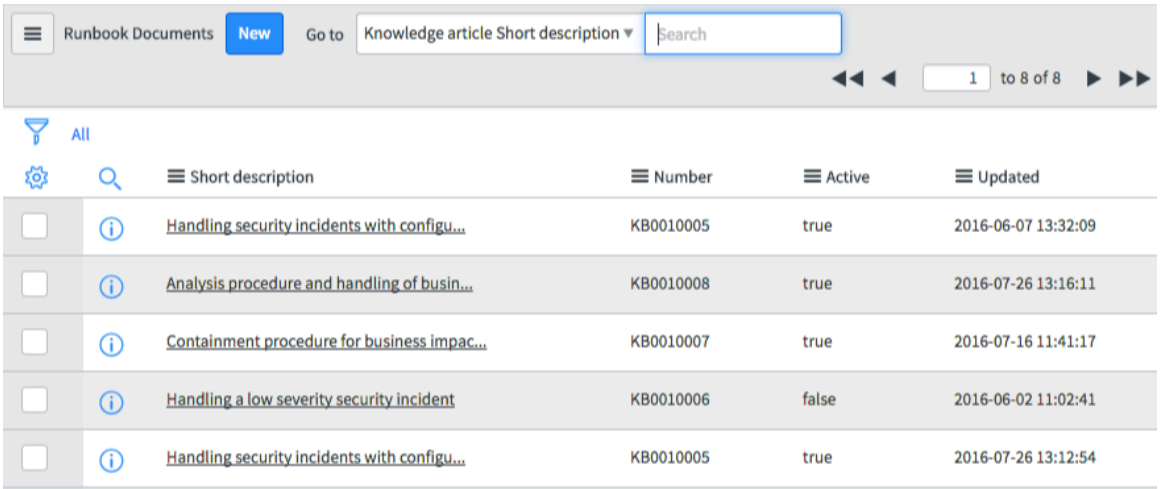
Rôle requis : sn.si.knowledge_admin

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Runbook manuel** > **Afficher les documents Runbook**.
2. Sélectionnez un runbook dans la liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour créer un runbook, cliquez sur **Nouveau**.
   Pour plus d'informations, consultez Créer un runbook.

Identifier tous les éléments de configuration affectés par un incident de sécurité

Si vous savez quelle ressource (serveur, bureau ou autre élément de configuration) est à l'origine d'un incident de sécurité et que vous souhaitez identifier les ressources connexes et les services d'entreprise qui peuvent être affectés, vous pouvez utiliser la carte Gestion des services d'entreprise (BSM).

Avant de commencer
Rôle requis : admin ou sn_si.admin

Pourquoi et quand exécuter cette tâche
La carte BSM affiche les dépendances en amont et en aval d'un CI racine sélectionné.

Il existe deux méthodes que vous pouvez utiliser pour afficher la carte BSM pour un CI :

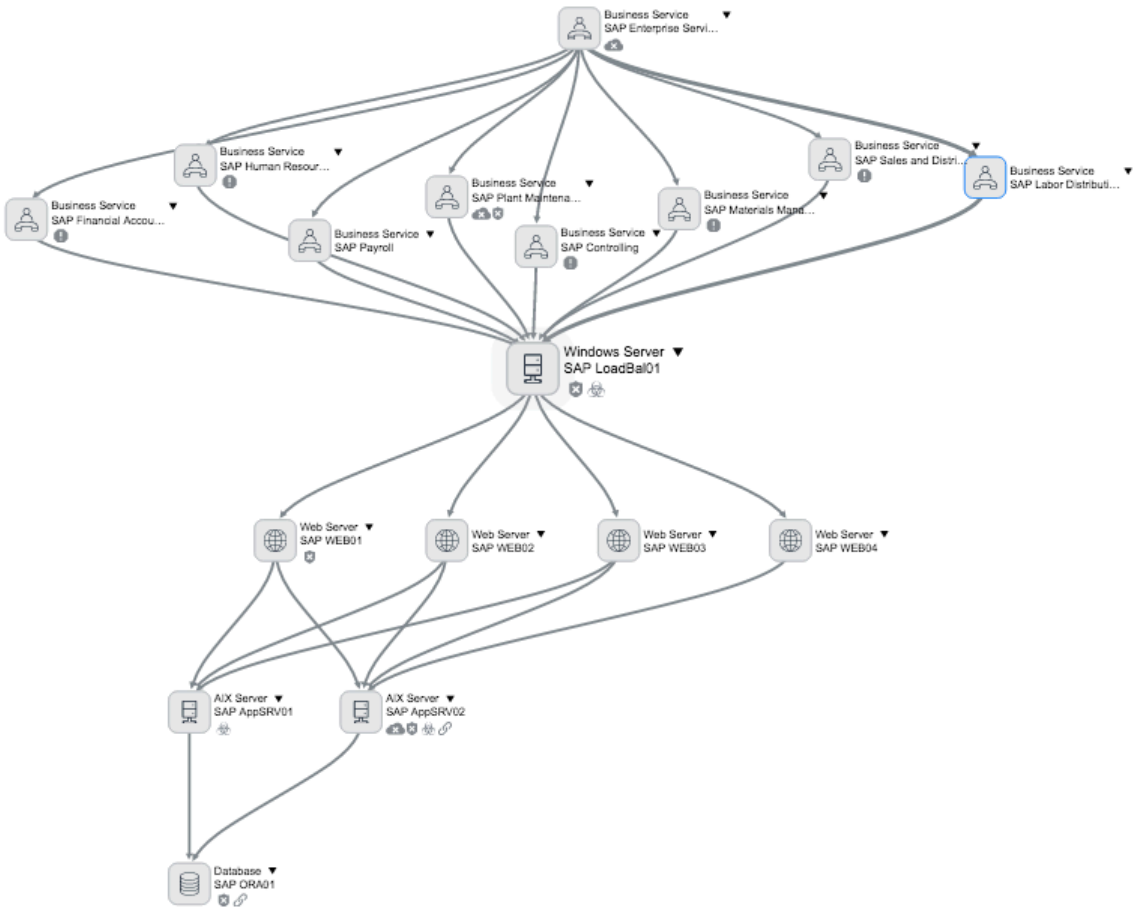
- Si vous souhaitez afficher les CI dans le contexte d'une tâche, affichez-les depuis le formulaire d'incident de sécurité.
- Si vous ne souhaitez pas afficher les CI du point de vue d'une tâche, affichez-les à partir de la barre de navigation.

Procédure

1. Dans le formulaire d'incident de sécurité, renseignez le champ **Élément de configuration** , puis cliquez sur l'icône de carte BSM ( ).
   L'écran de carte BSM affiche la carte du dernier incident auquel vous avez accédé dans Gestion des incidents ou du dernier incident de sécurité auquel vous avez accédé dans Gestion des incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Cliquez sur les icônes en regard d'un élément de configuration pour afficher différents types de détails sur la ressource (serveur, bureau ou autre CI).
   Par exemple, cliquez sur (⚠) pour afficher les alertes associées au CI.

   Remarque : Pour afficher une liste de toutes les icônes disponibles, cliquez sur **Filtres** au-dessus de la carte BSM et développez **Types de tâches de filtrage**.

3. Pour organiser la carte dans différentes configurations, sélectionnez l'un des formats répertoriés au-dessus de la carte (**Vertical**, **Horizontal**, **Radial**) ou cliquez sur **Filtres** pour filtrer la carte afin de faciliter son affichage.
4. Si vous avez ouvert la carte BSM à partir du formulaire d'incident de sécurité, vous pouvez ajouter un CI dépendant à l'incident de sécurité en cliquant avec le bouton droit sur le CI et en sélectionnant **Ajouter des CI affectés**.
   Vous pouvez également ajouter plusieurs CI à la fois. Faites glisser une zone autour des CI que vous souhaitez ajouter, cliquez dessus avec le bouton droit de la souris et sélectionnez **Ajouter des CI affectés**.
   Les CI sont ajoutés à la liste connexe CI affectés de l'incident de sécurité.

Calculer la gravité d'un incident de sécurité

Vous pouvez calculer la gravité d'un incident de sécurité à l'aide de calculateurs prédéfinis.

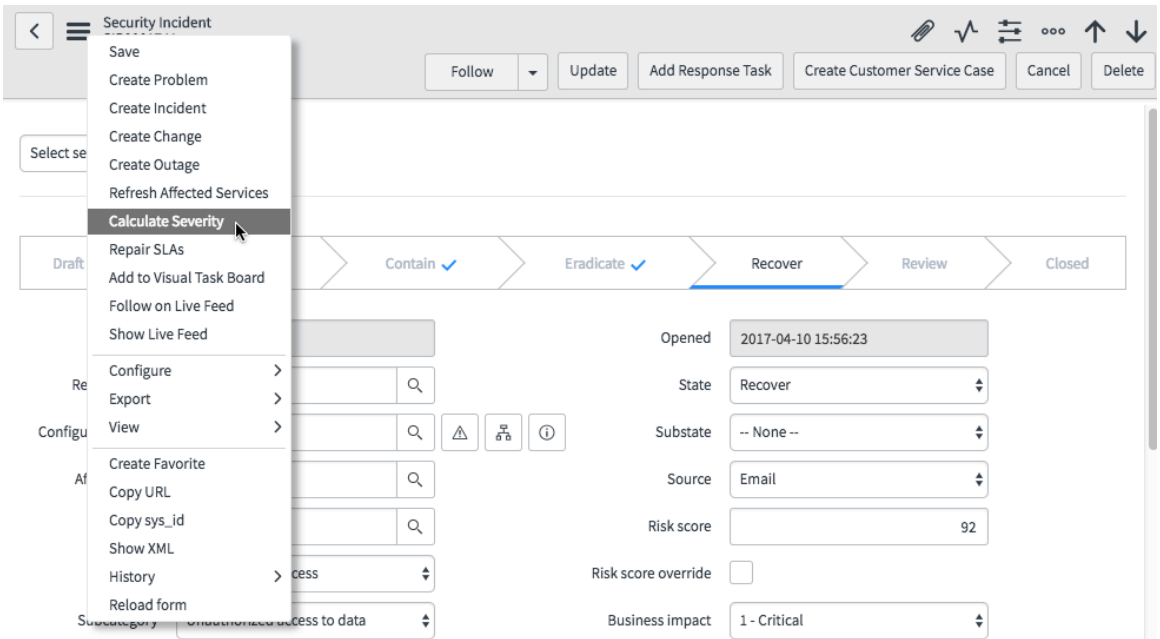
Avant de commencer
Rôle requis : sn_si.basic

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité dont vous souhaitez calculer la gravité.
2. Cliquez sur le menu contextuel de l'en-tête du formulaire et sélectionnez **Calculer la gravité** :



La gravité est calculée en fonction des règles prédéfinies pour les calculateurs de base. Pour plus d'informations, consultez Comprendre les calculateurs d'incidents de sécurité.

Rechercher et supprimer les e-mails d'hameçonnage

La suppression des e-mails d'hameçonnage peut aider à réduire l'exposition à une attaque spécifique au sein d'une organisation. Vous pouvez gérer les e-mails d'hameçonnage sur votre serveur de messagerie en les recherchant, en accordant des approbations et en les supprimant.

Avant de commencer

Rôles requis : sn_sec_cmn.cap_email_read

Vous pouvez déterminer combien d'utilisateurs ont été ciblés par une attaque de hameçonnage en interrogeant un enregistrement d'e-mail associé à un incident de sécurité.

Logiciels pris en charge :

- Microsoft® Exchange Server 2010

Limitation : lorsque vous effectuez une recherche dans le corps des e-mails, vous pouvez rechercher un maximum de 1 500 boîtes aux lettres.

Pourquoi et quand exécuter cette tâche

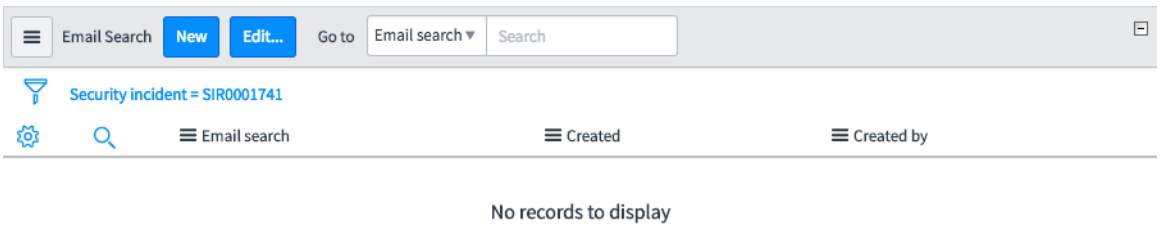
Cette fonctionnalité permet d'exécuter Security Operations Integration - Workflow de recherche et de suppression d'e-mail une requête sur votre serveur de messagerie. En fonction des critères de recherche que vous sélectionnez, la recherche identifie tous les e-mails contenus dans une attaque de phishing et renvoie le nombre total d'e-mails affectés ou des détails sur les e-mails affectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

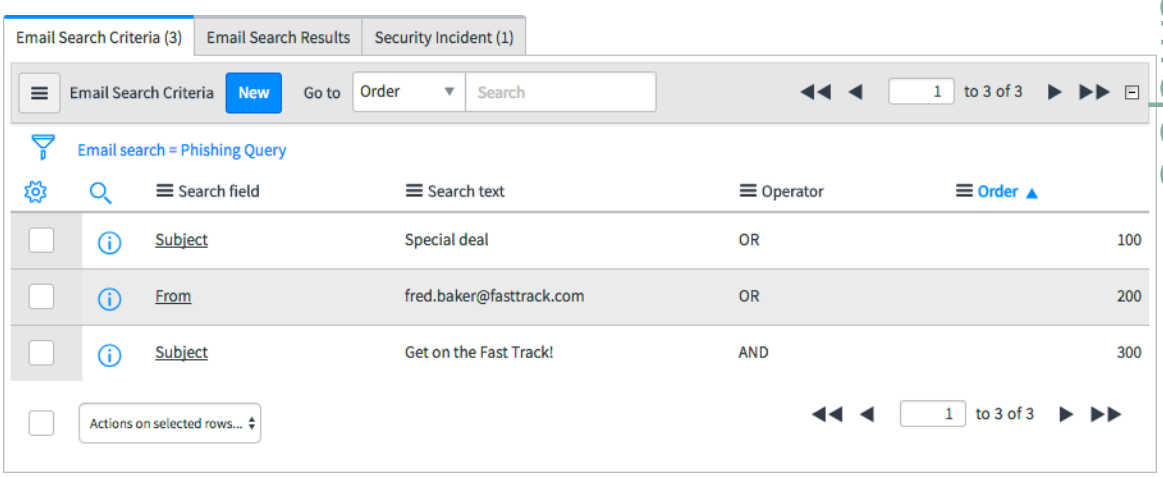
1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. Choisissez un incident de sécurité.
3. Si la liste connexe **Recherche d'e-mail** n'est pas visible, cliquez sur le lien connexe **Afficher tous les liens connexes** .
4. Cliquez sur la liste connexe **Recherche d'e-mail** .



5. Cliquez sur **Nouveau**.
6. Renseignez les champs comme il convient.

Champ	Description
Nom	Nom de la requête de recherche
Requête à partir de critères	Un aperçu de l'exécution de la requête sur le serveur de messagerie. Générée à partir de tous les enregistrements de critères de recherche actifs associés.
Description	Décrivez ce que la requête de recherche recherche.

7. Faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.



8. Cliquez sur l'onglet **Critères de recherche d'e-mail** , puis sur **Nouveau**.
9. Renseignez ou modifiez les champs selon vos besoins.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Recherche d'e-mail	Affiche le nom de la recherche d'e-mails. Vous pouvez le modifier si nécessaire.
Champ de recherche	Champ à rechercher dans le serveur de messagerie. Le champ de recherche comporte les choix suivants : Objet Ce critère recherche les e-mails qui contiennent le texte de ligne d'objet spécifié dans le champ **Texte de recherche** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d'e-mails d'hameçonnage et les détails de chaque e-mail, y compris la date de réception de l'e-mail, l'état de lecture de l'e-mail, le destinataire et l'ID du message, sont renvoyés. De Ce critère recherche les e-mails qui contiennent l'adresse e-mail complète de l'expéditeur (par exemple, jane.doe@abc.com) spécifiée dans le champ **de texte Rechercher** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d'e-mails d'hameçonnage et les détails de chaque e-mail, y compris la date de réception de l'e-mail, l'état de lecture de l'e-mail, le destinataire et l'ID du message, sont renvoyés. **Remarque :** Vous ne pouvez pas utiliser les champs **De** et **Destinataire** dans la même requête. Destinataire Ce critère recherche les e-mails qui contiennent l'adresse e-mail complète du destinataire (par exemple, john.doe@abc.com) spécifiée

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	dans le champ **de texte Rechercher** . Il recherche également les e-mails dans les champs À, Cc et Cci. Pour les e-mails qui répondent à ces critères de recherche, le nombre total d'e-mails d'hameçonnage et les détails de chaque e-mail, y compris la date de réception de l'e-mail, l'état de lecture de l'e-mail, le destinataire et l'ID du message, sont renvoyés. **Remarque :** Vous ne pouvez pas utiliser les champs **De** et **Destinataire** dans la même requête. Corps Ce critère recherche les e-mails qui contiennent le corps du texte spécifié dans le champ **Texte de recherche** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d'e-mails d'hameçonnage est renvoyé. **Remarque :** Lorsque vous effectuez une recherche dans le corps des e-mails, vous pouvez rechercher un maximum de 1 500 boîtes aux lettres. Cc : Ce critère recherche les e-mails qui contiennent l'adresse e-mail complète Cc (ex : jane.doe@abc.com) spécifiée dans le champ **de texte Rechercher** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d'e-mails d'hameçonnage est renvoyé. Bcc: Ce critère recherche les e-mails qui contiennent l'adresse e-mail complète Cci (ex : jane.doe@abc.com) spécifiée dans le champ **de texte**

Traduction automatique

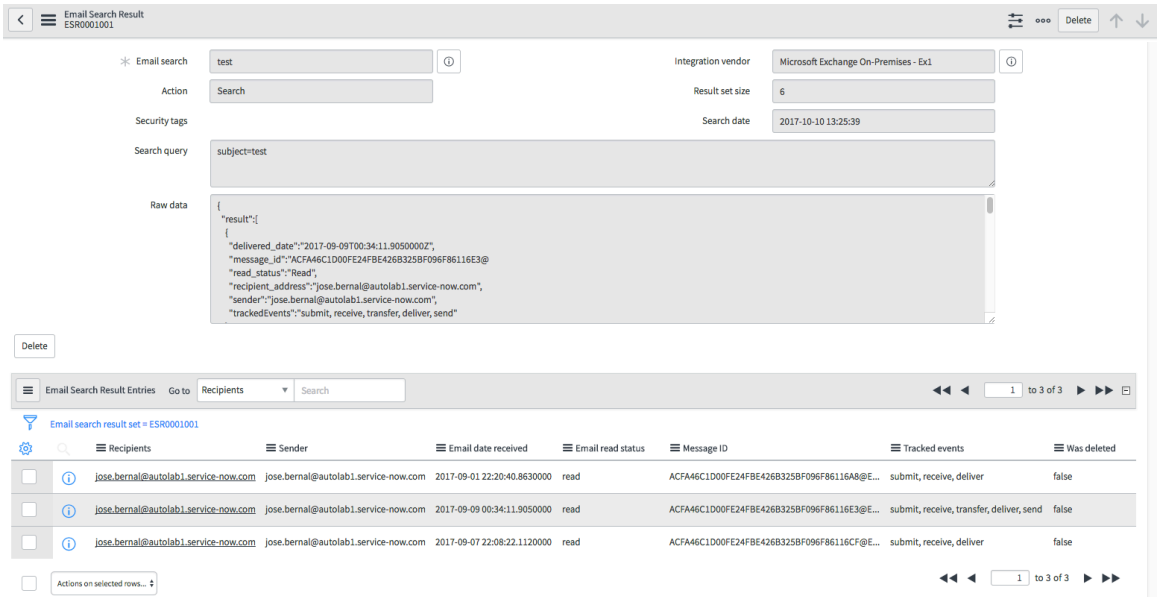
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Rechercher . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d'e-mails d'hameçonnage est renvoyé. Pièce jointe Ce critère recherche les e-mails qui contiennent soit le nom de fichier de pièce jointe, soit le contenu de la pièce jointe spécifié dans le champ **de texte Rechercher** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d'e-mails d'hameçonnage est renvoyé. **Remarque :** Seules les pièces jointes en texte brut sont prises en charge pour rechercher le contenu des pièces jointes. Politique de rétention Ce critère recherche les e-mails qui contiennent des numéros de politique de conservation spécifiés dans le champ **de texte Rechercher** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d'e-mails d'hameçonnage est renvoyé.
Actif	Cochez cette case pour activer cette requête de recherche d'e-mail.
Opérateur	Les valeurs possibles sont ET et OU. Vous pouvez définir comment les critères de recherche sont combinés pour s'exécuter dans le serveur de messagerie.
Ordre	Ordre dans lequel la requête de recherche est créée à partir des critères de recherche.
Texte de recherche	Texte à rechercher. Les guillemets simples, les guillemets doubles et les deux-points ne sont pas pris en charge.

10. Cliquez sur **Envoyer**.
11. Répétez l'opération au besoin pour définir d'autres critères de recherche.
12. Vous pouvez afficher les résultats de la recherche en cliquant sur l'onglet **Résultats de recherche d'e-mail** .

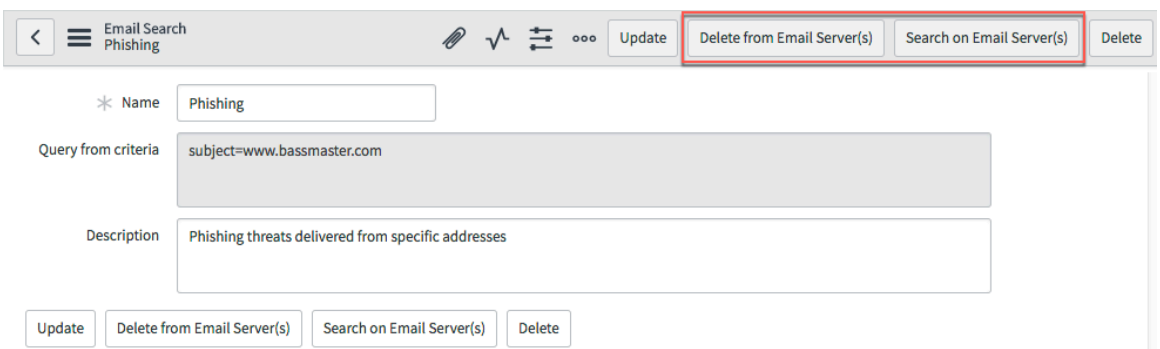
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Chaque ligne du formulaire Entrées des résultats de recherche d'e-mail représente un e-mail distinct.

13. Une fois que vous avez créé un enregistrement de critères de recherche, deux boutons apparaissent dans le formulaire Recherche d'e-mails : **Supprimer des serveurs de messagerie** et **Rechercher sur les serveurs de messagerie**.



14. Pour rechercher dans le serveur sélectionné des e-mails qui répondent aux critères de recherche que vous avez définis, cliquez sur **Rechercher sur le(s) serveur(s) de messagerie**.

Créer un article de la base de connaissances sur les incidents de sécurité

Lorsque vous travaillez sur les incidents de sécurité et les tâches de réponse, les articles de la base de connaissances s'affichent automatiquement pour fournir des informations pertinentes sur la tâche que vous effectuez. Votre organisation peut créer et gérer les articles de la base de connaissances des incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.knowledge_admin

Pourquoi et quand exécuter cette tâche

Les articles de la base de connaissances partagent des informations sur la sécurité, documentent les types de cybermenaces auxquelles votre organisation est confrontée et fournissent des réponses et des réponses à ces menaces.
Si nécessaire, vous pouvez organiser les articles de la base de connaissances en runbooks, qui créent des associations entre les articles et des tâches spécifiques. Par exemple, vous pouvez configurer un runbook avec des conditions qui provoquent l'affichage d'un article

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de la base de connaissances sur le hameçonnage lorsque vous créez un incident de sécurité pour une attaque de hameçonnage. Pour plus d'informations, consultez Créer un Runbook Security Incident Response.

Les articles de la base de connaissances dans les runbooks peuvent également être associés à des tâches spécifiques dans un playbook. Pour plus d'informations, consultez Associer un article de la base de connaissances à une tâche Playbook.

Les avantages des articles de la base de connaissances sont les suivants.

- Les employés ont une source d'information facile à consulter.
- Les informations peuvent être tenues à jour, car les articles de la base de connaissances ont un cycle de vie défini : création, révision et mise à jour, publication et mise hors service.
- Lorsque vous créez manuellement une demande de sécurité, un incident ou une tâche de réponse, une liste d'articles pertinents s'affiche au fur et à mesure que vous saisissez la brève description.

Remarque : Il est important d'affecter un gestionnaire de connaissances à chaque base de connaissances d'incident de sécurité.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Catalogue et base de connaissances** > **Base de connaissances**.
2. Cliquez sur l'icône Créer un article (icône 
3. Renseignez les champs du formulaire comme il convient.

Formulaire de connaissances

Champ	Description
Numéro	Numéro de la base de connaissances généré automatiquement.
Base de connaissances	Base de connaissances sélectionnée pour cet article.
Catégorie	Catégorie de cet article.
Publié	Quand cet article de la base de connaissances a été publié. Cette valeur est définie lors de la création de l'article et mise à jour lors de la publication de l'article.
Date de fin de validité	Quand cet article de la base de connaissances expire. Cet article n'apparaîtra plus dans les résultats de recherche après cette date ou si aucune date n'est sélectionnée.
Image	Image qui s'affiche en regard de l'article lors d'une recherche dans le portail de la base de connaissances hérité.
Workflow	[Lecture seule] État de publication de l'article, tel que Brouillon ou Publié. Quand lors de l'insertion d'un nouvel article à partir d'un article existant, l'état du nouvel article est réinitialisé à l'état **Brouillon**.
Source	Tâche à laquelle cet article de la base de connaissances a été créé, le cas échéant. Ce champ est défini automatiquement lorsque vous créez l'article de la base de connaissances à partir d'un enregistrement de tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Lien de la pièce jointe	Cochez la case pour télécharger automatiquement un fichier joint lorsqu'un utilisateur accède à l'article, au lieu d'ouvrir la vue de l'article. Ajoutez une pièce jointe à l'article pour utiliser cette option.
Afficher les pièces jointes	Case à cocher permettant d'afficher les pièces jointes aux utilisateurs qui consultent cet article de la base de connaissances. Les pièces jointes apparaissent sous le texte de l'article. Ajoutez une ou plusieurs pièces jointes à l'article pour utiliser cette option.
Description brève	Le titre de l'article. Ce titre s'affiche lors du parcours et de la recherche dans la base de connaissances, et en haut de l'article.
Texte	Contenu de l'article. Utilisez l'éditeur HTML WYSIWYG pour créer du contenu. Un aperçu du contenu s'affiche lors du parcours et de la recherche dans la base de connaissances.

Remarque : Si vous créez un article de la base de connaissances à associer à une tâche Playbook, définissez le champ de la **base de connaissances** sur **Runbook de Réponse aux incidents de sécurité**.

4. Cliquez sur **Envoyer** pour créer l'article.

Que faire ensuite

Toutes les étapes supplémentaires nécessaires à la publication de l'article, telles que les approbations, dépendent du Workflow de publication de la base de connaissances.

Information associée

Créer un Runbook Security Incident Response

Escalader un incident de sécurité

Si un chemin d'escalade existe pour un incident de sécurité, le bouton Escalader est disponible dans l'en-tête de l'incident de sécurité.

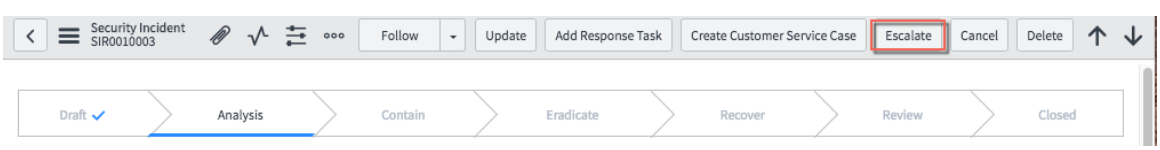
Avant de commencer

Rôle requis : sn_si.admin

Vous devez avoir créé un groupe d'escalade pour voir ce bouton. Consultez Créer un groupe d'escalade Opérations de sécurité défini par l'utilisateur pour plus d'informations.

Procédure

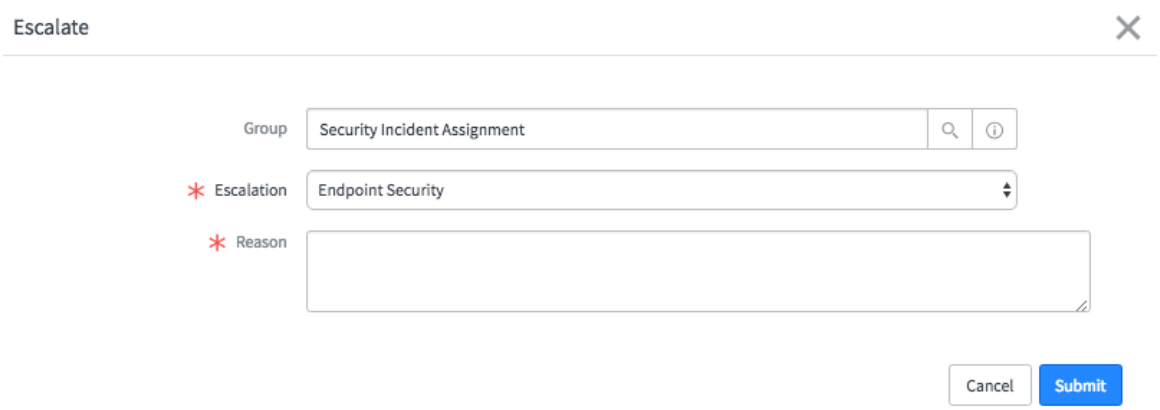
1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. Ouvrez l'incident que vous souhaitez escalader.
3. Cliquez sur le bouton **Escalader** .



4. Choisissez un groupe d'escalade.
5. Saisissez un motif pour l'escalade.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Envoyer**.
   Met à jour le **groupe d'affectation** et **l'affectation sur** l'incident de sécurité.

Gérer les activités post-incident

En fonction des besoins de votre entreprise, il est souvent nécessaire d'examiner l'origine et le traitement des incidents de sécurité.

Cette Revue post-incident fonctionnalité ServiceNow fournit de nombreux outils pour automatiser, suivre, auditer et simplifier ce processus.

Cette section décrit les points suivants :

- Affecter des rôles de révision post-incident
- Configurer une condition de déclenchement d'évaluation
- Effectuer une revue post-incident basée sur un questionnaire
- Créer des règles d'affectation PIR
- Rapport de revue post-incident

Affecter des rôles de révision post-incident

Vous pouvez cibler les questions sur des groupes prédéfinis spécifiques en affectant des rôles aux catégories de Revue post-incident (PIR).

Avant de commencer

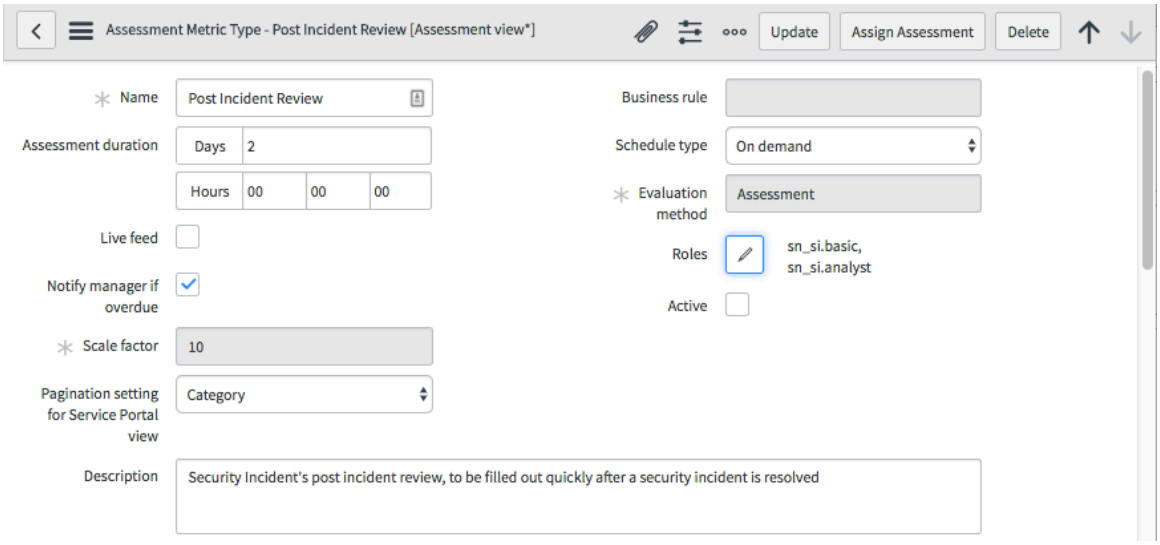
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Évaluations** > **Définition de la mesure** > **Types**.
2. Dans la colonne **Types** , recherchez un enregistrement **de revue post-incident** .
3. Ouvrez l'enregistrement.
4. Affectez un ou plusieurs rôles à cette catégorie de questions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Mettre à jour**.
6. Accédez à la **Administration utilisateurs** > **Utilisateurs**.
7. Choisir un utilisateur
8. Ajoutez un ou plusieurs rôles de type de mesure à l'enregistrement utilisateur.

> **Remarque :** Les rôles doivent correspondre aux rôles affectés dans la catégorie Revue post-incident.

Rapport de revue post-incident

La fonctionnalité Rapports de revue post-incident (PIR) vous permet de configurer et de télécharger les rapports de revue post-incident à l'aide de l'onglet Revue post-incident.

L'administrateur de sécurité peut créer et configurer des modèles de rapport et mapper ces modèles à l'incident de sécurité à l'aide de la configuration du rapport. Un analyste de sécurité peut ensuite afficher ou télécharger le rapport une fois que l'incident de sécurité est résolu et que l'état est mis à jour sur l'état Révision.

Un rapport PDF est généré et joint à l'incident de sécurité lorsque celui-ci passe à l'état Fermé une fois sa configuration réussie.

> **Remarque :** La fonctionnalité de rapports est applicable et prise en charge à partir d'Orlando Patch9.

Pour personnaliser vos rapports de revue post-incident, vous devez procéder à la configuration suivante.

1. **Modèles de rapport** : personnalisez et configurez les fonctionnalités de modèle de rapport suivantes pour ajouter des informations supplémentaires au rapport :
   a. Chronologie
   b. Marques
   c. Scripts de modèle
2. **Configuration du rapport**

Cette section décrit la procédure de configuration :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modèles de rapports

Utilisez la section Modèles de rapport pour créer des modèles de rapport primaires et supplémentaires qui sont appliqués aux incidents de sécurité afin de générer le rapport de revue post-incident. Vous pouvez formater et configurer le rapport en fonction de vos besoins. Les modèles vous permettent également d'y inclure les détails de l'évaluation.

Voici quelques étapes facultatives qui peuvent être effectuées lors de la création du modèle :

1. Configuration des informations sur la marque.
2. Définition de la taille et de la marge de la page.
3. Ajout de champs liés à un incident de sécurité (personnalisés et standard).
4. À l'aide des jetons personnalisés prédéfinis suivants :
   a. *$sessionUser*: renvoie le nom d'utilisateur connecté
   b. *$date*: renvoie la date du jour
   c. *$if_not_null_start* & *$if_not_null_end*: si ces balises sont utilisées avec des champs, les balises s'affichent uniquement si la valeur existe. Par exemple :
      - *${if_not_null_start:problem}*
      - *Problem Category: ${problem.category}*
      - *${if_not_null_end:problem}*
5. Inclusion des données de liste connexe à l'aide des scripts de modèle. Pour plus d'informations, consultez la section ci-dessous sur **les scripts de modèle.**
6. Inclure les informations de chronologie à l'aide des filtres de chronologie. Pour plus d'informations, consultez la section ci-dessous sur **la chronologie**.
7. Gestion et mise en forme du contenu du modèle comme les pièces jointes, les tables et les images.

Remarque : Les fonctionnalités améliorées de la barre d'outils du modèle de rapport ne sont disponibles qu'à partir de la version Paris.

Points clés des modèles de rapport :

1. Les images jointes au modèle de rapport ne sont affichées dans le rapport de revue post-incident que lorsqu'elles sont incluses dans la table sys_attachment.

   Remarque : Les images sélectionnées dans la table de db_image ne s'afficheront pas dans le rapport d'examen post-incident.

2. Les vidéos ne sont pas prises en charge dans le rapport d'examen post-incident.
3. Les URL du PDF ne sont pas cliquables. Pour activer les URL non cliquables (.) est notée (point).
4. Le rapport n'est pas généré si la taille du modèle de rapport dépasse 50 Mo.
5. La famille de polices sélectionnée pour le contenu du modèle de rapport ne sera pas appliquée au PDF si elle n'est pas prise en charge par le générateur PDF.

   Remarque : Si la police correspondante n'est pas là, le générateur de PDF identifiera la police alternative la plus proche, puis générera le PDF.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Si vous fournissez des valeurs de marge de page plus élevées, la génération d'un rapport de revue post-incident a échoué. Par exemple, les marges supérieure et inférieure > 450 et les marges gauche et droite > 450.
7. Si un texte de grande taille est inclus dans le modèle de rapport sans espace, le texte peut être tronqué. Prévisualisez le texte et modifiez-le en conséquence.

L'administrateur de sécurité peut prévisualiser le rapport à l'aide du bouton **Aperçu du rapport** disponible sur la page Modèle de rapport.

Remarque :

Sélectionnez un incident de sécurité pour prévisualiser un rapport avec cette option de modèle et cliquez sur **Aperçu du rapport**.

Marques

Vous pouvez ajouter le nom du modèle de marque, l'image d'en-tête et de pied de page, le texte d'en-tête et de pied de page, générer des numéros de page et inclure l'enregistrement de marque dans le modèle de rapport après sa création.

Voici un exemple de format de rapport de marque :

Points clés de la personnalisation du modèle de rapport :

1. La taille maximale autorisée pour les images d'en-tête et de pied de page est de 5 Mo. Si la taille dépasse la limite spécifiée, un message d'erreur « Impossible de reconnaître le format d'image » s'affiche dans l'incident de sécurité.
2. La longueur du texte du pied de page est limitée à 100 caractères.
   a. Si le texte de l'image de pied de page et le contenu du rapport se chevauchent lors de l'aperçu, vous devez apporter des modifications à l'enregistrement de la marque.
   b. Si le texte de pied de page contient un lien URL, il se peut qu'il chevauche l'image de pied de page. Prévisualisez-le et corrigez-le selon vos besoins.

Chronologie

La configuration de la chronologie vous permet de créer et de modifier les filtres de chronologie selon vos besoins. Vous pouvez filtrer les types d'activité qui doivent être inclus dans le rapport, configurer si les tâches enfants doivent être incluses ou exclues dans le rapport, et configurer si les images doivent être incluses ou exclues dans le rapport.

Si vous souhaitez utiliser et remplir n'importe quelle configuration de chronologie, vous devez ajouter la balise comme indiqué ci-dessous : `${timeline:timeline name}`. À titre d'exemple, deux exemples de configurations de chronologie sont fournis dans la configuration et sont utilisés dans le modèle de rapport d'hameçonnage et le modèle de rapport par défaut. Vous pouvez modifier et réutiliser les configurations.

Scripts de modèle

Utilisez les scripts de modèle pour inclure les données des listes connexes, l'horodatage et la date ainsi que toutes les autres données qui ne sont pas directement accessibles par une remontée pas à pas. Voici un exemple :

Construire un script de modèle pour afficher la liste connexe sur le modèle de rapport :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Pour préparer les données de liste connexe, appelez la méthode PostIncidentReportUtils.fetchRelatedListDataForReport.
2. Pour représenter les données de l'étape 1 au format et au style de la table, appelez la méthode ReportTemplateUtil.constructTablefunction.

Si vous souhaitez utiliser et remplir un script de modèle, vous devez ajouter la balise du script de modèle de balise en tant que *${template_script:script name}*.

Vous trouverez ci-dessous quelques exemples de scripts de modèle fournis pour configurer et modifier vos rapports post-incident.

Nom de script	Description
formatted_current_date	Renvoie la date et l'heure locales actuelles au format jjmmaaa 00h00 ou après-midi. Par exemple, 21 janv. 2021 3:51 PM PST.
si_affected_users	Renvoie les utilisateurs affectés de la liste connexe sous forme de tableau.
si_assessments	Renvoie les résultats de l'évaluation post-incident sous forme de tableau.
si_associated_phish_emails	Renvoie les e-mails d'hameçonnage associés de la liste connexe sous forme de tableau.
si_associated_phish_headers	Renvoie les en-têtes d'hameçonnage associés de la liste connexe sous forme de tableau.
si_business_criticality	Renvoie une valeur de criticité opérationnelle codée par couleur.
si_malicious_observables	Renvoie les observables malveillants de la liste connexe sous forme de tableau.
si_observables	Renvoie les observables de la liste connexe sous forme de tableau.
si_priority	Renvoie une valeur de priorité codée par couleur.
si_response_tasks	Renvoie les tâches de réponse de la liste connexe sous forme de tableau.
si_time_to_identify	Renvoie la durée passée à l'état de brouillon et d'analyse.
si_time_to_resolve	Renvoie l'heure de résolution de l'incident.

Points clés des scripts de modèle de rapport :

1. Si une liste connexe de plus de 5 colonnes est ajoutée, les données de table sont tronquées lors de la génération du PDF. La largeur minimale de chaque colonne est définie sur 124 px.
2. Si un script de modèle ne parvient pas à charger le contenu dans le modèle de rapport en raison de problèmes techniques, un message d'erreur s'affiche sur le rapport « Erreur lors de l'évaluation du script de modèle » et l'administrateur de sécurité doit évaluer l'exactitude du script pour résoudre le problème.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. si_assessments : par défaut, toutes les catégories d'évaluation sont ajoutées au rapport. L'administrateur de sécurité peut filtrer les données en modifiant le script de modèle selon les besoins. Ajoutez le `categories: sys_id1,# sys_id2;` paramètre pour filtrer les données.
4. Délai de résolution et temps d'identification des scripts : utilisez les enregistrements de définition qui font partie de la liste connexe des mesures. Si les enregistrements de définition ne sont pas disponibles pour l'incident de sécurité, créez ou ajoutez ces enregistrements de définition pour renseigner les valeurs des deux champs.

Remarque :

Par défaut, l'administrateur de sécurité n'a pas accès à l'affichage des enregistrements de version d'une table. Vous devez ajouter un rôle administrateur pour accéder aux enregistrements de version et revenir à la version précédente.

Configuration du rapport

Utilisez la section Configuration du rapport pour configurer les conditions et appliquer les modèles de rapport aux incidents de sécurité. Vous pouvez ajouter un rapport primaire et un ou plusieurs modèles de rapport supplémentaires à la même condition.

Voici un exemple de condition fournie pour appliquer le modèle de rapport d'hameçonnage aux incidents de catégorie d'hameçonnage et l'autre condition pour appliquer le modèle de rapport par défaut à tous les incidents de sécurité. Le modèle de rapport par défaut sera appliqué aux incidents de sécurité si les conditions ne sont pas remplies.

Procédure de désactivation de la nouvelle implémentation

1. Désactivez les règles métier suivantes :
   a. Générer un PDF PIR
   b. Créer un article de base de connaissances lors de la fermeture Nouveau
2. Activez les règles métier suivantes :
   a. Générer un rapport post-incident lors de l'examen et de la fermeture
   b. Créer un article de base de connaissances lors de la fermeture
   c. [Régénérer le PIR à la fermeture/à l'annulation/à la suppression]
3. Activez la règle d'interface utilisateur. `Hide PIR field when empty`
4. Accédez à la mise en page du formulaire d'incident de sécurité. Dans la section **Revue post-incident** :
   a. Supprimer le sélecteur de rapport PIR de la section PIR
   b. Ajouter un champ Rapport post-incident à la section PIR

Configurer les propriétés du rapport de revue post-incident (PIR) pour les incidents de sécurité enfants

Vous pouvez configurer les deux propriétés de rapport PIR suivantes pour les incidents de sécurité enfants :

- **sn_si.generate_pir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_pir**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les utilisateurs disposant du rôle d'administrateur système [admin] peuvent afficher les propriétés. Les utilisateurs disposant du rôle d'administrateur de sécurité [sn_si.admin] peuvent les modifier.

Configurer les propriétés du rapport PIR pour les incidents de sécurité enfants

Propriété	Utilisation
sn_si.generate_pir_report_for_child_si	Option permettant d'activer la génération de rapports de revue post-incident (PIR) pour les incidents de sécurité enfants. • **Type** : vrai | faux • **Valeur par défaut** : faux • **Emplacement** : accédez à Toutes les propriétés système > > Toutes les propriétés.
sn_si.include_child_si_timeline_in_pir	Option permettant d'inclure la chronologie des incidents de sécurité enfants dans le rapport PIR de l'incident de sécurité parent. • **Type** : vrai | faux • **Valeur par défaut** : faux • **Emplacement** : accédez à Toutes les propriétés système > > Toutes les propriétés.

Gérer le rapport de revue post-incident

Le rapport Gérer la revue post-incident inclut les informations qui ont été configurées et appliquées par l'administrateur de sécurité. Les analystes de sécurité peuvent modifier les filtres de chronologie lors de l'exécution et le télécharger.

Avant de commencer
Rôle requis :sn.si_analyst

Pourquoi et quand exécuter cette tâche
L'analyste de la sécurité peut sélectionner l'un des modèles de rapport primaires ou supplémentaires disponibles, configurer les filtres de chronologie, prévisualiser et télécharger le rapport. L'analyste de la sécurité peut également télécharger directement le rapport avec la configuration de la chronologie qui a été appliquée pour la dernière fois.

L'analyste de la sécurité peut accéder aux rapports à l'aide de l'onglet Revue post-incident.

Procédure

1. Accédez à l'incident de sécurité dont l'état est Révision.
2. Cliquez sur **l'onglet Revue post-incident** .
3. Si l'incident de sécurité est à l'état **de révision** :
   Modèle de rapport :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Par défaut, le modèle de rapport primaire configuré sur la page de configuration est appliqué à l'incident de sécurité et peut être téléchargé.

- L'analyste peut choisir d'autres rapports dans la liste déroulante pour configurer et télécharger le rapport.

4. **Configurer/Prévisualiser :**

   Un analyste de sécurité peut prévisualiser et modifier la configuration du modèle de rapport. Dans la configuration actuelle, l'analyste de sécurité ne peut modifier que les filtres de chronologie.

   Si la configuration est modifiée pour le rapport primaire avant la fermeture de l'incident de sécurité, le rapport de revue post-incident joint à l'incident de sécurité est mis à jour en fonction des modifications apportées par l'analyste de sécurité. Après la fermeture, l'analyste sera en mesure de modifier la configuration et de télécharger le rapport en déplacement. Toutefois, le rapport ci-joint suivrait la dernière configuration avant la fermeture.

   Pour configurer/prévisualiser le rapport, procédez comme suit :

   a. Sélectionnez le modèle de rapport souhaité dans la liste déroulante **Modèle de rapport** de l'onglet **Revue post-incident** .

   b. Cliquez sur **l'onglet Configurer/Aperçu** .

   c. **Mettez à jour** ou configurez les filtres de chronologie selon vos besoins.

   d. Utilisez la case à cocher **Afficher les images** pour inclure ou exclure les images de la chronologie. Si cette option n'est pas cochée, seuls les noms des images sont inclus dans la section de chronologie.

   e. Utilisez la case à cocher **Afficher les tâches enfants** pour répertorier toutes les tâches enfants associées à l'incident de sécurité.

5. **Enregistrez** la configuration et cliquez sur l'onglet **Aperçu** pour prévisualiser et télécharger le rapport.

6. Cliquez sur **Télécharger** pour télécharger directement le rapport.

Configurer une condition de déclenchement d'évaluation

Définissez les conditions des règles et générez des évaluations obligatoires et facultatives pour des incidents de sécurité spécifiques.

Avant de commencer

Rôle requis : sn_si.admin

Remarque : Pour utiliser la fonctionnalité Conditions de déclenchement de l'évaluation de la revue post-incident, vous devez effectuer une mise à niveau vers Réponse aux incidents de sécurité la version 11.0. Avant de procéder à la mise à niveau, vous devez rétablir toutes les personnalisations apportées au type de mesure et aux conditions de déclenchement de la revue post-incident. En outre, vous devrez peut-être rétablir les personnalisations apportées aux règles métier spécifiques à la revue post-incident.

- Exiger que les évaluations soient terminées
- Stocker le délégataire

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Administration** > **Revue post-incident : configuration des évaluations**.
2. Dans la section **Configuration des conditions de déclenchement de l'évaluation** , cliquez sur **Configurer**.

   Remarque : Dans le formulaire Configurations de l'évaluation et dans la section Configurations des évaluations, la case à cocher **Générer les évaluations** est sélectionnée par défaut.

   - Lorsque vous cochez la case, une évaluation facultative est créée pour chaque incident de sécurité.
   - Lorsque vous décochez la case, les évaluations ne sont pas générées. Les règles d'évaluation ne sont pas affichées et vous ne pouvez pas configurer de conditions pour les incidents de sécurité.

3. Dans le formulaire Configurations de l'évaluation, dans la section Conditions, spécifiez les informations requises.

   a. Dans le champ **Nom** , spécifiez le nom de la règle.

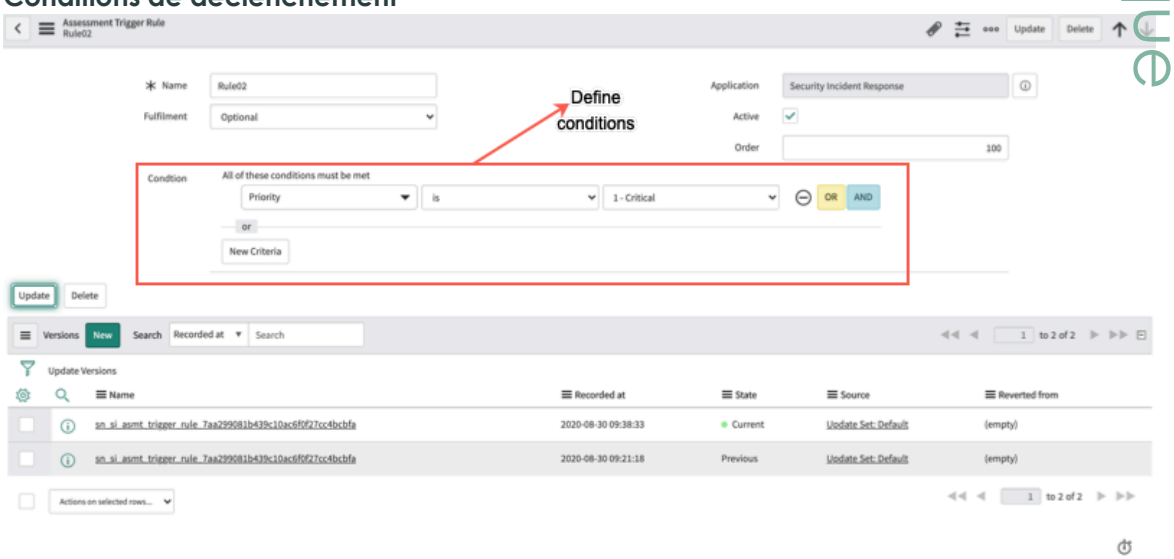
   b. Dans le champ **Exécution** , spécifiez le type d'exécution.

   c. Pour configurer une condition, cliquez sur l'enregistrement de règle et définissez les conditions dans le champ **Condition** .

   Remarque :

   - Si vous créez une règle sans définir de condition dans le champ **Condition** , alors la condition est évaluée comme vraie et la règle est applicable pour tous les incidents de sécurité.
   - Vous pouvez définir une règle spécifique pour rendre les évaluations obligatoires ou facultatives, et les évaluations ne sont pas générées pour les autres incidents de sécurité, qui ne correspondent pas aux règles définies.

Conditions de déclenchement



Traduction automatique

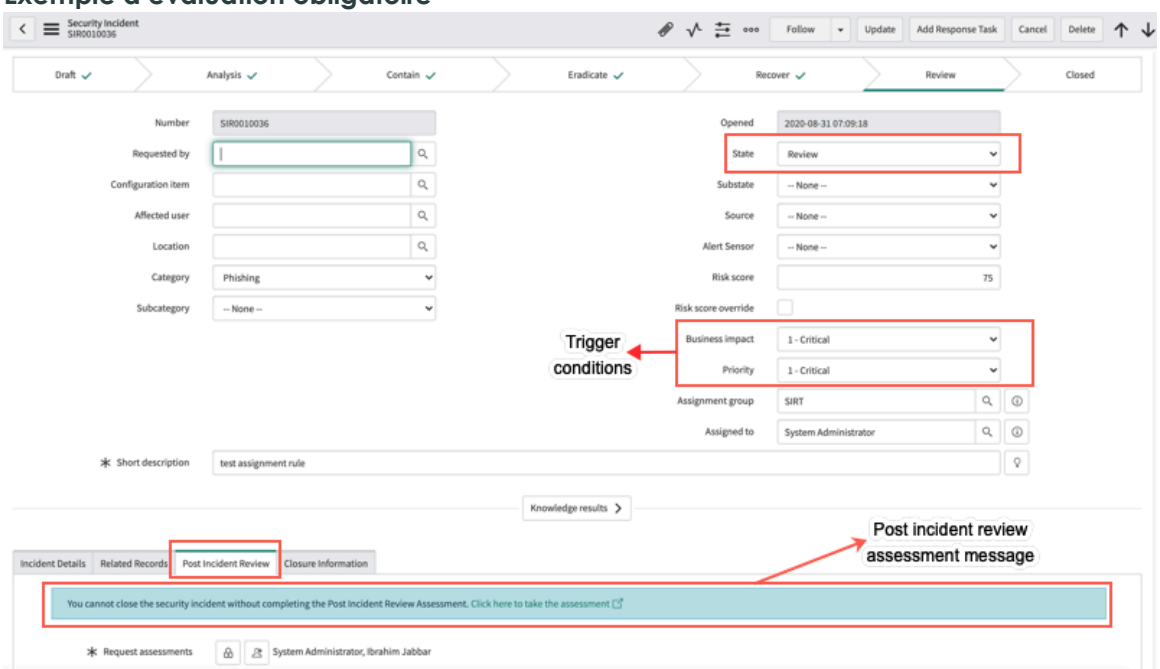
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemples de conditions de déclenchement de l'évaluation

Les exemples suivants fournissent différents scénarios sur la façon dont les conditions de déclenchement des évaluations obligatoires et facultatives sont générées.

- Sur le formulaire Condition de déclenchement de l'évaluation, générez des évaluations obligatoires lorsque la **priorité** et **l'impact sur l'entreprise** d'un incident de sécurité sont définis sur **Critique** sur la page **Règle de déclencheur d'évaluation** . Dans ce cas, les analystes de sécurité ne peuvent pas fermer l'incident tant que les évaluations obligatoires ne sont pas terminées.

Exemple d'évaluation obligatoire



- Comme vous pouvez le voir dans cet exemple, si un incident de sécurité est à l'état **Révision** , les analystes de sécurité ne peuvent pas fermer l'incident de sécurité sans avoir terminé **l'évaluation de la revue post-incident**. Un lien d'évaluation est disponible pour transmettre l'évaluation aux analystes de sécurité qui sont affectés (ou qui ont demandé l'évaluation) à l'incident.
- Sur le formulaire Condition de déclenchement de l'évaluation, générez des évaluations facultatives lorsque la **priorité** et **l'impact sur l'entreprise** d'un incident de sécurité sont définis sur **Élevé**. Dans cet exemple, si les analystes de sécurité ne terminent pas les évaluations et ferment l'incident de sécurité, les évaluations sont automatiquement annulées.
- Si les évaluations obligatoires ou facultatives ne correspondent pas à l'incident de sécurité, les évaluations ne sont pas générées pour ces incidents de sécurité. Un analyste de sécurité peut fermer l'incident de sécurité sans terminer l'évaluation de la revue post-incident.

Effectuer une revue post-incident basée sur un questionnaire

Vous pouvez décider qu'un examen post-incident de l'incident de sécurité est justifié. Une revue post-incident décrit ce qui s'est passé, permet de déterminer pourquoi l'incident s'est produit et identifie comment il peut être évité ou géré à l'avenir.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager, sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Quel que soit son rôle, tous les utilisateurs peuvent participer à un questionnaire d'examen post-incident. Les rôles peuvent être affectés à une révision.

Pourquoi et quand exécuter cette tâche

L'application ServiceNow Réponse aux incidents de sécurité peut automatiser la collecte d'informations de revue post-incident auprès de toutes les personnes impliquées dans un incident de sécurité à l'aide de questionnaires. Si vous décidez d'utiliser un questionnaire dans le cadre d'un examen post-incident, une liste de questions, pertinentes pour l'incident de sécurité, est envoyée à la liste des participants définie par l'utilisateur. Le rapport post-incident est généré automatiquement à chaque utilisateur. Le rapport compile toutes les informations relatives à l'incident de sécurité, ainsi que toutes les réponses à l'examen post-incident.

Bien qu'une liste initiale de questions soit fournie avec le système de base, elles sont personnalisables. Vous pouvez créer des catégories et y ajouter de nouvelles questions, ou modifier des questions individuelles dans des catégories existantes. Vous pouvez poser des questions en fonction des rôles. Vous pouvez définir à quel moment certaines questions sont posées. Il peut y avoir des questions que vous posez uniquement pour vos serveurs UNIX, par exemple, ou uniquement lorsqu'il y a une activité criminelle. Vous pouvez définir des questions qui sont posées en fonction de la réponse à une autre question ou de la valeur d'un champ du formulaire. Il peut même y avoir des questions qui sont entièrement remplies en interrogeant la base de données.

Une fois l'incident de sécurité résolu et passé à l'état **Réviser** , des évaluations sont générées pour tous les utilisateurs affectés et les utilisateurs qui sont directement ajoutés à partir de la liste **d'évaluation des demandes** .

Le questionnaire peut être un outil utile pour recueillir des informations sur la gestion de l'incident de sécurité à partir de diverses sources.

Au cours de l'examen, vous pouvez ajouter d'autres utilisateurs à la liste ou supprimer des utilisateurs existants de la liste, à moins qu'ils aient déjà commencé à remplir le questionnaire. Si vous ajoutez de nouveaux utilisateurs à la liste, ils recevront les questions lorsque l'enregistrement sera enregistré. L'incident de sécurité ne peut pas être fermé tant que tous les questionnaires n'ont pas été remplis. Au fur et à mesure que les questionnaires sont remplis par chaque utilisateur, le rapport post-incident est automatiquement généré (et régénéré) et affiché dans l'onglet **Revue post-incident** .

Pour commencer une revue post-incident :

Procédure

1. Créez un incident de sécurité ou ouvrez un incident existant en accédant à **Incident de sécurité** > **Incidents** > **Affectés à moi (ou affectés à l'équipe ou incidents non affectés)**.
2. Cliquez sur l'onglet **Post Incident Review (Revue post-incident**).
3. Le champ **Évaluations des demandes** est défini par défaut sur la personne dans le champ **Affecté à** .
   Cliquez sur l'icône de verrou pour ajouter d'autres utilisateurs à la liste de révision. Une fois le champ déverrouillé, des options sont disponibles pour ajouter ou supprimer plusieurs utilisateurs ou rôles ou pour saisir des adresses e-mail d'utilisateur.
4. Lorsque vous avez terminé vos saisies, cliquez sur l'icône de verrou pour verrouiller le champ.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez également définir des conditions qui, lorsqu'elles sont remplies dans un incident de sécurité, peuvent entraîner l'ajout automatique d'utilisateurs spécifiques au champ **Évaluations des demandes** pour cet incident de sécurité. Par exemple, lorsqu'une **catégorie** d'incident de sécurité est changée en **Hameçonnage**, des personnes spécifiques ayant une expertise dans les menaces de hameçonnage peuvent être ajoutées à la liste de revue post-incident. Pour plus d'informations, consultez Créer des règles d'affectation PIR.

5. Cliquez sur **Mettre à jour**.
   Lorsque l'incident passe à l'état **Examiner** (ou immédiatement, s'il est déjà à l'état **Réviser**), chacun des utilisateurs de la liste d'examen reçoit une première notification par e-mail . Les rappels sont envoyés à l'approche de la date d'échéance. Lorsque chaque utilisateur accède au questionnaire à partir du lien de l'e-mail ou en accédant à **Revue post-incident** > **Mes vérifications en attente**, les questions affichées sont tirées de toutes les catégories correspondant à cet incident de sécurité. Si de nouveaux utilisateurs sont ajoutés à la liste d'examen avant que la date d'échéance ne soit atteinte, ils reçoivent des notifications lorsque l'incident de sécurité est enregistré.

   Au fur et à mesure que les utilisateurs remplissent leurs questionnaires, le rapport post-incident compile les données et affiche le rapport dans l'onglet **Examen post-incident** . Les données du questionnaire sont affichées dans l'onglet **Résultats** .

Créer des catégories de questionnaire de revue post-incident

Vous pouvez utiliser les catégories de questionnaire fournies avec le système de base ou créer vos propres catégories.

Avant de commencer
Rôle requis : sn.si_admin

Pourquoi et quand exécuter cette tâche
Pour créer une nouvelle catégorie de questions :

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Revue post-incident**.
2. Cliquez sur **Passer en revue les questions**.
   Une liste de catégories s'affiche, ainsi que leur ordre et leurs filtres qui définissent les conditions dans lesquelles les questions sont posées (par exemple, uniquement lorsque la catégorie d'incident de sécurité est *Activité criminelle*). Chaque catégorie est une section du questionnaire de revue post-incident et les questions de chaque catégorie sont incluses uniquement lorsque l'incident de sécurité correspond au filtre Condition. Par exemple, pour une catégorie de questions s'appliquant uniquement aux serveurs Linux, vous devez configurer un filtre qui sélectionne les incidents de sécurité où le type de ressource affecté est Serveur Linux. Dans cette catégorie, vous devez ensuite créer toutes les questions nécessaires lorsqu'un incident de sécurité se produit sur un serveur Linux. Vous utilisez l'une des catégories fournies dans le système de base ou vous en créez une. Cette procédure suppose que vous souhaitez créer une nouvelle catégorie avant de définir les questions.
3. Cliquez sur **Nouveau** dans la liste des catégories.
4. Renseignez les champs du formulaire comme il convient.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incident de sécurité

Champ	Description
Nom	Nom de la catégorie qui apparaît dans le questionnaire d'incident de sécurité.
Type	L'examen post-incident est l'option par défaut.
Créer les personnes concernées	Non utilisé par Réponse aux incidents de sécurité.
Table	Ce champ est affecté automatiquement une fois le formulaire soumis.
Filtre	Entrez la condition qui détermine quand les questions de cette catégorie sont utilisées. Si un enregistrement d'incident de sécurité correspond à ce filtre, les questions sont incluses dans une revue post-incident pour cet incident de sécurité. Les filtres peuvent utiliser n'importe quelle donnée de l'enregistrement ou d'autres enregistrements liés à cet enregistrement. Par exemple, le département du gestionnaire de l'utilisateur demandeur.
Application	Application du périmètre pour l'incident.
Poids	Valeur numérique qui représente l'importance de cette mesure par rapport à d'autres mesures de la même catégorie. Par défaut, le poids est de 10.
Nombre total de mesures	Nombre de mesures utilisées par la catégorie.
Description	Description du questionnaire.

5. Cliquez sur **Soumettre** pour enregistrer la catégorie.

Rédiger des questions de révision post-incident

Vous pouvez utiliser les questions fournies avec le système de base ou créer vos propres questions.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Les méthodes de collecte d'informations sur l'examen post-incident peuvent prendre la forme de questions ou de données collectées automatiquement à l'aide de scripts.

Les questions peuvent dépendre des réponses à d'autres questions. Par exemple, vous pouvez demander si tous les journaux nécessaires sont disponibles. Si la réponse est non, posez une question de suivi pour déterminer lesquels des journaux nécessaires n'ont pas été activés.

La collecte de données scriptées, également appelées mesures de script, collecte les données relatives à l'incident de sécurité via les scripts que vous écrivez. Cette action peut aller bien au-delà des données contenues dans l'enregistrement d'incident de sécurité lui-même. Par exemple, une mesure de script peut recueillir l'heure de panne récente d'un serveur affecté par cet incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enfin, vous pouvez mélanger les deux types. Les questions peuvent avoir des valeurs par défaut extraites d'un script ou simplement d'un champ de l'enregistrement d'incident de sécurité. Lorsque vous utilisez une question de type `Réponse par défaut à partir de...`, vous pouvez choisir si vous souhaitez que l'utilisateur réponde toujours à la question (la valeur par défaut lui fournissant une valeur initiale) ou si vous souhaitez que la question ne soit posée à l'utilisateur que si le script ou le champ est vide.

Pour créer une nouvelle question :

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Revue post-incident**.
2. Cliquez sur la catégorie pour laquelle vous souhaitez créer une nouvelle question.
3. Cliquez sur l'onglet **Mesures d'évaluation** .
4. Cliquez sur **Nouveau**.
   Vous pouvez également cliquer sur une question existante pour la modifier.
5. Renseignez les champs du formulaire comme il convient.

Formulaire Métrique

Champ	Description
Nom	Nom de la mesure (question ou script). Si la mesure est une collection de données scriptée, ce nom apparaît dans le rapport post-incident.
Catégorie	Catégorie à laquelle la mesure appartient. Le système remplit automatiquement cette catégorie si vous créez une mesure à partir du formulaire de catégorie de mesure. **Remarque :** Vous ne pouvez pas modifier la catégorie si le champ **Dépend du champ est** défini ou si une autre mesure dépend de cette mesure
Méthode	Indique le type de mesure, comme suit : ◦ *Assessment*: une question qui n'a pas de valeur par défaut. Plusieurs types de données peuvent être définis dans le champ **Type de données** de l'onglet **Type de champ** , tels que les cases à cocher, les listes de choix, la saisie de texte. ◦ *Script*: mesure scriptée. Obtenir des valeurs en écrivant un script personnalisé. La *Script* méthode est compatible avec les types de données **Durée**, **Nombre** et **Pourcentage** . ◦ *Default answer from field*: question dont la réponse par défaut provient d'un champ sélectionné dans l'incident de sécurité. La sélection de cette option ajoute deux champs à l'onglet **Général** : ▪ *Default answer*: sélectionner le champ dans l'incident de sécurité qui contient la réponse par défaut à la question. Par exemple, pour la question : « Qui a initialement signalé cet incident ? », le champ **Demandé par** est un choix probable.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ *Ask question*: spécifie quand poser la question : toujours ou seulement si le champ **de réponse par défaut** est vide. À l'aide de l'exemple ci-dessus, la question sera posée si le champ **Demandé par** est vide. ◦ *Default answer from script*: question dont la réponse par défaut provient d'un script. La réponse peut être un nombre, une chaîne ou un pourcentage. L'onglet **Général** ajoute un champ : *Ask question*: comme spécifie quand poser la question : toujours ou seulement si le script ne fournit pas de réponse par défaut. Le script est défini dans l'onglet **Type de champ** . **Remarque :** Si vous sélectionnez un **type de données** incompatible avec la **méthode** sélectionnée, le système remplace automatiquement la **méthode** par une valeur compatible.
Poids	[Obligatoire] Valeur numérique qui représente l'importance de cette mesure par rapport à d'autres mesures de la même catégorie. Par défaut, le poids est de 10. Ce champ est visible et requis, sauf si le **type de données** est **Date**, **Date/Heure** ou **Chaîne**. Ces types de données ne sont pas inclus dans les calculs des résultats.
Ordre	[Obligatoire] Valeur numérique qui détermine l'ordre de la question de mesure dans les questionnaires d'évaluation, par rapport à d'autres questions de mesure de la même catégorie. La mesure dont la valeur d'ordre est la plus petite apparaît comme première question dans la section des catégories. Par défaut, l'ordre est 100. **Remarque :** La valeur d'ordre que vous utilisez pour les mesures avec la méthode Script n'a pas d'importance, car elles n'apparaissent pas dans les questionnaires.
Actif	Case à cocher qui détermine si cette mesure est utilisée. Si la case n'est pas cochée, c'est comme si l'enregistrement de mesure n'existait pas.
Obligatoire	Case à cocher qui rend la question de mesure obligatoire (sélectionnée) ou facultative (décochée) dans les questionnaires d'évaluation. Les utilisateurs ne peuvent pas soumettre de questionnaires tant qu'ils n'ont pas fourni de réponses valides à toutes les questions obligatoires, qui sont indiquées par un indicateur d'état de champ rouge. Ce champ n'est visible que si le champ **Dépend de** est vide et que le type de données n'est pas **Case à cocher**.

6. Cliquez sur l'onglet **Général** et renseignez les champs comme il convient.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Général

Champ	Description
Question	Texte à utiliser comme question dans les questionnaires d'examen des incidents de sécurité. Saisissez une question claire, simple et à laquelle il est facile de répondre, par exemple **Comment avons-nous maîtrisé l'incident**
Description	Informations sur la mesure et ce qu'elle évalue. S'il s'agit **d'une***Method*'évaluation, incluez des détails qui aident les utilisateurs à comprendre comment répondre à la question. Ce texte s'affiche en tant que conseil lorsqu'un utilisateur pointe sur le texte de la question dans le questionnaire.
Dépend de et s'affiche quand	Dans le champ **Dépend** de, sélectionnez une question dont dépend la question actuelle. Par exemple, la question « Quels journaux supplémentaires étaient nécessaires ? » dépend de la question « Tous les journaux nécessaires étaient-ils disponibles ? ». Ensuite, utilisez le champ **Affiché quand** pour identifier à quel moment vous souhaitez que la question dépendante apparaisse dans les questionnaires. Par exemple, si vous souhaitez que la question dépendante soit posée uniquement lorsque l'utilisateur répond **Non** à la question « Tous les journaux nécessaires étaient-ils disponibles ? », sélectionnez **Non** dans le champ **Affiché quand** . **Remarque :** Le système empêche la création de dépendances récursives entre les mesures. Par exemple, si la mesure A dépend de la mesure B, la mesure B ne peut pas dépendre de la mesure A.

7. Cliquez sur l'onglet **Type de champ** et renseignez les champs comme il convient.

Onglet Type de champ

Champ	Description
Type de données	Type de données de la réponse attendue dont la liste des types disponibles dépend pour la méthode sélectionnée. Si la méthode est **Évaluation**, le type de données détermine la façon dont les utilisateurs répondent à la question correspondante sur les questionnaires. Si la méthode est **Script**, le type de données détermine la manière dont le système calcule les résultats d'évaluation. **Remarque :** Si une autre mesure dépend de cette mesure, vous ne pouvez pas modifier le type de données.
Définir de façon aléatoire les réponses	Case à cocher qui détermine s'il convient de présenter les options de réponse pour cette question de mesure dans un ordre aléatoire chaque fois qu'un utilisateur ouvre un questionnaire d'évaluation qui contient la question. La préférence de réponse peut être influencée par l'ordre dans lequel les options de réponse apparaissent. Cela

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	peut entraîner des résultats biaisés. La randomisation des options de réponse peut aider à éviter ce biais. Ce champ n'est visible que si vous sélectionnez **Échelle de Likert** ou **Choix** dans le champ **Type de données** .
Module d'extension dépendant	[Obligatoire s'il s'agit d'un *Method* **script**.] Module d'extension qui contient les tables interrogées dans le script. Le système exécute le script de mesure uniquement si le module d'extension est actif. Les valeurs disponibles par défaut sont **Gestion des actifs**, **CMDB**, **Core**, **Gestion des coûts**, **Approvisionnement** et **Gestion des actifs logiciels**. Ce champ n'est visible que s'il s'agit d'un *Method* **script**. **Remarque :** ◦ Si la valeur principale par défaut est utilisée, le script est toujours exécuté. ◦ Si vous êtes administrateur, vous pouvez ajouter d'autres choix de modules d'extension au champ.
Définition d'échelle	Paramètre qui détermine si des valeurs numériques inférieures ou supérieures correspondent à un bon score dans les calculs de résultat d'évaluation. Sélectionnez **Faible** si les valeurs numériques inférieures sont préférables, par exemple pour une mesure qui mesure le nombre de défauts pour un fournisseur. Sélectionnez **Élevé** si des valeurs numériques plus élevées sont préférables, par exemple pour une mesure qui mesure la satisfaction des utilisateurs sur une échelle de un à cinq. La valeur par défaut est **Élevé**. Ce champ est visible et requis, sauf s'il s'agit **d'une Date**, **d'une Date/Heure** ou **d'une** *Data type* chaîne. Les résultats de ces types de données ne sont pas inclus dans les calculs des résultats.
Min.	Valeur numérique la plus faible à utiliser comme option de réponse sur les évaluations ou comme valeur adaptée dans une mesure scriptée. Ce champ n'est visible et requis que si certains types de données sont sélectionnés. Si le type de données est **Choix** ou **Échelle de Likert**, ce champ est en lecture seule et est défini automatiquement en fonction de la plus petite définition *Value* de mesure.
Max.	Valeur numérique la plus élevée à utiliser comme option de réponse ou valeur adaptée. Ce champ n'est visible et requis que si certains types de données sont sélectionnés. Si le type de données est **Choix** ou **Échelle de Likert**, ce champ est en lecture seule et est défini automatiquement en fonction de la définition *Value* de mesure la plus grande.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Script	Script qui obtient les informations système souhaitées. Le script comporte une variable d'entrée, définie avec l'ID de l'incident de sécurité (primaire), et trois variables de sortie possibles définies par le script, string_result, scaled_result et actual_result. Lorsque le type de données est Chaîne, seule la string_result est requise. Ce champ est visible et requis lorsque le *Method* champ est **Script**, ou lorsque la valeur par défaut provient d'un script.
Modèle	Un ensemble prédéfini de réponses courantes à utiliser pour la question. Par exemple, un modèle de fréquence commencerait probablement par une valeur « Jamais » et irait jusqu'à la valeur supérieure « Toujours ». Ce champ n'est visible et requis que s'il s'agit d'un *Data type* **modèle**. **Remarque :** Si une autre mesure dépend de cette mesure, vous ne pouvez pas modifier le modèle.

8. Facultatif : Lorsque vous avez terminé vos saisies, cliquez sur **Mettre à jour**.

Créer des règles d'affectation PIR

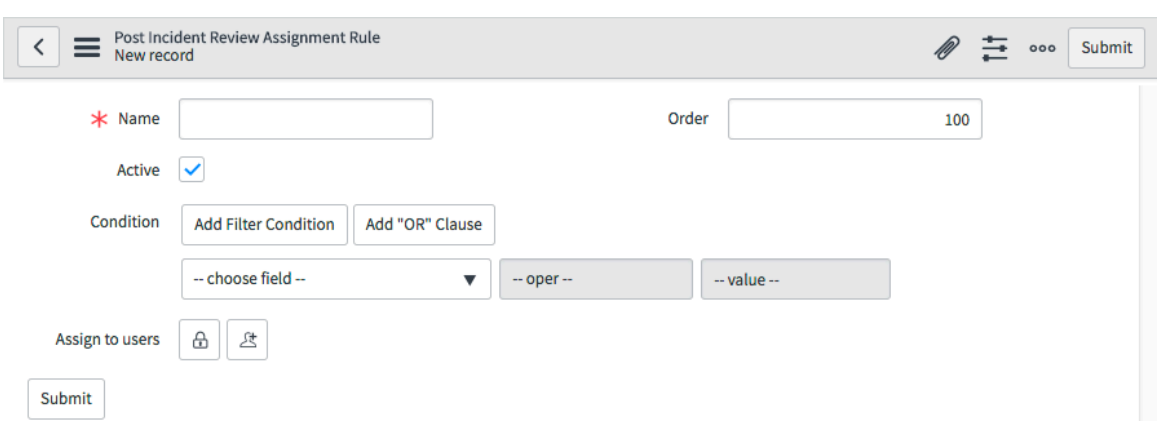
En plus d'ajouter manuellement des utilisateurs dans la liste d'évaluation de revue post-incident pour un incident de sécurité, vous pouvez définir des règles d'affectation pour ajouter automatiquement des utilisateurs à la liste.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager, sn_si.analyst

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Administration** > **Revue post-incident : configuration des évaluations**.
2. Explorez la section **Règles d'affectation d'utilisateur** .
3. Cliquez sur **Configurer**.
4. Cliquez sur **Nouveau**.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Renseignez les champs nécessaires.

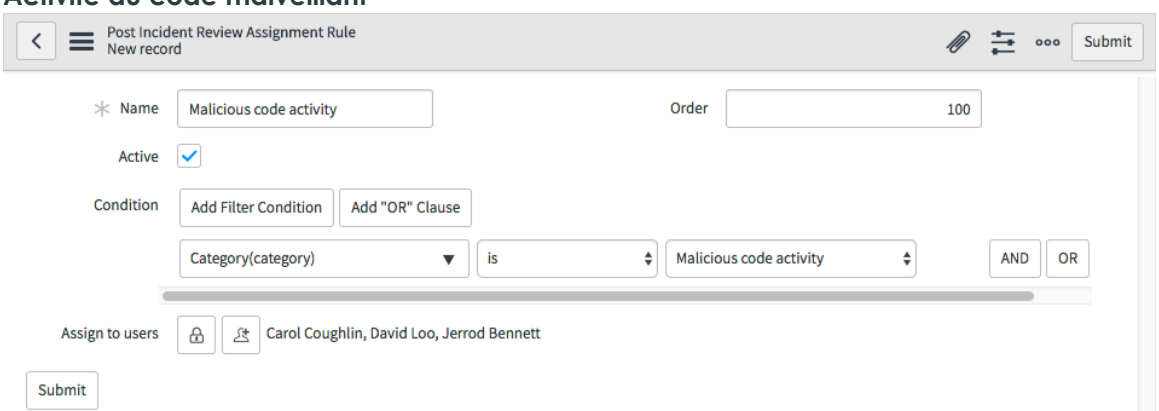
Champ	Description
Nom	Nom de cette règle d'affectation.
Actif	Cochez cette case pour rendre la règle active.
Ordre	Entrez une valeur numérique pour indiquer où cette règle doit apparaître dans la liste des règles d'affectation. Les nombres inférieurs apparaissent en haut de la liste. **Remarque :** Seule la première règle d'affectation correspondante est exécutée et seuls les utilisateurs définis dans cette règle sont ajoutés à la liste d'évaluation.
Condition	Utiliser le Créateur de conditions pour définir les conditions qui doivent être remplies dans l'incident de sécurité pour que cette règle soit exécutée. Pour plus d'informations, voir l'exemple ci-dessous.
Affecter aux utilisateurs	Cliquez sur l'icône de verrou pour ajouter des utilisateurs à la liste d'examen. Une fois le champ déverrouillé, des options sont disponibles pour ajouter ou supprimer plusieurs utilisateurs ou rôles ou pour saisir des adresses e-mail d'utilisateur.

6. Cliquez sur **Envoyer**.

Example: Activité du code malveillant

Dans la règle d'affectation de révision post-incident présentée ici, lorsqu'un incident de sécurité avec le champ **Catégorie** défini sur **Activité de code malveillant** passe à l'état **Réviser** , les trois utilisateurs identifiés (qui se trouvent être des experts dans la gestion de l'activité de code malveillant) sont ajoutés à la liste des utilisateurs qui recevront le questionnaire de revue post-incident pour cet incident de sécurité.

Activité du code malveillant



Fermer les incidents de sécurité

Lorsqu'un incident de sécurité est passé à l'état Révision, il est possible de le fermer et d'entrer un code de fermeture approprié. Les codes de fermeture peuvent être recherchés ultérieurement pour faciliter la localisation.

Avant de commencer

Rôle requis : sn_si.write

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Remarque : Dans les versions précédentes de Réponse aux incidents de sécurité, les utilisateurs pouvaient fermer les incidents de sécurité ou les requêtes en tant que spam. Dans la Istanbul version, l'option spam n'est plus disponible. Les incidents de sécurité ou les demandes de courrier indésirable peuvent être annulés ou supprimés, le cas échéant.

Procédure

1. Si l'incident de sécurité que vous voulez fermer n'est pas déjà ouvert, accédez à **Incident de sécurité** > **Incidents** > **Afficher les incidents**et localisez l'incident de sécurité que vous souhaitez fermer.

   Remarque : S'il existe des évaluations de revue post-incident qui n'ont pas été terminées pour cet incident de sécurité, l'incident de sécurité ne peut pas être fermé. Retourner à **Incident de sécurité** > **Revue post-incident** > **Toutes les révisions incomplètes**, localisez les révisions incomplètes et demandez aux examinateurs de terminer leurs révisions ou annulez les évaluations restantes.

2. Cliquez sur l'onglet **Informations sur la fermeture** et renseignez les champs comme il convient.

Incident de sécurité

Champ	Description
Créer un article de la base de connaissances	Sélectionnez ce champ pour créer automatiquement un brouillon d'article de la base de connaissances contenant le contenu de la revue post-incident.
Code de fermeture	Sélectionnez le code de fermeture qui décrit le mieux la raison pour laquelle vous fermez cet incident de sécurité. ◦ Enquête terminée ◦ Menace réduite ◦ Vulnérabilité corrigée ◦ Vulnérabilité non valide ◦ Non résolu ◦ Faux positif
Fermé par	Affiche l'utilisateur qui a fermé l'incident de sécurité après la mise à jour de l'enregistrement.
Fermé	Affiche la date et l'heure de fermeture après la mise à jour de l'enregistrement.
Fermer les notes	Entrez toutes les notes supplémentaires qui décrivent le résultat de la fermeture de cet incident de sécurité.

3. Cliquez sur **Mettre à jour**.
4. L'utilisateur affecté peut changer manuellement **l'état** en **Fermé**.
   Lorsqu'un incident parent est fermé, toutes les tâches de réponse appartenant à l'incident enfant sont annulées. S'il n'existe pas d'autres types de tâches, l'incident enfant est également fermé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter des informations sur la fermeture à un incident de sécurité

Lorsqu'un incident de sécurité est à l'état Examen ou Fermé, vous pouvez saisir les informations de fermeture.

Avant de commencer
Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité que vous souhaitez mettre à jour.
2. Cliquez sur l'onglet **Enregistrements connexes** .
3. Renseignez les champs nécessaires.

Champ	Description
Créer un article de la base de connaissances	Cochez cette case pour générer un article de la base de connaissances à l'aide du contenu du rapport post-incident.
Code de fermeture	Sélectionnez le code de fermeture qui décrit le mieux le motif de fermeture de l'incident de sécurité.
Fermé par	[Lecture seule] Affiche l'utilisateur qui a fermé l'incident de sécurité.
Fermé	[Lecture seule] Affiche la date et l'heure de clôture de l'incident de sécurité.
Fermer les notes	Comment l'incident de sécurité a été clos, y compris les enseignements tirés, la résolution, etc.

4. Cliquez sur l'un des onglets suivants pour mettre à jour l'incident de sécurité :
   - Détails de l'incident
   - Revue post-incident
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Restreindre l'accès aux incidents de sécurité

Gérez l'accès aux incidents de sécurité qui contiennent des informations sensibles. Vous pouvez appliquer des restrictions d'incident de sécurité pour déterminer qui peut accéder à un incident donné et limiter l'accès uniquement à des utilisateurs ou groupes spécifiques.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Les restrictions d'incidents de sécurité vous permettent de masquer l'accès aux incidents de sécurité critiques par d'autres utilisateurs d'une organisation particulière. Ces restrictions vous permettent de fournir un moyen plus granulaire de contrôler les incidents de sécurité auxquels un utilisateur peut accéder. Vous pouvez appliquer une restriction d'incident de sécurité en cochant la case **Appliquer la restriction** , puis en sélectionnant les utilisateurs ou les groupes autorisés à accéder à l'incident de sécurité en question.

Une fois que vous avez appliqué la restriction à des incidents de sécurité spécifiques et limité l'accès à certains utilisateurs ou groupes, tous les autres utilisateurs restants de votre organisation ne peuvent pas accéder à ces incidents de sécurité, même s'ils recherchent un incident de sécurité restreint particulier.

Traduction automatique

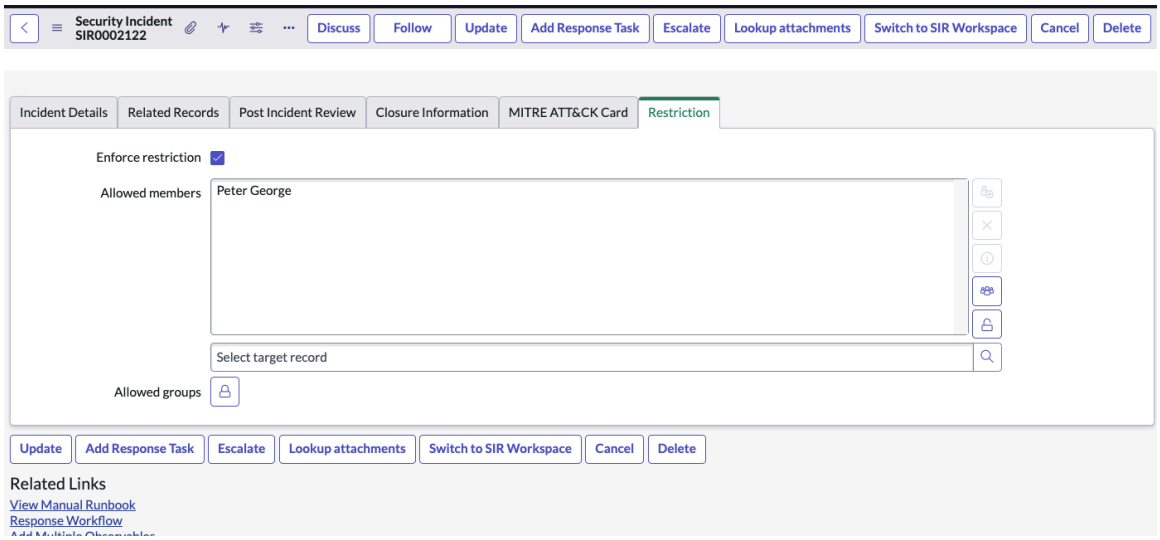
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez un incident de sécurité que vous souhaitez limiter.
2. Si vous utilisez l'interface utilisateur classique, procédez comme suit :

   a. Cliquez sur l'onglet **Restriction** .

   b. Cochez la case **Appliquer la restriction** pour activer la restriction de l'incident de sécurité.



   c. Dans le champ Membres autorisés, cliquez sur pour sélectionner les utilisateurs qui peuvent accéder à l'incident de sécurité.

   d. Sélectionnez pour vous ajouter en tant qu'utilisateur autorisé.

   e. Sélectionnez l'icône pour ajouter ou supprimer des utilisateurs.

   f. Dans le champ Groupes autorisés, cliquez sur pour sélectionner les groupes qui peuvent accéder à l'incident de sécurité.

   g. Sélectionnez l'icône pour ajouter ou supprimer des groupes.

   > **Remarque :** Une fois la case à cocher **Appliquer la restriction** activée pour l'incident de sécurité, seuls le sn_si.admin et les membres ou groupes autorisés auront accès à l'incident de sécurité.

   h. Cliquez sur **Mettre à jour**.

3. Si vous utilisez l'espace de travail SIR, effectuez les opérations suivantes :

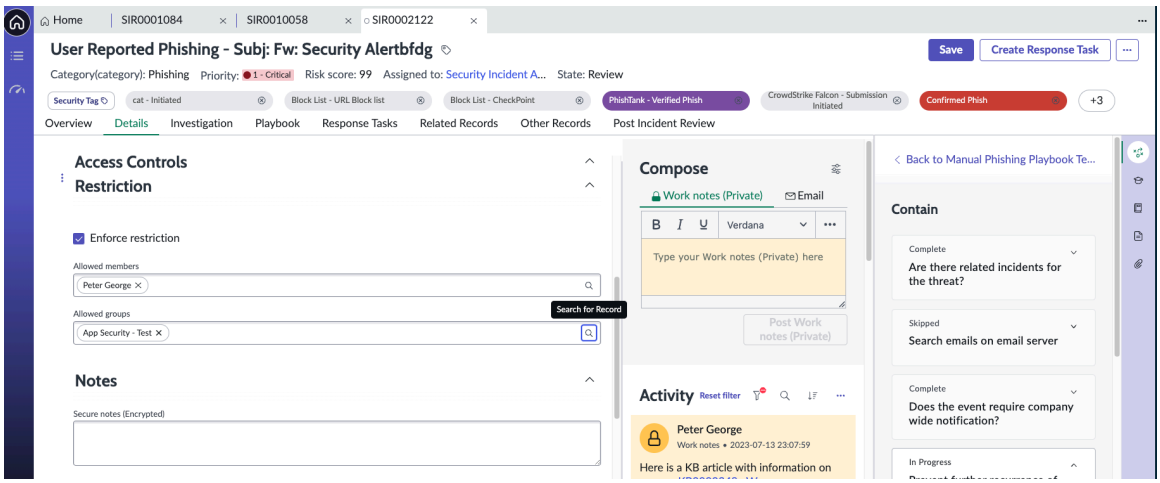
   a. Dans l'incident de sécurité, cliquez sur l'onglet **Détails** .

   b. Faites défiler vers le bas et cliquez sur la section **Restriction** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Cochez la case **Appliquer la restriction** pour activer la restriction de l'incident de sécurité.



d. Dans le champ Membres autorisés, sélectionnez les utilisateurs qui peuvent accéder à l'incident de sécurité à l'aide de l'option Rechercher.

e. Dans le champ Groupes autorisés, sélectionnez les groupes qui peuvent accéder à l'incident de sécurité à l'aide de l'option Rechercher.

> **Remarque :** Une fois la case à cocher **Appliquer la restriction** activée pour l'incident de sécurité, seuls le sn_si.admin et les membres ou groupes autorisés auront accès à l'incident de sécurité.

f. Cliquez sur **Enregistrer**.

Gérer les menaces de sécurité à l'aide de l' Security Analyst Workspace

Réponse aux incidents de sécurité comprend une nouvelle interface utilisateur appelée Qui Security Analyst Workspace comprend des outils puissants d'aide à l'analyse, notamment le playbook, la vue coup d'œil et des onglets pour travailler sur plusieurs incidents de sécurité.

Spécialement conçus pour les analystes de sécurité, les puissants outils de l'vous Security Analyst Workspace permettent d'analyser le volume toujours croissant de données associées aux incidents de sécurité. De plus, les actions automatisées réduisent considérablement le temps d'enquête sur les incidents de sécurité, ce qui peut faire la différence entre l'arrêt d'une attaque et la violation d'une violation.

Avant d'utiliser l'option Security Analyst Workspace

Avant de pouvoir commencer à utiliser le Security Analyst Workspace, vous devez vous assurer qu'au moins London Patch 3 est installé sur votre instance, que vous avez défini les rôles appropriés et que vous disposez de a téléchargé l'application Security Incident Response UI à partir du ServiceNow Store.

> **Remarque :** Si votre instance exécute une version antérieure à London Patch 3, vous devez demander le module d'extension Security Incident Response UI via le système HI Customer Service.

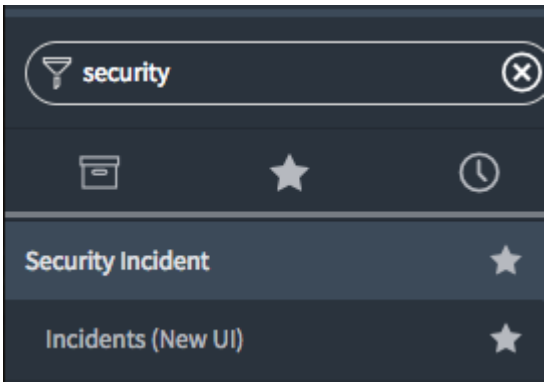
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accéder à Security Analyst Workspace

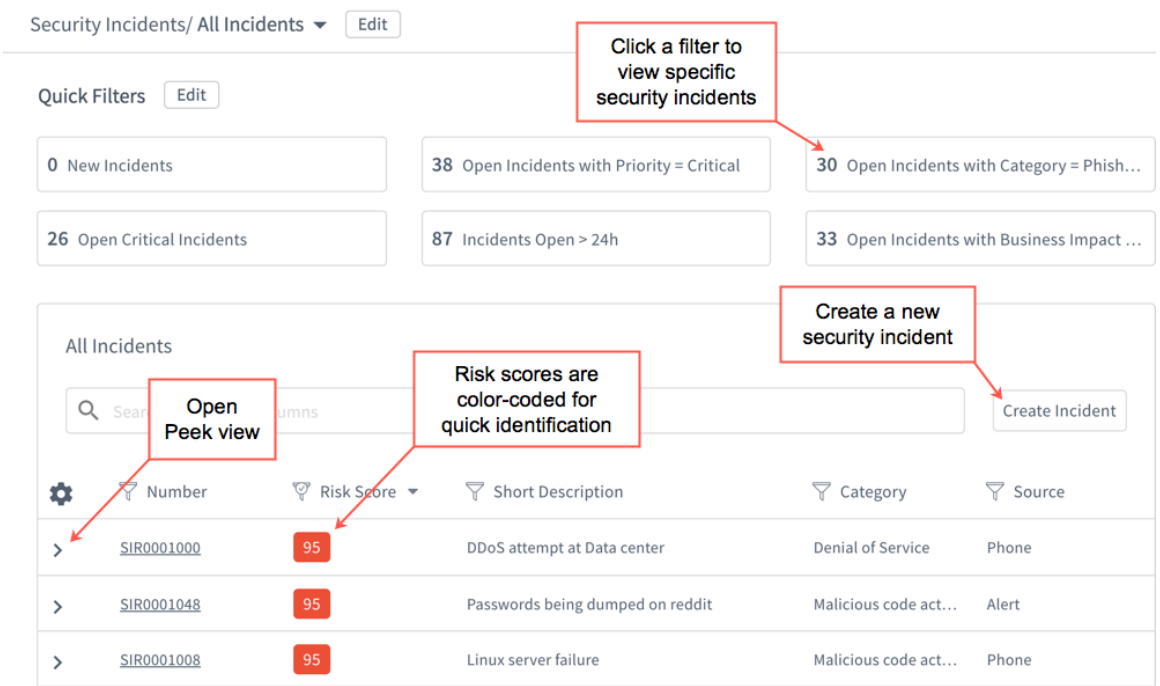
Pour accéder à ce nouvel espace de travail, accédez à **Incident de sécurité** > **Incidents (nouvelle UI)**.

Incident de sécurité



L'espace de travail s'ouvre dans un onglet de navigateur distinct.

Incidents de sécurité

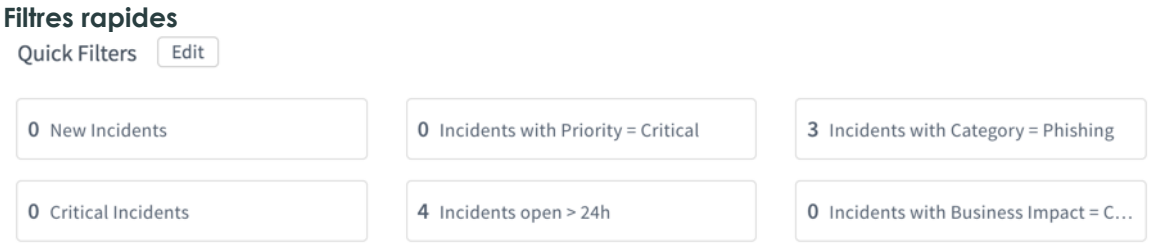


Localisez les incidents de sécurité que vous souhaitez analyser avec les filtres rapides

Le Security Analyst Workspace fournit plusieurs outils pour filtrer la liste des incidents de sécurité afin que vous puissiez trouver rapidement les incidents de sécurité que vous souhaitez analyser. Les filtres rapides vous permettent de sélectionner un sous-ensemble d'incidents de sécurité en fonction des critères du filtre.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



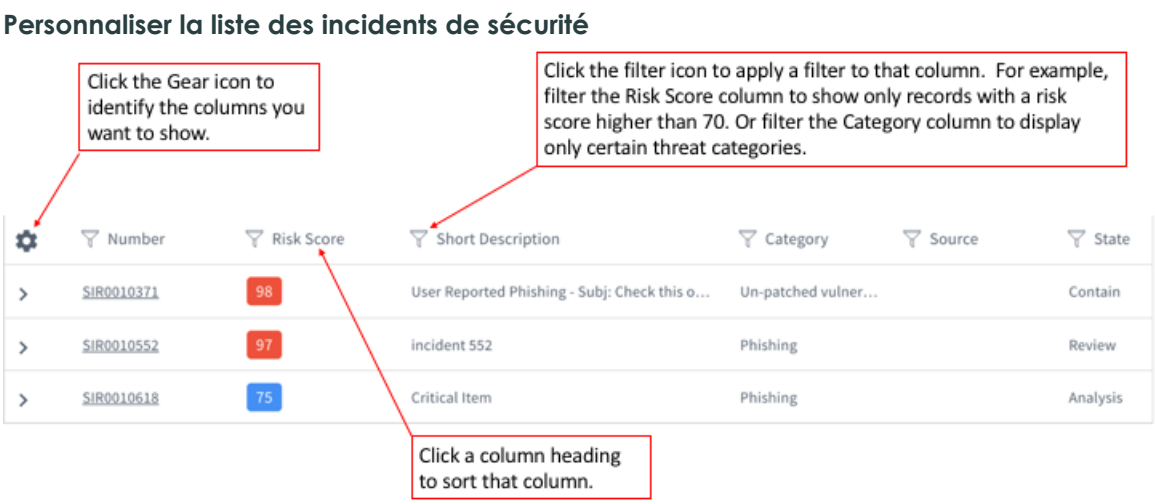
Il vous suffit de cliquer sur le filtre rapide que vous souhaitez utiliser.

Remarque : Vous pouvez cliquer sur un bouton **Modifier** pour identifier les filtres rapides que vous souhaitez afficher sur l'écran de liste. Un filtre minimum doit être sélectionné, jusqu'à un maximum de six.

Vous pouvez définir des filtres rapides supplémentaires, ainsi que des filtres primaires pour le , à l'aide de Security Analyst Workspacel'environnement classique. Pour plus d'informations, consultez Configurer des filtres primaires et secondaires pour Security Analyst Workspace.

Personnaliser la liste des incidents de sécurité

Comme pour toutes les listes de votre instance, le Security Analyst Workspace fournit des outils pour personnaliser la liste et trier les informations affichées afin de répondre à vos besoins d'analyse.



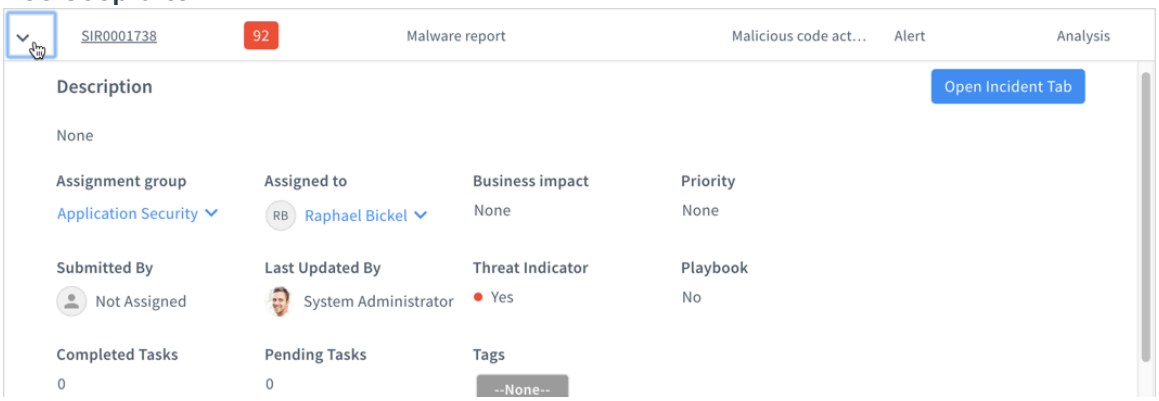
Gagnez du temps avec le mode Coup d'œil

Avant d'ouvrir un enregistrement d'incident de sécurité, vous pouvez gagner du temps en utilisant le mode Coup d'œil. Cette fonctionnalité vous permet de localiser rapidement les artefacts de sécurité vitaux sans avoir à recharger la page entière. Il vous suffit de cliquer sur l'icône **de >** à gauche d'un numéro d'incident de sécurité pour en jeter un coup d'œil.

Traduction automatique

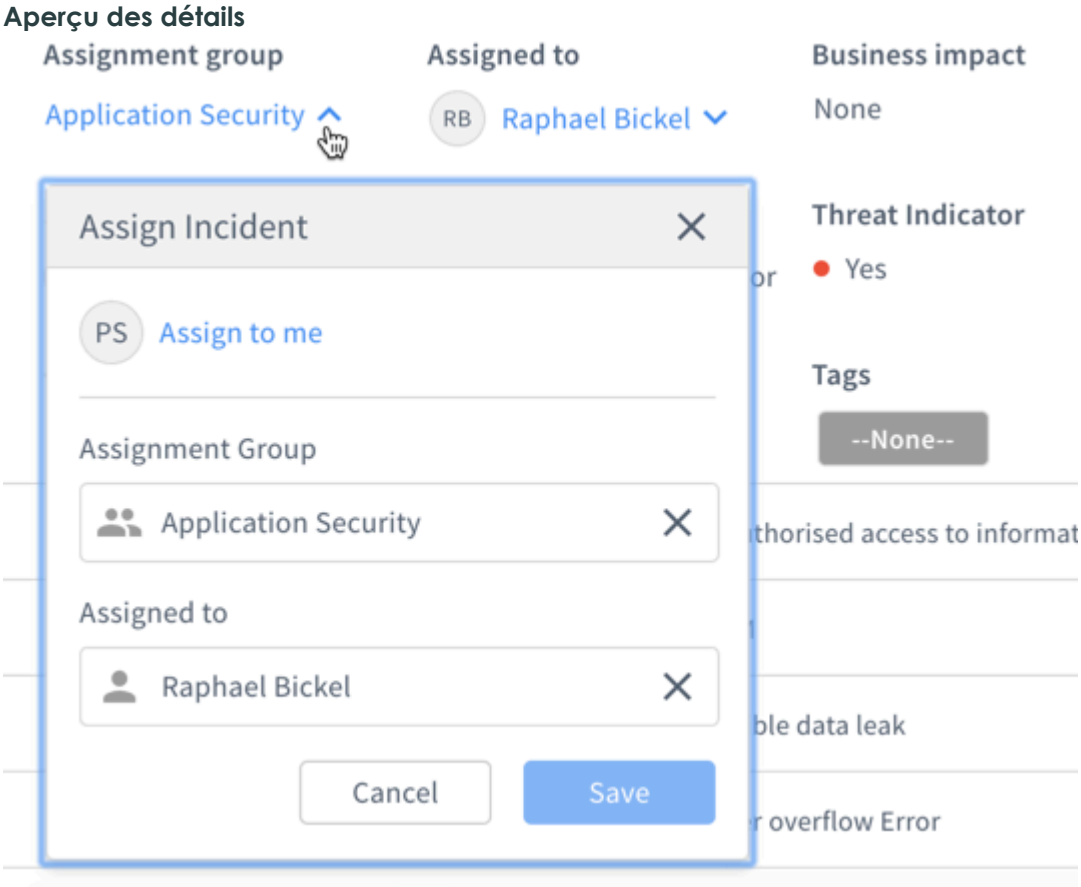
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue coup d'œil



Le mode d'aperçu fournit un instantané des informations vitales dans une vue unique. Cette vue peut vous faire gagner un temps précieux lorsque vous travaillez sur plusieurs incidents. Vous pouvez cliquer sur les flèches vers le bas de certains champs pour effectuer des mises à jour à la volée, telles que l'affectation d'un groupe d'affectation ou d'un analyste spécifique.

Aperçu des détails



Effectuer des actions rapides sur un incident de sécurité

Une fois que vous avez sélectionné et ouvert un incident de sécurité spécifique, vous pouvez effectuer des actions permettant de gagner du temps sur l'enregistrement.

Traduction automatique

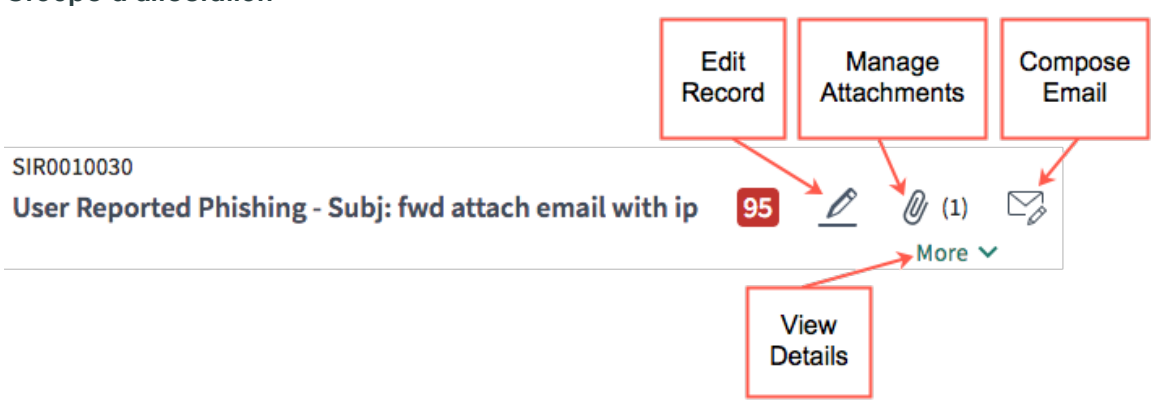
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si votre incident de sécurité est ouvert, cliquez sur l'icône **Modifier l'enregistrement** pour apporter des modifications rapides à l'un de ses champs. Si l'enregistrement est fermé, vous ne pouvez modifier que sa balise.
- Cliquez sur **Gérer les pièces jointes** pour joindre des fichiers à l'incident de sécurité. Vous pouvez également télécharger ou supprimer des fichiers joints et modifier le chiffrement appliqué aux pièces jointes.
- Cliquez sur **Composer un e-mail** pour envoyer un e-mail rapide à un collègue. Les e-mails peuvent être de forme libre ou vous pouvez envoyer des e-mails prédéfinis sélectionnés dans une liste de modèles. Les e-mails envoyés et les réponses reçues sont capturés dans la chronologie des incidents.

  Remarque : Vous pouvez créer des modèles personnalisés qui contiennent du contenu réutilisable pour les e-mails et les notifications par e-mail. Les variables peuvent être utilisées pour insérer des informations spécifiques à l'incident de sécurité ou à l'alerte, telles que la ligne d'objet, la priorité ou la catégorie de menace. Utilisez la table Incident de sécurité [sn_si_incident] pour les e-mails et les notifications par e-mail associés à Réponse aux incidents de sécurité. Pour plus d'informations, voir Modèles d'e-mail

- Cliquez sur **Plus** pour afficher un instantané rapide de l'incident de sécurité, tel que la description, l'impact sur l'entreprise et la priorité. Vous pouvez également cliquer sur la flèche vers le bas dans les champs **Groupe d'affectation** et **Affecté à** pour apporter des modifications à la volée à ces champs.

Groupe d'affectation



Travailler avec plusieurs incidents de sécurité

L'interface à onglets vous permet de garder plusieurs incidents de sécurité ouverts simultanément afin de pouvoir passer de l'un à l'autre en un seul clic. Cela peut vous faire gagner du temps et vous permettre d'avoir une vue d'ensemble lorsque des menaces provenant de plusieurs sources sont identifiées.

Travailler avec plusieurs incidents de sécurité



Afficher les informations d'analyse dans les onglets d'incident de sécurité

Lorsque vous ouvrez un enregistrement d'incident de sécurité, trois onglets s'affichent :

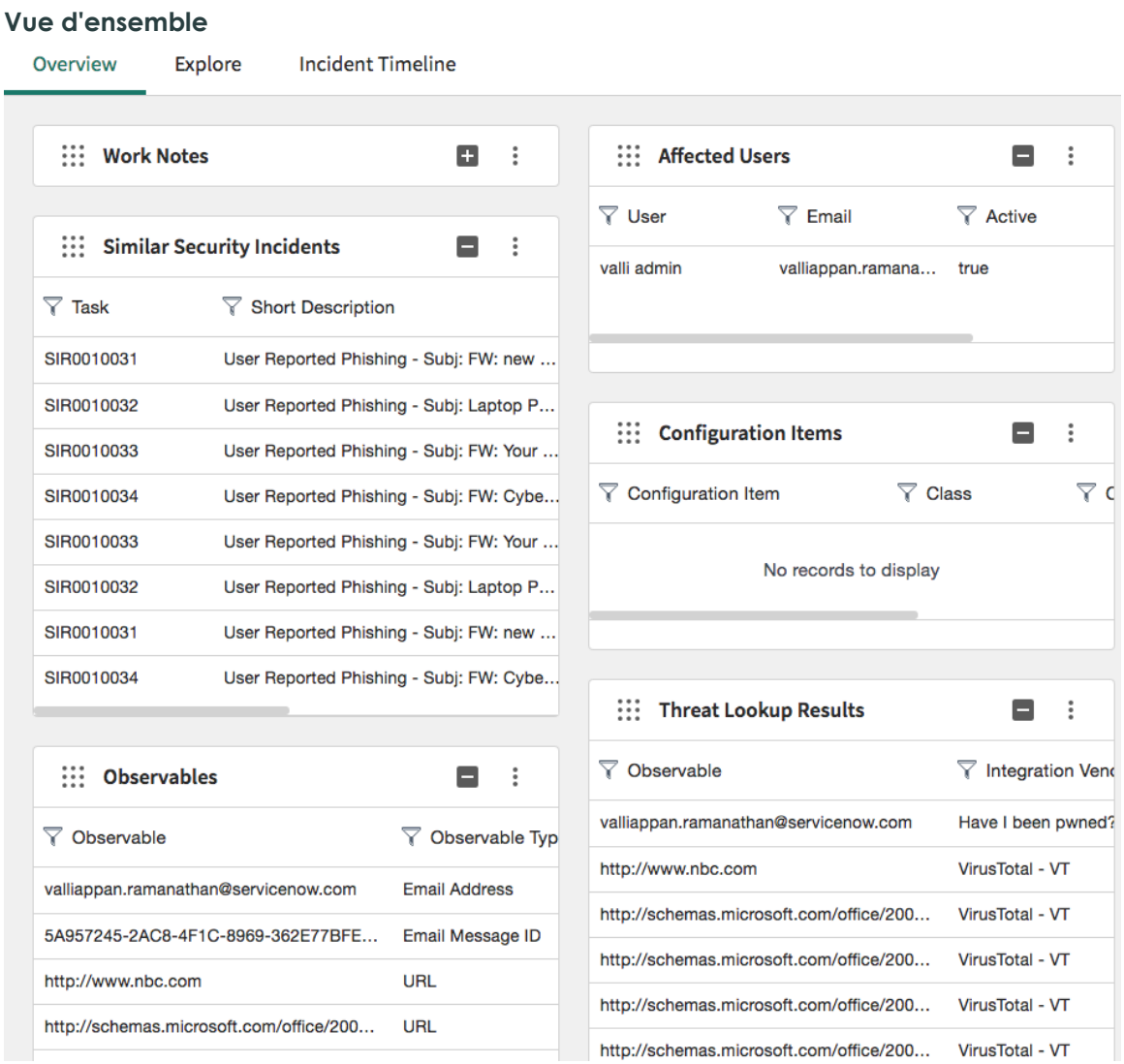
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vue d'ensemble
- Explorer
- Chronologie des incidents

Onglet Vue d'ensemble

Utilisez l'onglet **Vue d'ensemble** pour afficher les informations d'un incident de sécurité à un seul emplacement. Inutile d'ouvrir une autre application ou console.

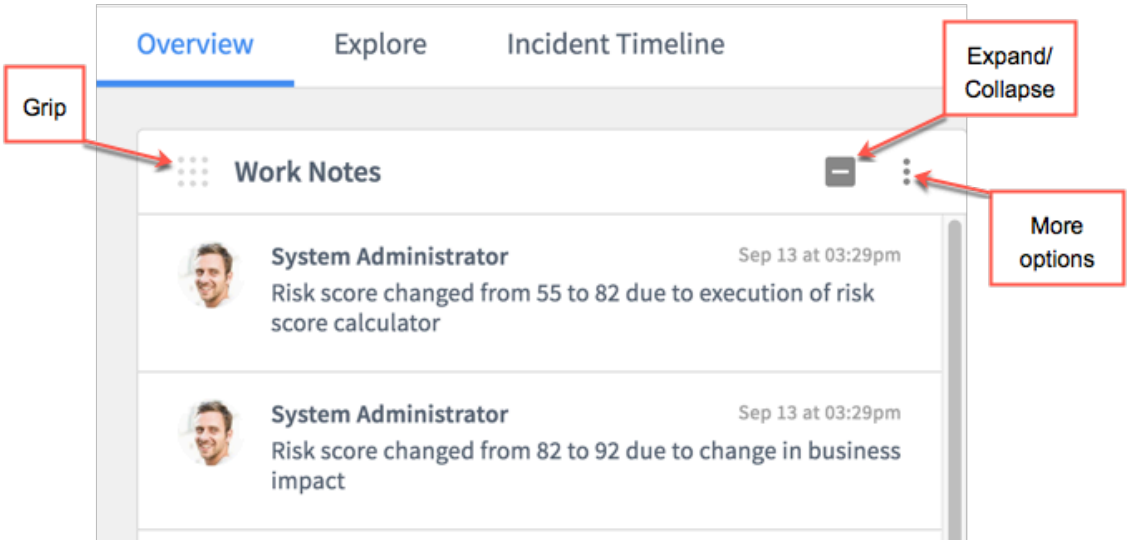


Les vignettes affichées dans l'onglet **Vue d'ensemble** sont personnalisables. Vous pouvez les réduire et les développer selon vos besoins, et vous pouvez les déplacer en faisant glisser l'icône **Poignée** . Cliquez sur l'icône **Autres options** pour supprimer une vignette ou modifier son texte d'en-tête.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

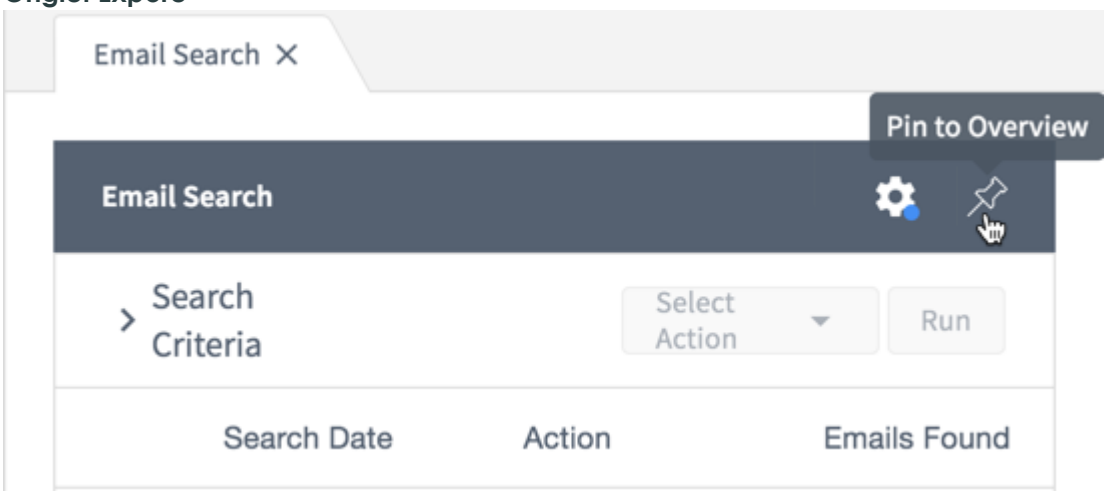
Onglet Vue d'ensemble



Onglet Explorer

Configurez les vignettes affichées dans l'onglet **Vue d'ensemble** à l'aide de l'onglet **Explorer** . Il vous suffit de sélectionner les tuiles que vous souhaitez afficher dans le volet de gauche, puis de cliquer sur l'icône **Épingler** . Les vignettes épinglées s'affichent automatiquement dans l'onglet **Vue d'ensemble** .

Onglet Expore



Le volet gauche de l'onglet **Explorer** comprend une grande variété d'informations que vous pouvez afficher dans l'onglet **Vue d'ensemble** . Par exemple, **développez Observables** pour afficher ces listes connexes.

- Observables
- Résultats de la recherche de menace
- Résultats de l'analyse de sécurité
- Recherches de domaine
- Enrichissement des éléments observables

D'autres listes connexes sont disponibles sous **Utilisateurs**, **Éléments de configuration** et **Incidents**.

Traduction automatique

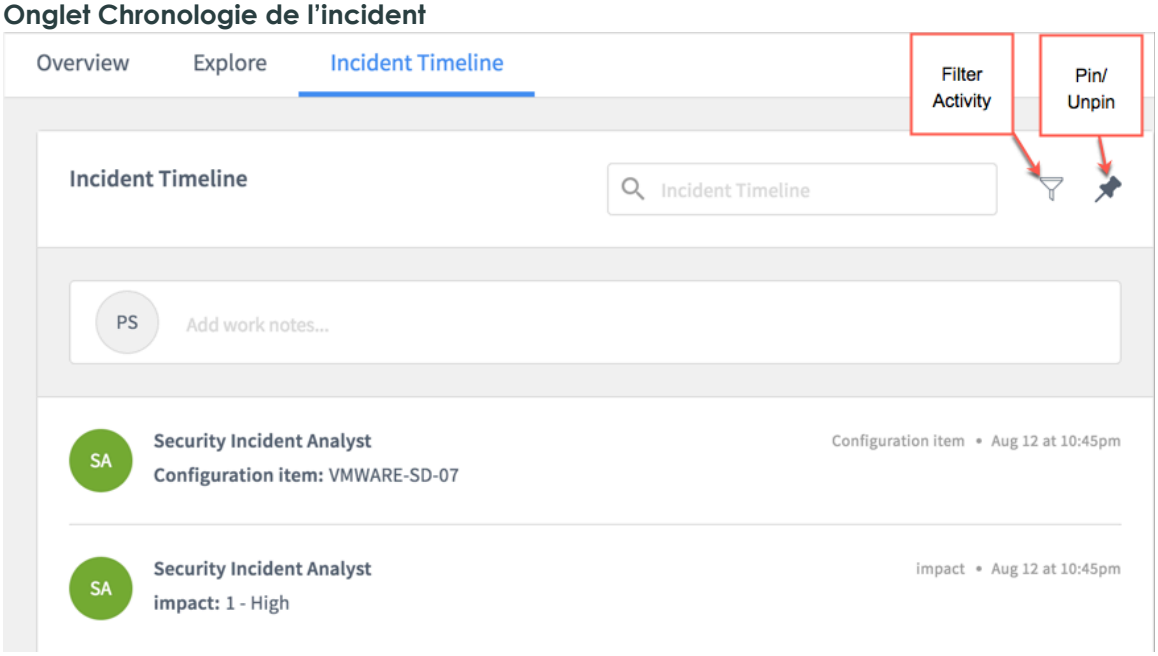
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Chronologie de l'incident

Utilisez l'onglet **Chronologie des incidents** au cours de votre enquête à des fins de suivi. Chaque fois qu'une action est effectuée sur un incident de sécurité, le système l'enregistre dans la chronologie de l'incident.

- Vous pouvez également ajouter manuellement des notes de travail à la chronologie en les saisissant dans la zone **Ajouter des notes de travail** et en cliquant sur **Publier**.
- Vous pouvez rechercher une activité de chronologie spécifique à l'aide de la zone de recherche.
- L'icône **Filtrer l'activité** vous permet d'afficher uniquement les types d'activités de chronologie que vous souhaitez voir (par exemple, uniquement les incidents créés par un analyste spécifique).
- Vous pouvez ajouter ou supprimer la chronologie des incidents à partir de l'onglet **Vue d'ensemble** à l'aide de l'icône **Épingler/Détacher** .

Onglet Chronologie de l'incident



Gérer les incidents de sécurité à l'aide du Playbook

Résolvez certains types de menaces à la sécurité étape par étape à l'aide des playbooks d'analyste de la sécurité intégrés. Par exemple, un analyste peut utiliser le playbook pour résoudre les attaques de hameçonnage et les menaces causées par des activités de code malveillant. Pour plus d'informations, consultez Résoudre les menaces de sécurité avec le playbook.

Résoudre les menaces de sécurité avec le playbook

Utilisez le Playbook pour résoudre certains types de menaces à la sécurité étape par étape. Par exemple, vous pouvez résoudre les attaques de hameçonnage et les menaces causées par une activité de code malveillant à l'aide de playbooks.

Avant de commencer

Rôle requis : sn_si.admin ou admin

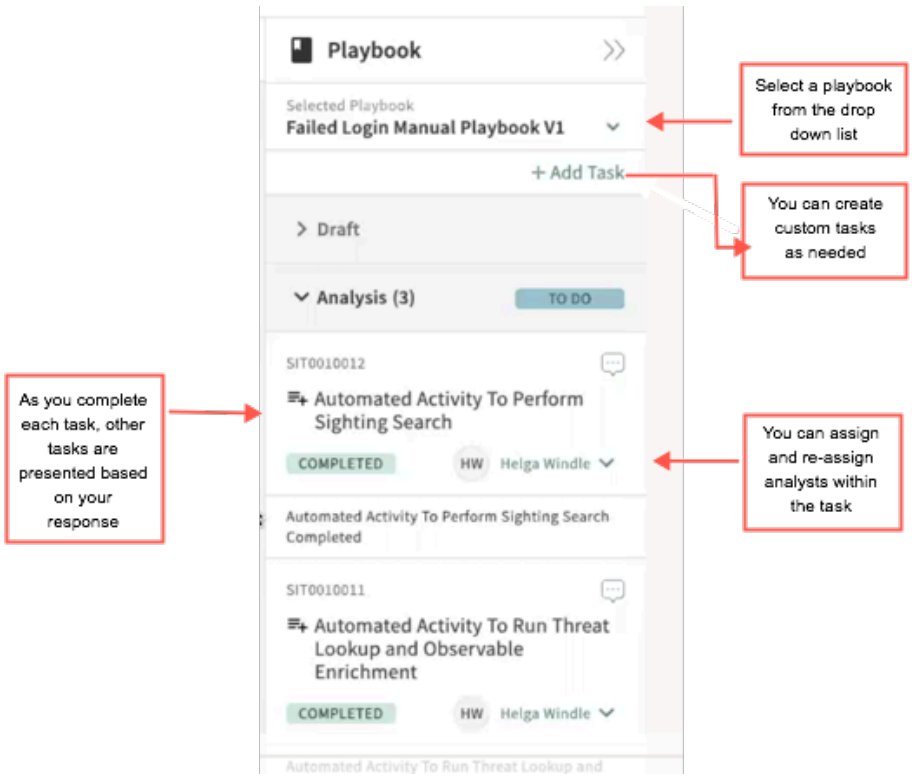
Pourquoi et quand exécuter cette tâche

Chaque groupe de tâches (Analyse, Contenir, etc.) vous guide à travers une série de questions et d'autres activités pour résoudre la menace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

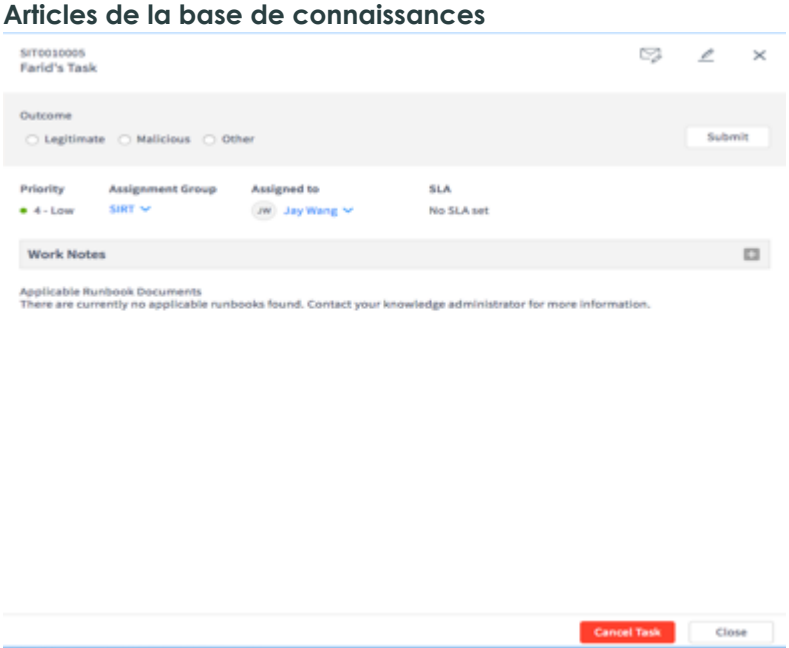
Playbook



Au fur et à mesure que vous accomplissez chaque tâche, saisissez des notes de travail pour faciliter l'analyse des attaques similaires à l'avenir. Une fois qu'une menace est identifiée, vous pouvez également utiliser les informations du playbook pour mettre la menace en quarantaine, isoler les ressources affectées de manière similaire et supprimer les programmes malveillants.

Les articles de la base de connaissances, inclus dans chaque tâche, fournissent des conseils et d'autres informations pour vous aider à effectuer les étapes nécessaires.

Articles de la base de connaissances



Traduction automatique

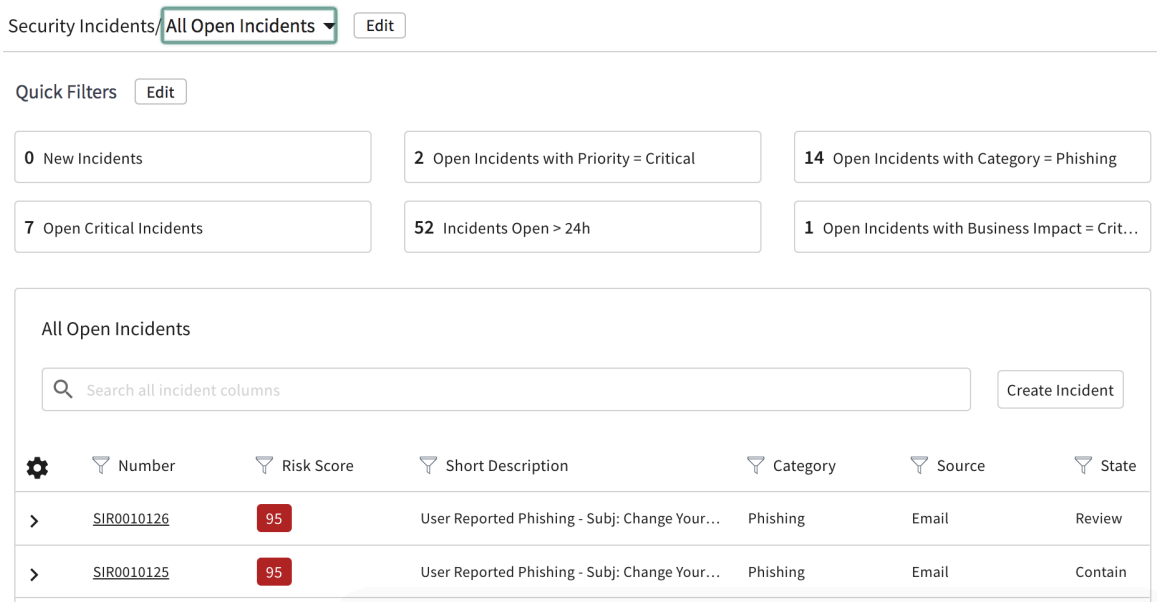
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le système de base inclut des articles de la base de connaissances pour chacune des tâches du playbook. Vous pouvez toutefois écrire vos propres articles de la base de connaissances et les associer à des tâches de playbook.

Remarque : Pour obtenir un exemple d'utilisation du playbook pour analyser et résoudre une menace spécifique, reportez-vous à la section Résolution des attaques de hameçonnage signalées par les utilisateurs avec le playbook.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents (nouvelle UI)**.
   L'écran Incidents de sécurité affiche les incidents de sécurité qui vous ont été affectés.



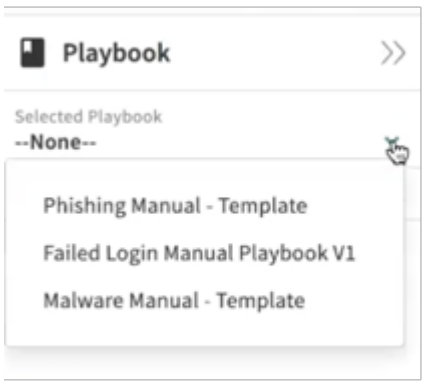
2. Vous pouvez cliquer sur la liste de choix **Affectés à moi** pour sélectionner un autre filtre, comme tous les incidents ouverts ou tous les incidents non affectés.
   Vous pouvez également cliquer sur l'un des filtres rapides pour afficher les incidents de sécurité d'un type particulier, tels que les incidents critiques uniquement.
3. Cliquez sur l'incident de sécurité que vous souhaitez analyser.

   Envisagez de donner la priorité aux incidents de sécurité avec des scores de risque élevés.

4. Si le volet playbook sur le bord droit de l'écran est fermé, cliquez sur l'icône playbook ( ) pour l'ouvrir.
   Si aucun playbook n'est affecté à l'incident de sécurité, vous pouvez sélectionner un playbook dans la liste de choix de Playbooks sélectionnés, comme indiqué ci-dessous :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez également affecter un playbook différent à l'incident de sécurité. Pour inclure un playbook dans la liste de choix de Playbooks sélectionnés ou pour modifier le playbook pour un incident de sécurité, consultez Activer les playbooks pour la sélection d'analystes pour en savoir plus.

Le playbook spécifique au type de menace de sécurité s'ouvre. Il est divisé en catégories de tâches similaires. Par exemple, vous utilisez les tâches du groupe **Analyse** pour déterminer la validité et l'étendue de la menace. Le groupe **Contenir** comprend des tâches permettant d'isoler la menace pour un utilisateur ou un actif spécifique. Les tâches du groupe **Éradiquer** vous guident tout au long du processus de suppression du programme malveillant ou de re-mise en image de l'hôte.

5. Cliquez sur le premier groupe (**Analyse**), puis sur la première tâche dans le playbook.
6. Suivez les invites de la tâche.
   - Certaines tâches posent une question, par exemple « L'e-mail fait-il partie de la campagne ? » Effectuez l'analyse nécessaire pour répondre à la question et sélectionnez **Oui** ou **Non**.
   - Si vous avez défini des articles de la base de connaissances et les avez associés à des tâches de playbook, les articles s'affichent lorsque vous commencez à travailler sur une tâche.
   - Certaines tâches sont transitoires. Ils vous demandent simplement d'effectuer une action, comme l'ajout d'observables à un incident de sécurité. Une fois que vous avez terminé l'action, cliquez sur **Marquer comme terminé**.

   Au fur et à mesure que vous effectuez des tâches, les tâches suivantes vous sont présentées en fonction des choix que vous faites. Les groupes grisés (tels que **Récupérer**, **Examiner**, etc.) peuvent être activés par vos choix.
7. Continuez à travailler sur chaque tâche qui vous est présentée jusqu'à ce que vous ayez terminé toutes les tâches afin de résoudre la menace et de fermer l'incident de sécurité.

Information associée

Ajouter une tâche personnalisée au playbook

Résolution des attaques de hameçonnage signalées par les utilisateurs avec le playbook

Le manuel Hameçonnage vous guide dans les tâches nécessaires à l'analyse et à la résolution d'une attaque d'hameçonnage signalée par l'un des employés de votre entreprise.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

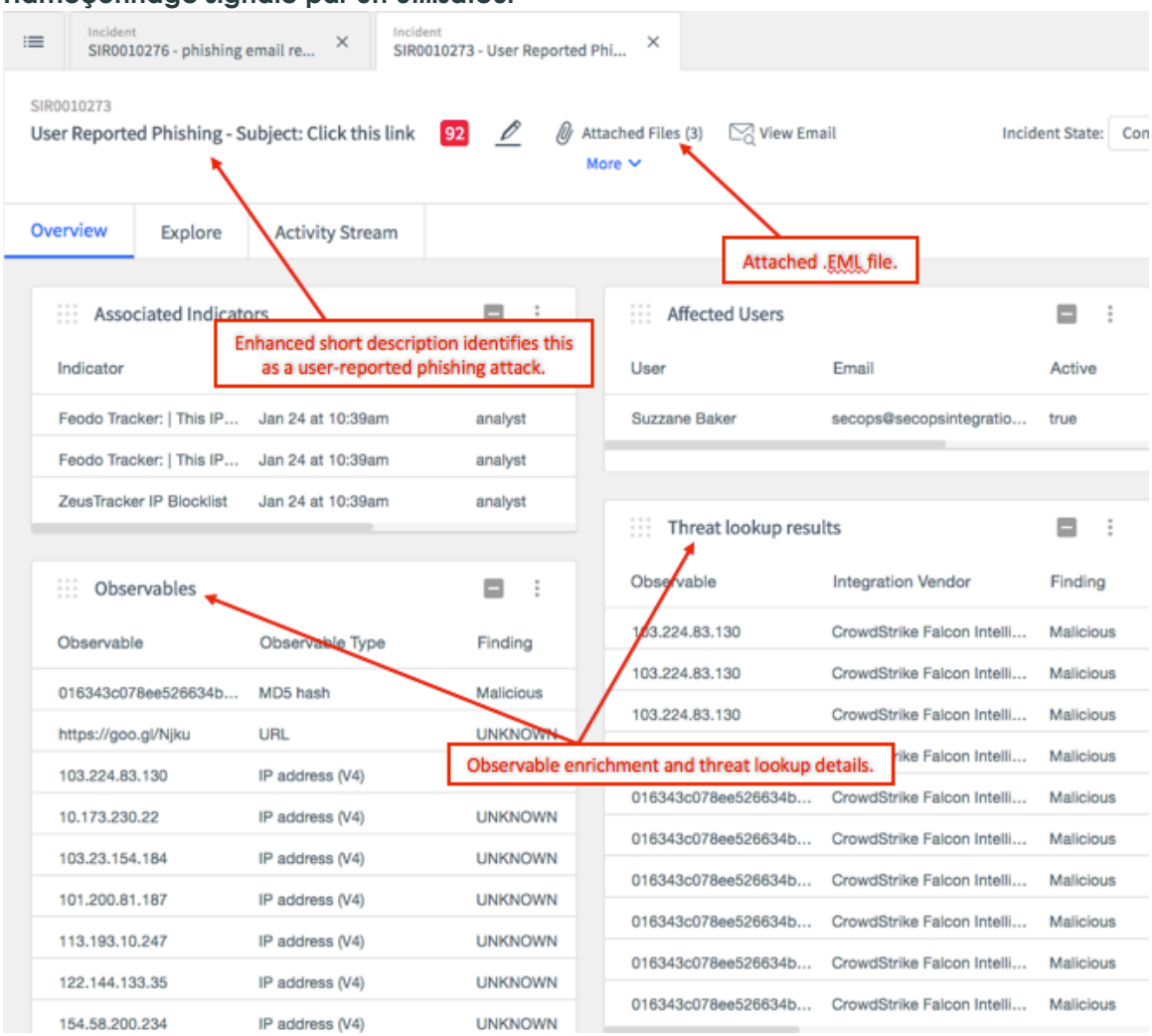
Comment les incidents de sécurité sont créés à partir d'attaques de phishing signalées par les utilisateurs

Lors de la configuration de Security Incident Response, votre administrateur système crée une série de règles de correspondance des e-mails qui peuvent identifier les e-mails contenant des signes d'attaque de phishing. Lorsque les employés reçoivent un e-mail suspect contenant les signes courants d'une attaque par hameçonnage (tels que définis par vos politiques de sécurité), ils peuvent l'envoyer en tant que fichier . Pièce jointe EML à l'adresse e-mail d'hameçonnage définie par votre organisation.

Lorsque l'e-mail est reçu à l'adresse e-mail d'hameçonnage, le fichier . La pièce jointe EML est analysée et ses informations sont comparées aux règles de correspondance des e-mails. Si une correspondance est trouvée, un incident de sécurité contenant les informations suivantes est créé :

- La brève description inclut le hameçonnage signalé par l'utilisateur, suivi de l'objet réel de l'e-mail d'origine.
- Le. Le fichier EML est joint à l'incident de sécurité.
- Si l'extension . EML contient tous les observables, ils sont analysés et l'enrichissement et les recherches de menaces sont automatiquement effectués.

Hameçonnage signalé par un utilisateur

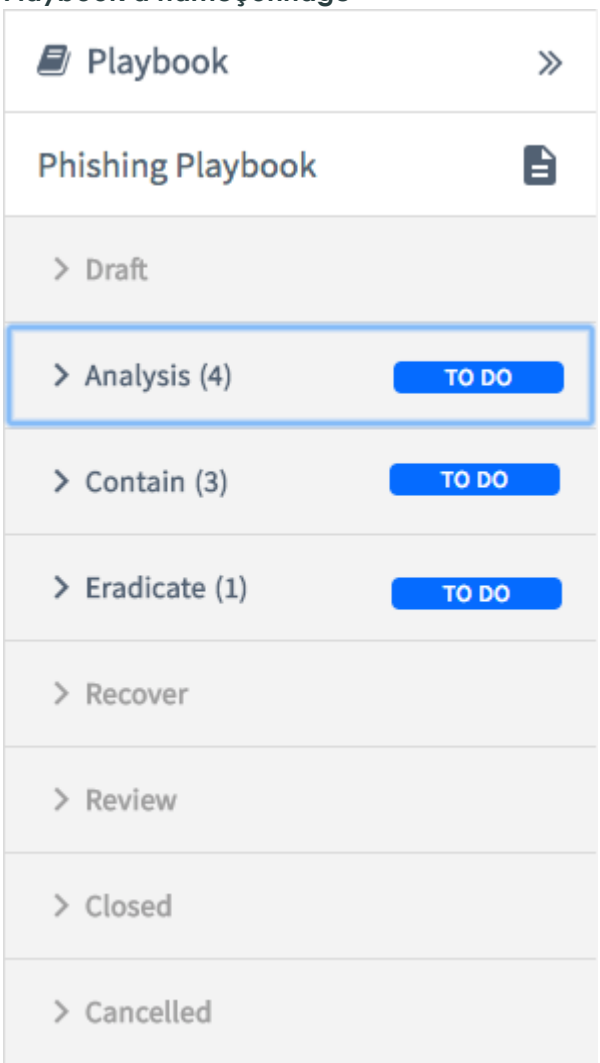


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsqu'un incident de sécurité de catégorie Hameçonnage est ouvert, le Playbook Hameçonnage est automatiquement disponible. Cliquez simplement sur l'icône du playbook ( ) pour ouvrir le playbook.

Playbook d'hameçonnage



Le playbook Hameçonnage contient des tâches pour vous aider à analyser, contenir et éradiquer une menace de hameçonnage. Les tâches sont organisées en états (par exemple, **Analyse**, **Contenir**, etc.). Lorsque toutes les tâches d'un état ont été terminées, le playbook vous guide vers l'état suivant.

Analyse des détails de l'incident de sécurité

Lorsque l'incident de sécurité est à l'état Analyse, vous recevez des tâches pour enquêter de base sur l'incident, notamment :

- Détermination de la validité de l'incident.
- Étudier l'impact de la menace potentielle.
- Coordonner une réponse efficace à l'incident.

Au fur et à mesure que vous effectuez les tâches :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Familiarisez-vous avec les articles de la base de connaissances.
- Ouvrez la pièce jointe de l'e-mail et examinez-la à la recherche de signes d'éléments d'hameçonnage courants.
- Examinez les résultats de la recherche de menaces.

Contenir l'incident de sécurité

Lorsque l'incident de sécurité est à l'état **Contenir** , vous êtes chargé d'examiner les détails de l'e-mail. Pour vous assurer que les menaces ne peuvent pas pénétrer dans votre organisation, mettez à jour les défenses de votre réseau, sous la forme de signatures et de règles des systèmes de défense contre les intrusions (IDS) et de systèmes de prévention des intrusions (IPS).

Au fur et à mesure que vous effectuez les tâches :

- Prenez des mesures pour limiter les impacts des menaces, telles que l'isolement des appareils impactés.
- Examinez les observables joints à l'e-mail.
- Déterminez si des contenus d'e-mail sont associés à une menace connue, notamment :
  - URL
  - Expéditeur d'e-mail
  - URL de hameçonnage
  - Adresse IP du serveur SMTP de l'expéditeur

Éradiquer le logiciel malveillant

Une fois que vous avez déployé des signatures et des règles mises à jour dans votre solution antivirus, utilisez les tâches à l'état **Éradiquer** pour déterminer si un programme malveillant est présent et traitez-le en conséquence.

Au fur et à mesure que vous accomplissez les tâches :

- Analysez les points de terminaison des appareils affectés pour détecter la présence de logiciels malveillants.
- Supprimez tous les logiciels malveillants détectés.
- En dernier recours, effacez et recréez l'image des appareils hôtes.

Examen de l'incident de sécurité

Si vous avez déterminé qu'une attaque de hameçonnage était une fausse alerte lors de l'exécution des tâches d'analyse, l'incident de sécurité passe à l'état **Examiner** et vous devez en informer vos utilisateurs afin qu'ils sachent qu'ils peuvent ouvrir la pièce jointe de l'e-mail en toute sécurité.

Clôture de l'incident de sécurité

Lorsque toutes les tâches du playbook ont été terminées, l'incident de sécurité passe à l'état **Fermé** . Vous devez saisir des commentaires de fermeture pour pouvoir fermer l'incident.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Annulation d'un incident de sécurité

Lorsqu'un incident de sécurité est à l'état **Examiner** et que vous avez informé vos utilisateurs que l'e-mail n'est pas une menace, l'état **Annulé** devient actif et vous pouvez annuler l'incident de sécurité.

Remarque : La tâche Récupérer n'est pas utilisée dans le playbook Hameçonnage.

Associer un article de la base de connaissances à une tâche Playbook

Lorsque vous analysez les menaces de sécurité à l'aide du Réponse aux incidents de sécurité playbook, vous pouvez afficher les articles de la base de connaissances pour chaque tâche si définie par votre organisation. Si les articles de la base de connaissances ne sont pas présents, vous pouvez les créer et les associer à des tâches de playbook.

Avant de commencer

Lorsque vous utilisez le playbook dans Réponse aux incidents de sécurité, notez le texte associé à chaque tâche. Par exemple, la première tâche de la catégorie Hameçonnage est **L'alerte a-t-elle été envoyée par l'employé ?** Il s'agit de la brève description de la tâche. Vous avez besoin de ce texte (exactement tel qu'il apparaît dans le playbook) pour associer un article de la base de connaissances à la tâche.

Rôle requis : sn_sir.knowledge_admin et sn_si.admin ou admin

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Catalogue et base de connaissances** > **Base de connaissances**.
2. Créez et publiez un article de la base de connaissances pour une tâche Playbook spécifique.
3. Accédez à la **Incident de sécurité** > **Runbook manuel** > **Créer un nouveau Runbook**.
4. Créez un runbook en renseignant les informations suivantes :

Champ	Description
Article de la base de connaissances	Sélectionnez l'article de la base de connaissances publié que vous souhaitez associer à la tâche Playbook.
Table	Sélectionnez Réponse aux incidents de sécurité la tâche [sn_si_task].
Condition	Définissez le générateur de conditions sur : ◦ **Option:** Sélectionnez **Brève description**. ◦ **Opérateur:**Sélectionnez **est**. ◦ **Valeur d'entrée :** Saisissez la brève description de la tâche, exactement telle qu'elle apparaît dans le playbook.

5. Cliquez sur **Envoyer**.
   La prochaine fois que vous exécuterez le playbook et sélectionnerez cette tâche, l'article de la base de connaissances associé s'affichera.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

- Créer un article de la base de connaissances sur les incidents de sécurité
- Créer un Runbook Security Incident Response

Ajouter une tâche personnalisée au playbook

Le Security Analyst Workspace système de base comprend une série de tâches pour chaque catégorie de menace. Vous pouvez créer des tâches personnalisées qui répondent aux besoins uniques de votre système ou de vos clients.

Avant de commencer

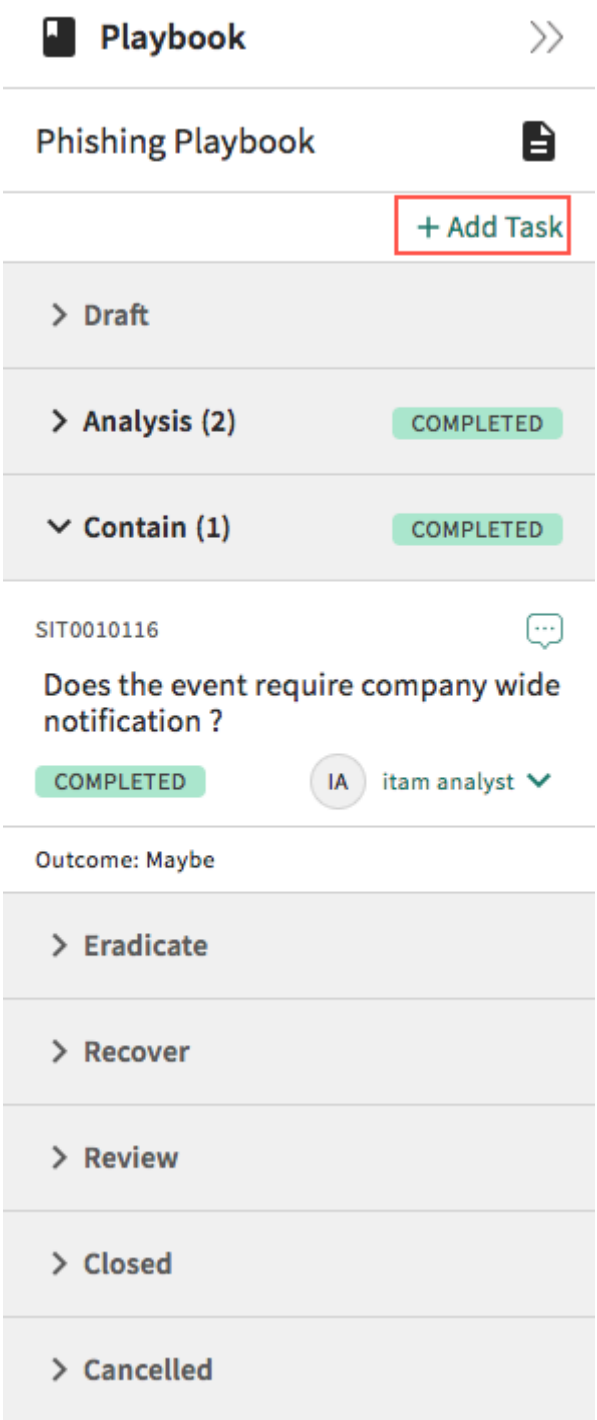
Rôle requis : sn_si.basic ou security_admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

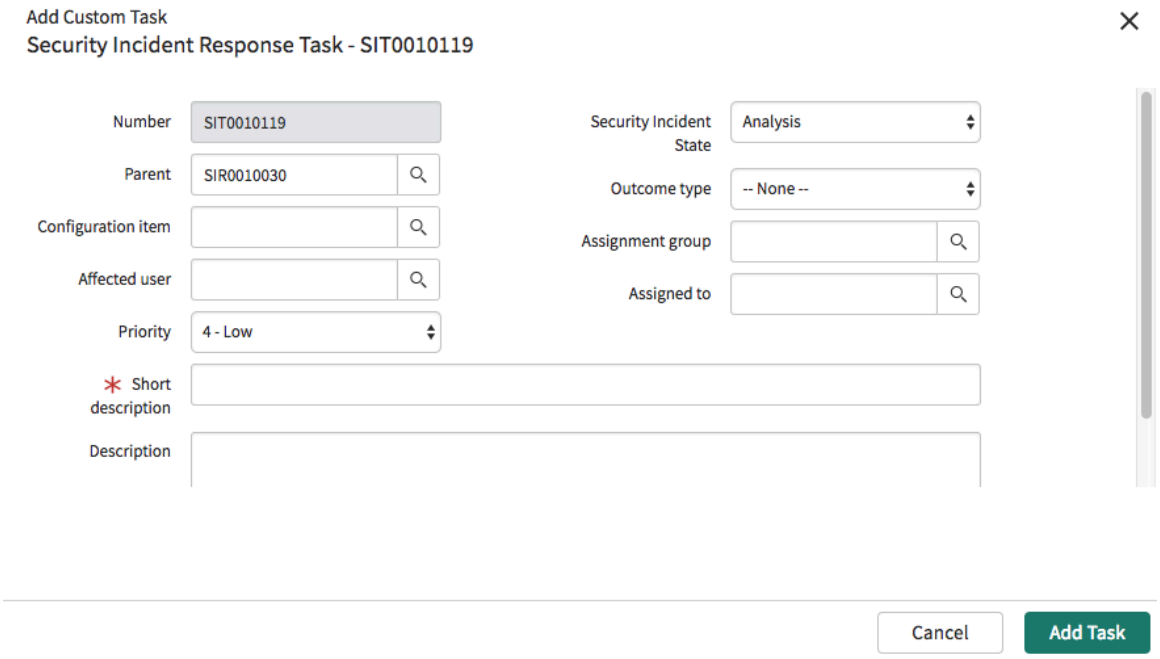
1. Une fois le playbook ouvert, cliquez sur **Ajouter une tâche**.



L'écran Ajouter une tâche personnalisée s'ouvre.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Renseignez les champs nécessaires.

Champ	Description
Numéro	[Lecture seule] Numéro de tâche d'incident de sécurité généré automatiquement.
Parent	Numéro de l'incident de sécurité associé.
Élément de configuration	Élément de configuration affecté par le problème de sécurité, le cas échéant.
Utilisateur affecté	Utilisateur affecté par le problème de sécurité, le cas échéant.
Priorité	Sélectionnez la priorité utilisée pour déterminer quand cette tâche doit être effectuée.
État de l'incident de sécurité	État actuel de la tâche de réponse de sécurité. Vous pouvez sélectionner un état futur, si nécessaire.
Type de résultat	Si vous disposez du rôle sn_si.basic, sélectionnez **Oui/Non** comme type de résultat. Si vous disposez du rôle security_admin, vous pouvez créer un type de résultat personnalisé avec plusieurs valeurs de sortie personnalisées. Par exemple, vous pouvez définir une tâche avec des valeurs dépendantes en fonction de la catégorie de menace. Pour plus d'informations, consultez Listes de choix
Groupe d'affectation	Groupe d'affectation à partir duquel l'agent affecté sera sélectionné.
Affecté à	Personne affectée à l'exécution de la tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description brève	Description de la tâche du playbook d'incident de sécurité.
Description	Entrez une description pour la tâche sélectionnée.

3. Lorsque vous avez terminé vos entrées, cliquez sur **Ajouter une tâche**.
   La tâche est insérée dans le playbook après la tâche actuelle.

Recherches de perception sur les attaques de hameçonnage et de programme malveillant signalées par les utilisateurs

Effectuez des recherches de perceptions sur les e-mails ou les observables pour déterminer la fréquence à laquelle certains types d'attaques, telles que les attaques de hameçonnage ou les communications avec une adresse IP ou une URL malveillante, se produisent dans votre réseau. Chaque occurrence est considérée comme une observation. Les recherches de perceptions pour les observables doivent être configurées pour vos magasins de journaux ou Gestion des informations et des événements et de sécurité (SIEM).

Comment utiliser la fonctionnalité de recherche de perception pour localiser les utilisateurs victimes d'hameçonnage et suivre les observables d'hameçonnage et de programmes malveillants dans le magasin de journaux de votre réseau.

Regardez cette vidéo de trois minutes pour apprendre à utiliser la fonctionnalité de recherche de perception afin de localiser les utilisateurs victimes d'hameçonnage et de suivre les observables liés au hameçonnage et aux programmes malveillants dans le magasin de journaux de votre réseau.

Les termes suivants sont utilisés pour décrire les attaques de hameçonnage signalées par les utilisateurs :

- Utilisateur victime d'hameçonnage : utilisateur qui a reçu un e-mail d'hameçonnage.
- Utilisateur victime : utilisateur qui a interagi avec l'URL d'hameçonnage, généralement en cliquant sur un lien contenu dans l'e-mail d'hameçonnage. Cette action expose potentiellement les informations d'identification à l'attaquant.

Lorsque vous commencez à analyser un incident de hameçonnage, vous pouvez effectuer une recherche de perceptions d'e-mails ou unerecherche de perceptions d'observables pour identifier d'autres utilisateurs de votre organisation qui sont touchés par la même attaque de hameçonnage. Effectuez une recherche dans vos magasins de journaux pour identifier les utilisateurs victimes d'hameçonnage et les victimes. Une fois que vous avez identifié la liste des utilisateurs affectés, créez des incidents de sécurité enfants pour exécuter des procédures complètes de réponse aux incidents à l'aide des outils disponibles dans Réponse aux incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez également utiliser l'approche suivante pour effectuer une recherche de perceptions :

- Accédez à la **Incidents de sécurité** > **Afficher les incidents** et cliquez sur un incident de sécurité.
- Cliquez sur **Afficher IoC** sous Liens connexes. Une liste d'observables s'affiche.
- Sélectionnez un observable dans la liste, puis dans la liste **Actions** , sélectionnez l'une des options suivantes :
  - Exécuter la recherche de perception du trafic web
  - Exécuter la recherche de perception du trafic des e-mails
- Spécifiez le délai et cliquez sur **Rechercher** pour effectuer une recherche d'observations.

Configurations de recherche de perceptions enregistrées

Configurez les recherches de perception et créez des configurations enregistrées pour les SIEM ou d'autres magasins de journaux pour les instances d'observables afin de déterminer la présence d'observables malveillants dans votre environnement.

Remarque : Les recherches enregistrées et les requêtes sur place ne sont prises en charge que pour Splunk Integration.

Information associée

Créer des enregistrements de configuration de recherche d'observations

Effectuer une recherche de perceptions des e-mails pour les attaques de hameçonnage signalées par les utilisateurs

Recherchez les utilisateurs qui ont reçu des e-mails d'hameçonnage en fonction d'observables tels que l'objet de l'e-mail, le nom de l'expéditeur ou l'ID du message. Vous pouvez ensuite contenir et supprimer ces e-mails d'hameçonnage de votre organisation.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Effectuez une recherche dans les journaux de trafic de messagerie Splunk pour recueillir la liste des destinataires d'un e-mail suspect. La recherche peut être effectuée à l'aide de l'expéditeur de l'e-mail, de l'ID de l'e-mail ou de l'objet de l'e-mail associé à un incident de sécurité comme critères.

Remarque :

- Cette implémentation de la recherche de perception pour les observables basés sur l'e-mail a été testée uniquement avec le magasin de journaux Splunk Enterprise.
- Les événements du journal Splunk doivent être conformes au modèle d'information commun (CIM) pour que la requête de recherche de perceptions renvoie des résultats précis.

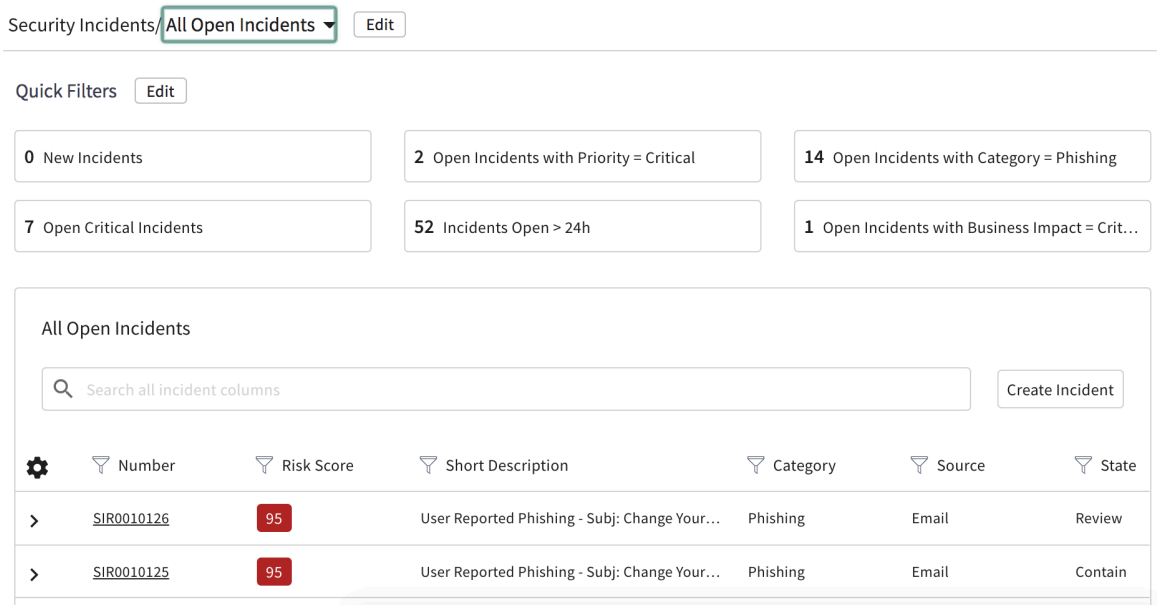
Procédure

1. Pour afficher les incidents de sécurité affectés à votre équipe, accédez à **Incident de sécurité** > **Incidents (nouvelle UI)**.
2. Dans la liste **Incidents de sécurité** , sélectionnez l'un des filtres, tels que tous les **incidents ouverts**, **tous les incidents qui vous sont affectés** ou **tous les incidents**.

Traduction automatique

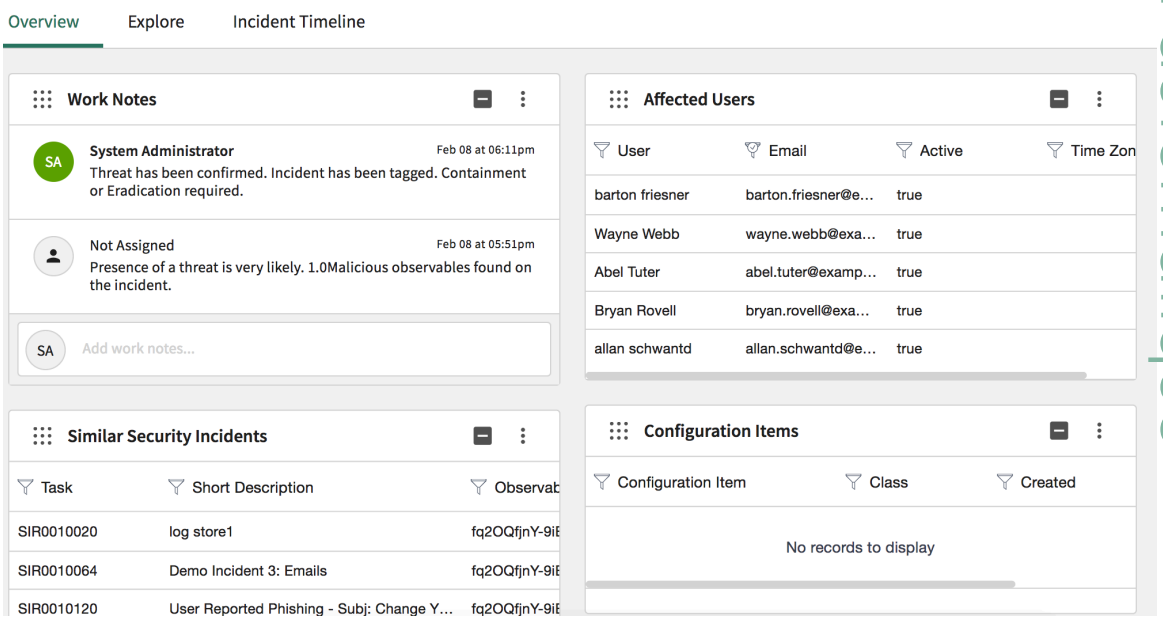
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour afficher les incidents de sécurité d'un type particulier, tels que les incidents critiques ou les e-mails d'hameçonnage, cliquez sur l'un des **filtres rapides**.



3. Cliquez sur l'incident de sécurité que vous souhaitez analyser.

L'onglet Vue d'ensemble fournit une vue d'ensemble de l'incident de sécurité, y compris une liste des observables, des utilisateurs affectés et des incidents de sécurité similaires.

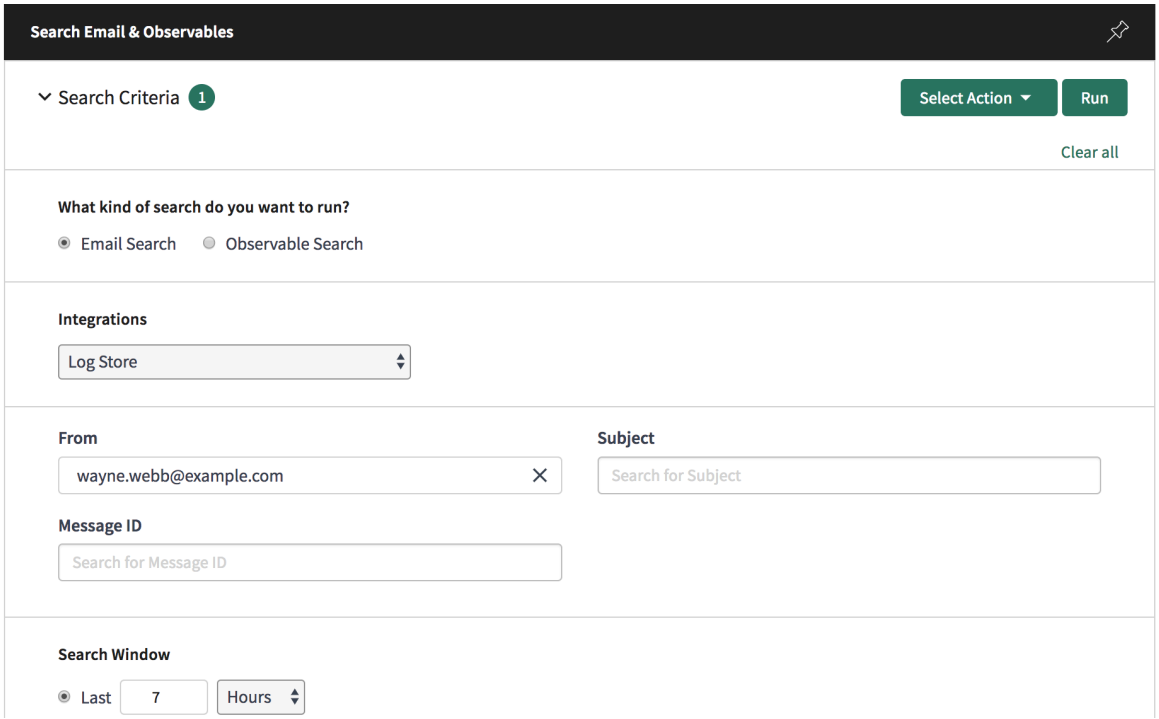


4. Cliquez sur l'onglet **Explorer** .

5. Sous **Données d'incident**, accédez à **Examen** > **Rechercher un e-mail et des observables**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Développez la section Critères de recherche.
7. Sélectionnez **Recherche d'e-mail** comme type de recherche que vous souhaitez exécuter, puis spécifiez le reste des critères de recherche.

Formulaire Critères de recherche

Champ	Description
Intégrations	Type d'intégrations. Sélectionnez **Log Store** dans la liste. **Remarque :** Cette fonctionnalité n'est prise en charge qu'avec le magasin de journaux Splunk.
De	Adresse e-mail complète de l'expéditeur (par exemple, jane.doe@example.com).
ID de message	ID de message électronique du magasin de journaux.
Objet	Objet de l'e-mail d'hameçonnage.
Fenêtre de recherche	Fenêtre de temps pour la recherche (par exemple, les dernières 24 heures).

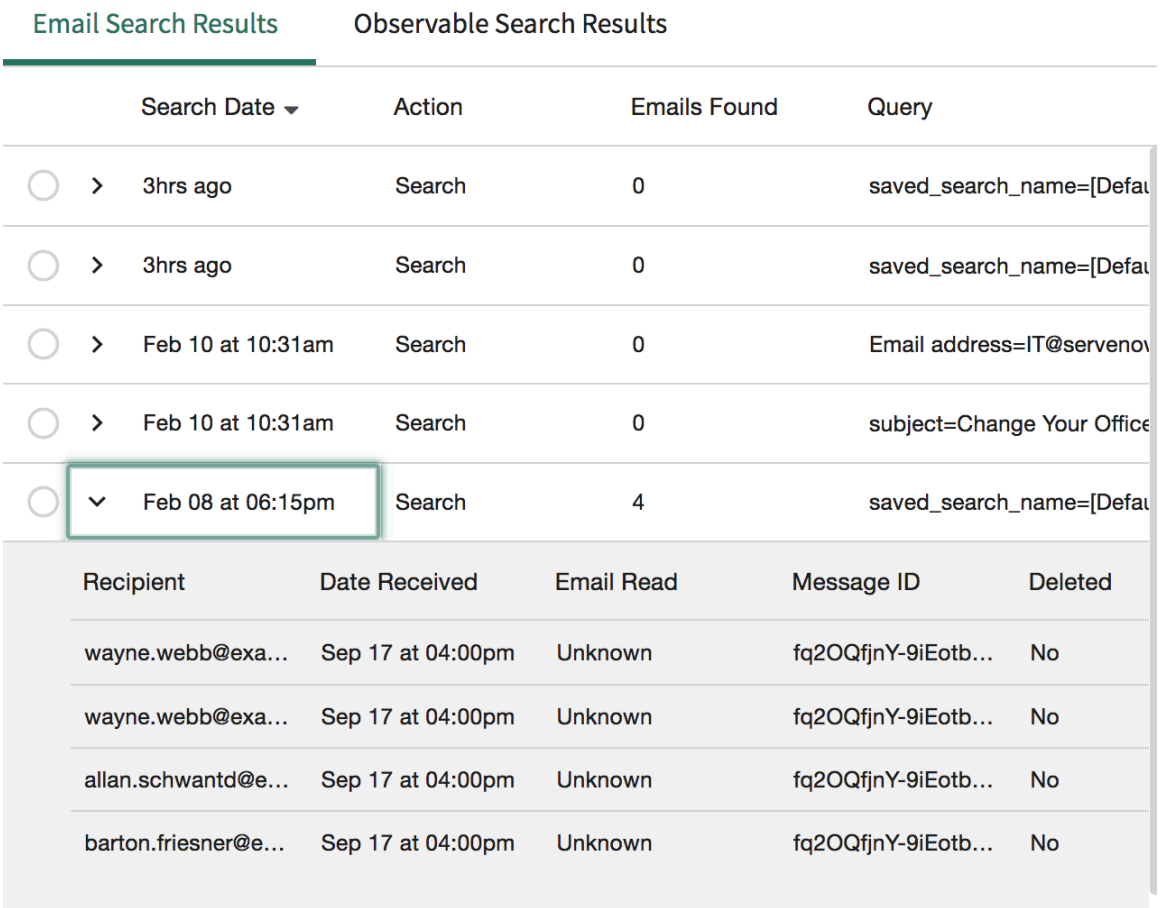
8. Dans la liste **Sélectionner une action** , sélectionnez **Rechercher** , puis cliquez sur **Exécuter**.

   La recherche s'effectue dans le magasin de journaux Splunk à l'aide des critères que vous entrez, et les utilisateurs ciblés par l'attaque de phishing sont affichés dans l'onglet **Résultats de recherche d'e-mails** . Le nombre total d'e-mails d'hameçonnage et les détails de chaque e-mail, y compris la date de réception de l'e-mail, le destinataire et l'ID du message, sont affichés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Pour afficher la liste des utilisateurs ayant reçu l'e-mail d'hameçonnage, cliquez sur le symbole **>** dans la colonne Date de recherche.



10. Pour afficher la liste des utilisateurs ayant reçu l'e-mail, accédez à **Utilisateurs** > **Utilisateurs affectés**.

    La colonne Utilisateur victime d'hameçonnage identifie les destinataires de l'e-mail.

    Remarque : La page Utilisateurs affectés affiche uniquement les enregistrements utilisateur présents sur l'instance ServiceNow.

11. Pour enquêter plus en détail sur les utilisateurs qui sont la cible de l'attaque de phishing, procédez comme suit :

    a. Cochez les cases en regard des noms d'utilisateur.

    b. Dans la liste, sélectionnez **Créer un incident de sécurité enfant**, puis cliquez sur **Exécuter**. Un message s'affiche pour indiquer qu'un incident de sécurité enfant a été créé. Pour afficher les incidents de sécurité enfants associés à un incident parent, cliquez sur l'onglet **Explorer** et accédez à **Incidents** > **Incidents de sécurité enfants**.

Résultats
La liste des utilisateurs victimes d'hameçonnage s'affiche.

Effectuer une recherche de perceptions observables pour les attaques de hameçonnage et de programme malveillant signalées par les utilisateurs

Effectuez des recherches de perception sur les observables pour savoir combien d'utilisateurs ont visité un site Web malveillant ou suspect au cours d'une période spécifique.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Vous pouvez effectuer une recherche de trafic réseau sur des observables tels que l'URL, l'hôte de destination ou l'adresse IP de destination associée à un incident de sécurité.

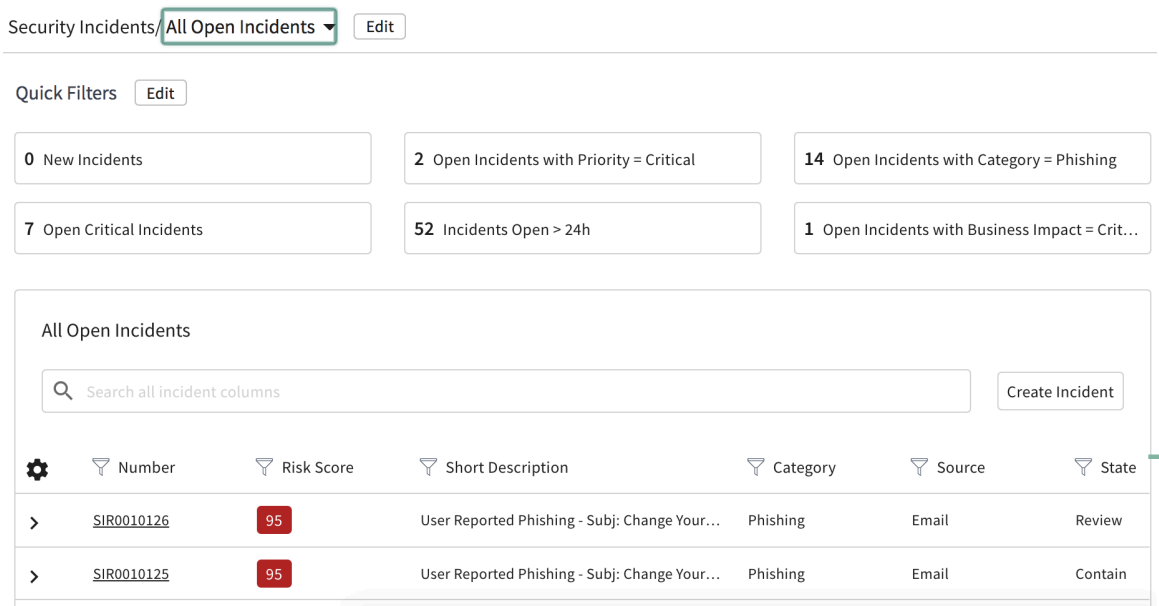
Remarque :

- Cette implémentation de la recherche de perceptions pour les observables a été testée uniquement avec le magasin de journaux Splunk Enterprise.
- Les événements du journal Splunk doivent être conformes au modèle d'information commun (CIM) pour que la requête de recherche de perceptions renvoie des résultats précis.

Procédure

1. Pour afficher les incidents de sécurité qui sont affectés à votre équipe, accédez à **Incident de sécurité** > **Incidents (nouvelle UI)**.
2. Dans la liste **Incidents de sécurité** , sélectionnez un autre filtre, comme Tous les **incidents qui me sont affectés**, **Tous les incidents ouverts** ou **Tous les incidents**.

   Pour afficher les incidents de sécurité d'un type particulier, tels que les incidents critiques ou les e-mails d'hameçonnage, cliquez sur l'un des **filtres rapides**.

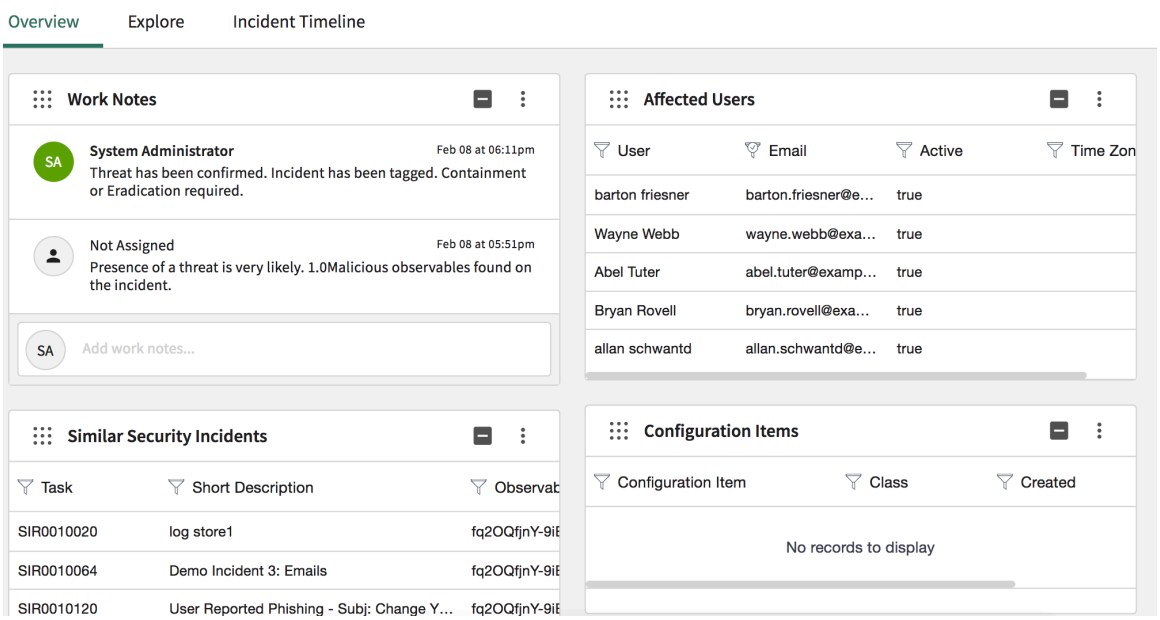


3. Cliquez sur l'incident de sécurité que vous souhaitez analyser.

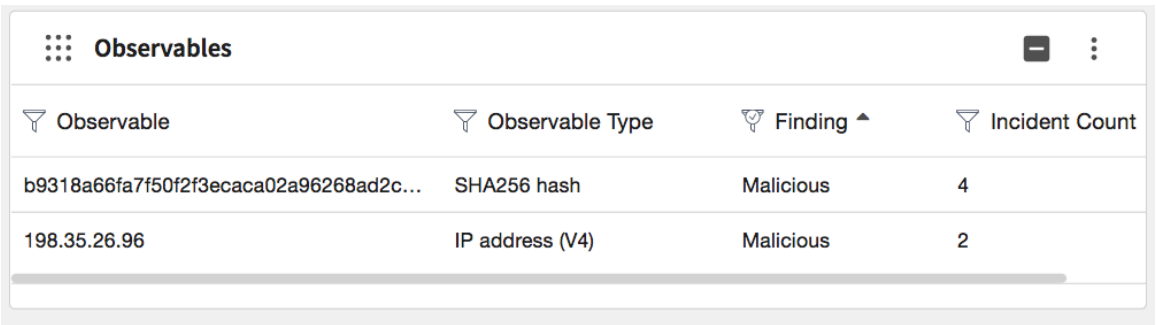
   Vous pouvez afficher une vue d'ensemble de l'incident de sécurité, y compris une liste des observables, des utilisateurs affectés et des incidents de sécurité similaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



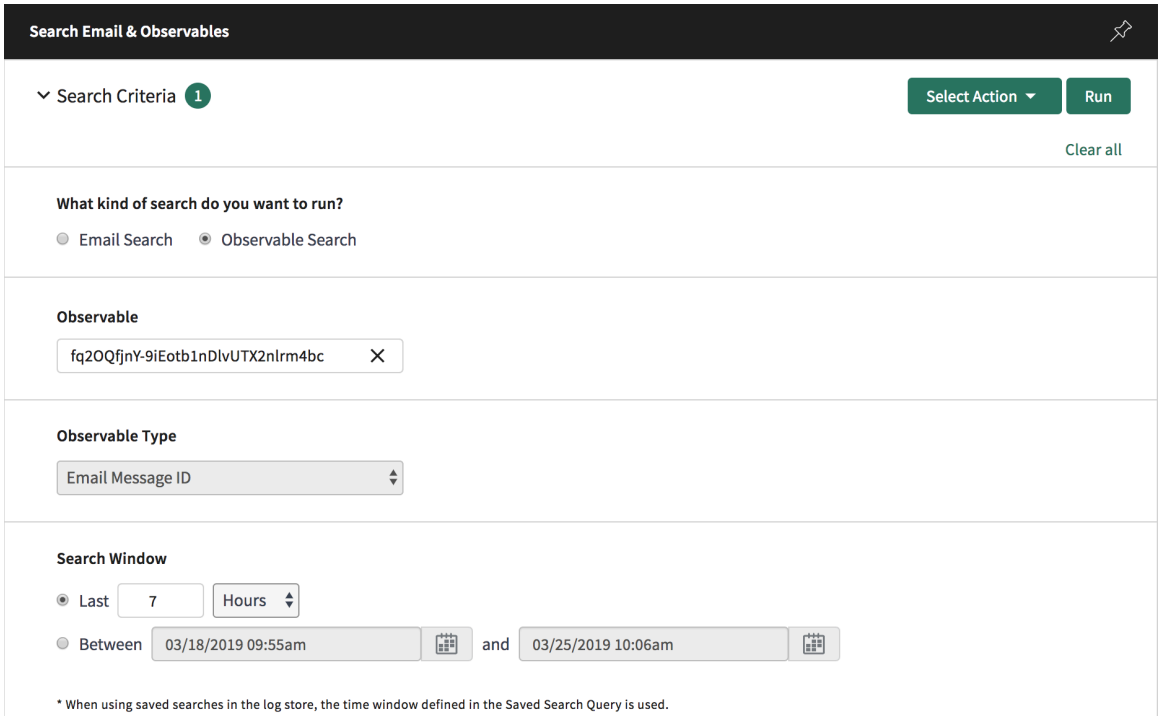
Dans la section Observables, notez que la colonne Observable affiche l'adresse e-mail, l'objet et l'URL. Notez également que la colonne Résultat indique que l'URL a été automatiquement analysée lors de l'envoi de l'e-mail d'hameçonnage et qu'il a été déterminé qu'il s'agit d'une URL malveillante connue. La colonne Nombre d'incidents affiche les autres incidents qui partagent le même observable. Ces artefacts indiquent que vous êtes probablement prêt à passer aux procédures de maîtrise de cette attaque de hameçonnage, notamment en déterminant combien d'utilisateurs de l'organisation ont été affectés.



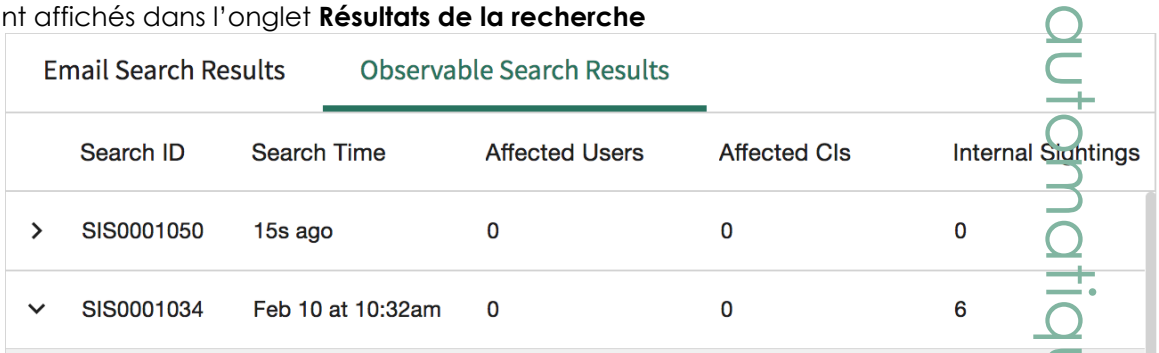
4. Accédez à la **Explorer** > **Examen** > **Rechercher un e-mail et des observables**.
5. Développez la section Search Criteria (Critères de recherche) et cliquez sur **Observable Search (Recherche d'observables)**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Entrez l'observable que vous recherchez et une fenêtre de temps pour la recherche (par exemple, 24 dernières heures).
7. Dans la liste **Sélectionner une action** , sélectionnez **Rechercher**.
   La recherche s'effectue dans le magasin de journaux Splunk à l'aide des critères que vous avez saisis et les utilisateurs clés ciblés par l'attaque malveillante sont affichés dans l'onglet **Résultats de la recherche d'observables** .



8. Pour afficher les utilisateurs qui ont reçu l'e-mail, accédez à **Utilisateurs** > **Utilisateurs affectés**.

   La colonne Utilisateur victime d'hameçonnage identifie les destinataires de l'e-mail d'hameçonnage et la colonne Interaction de l'utilisateur identifie les utilisateurs qui ont cliqué sur une URL d'hameçonnage ou interagi avec une adresse e-mail suspecte. La colonne Interaction de l'utilisateur est définie sur vrai ou faux, selon que l'utilisateur a cliqué sur le lien malveillant ou sur l'adresse IP.

   Remarque : La page Utilisateurs affectés affiche uniquement les enregistrements utilisateur présents sur l'instance ServiceNow.

9. Pour enquêter plus en détail sur les utilisateurs qui ont cliqué sur l'e-mail d'hameçonnage et potentiellement compromis leurs informations d'identification :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans les colonnes Utilisateur victime d'hameçonnage et Interaction de l'utilisateur, cochez les cases en regard des noms d'utilisateur qui affichent **vrai**.

b. Cliquez sur **Créer un incident de sécurité enfant** , puis sur **Exécuter**.
Un message s'affiche pour indiquer qu'un incident de sécurité enfant a été créé. Pour afficher les incidents de sécurité enfants associés à un incident parent, cliquez sur l'onglet **Explorer** et accédez à **Incidents** > **Incidents de sécurité enfants**.

Résultats
La liste des utilisateurs victimes d'hameçonnage s'affiche.

Créer des enregistrements de configuration de recherche d'observations

Créez plusieurs enregistrements de configuration de recherche de perceptions et utilisez-les lors de l'interrogation de plusieurs magasins de journaux ou de la modification des paramètres de recherche.

Avant de commencer
Rôle requis : sn_si.admin

- Le module complémentaire CIM doit être installé sur l'instance Splunk.
- Les recherches enregistrées et les requêtes sur place ne sont prises en charge que pour Splunk Integration.

Pourquoi et quand exécuter cette tâche
Vous pouvez également créer des enregistrements de configuration de recherche de perceptions pour appeler des recherches enregistrées dans le magasin de journaux d'entreprise Splunk.

Remarque : Les requêtes de configuration de recherche s'appuient sur les données du journal Splunk pour être conformes au modèle d'information commun (CIM) Splunk.

Avec les configurations de recherche enregistrées, vous pouvez :

- Créez des recherches personnalisées qui combinent plusieurs enregistrements d'événements.
- Concevez des recherches efficaces et efficientes.
- Utiliser des entrées paramétrées dans la recherche enregistrée Splunk.

Le système de base inclut les exemples de configurations, comme illustré dans cette image :

Configurations de recherche enregistrées

		Name	Observable type	Search	Is saved search
		Search	Search	Search	Search
☐	ⓘ	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
☐	ⓘ	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
☐	ⓘ	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

La recherche enregistrée et les requêtes de configuration sur place sont des exemples de requêtes et peuvent être remplacées par des paramètres appropriés pour votre environnement. Créez des configurations de recherche enregistrées supplémentaires selon

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vos besoins. Lorsque vous définissez une configuration de recherche enregistrée, le nom et les paramètres de la requête de recherche doivent correspondre à la configuration enregistrée définie sur votre instance Splunk. Si le nom et les paramètres ne sont pas les mêmes, vous risquez de ne pas voir de résultats précis lorsque vous effectuez une recherche d'observations.

Remarque : Sur votre instance Splunk, accédez à la page Recherches, rapports et alertes et localisez votre requête de recherche enregistrée. Cliquez sur le lien **Autorisations** pour accéder à la page Autorisations. Sélectionnez la case d'option **Toutes les applications** et activez l'option **Autorisation de lecture** pour **Tout le monde**. Cela modifiera la valeur de la colonne Partage de Privé à Application pour votre requête de recherche enregistrée. Si cette option n'est pas définie, la requête de recherche enregistrée peut ne pas renvoyer de résultats.

Pour vérifier si la configuration de recherche enregistrée correspond à la configuration définie sur votre instance Splunk :

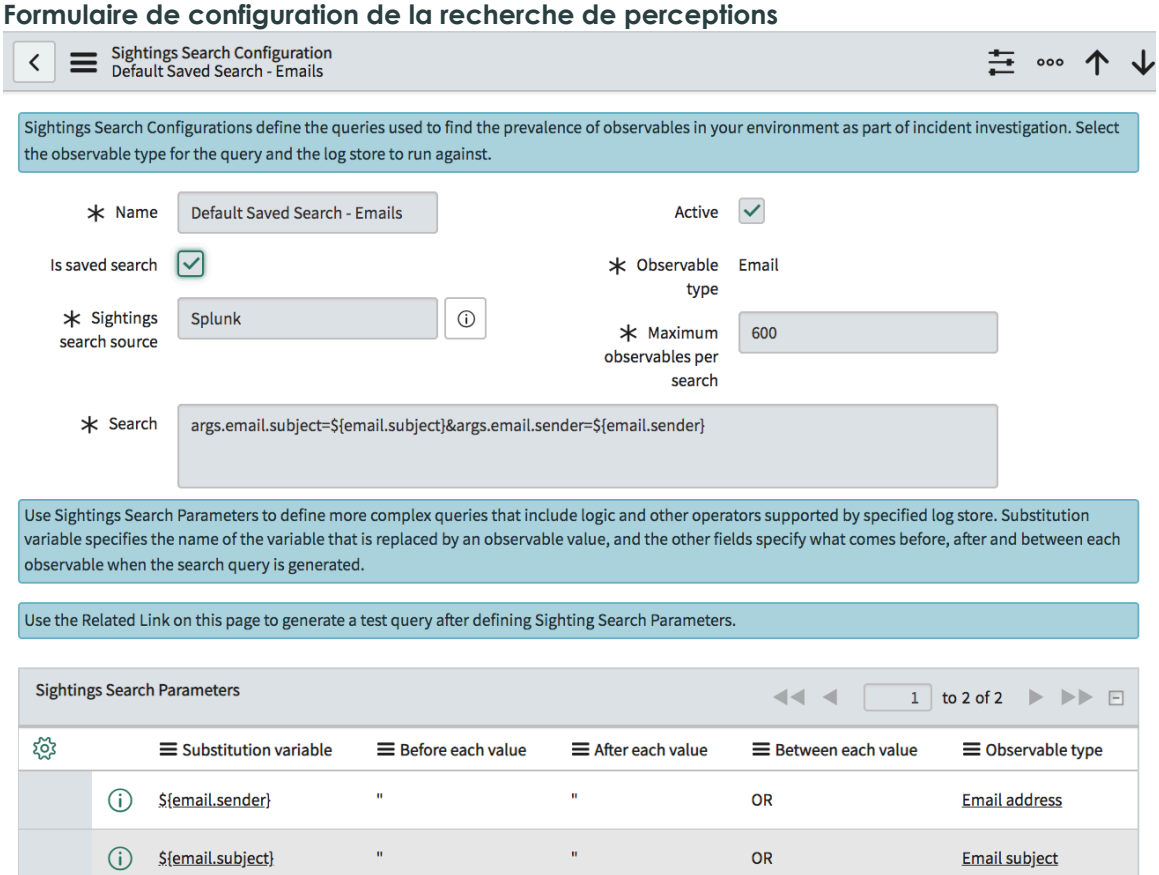
1. Accédez à la **Paramètres** > **Recherches, rapports et alertes**.
2. Définissez **tous lescontextes de l'application**.

   Une liste des rapports de recherche s'affiche.

3. Confirmez que la requête de recherche enregistrée figure dans la liste.

Par exemple, le formulaire de configuration de recherche de perceptions contient l'adresse e-mail et l'expéditeur d'e-mail comme paramètres de recherche :

Formulaire de configuration de la recherche de perceptions



Dans votre instance Splunk, définissez la recherche enregistrée avec le même nom, la recherche enregistrée par défaut : e-mails, et les mêmes paramètres de recherche pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'adresse e-mail et l'objet de l'e-mail. Si le nom et les paramètres de recherche ne sont pas les mêmes, la recherche de perceptions ne génère pas de résultat précis.

Procédure

1. Accédez à la **Security Operations** > **Intégrations** > **Configuration de la recherche de perceptions** et créez un nouvel enregistrement (voir la table des descriptions de champ).

Formulaire de configuration de la recherche de perceptions

Champ	Description
Nom	Nom de la configuration.
Est une recherche enregistrée	La configuration de recherche enregistrée est créée si vous sélectionnez cette option.
Source de recherche de perceptions	La source de la recherche d'observations. Sélectionnez le magasin de journaux Splunk comme source.
Actif	Option pour l'état de la recherche enregistrée. Seules les configurations de recherche actives peuvent être utilisées pour effectuer une recherche de perceptions.
Type d'observable	Le type d'observable peut être n'importe quel type d'observable tel qu'une adresse IP, une valeur de hachage, une URL, un nom de domaine, etc.
Nombre maximum d'observables par recherche	Nombre maximal d'observables à renvoyer à partir de la recherche.
Rechercher	La chaîne de recherche par défaut est `$(observable),` mais vous pouvez définir votre propre requête de recherche en spécifiant les paramètres pris en charge par le magasin de journaux Splunk.

2. Cliquez sur **Envoyer**.

Résultats
Vous avez créé un enregistrement de configuration de recherche de perceptions.

Que faire ensuite
Après avoir défini la requête de recherche, cliquez sur **Générer une requête de test de recherche de détections**, puis spécifiez une liste de valeurs observables pour générer une requête de test basée sur cette configuration de recherche enregistrée.

Ressources Playbook

Security Incident Response fournit un ensemble riche de ressources Playbook qui incluent une bibliothèque complète de playbooks, de flux secondaires et d'actions. Vous pouvez créer ou configurer des playbooks rapidement et facilement sans écrire de code compliqué. Vous pouvez utiliser ces playbooks pour résoudre les menaces de sécurité étape par étape.

Les ressources Playbook sont les suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux incidents de sécurité Playbooks	Actions du playbook Security Incident Response
Les playbooks fournis avec le système de base sont conçus pour accélérer le processus d'enquête sur les incidents de sécurité en automatisant les tâches complexes et banales. Les Playbooks sont hautement configurables et créés à l'aide de la technologie Flow Designer de ServiceNow. Pour le configurer, copiez le playbook fourni avec le système de base et modifiez-le à l'aide de l'interface graphique simple par glisser-déposer. Consultez Réponse aux incidents de sécurité Playbooks.	Les actions complexes qui sont essentielles à la création de playbooks sont disponibles en tant que **bibliothèques d'actions**. Ces bibliothèques d'actions permettent aux administrateurs de sécurité de créer des playbooks sans écrire de code complexe. Consultez Actions du playbook Security Incident Response.

Activer un Réponse aux incidents de sécurité flux

Les administrateurs de sécurité et les concepteurs de flux peuvent utiliser les Réponse aux incidents de sécurité flux pour automatiser le processus de résolution des incidents de sécurité au sein de l'organisation.

Avant de commencer

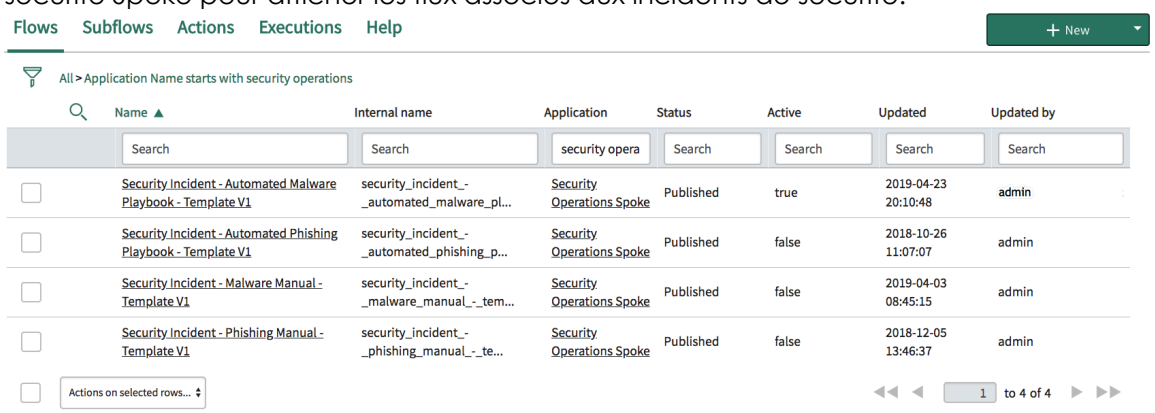
Rôle requis : sn_si.admin, action_designer et flow_designer

Pourquoi et quand exécuter cette tâche

Les flux fournis avec le système de base sont dans un état inactif. Activez ces flux avant de les utiliser.

Procédure

1. Téléchargez et installez l'application Opérations de sécurité Spoke.
   Cette application de spoke fournit des actions d'opérations de sécurité que vous pouvez utiliser lors de la définition Réponse aux incidents de sécurité des flux.
2. Accédez à la **Concepteur de flux** > **Concepteur** et recherchez l'application Opérations de sécurité Spoke pour afficher les flux associés aux incidents de sécurité.

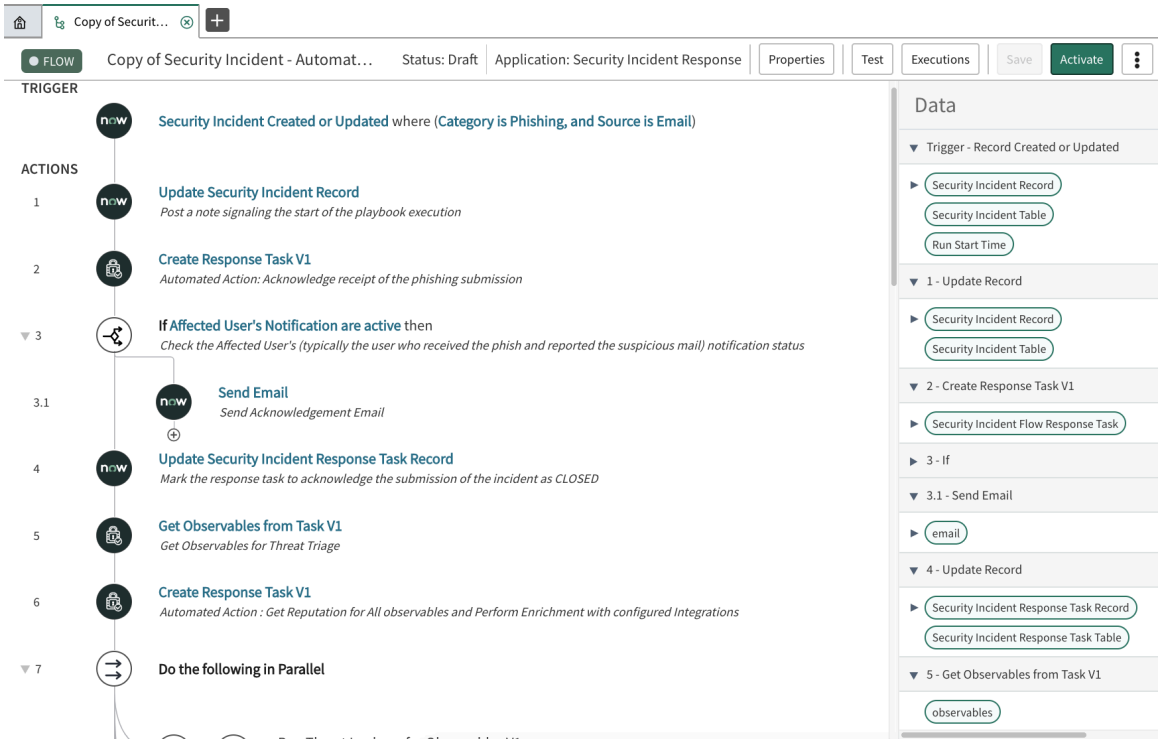


Notez que les flux ont un statut publié et sont inactifs.

3. Par exemple, si vous souhaitez activer le flux Playbook de programme malveillant automatisé, cliquez sur le lien **Incident de sécurité - Playbook d'hameçonnage automatisé - Modèle V1** pour afficher le flux.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Vous ne pouvez pas modifier les flux fournis avec le système de base car il s'agit de flux en lecture seule. Vous pouvez utiliser ces flux tels quels ou en faire une copie et les modifier selon vos besoins.

4. Cliquez sur **Activer** pour activer le flux.

Résultats

Le flux du playbook d'hameçonnage automatisé est actif et prêt à l'emploi.

Réponse aux incidents de sécurité Playbooks

Vous pouvez invoquer le flux du playbook d'incident de sécurité automatiquement ou manuellement.

Un Playbook n'est visible que si au moins un Playbook est associé à un incident de sécurité. Le composant Playbook fonctionne uniquement pour les processus créés par Concepteur d'automatisation de processus (PAD) et non pour les flux créés par Flow Designer. Pour les flux existants activés par Flow Designer, cela continuera de fonctionner et les activités continueront d'être restituées en tant que tâches de réponse.

Réponse aux incidents de sécurité prend en charge deux types de Playbooks :

- Playbooks basés sur les processus
- Playbooks basés sur le flux

Outre les playbooks répertoriés, il existe également des flux secondaires dans le spoke Security Operations qui peuvent être appelés à partir du playbook de flux. Les rançongiciels sont l'un de ces flux secondaires.

Activez ces flux avant de les utiliser. Pour plus d'informations, consultez Activer un flux Security Incident Response.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbooks basés sur les processus

Le composant playbook fonctionne uniquement pour les playbooks intégrés Studio de workflow et non pour les flux. Toutefois, les playbooks basés sur le flux existants continueront de fonctionner et les activités continueront d'être restituées en tant que tâches de réponse.

Réponse aux incidents de sécurité fournit les playbooks suivants avec le système de base.

Playbook pour l'hameçonnage manuel

Le playbook d'hameçonnage manuel fournit des conseils étape par étape à vos analystes sur la façon dont ils peuvent résoudre manuellement des types spécifiques de menaces de sécurité dans le cadre de vos activités d'hameçonnage.

Vue d'ensemble

Le modèle Playbook d'hameçonnage manuel est conçu pour effectuer manuellement les tâches de réponse d'hameçonnage et comprend une séquence d'actions qui inclut des conditions de déclenchement. Vous pouvez utiliser les modèles PAD pour effectuer les étapes du playbook de réponse d'hameçonnage et résoudre efficacement ces incidents.

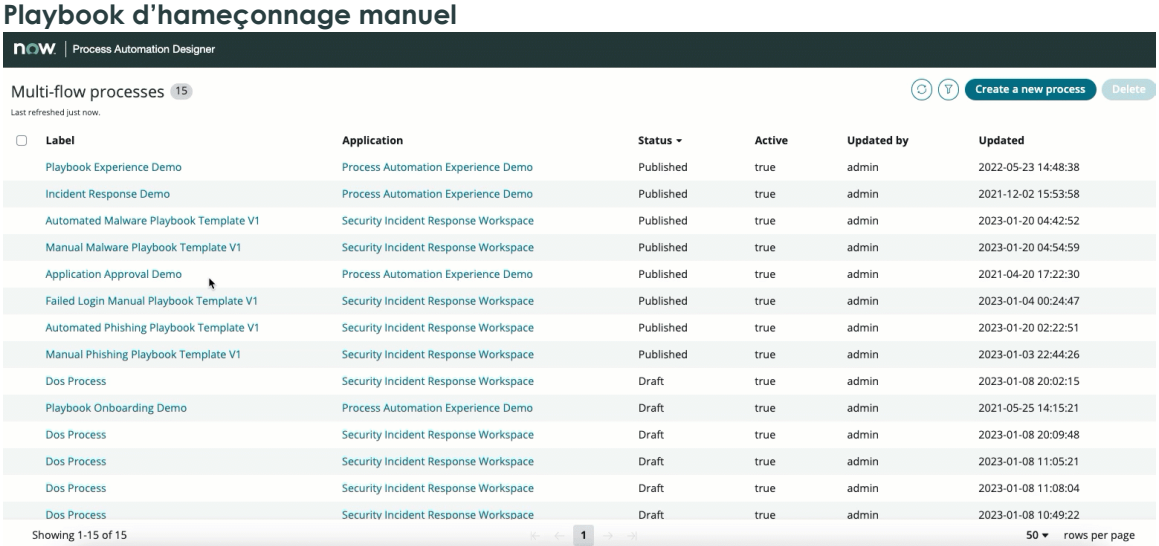
Ce playbook peut être utilisé si un incident de sécurité est créé ou mis à jour. Vous devez activer le playbook d'hameçonnage manuel sur Process Automation Designer (PAD), puis effectuer toutes les tâches, telles que l'analyse, le contenu, l'éradication et l'examen.

Les étapes suivantes constituent les étapes de la définition du processus et correspondent à l'état de l'incident de sécurité :

- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

Playbook d'hameçonnage manuel



Une fois que vous marquez une tâche comme terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche lorsque vous continuez à accomplir des tâches et des étapes. Un

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les informations que vous avez saisies à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des playbooks pour le hameçonnage manuel dans Studio de workflow

Suivez ces étapes pour créer des playbooks pour le hameçonnage manuel dans Studio de workflow.

Avant de commencer

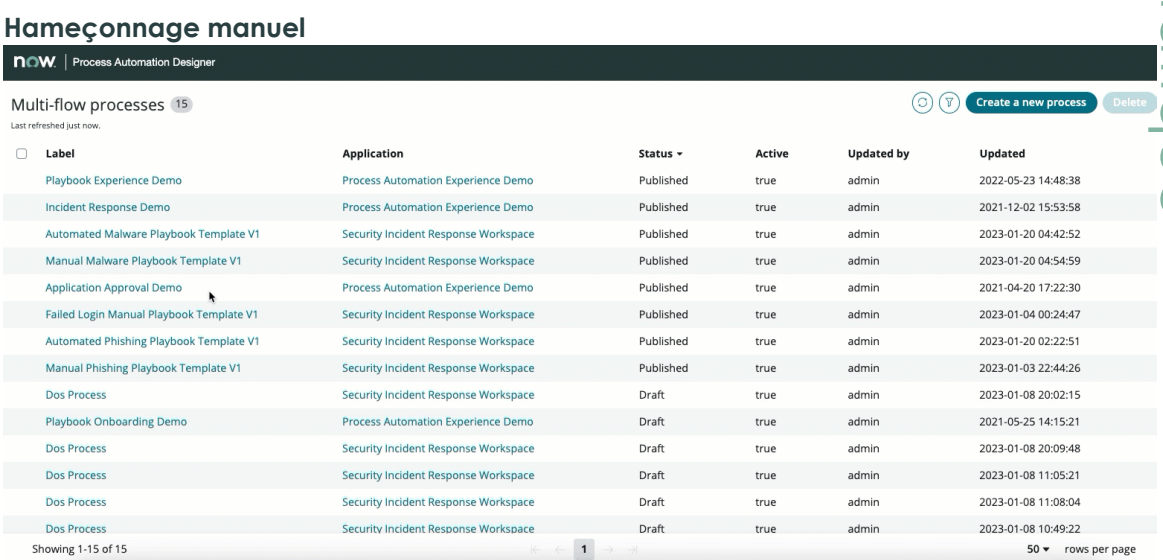
Rôle requis : sn_si.admin ou sn_si.manager

Procédure

1. Cliquer sur **Tout** > **Concepteur d'automatisation de processus** > > **Nouveau** et sélectionnez **Playbook**.

   Par exemple, Playbook d'hameçonnage manuel : modèle V1.

2. Entrez un nom pour le playbook, la description et l'application pour laquelle le playbook est en cours de création.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour l'exécution de votre processus**, puis sélectionnez la condition de déclenchement pour le moment où votre playbook doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions à définir à quel moment votre playbook doit s'exécuter en sélectionnant une table et en remplissant les conditions.
   Par exemple, la condition de déclenchement est la création d'un incident de sécurité de la catégorie Hameçonnage.



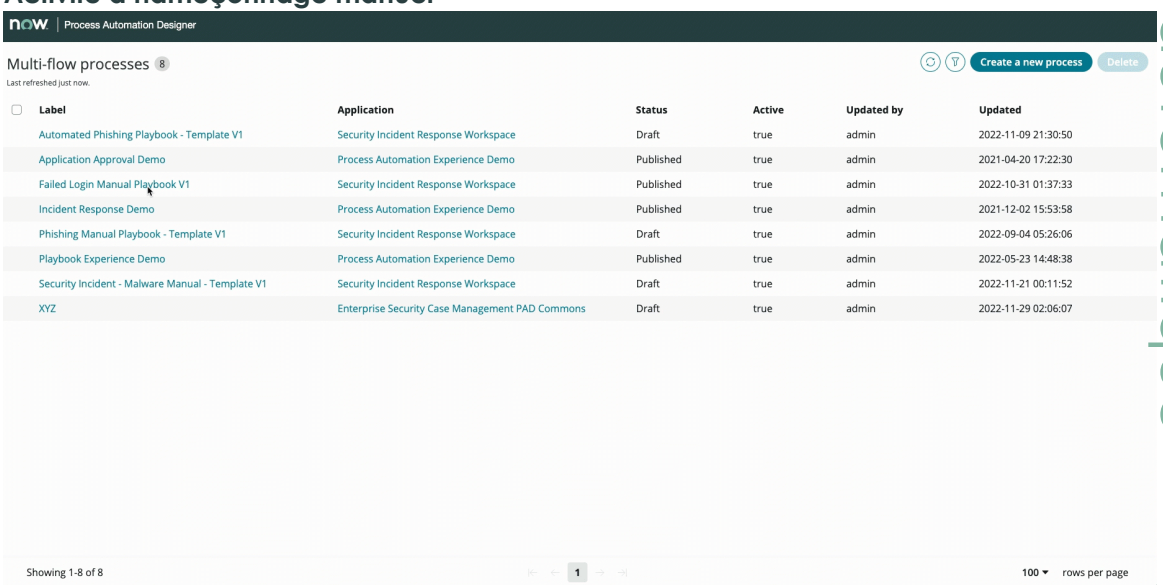
7. Cliquez sur **Accéder à Designer**.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Dans le volet des propriétés de l'étape, entrez les détails suivants : **nom**, **description**, **condition d'exécution** et **indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer** impliquent la date d'exécution de l'étape.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour les options Analyse, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a aucune condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité** sous une étape particulière (par exemple, Étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus à chaque étape.

Activité d'hameçonnage manuel



14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité à partir de la définition d'activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter des activités parallèles

Si le champ **Quand démarrer** est défini sur **Avec précédent**, des activités parallèles peuvent être lancées.

Pour passer d'une étape à l'étape suivante

Si aucune condition d'exécution n'est définie, les étapes et les activités sont exécutées séquentiellement.

Vous pouvez utiliser la condition d'exécution pour ignorer des activités ou des étapes. Dans cet exemple, **l'étape Contenir commence lorsque le résultat de « L'e-mail comporte-t-il des indicateurs de menace ? » est Oui**.

Pour passer d'une étape à une autre, vous pouvez utiliser la définition d'activité fournie par la plateforme **: Mettre à jour l'enregistrement**. Cela mettra à jour le champ État de l'incident de sécurité et reprendra l'exécution du playbook à l'étape suivante.

Toutefois, la difficulté avec cette définition d'activité est que, si, par exemple, le playbook est à l'étape d'analyse et si l'utilisateur a mis à jour manuellement l'état sur Dire réviser, l'activité Mettre à jour l'enregistrement changera à nouveau l'état en Maîtriser pour continuer l'exécution du playbook. Cela remplacera le changement manuel effectué.

Pour surmonter ce problème, dans le système de base, une définition d'activité appelée **Mettre à jour l'état de la tâche** est fournie. Cette activité ne remplacera pas l'état de l'incident de sécurité si l'état actuel de la sécurité est en avance sur l'étape du playbook.

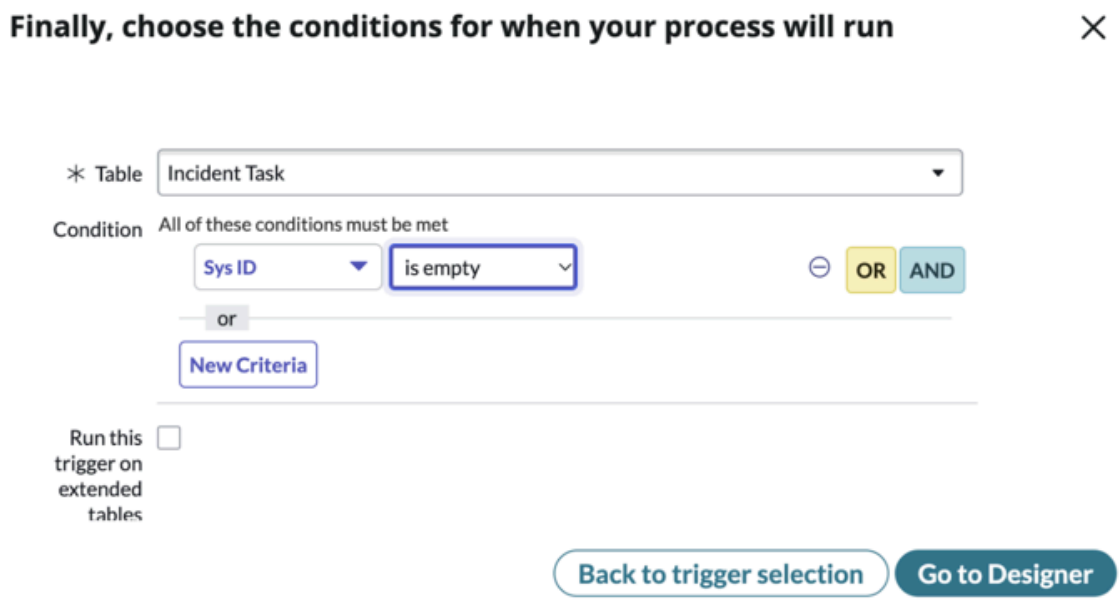
Créer une définition de processus avec une condition de déclenchement factice

Une définition de processus nécessite toujours une condition de déclenchement. Toutefois, si vous n'êtes pas sûr du moment où le processus doit être déclenché, vous pouvez toujours créer une définition de processus avec une condition de déclenchement factice. Définissez la condition de déclenchement, car **sys_id est vide**. Cette condition ne sera jamais remplie.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions du processus



Traduction automatique

Utilisation du playbook d'hameçonnage manuel

Suivez ces étapes pour apprendre à utiliser le playbook Hameçonnage manuel dans l'espace de travail de l'analyste SIR et ses options.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

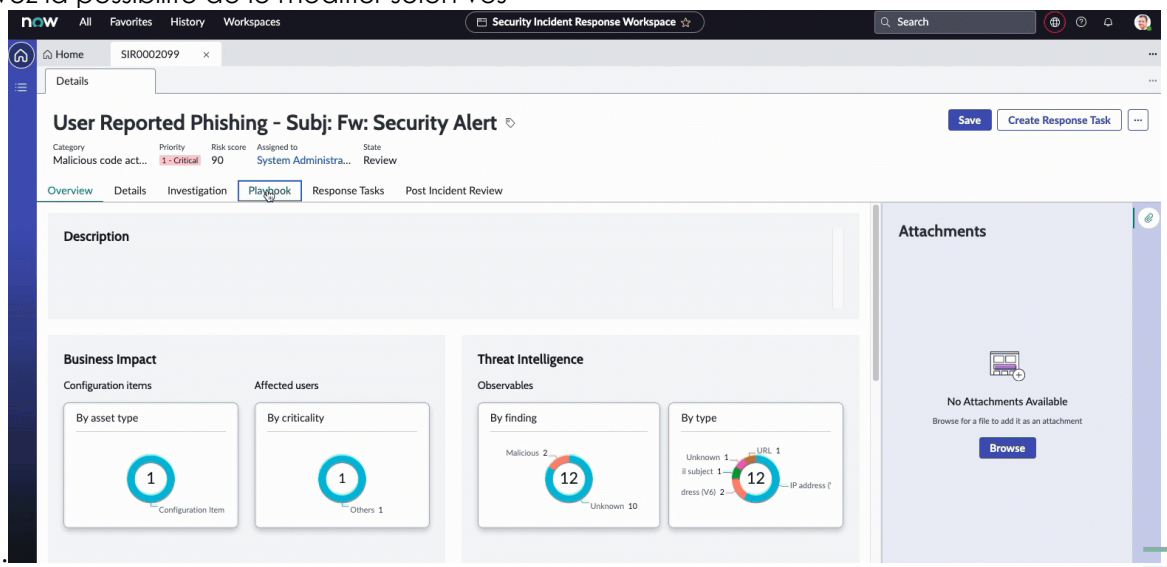
   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de le voir dans l'onglet **Playbook** .

3. Cliquez sur le **Playbook d'hameçonnage manuel**.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Réviser pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action utilisateur à effectuer, elle est affichée dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase concernée et effectuez l'action pour terminer l'activité.

Résumé du playbook d'espace de travail

Ce qui suit décrit le résumé du processus.

- Comprendre le playbook basé sur le flux hérité.
- Répertoriez les activités et étapes possibles après avoir analysé le flux. Recherchez les étapes où une véritable orchestration peut être créée.
- Prenez chaque activité et vérifiez si la définition d'activité fournie par le système de base peut répondre au cas d'utilisation ou non.
- Répertoriez les cas d'utilisation d'activité nécessitant l'implémentation de nouvelles définitions d'activité. Clamiez-les : interactifs, non interactifs ou automatisés. Pour créer une définition d'activité :
  - Créez un flux secondaire ou une action pour le cas d'utilisation.
  - Décidez si les données associées doivent être capturées dans une table de données de flux ou dans une table personnalisée.
  - Si vous utilisez la table de données de flux, créez une définition des données de flux dans **sys_flow_data_definition**. Lors de la création d'un enregistrement de données de flux dans le flux secondaire, sélectionnez la définition de données de flux créée.
  - Créez une **définition d'activité**.
  - Mappez le plan d'automatisation.
  - Renseignez les propriétés de **l'expérience d'activité** .
  - Créez une action sous Actions Playbook. Il doit exister une action d'activité pour l'affecter à la définition d'activité.
  - Pour remplacer l'expérience de carte par défaut en fonction du type d'expérience sélectionné, ajoutez un remplacement playbook à l'aide du concept d'interface utilisateur d'activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Certaines activités peuvent être rendues à la fois automatiques et interactives à l'aide du marqueur d'attente d'entrée de l'utilisateur dans le flux secondaire. Cette entrée peut être transmise lors de la configuration de l'activité dans la définition du processus.
- Une fois que vous avez toutes les définitions d'activité requises pour votre processus, commencez à créer la définition du processus à l'aide de Studio de workflow.

Playbook pour l'hameçonnage automatisé

Le playbook Hameçonnage automatisé fournit des conseils étape par étape à vos analystes sur la façon dont ils peuvent résoudre des types spécifiques de menaces à la sécurité dans vos activités d'hameçonnage automatisé.

Vue d'ensemble

Le modèle de playbook Hameçonnage automatisé est conçu pour automatiser les tâches de réponse d'hameçonnage et contient une séquence d'actions qui inclut des conditions de déclenchement. Vous pouvez utiliser les modèles de playbook pour Studio de workflow automatiser les étapes du playbook de réponse d'hameçonnage et résoudre efficacement ces incidents. Ce modèle de playbook contient une séquence d'actions réutilisables conçues pour répondre aux attaques de hameçonnage. Chaque flux a un déclencheur (condition), une séquence d'actions et des flux secondaires que vous pouvez annoter.

Dans ce playbook, il n'y a aucune interaction de l'utilisateur lorsque la catégorie d'un incident de sécurité est définie sur Hameçonnage. Ce playbook peut être utilisé si un incident de sécurité est créé ou mis à jour. Vous devez activer le playbook d'hameçonnage automatisé dans Studio de workflow, et ce playbook effectue automatiquement toutes les tâches, telles que l'analyse, le confinement, l'élimination et l'examen.

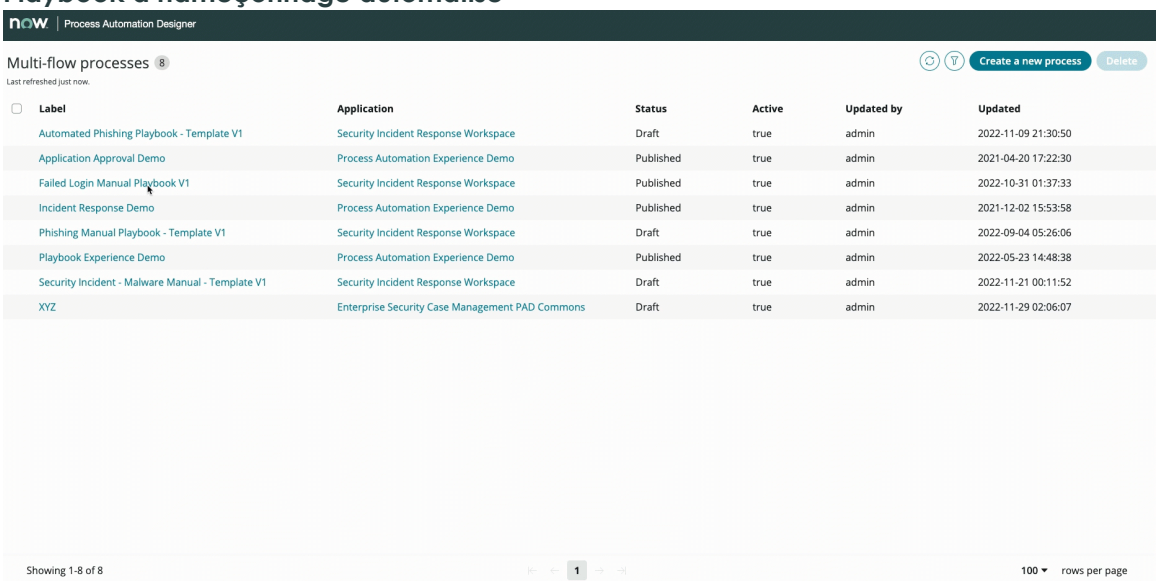
Les étapes suivantes constituent les étapes de la définition du processus et correspondent à l'état de l'incident de sécurité :

- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook d'hameçonnage automatisé



Une fois que vous marquez une tâche comme terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche lorsque vous continuez à accomplir des tâches et des étapes. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les informations que vous avez saisies à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des processus pour le hameçonnage automatisé dans PAD

Suivez ces étapes pour créer des processus pour le hameçonnage automatisé dans Process Automation Designer (PAD).

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.manager

Procédure

1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

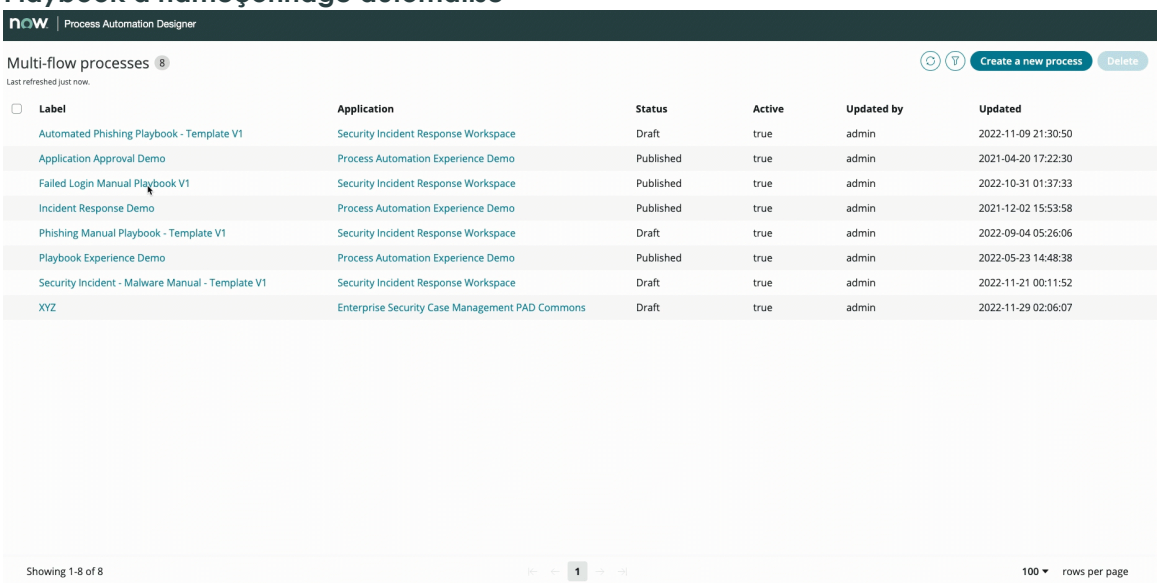
   Par exemple, Playbook d'hameçonnage automatisé : modèle V1.

2. Entrez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour l'exécution de votre processus** et sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions à définir à quel moment votre processus doit s'exécuter en sélectionnant une table et en renseignant les conditions.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, la condition de déclenchement est la création d'un incident de sécurité de la catégorie Hameçonnage.

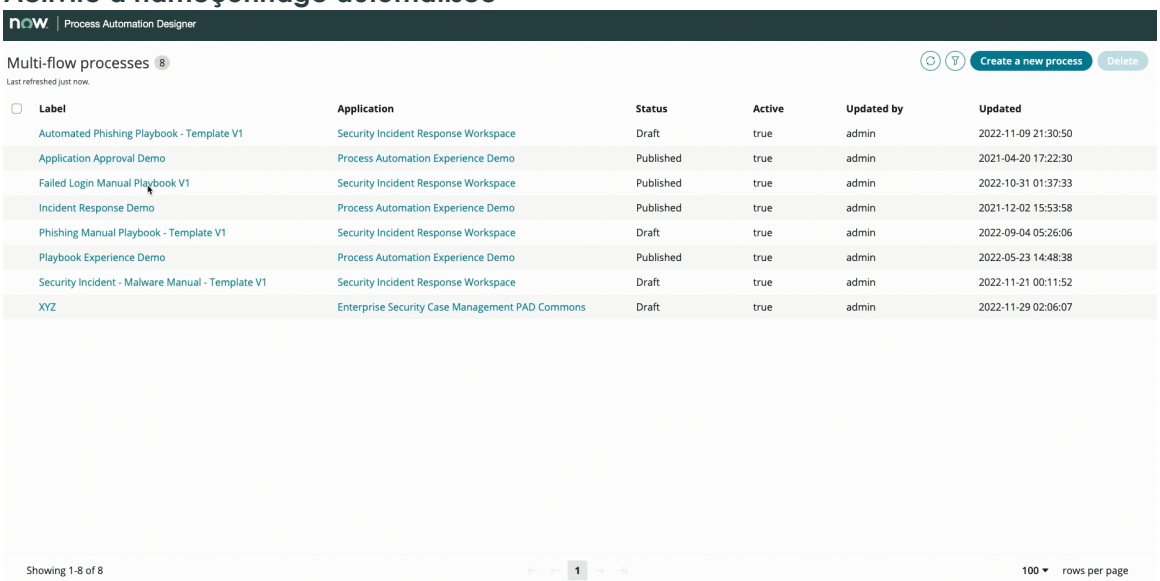
Playbook d'hameçonnage automatisé



7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans le volet des propriétés de l'étape, entrez les détails suivants : **nom**, **description**, **condition d'exécution** et **indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer** impliquent la date d'exécution de l'étape.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour les options Analyse, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a aucune condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité de processus** sous une étape particulière (par exemple, Étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus à chaque étape.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activité d'hameçonnage automatisée



14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité du processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité à partir de la définition d'activité.

Utilisation du playbook d'hameçonnage automatisé

Suivez ces étapes pour apprendre à utiliser le playbook Hameçonnage automatisé dans l'espace de travail de l'analyste SIR et ses options.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

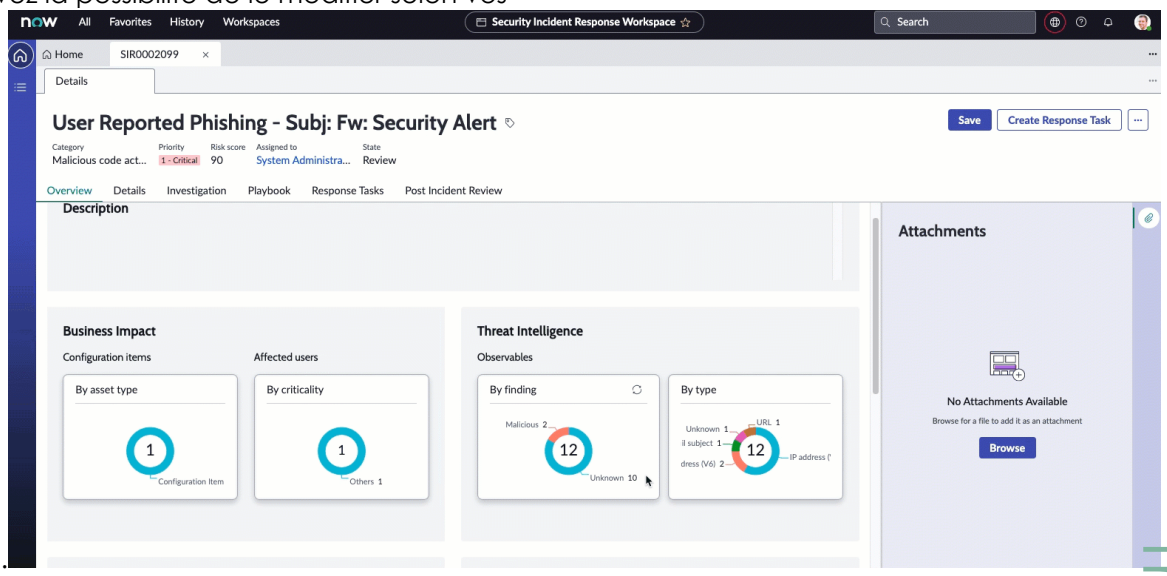
   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de le voir dans l'onglet **Playbook** .

3. Cliquez sur le **Playbook d'hameçonnage automatisé**.
   Dans le cas de l'hameçonnage automatisé, les tâches sont automatiquement exécutées pour l'incident de sécurité.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Réviser pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action utilisateur à effectuer, elle est affichée dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase concernée et effectuez l'action pour terminer l'activité.

Playbook pour les programmes malveillants manuels

Le playbook de programme malveillant manuel fournit des conseils étape par étape sur la façon dont les analystes peuvent résoudre plus efficacement les alertes de programme malveillant.

Le modèle Playbook de programme malveillant manuel est conçu pour effectuer manuellement les étapes impliquées dans la gestion des alertes de programme malveillant provenant du point de terminaison ou du réseau. Vous pouvez utiliser les modèles de playbook dans Studio de workflow pour effectuer les étapes du playbook de programme malveillant manuel et résoudre efficacement ces alertes. Ce playbook comprend des conditions de déclenchement, une séquence d'actions et des flux secondaires que vous pouvez annoter. Ce playbook contient une séquence d'actions réutilisables conçues pour répondre aux attaques de logiciels malveillants. Chaque flux dispose d'un déclencheur (condition), d'une séquence d'actions et de flux secondaires pour l'annotation.

Ce playbook peut être utilisé si un programme malveillant est créé ou mis à jour. Vous devez activer le Playbook de logiciel malveillant manuel dans Studio de workflow et créer toutes les tâches, telles que l'analyse, le confinement, l'élimination et l'examen.

Les étapes suivantes de la définition du processus correspondent à l'état d'alerte de programme malveillant :

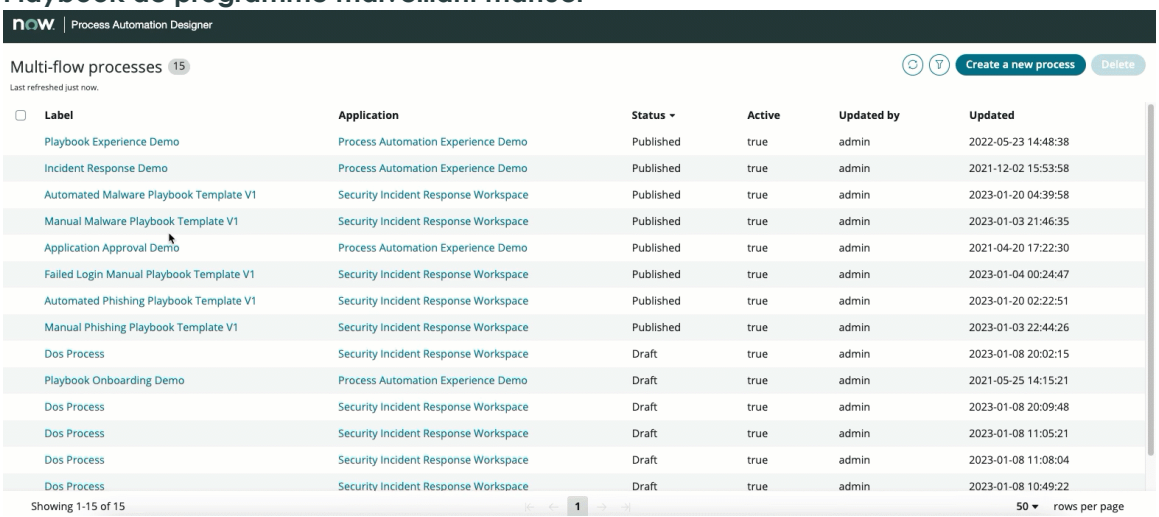
- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de programme malveillant manuel



Une fois que vous avez marqué une tâche comme terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche lorsque vous continuez à accomplir des tâches et des étapes. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les informations que vous avez saisies à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des processus pour les programmes malveillants manuels dans PAD

Suivez ces étapes pour créer des processus pour les programmes malveillants manuels dans Process Automation Designer (PAD).

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.manager

Procédure

1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

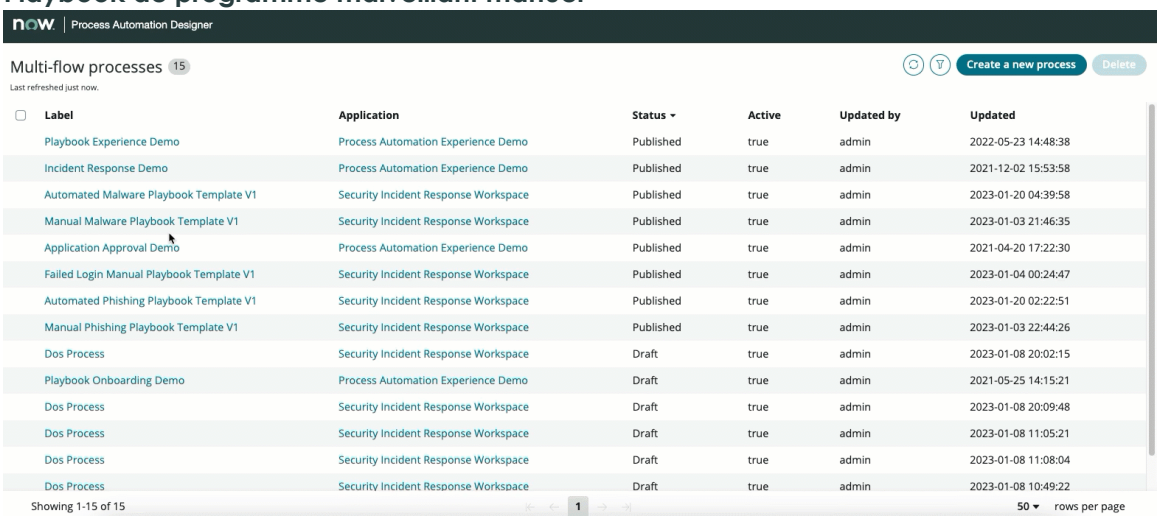
   Par exemple, Playbook de programme malveillant manuel : modèle V1.

2. Entrez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour l'exécution de votre processus** et sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions à définir à quel moment votre processus doit s'exécuter en sélectionnant une table et en renseignant les conditions.
   Par exemple, la condition de déclenchement est la création d'un incident de sécurité de la catégorie Hameçonnage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de programme malveillant manuel

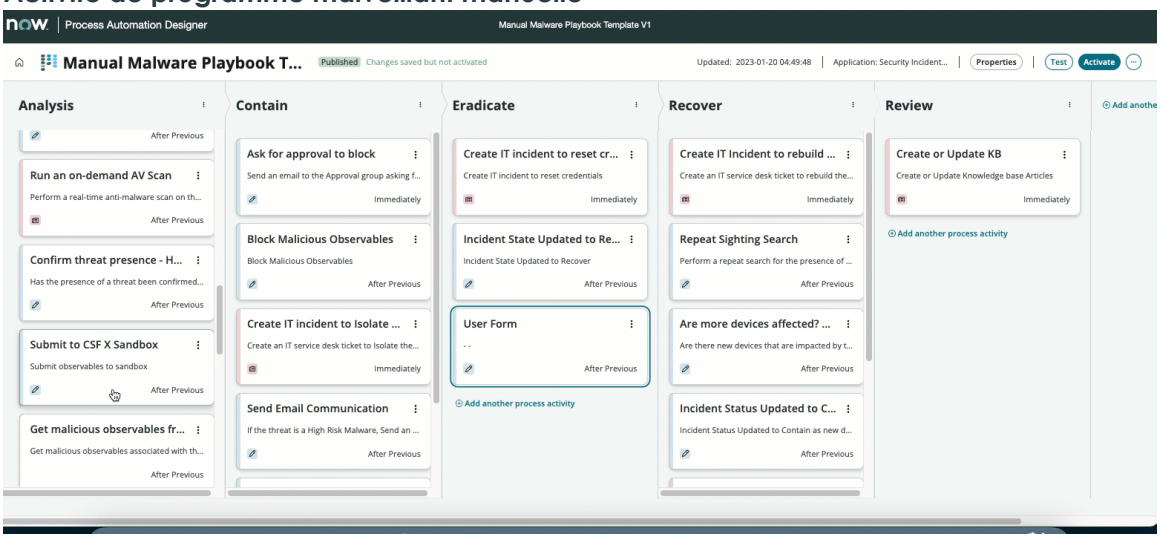


7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans le volet des propriétés de l'étape, entrez les détails suivants : **nom**, **description**, **condition d'exécution** et **indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer** impliquent la date d'exécution de l'étape.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour les options Analyse, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a aucune condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité de processus** sous une étape particulière (par exemple, Étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus à chaque étape.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activité de programme malveillant manuelle



14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité du processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité à partir de la définition d'activité.

Utilisation du playbook de programme malveillant manuel

Suivez ces étapes pour apprendre à utiliser le playbook de programme malveillant manuel dans l'espace de travail d'analyste SIR et ses options.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

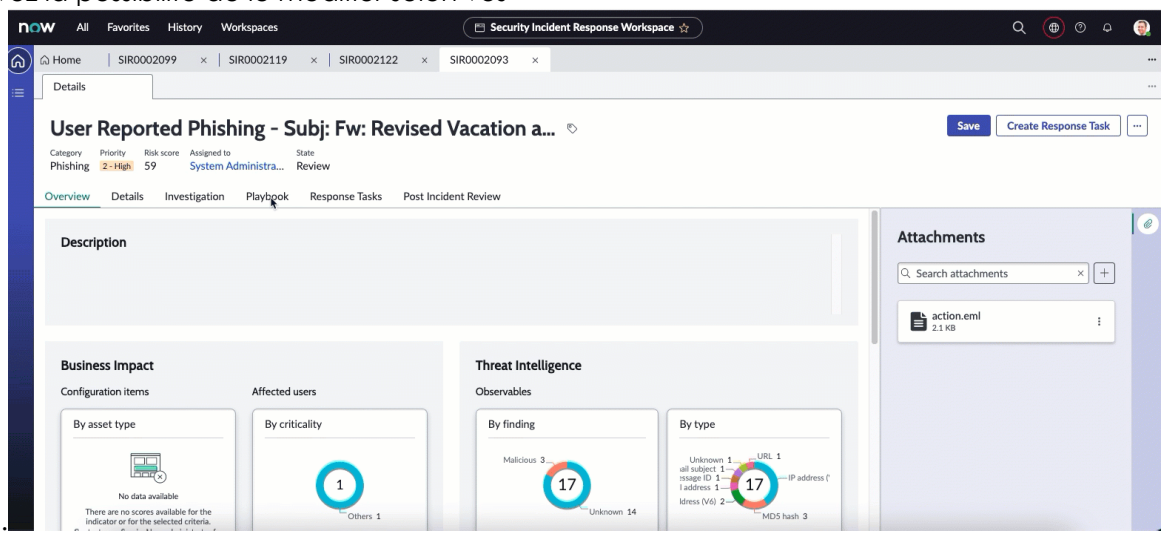
   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de le voir dans l'onglet **Playbook** .

3. Cliquez sur le **Playbook de programme malveillant manuel**.
   Pour les programmes malveillants manuels, les tâches sont automatiquement exécutées pour l'incident de sécurité.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Réviser pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action utilisateur à effectuer, elle est affichée dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase concernée et effectuez l'action pour terminer l'activité.

Playbook pour les programmes malveillants automatisés

Le Playbook de programme malveillant automatisé fournit une séquence d'étapes automatisées qui aide les analystes à résoudre les alertes de programme malveillant plus efficacement.

Le modèle Playbook de programme malveillant automatisé est conçu pour automatiser les étapes impliquées dans la gestion des alertes de programme malveillant provenant du point de terminaison ou du réseau. Vous pouvez utiliser les modèles de playbook dans Studio de workflow pour automatiser les étapes du playbook contre les programmes malveillants automatisés et résoudre efficacement ces alertes. Ce playbook comprend des conditions de déclenchement, une séquence d'actions et des flux secondaires que vous pouvez annoter. Ce playbook contient une séquence d'actions réutilisables conçues pour répondre aux attaques de logiciels malveillants. Chaque flux dispose d'un déclencheur (condition), d'une séquence d'actions et de flux secondaires pour l'annotation.

Ce playbook peut être utilisé si un incident de sécurité est créé ou mis à jour. Vous devez activer le playbook Automated Malware dans Studio de workflow, et ce playbook effectue automatiquement toutes les tâches, telles que l'analyse, le confinement, l'élimination et l'examen.

Les étapes suivantes constituent les étapes de la définition du processus et correspondent à l'état de l'incident de sécurité :

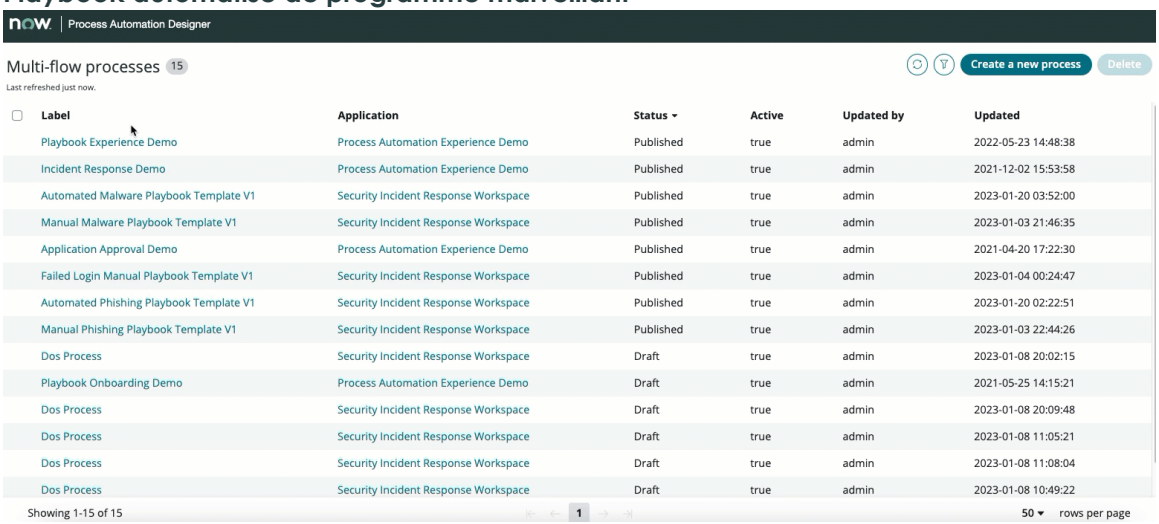
- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook automatisé de programme malveillant



Une fois que vous marquez une tâche comme terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche lorsque vous continuez à accomplir des tâches et des étapes. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les informations que vous avez saisies à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des processus Automated Malware dans PAD

Suivez ces étapes pour créer des processus pour les programmes malveillants automatisés dans Process Automation Designer (PAD).

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.manager

Procédure

1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

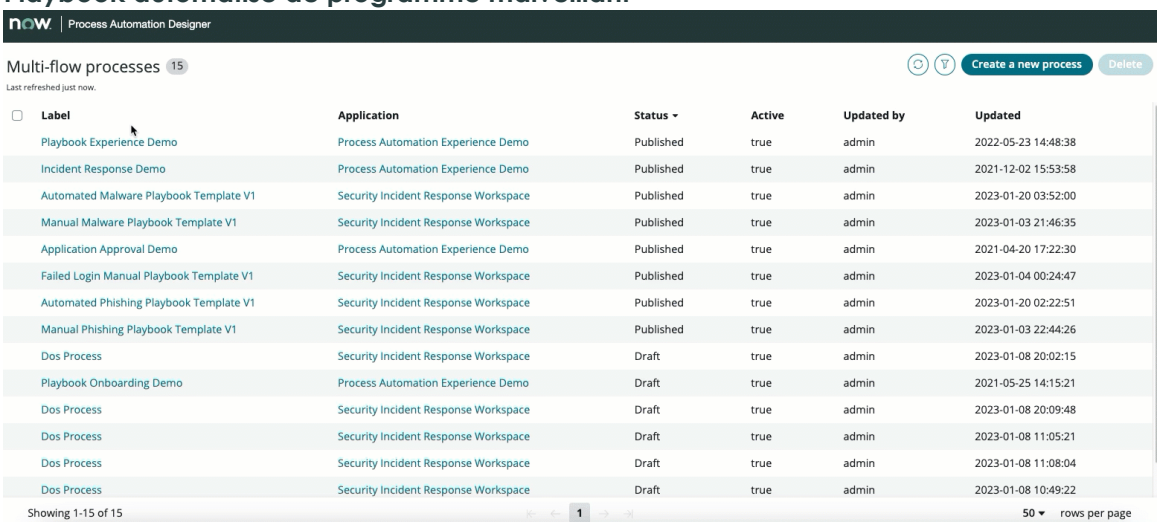
   Par exemple, Playbook de programme malveillant automatisé : modèle V1.

2. Entrez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour l'exécution de votre processus** et sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions à définir à quel moment votre processus doit s'exécuter en sélectionnant une table et en renseignant les conditions.
   Par exemple, la condition de déclenchement est la création d'un incident de sécurité de la catégorie Hameçonnage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

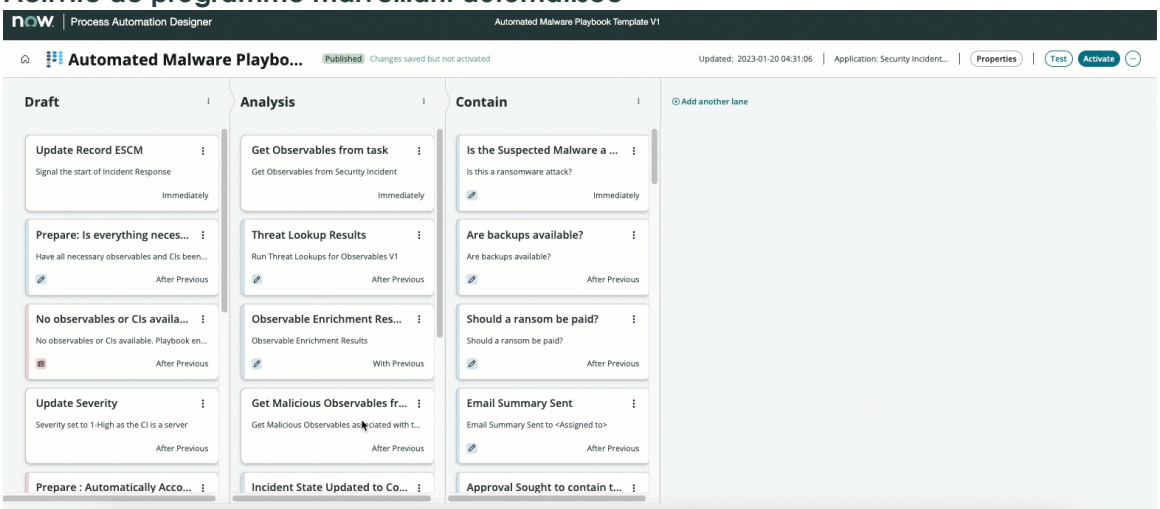
Playbook automatisé de programme malveillant



7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans le volet des propriétés de l'étape, entrez les détails suivants : **nom**, **description**, **condition d'exécution** et **indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer** impliquent la date d'exécution de l'étape.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour les options Analyse, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a aucune condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité de processus** sous une étape particulière (par exemple, Étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus à chaque étape.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activité de programme malveillant automatisée



14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité du processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité à partir de la définition d'activité.

Utilisation du playbook de programme malveillant automatisé

Suivez ces étapes pour apprendre à utiliser le Playbook de programme malveillant automatisé dans l'espace de travail de l'analyste SIR et ses options.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

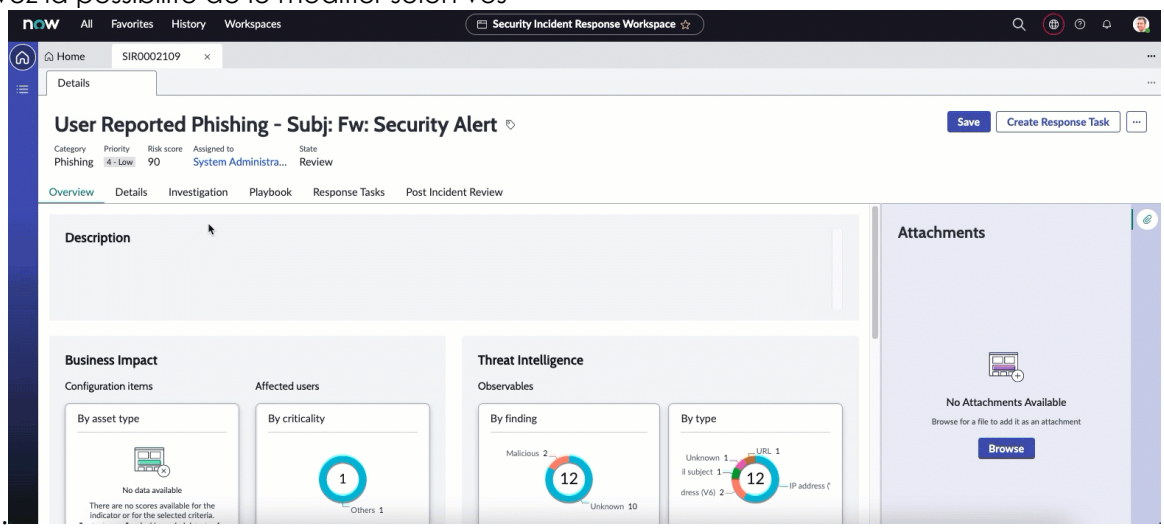
   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de le voir dans l'onglet **Playbook** .

3. Cliquez sur le **Playbook de programme malveillant automatisé**.
   Dans le cas des programmes malveillants automatisés, les tâches sont automatiquement exécutées pour l'incident de sécurité.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Réviser pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action utilisateur à effectuer, elle s'affiche dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase concernée et effectuez l'action pour terminer l'activité.

Playbook pour Échec de connexion manuelle

Le playbook Échec de connexion manuelle fournit des conseils et permet d'optimiser l'enquête sur les incidents de sécurité liés à l'échec de connexion.

Lorsqu'un utilisateur effectue certaines tentatives de connexion infructueuses (conformément à la configuration SIM), un incident de sécurité est créé. Ces tentatives de connexion infructueuses peuvent être des faux positifs ou des tentatives effectuées par des attaquants pour obtenir l'accès aux comptes de messagerie des utilisateurs.

Vous pouvez utiliser les modèles de playbook dans Studio de workflow pour effectuer les étapes du playbook Échec de connexion et résoudre efficacement les incidents de sécurité liés à l'échec de connexion. Ce playbook comprend des conditions de déclenchement, une séquence d'actions et des flux secondaires que vous pouvez annoter. Ce playbook contient une séquence d'actions réutilisables conçues pour répondre aux incidents de sécurité liés à l'échec de connexion. Chaque flux dispose d'un déclencheur (condition), d'une séquence d'actions et de flux secondaires pour l'annotation.

Ce playbook peut être utilisé si un incident de sécurité lié à un échec de connexion est créé ou mis à jour. Vous devez activer le Playbook manuel en cas d'échec de connexion et Studio de workflow créer toutes les tâches, telles que l'analyse, le confinement, l'élimination et la révision.

Les étapes suivantes constituent les étapes de la définition du processus et correspondent à l'état de l'incident de sécurité :

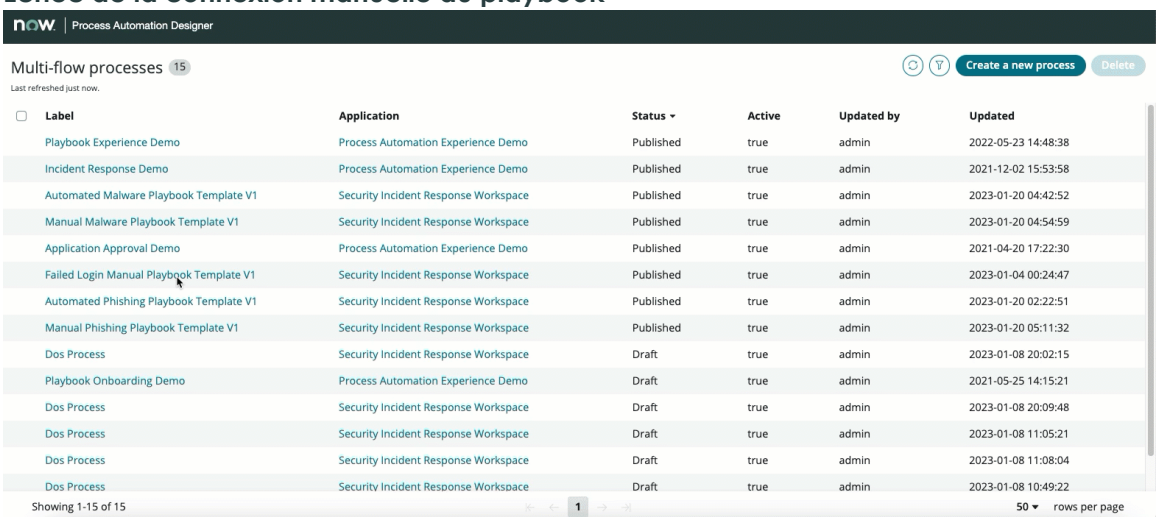
- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Échec de la connexion manuelle au playbook



Une fois que vous marquez une tâche comme terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche lorsque vous continuez à accomplir des tâches et des étapes. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les informations que vous avez saisies à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des processus en cas d'échec de connexion manuelle dans PAD

Suivez ces étapes pour créer des processus pour l'échec de connexion manuelle dans Concepteur d'automatisation de processus (PAD).

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.manager

Procédure

1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

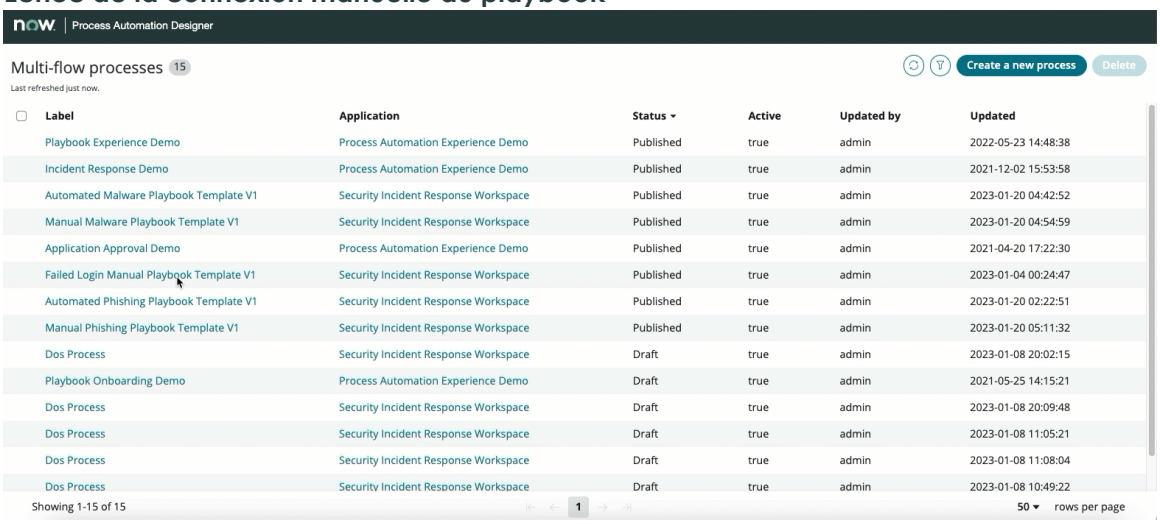
   Par exemple, Échec de la connexion manuelle à Playbook : modèle V1.

2. Entrez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour l'exécution de votre processus** et sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions à définir à quel moment votre processus doit s'exécuter en sélectionnant une table et en renseignant les conditions.
   Par exemple, la condition de déclenchement est la création d'un incident de sécurité de la catégorie Hameçonnage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Échec de la connexion manuelle au playbook

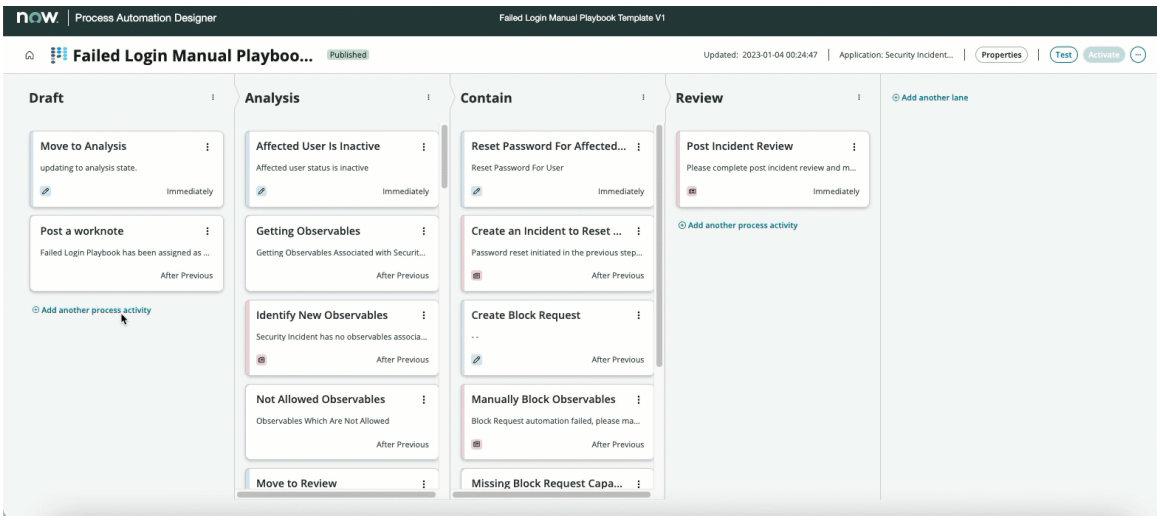


7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans le volet des propriétés de l'étape, entrez les détails suivants : **nom**, **description**, **condition d'exécution** et **indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer** impliquent la date d'exécution de l'étape.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour les options Analyse, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a aucune condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité de processus** sous une étape particulière (par exemple, Étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus à chaque étape.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Échec de la connexion à l'activité manuelle



14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité du processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité à partir de la définition d'activité.

Utilisation du playbook Échec de la connexion manuelle

Suivez ces étapes pour découvrir comment utiliser le playbook Échec de connexion manuelle dans l'espace de travail de l'analyste SIR et ses options.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

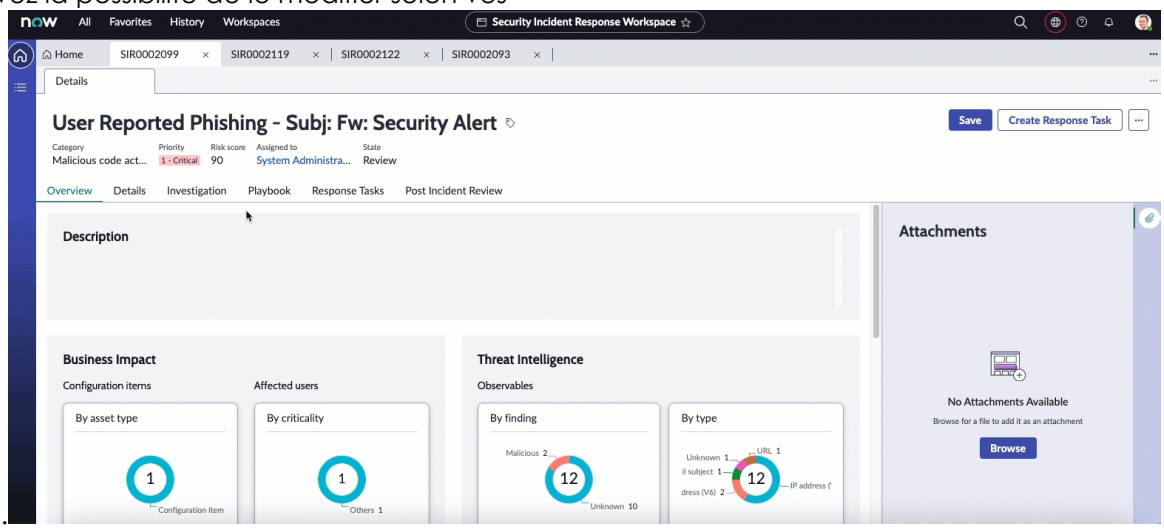
   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de le voir dans l'onglet **Playbook** .

3. Cliquez sur le **playbook manuel Échec de la connexion**.
   En cas d'échec de connexion manuelle, les tâches sont automatiquement exécutées pour l'incident de sécurité.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Réviser pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action utilisateur à effectuer, elle s'affiche dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase concernée et effectuez l'action pour terminer l'activité.

Playbooks basés sur le flux

À l'aide de Flow Designer, les administrateurs de sécurité et les auteurs de conception de flux peuvent plus facilement passer de playbooks manuels ou non documentés à des playbooks automatisés et reproductibles. La fonction glisser-déposer offre une flexibilité dans le déplacement d'objets, les vérifications de conditions, les branches parallèles, les tables de décision, etc.

Réponse aux incidents de sécurité fournit les playbooks suivants avec le système de base.

Outre les playbooks répertoriés, il existe également des flux secondaires dans le spoke Security Operations qui peuvent être appelés à partir du playbook de flux. Les rançongiciels sont l'un de ces flux secondaires.

Activez ces flux avant de les utiliser. Pour plus d'informations, consultez Activer un flux Security Incident Response.

Playbook pour l'hameçonnage automatisé

Le playbook Hameçonnage automatisé vous aide à résoudre certains types de menaces à la sécurité étape par étape. Avec les modèles Flow Designer, vous pouvez automatiser les étapes du playbook de réponse à l'hameçonnage et résoudre les incidents rapidement et efficacement.

Vous pouvez utiliser des modèles créés avec Concepteur de flux pour automatiser les tâches du Playbook de réponse d'hameçonnage afin d'analyser et de résoudre les attaques d'hameçonnage dans votre organisation.

Le playbook de réponse d'hameçonnage comprend les flux et flux secondaires suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Incident de sécurité - Modèle de réponse d'hameçonnage automatisé : ce modèle est conçu pour automatiser les tâches de réponse d'hameçonnage et contient une séquence d'actions, y compris un déclencheur.
- Incident de sécurité - Modèle manuel d'hameçonnage : ce modèle est le workflow de réponse d'hameçonnage manuel existant. Définissez la catégorie sur Hameçonnage pour activer le flux.

Ces modèles contiennent une séquence d'actions réutilisables conçues pour répondre aux attaques de hameçonnage. Chaque flux dispose d'un déclencheur (condition), d'une séquence d'actions et de flux secondaires que vous pouvez annoter pour plus de lisibilité. Pour accéder à ces flux, vous devez installer lespoke Security Operations .

Remarque : Activez ces modèles avant de pouvoir les utiliser. Pour en savoir plus, consultez Activer un flux Security Incident Response .

- Exécuter des recherches de menace pour les observables : effectue des recherches de menaces sur les observables sélectionnés.
- Enrichir les observables : permet d'enrichir les observables avec des informations supplémentaires provenant de diverses sources.
- Évaluer l'impact de l'e-mail d'hameçonnage : vous permet d'évaluer l'impact de l'e-mail d'hameçonnage. Lorsque vous recevez un e-mail à l'adresse e-mail d'hameçonnage, ce flux secondaire analyse le fichier . pièce jointe EML et compare les informations aux règles de correspondance des e-mails.
- Éradiquer les e-mails d'hameçonnage : vous permet de supprimer ou d'éradiquer les e-mails d'hameçonnage afin de réduire l'exposition à une attaque spécifique.
- Exécuter une recherche de perception sur les observables : détermine la prévalence d'une menace dans le temps ou teste les efforts de rattrapage ou d'éradication.
- Créer des demandes de bloc : bloque la communication avec les observables associés à l'incident.

Ces flux secondaires représentent un ensemble d'opérations réutilisables que vous pouvez utiliser dans plusieurs playbooks. Vous pouvez utiliser ces flux secondaires pour définir des modèles personnalisés (flux) en fonction de vos besoins.

Pour créer des modèles personnalisés (flux), suivez les instructions de la section Flux .

Exécuter le flux du playbook de réponse d'hameçonnage automatisé

À l'aide du concepteur de flux, vous pouvez définir et automatiser des tâches dans le playbook pour analyser et résoudre les attaques de hameçonnage contre votre organisation.

Avant de commencer

- Rôle requis : sn_si.admin, flow_designer et action_designer
- Installez et configurez les intégrations suivantes avec les bonnes informations d'identification :
  - Demande de bloc (Opérations de sécurité intégration de Palo Alto Networks NGFW)
  - Enrichissement des éléments observables
  - Recherche de perception
  - Recherche de menace
  - Microsoft Office Exchange

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

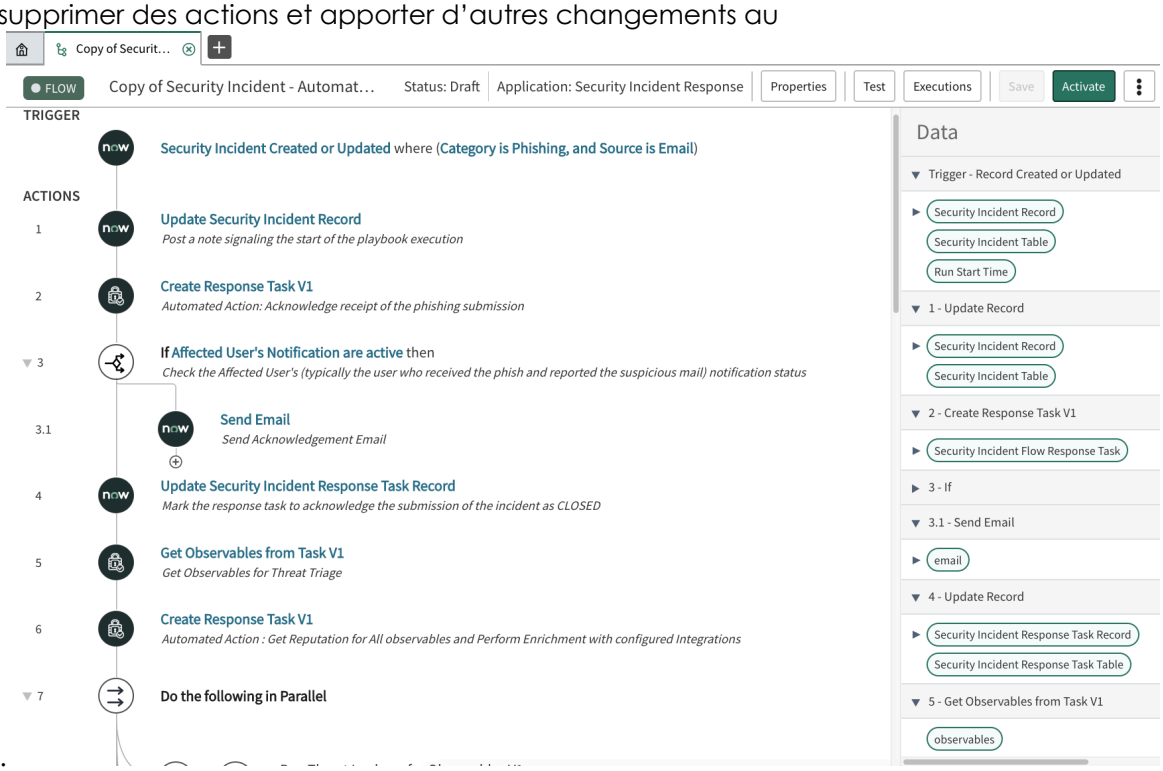
Lorsque les employés reçoivent un e-mail suspect contenant les signes courants d'une attaque par hameçonnage (tels que définis par vos politiques de sécurité), ils peuvent l'envoyer en tant que fichier . Pièce jointe EML à l'adresse e-mail d'hameçonnage définie par votre organisation. À l'aide des tâches définies dans le flux du playbook d'hameçonnage automatisé, vous pouvez trier, analyser, contenir et éradiquer une menace d'hameçonnage. Ces tâches peuvent être invoquées dans le cadre de différents états d'incident (par exemple, Analyse, Contenir, etc.). Lorsqu'un incident de sécurité de hameçonnage est créé, le flux d'hameçonnage automatisé peut être déclenché automatiquement. À l'aide de Concepteur de flux, vous pouvez afficher les détails des différentes actions de réponse aux incidents au fur et à mesure qu'elles sont invoquées.

Remarque : Le flux de playbook Incident de sécurité - Modèle de réponse d'hameçonnage automatisé V1 est en lecture seule. Vous pouvez effectuer une copie du flux et apporter les modifications nécessaires.

Les étapes suivantes décrivent comment faire une copie du modèle de playbook d'hameçonnage et vous guident à travers certaines des tâches du flux.

Procédure

1. Accédez à la **Tout** > **Concepteur de flux** > **Concepteur** pour afficher les flux disponibles avec le Opérations de sécurité spoke.
2. Cliquez sur le lien **Security Incident - Automated Phishing Response Template VI (Incident de sécurité - Automated Phishing Response Template**) VI.
3. Sur la page Flux, cliquez sur l'icône , faites une copie du flux et ouvrez-la pour votre utilisation.
   Vous pouvez modifier les conditions de déclenchement, ajouter ou supprimer des actions et apporter d'autres changements au flux.



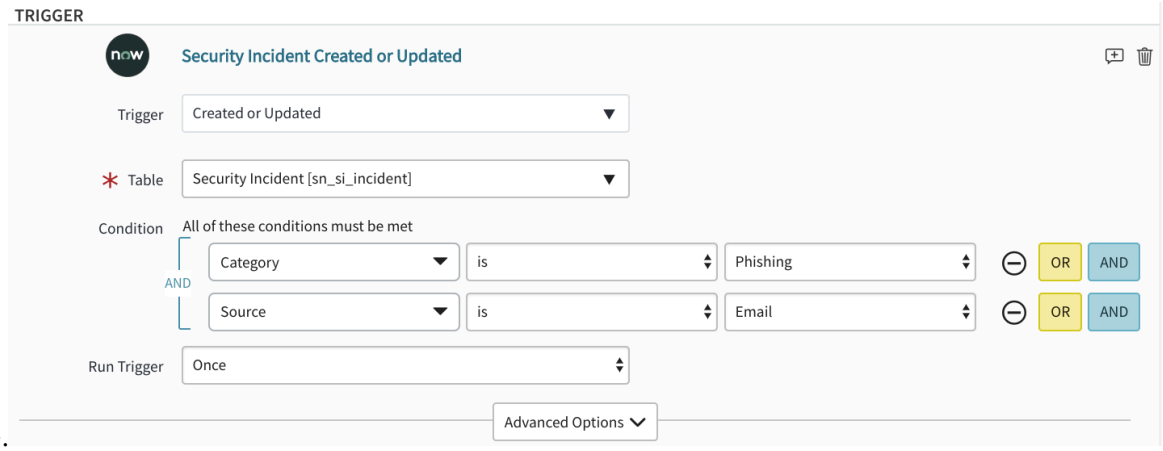
   Cette image montre les conditions de déclenchement et les étapes exécutées par le flux. Le panneau de droite montre le flux de données. Cliquez sur une icône pour développer l'étape et afficher les détails.

4. Cliquez sur l'icône **Déclencheur** .

Traduction automatique

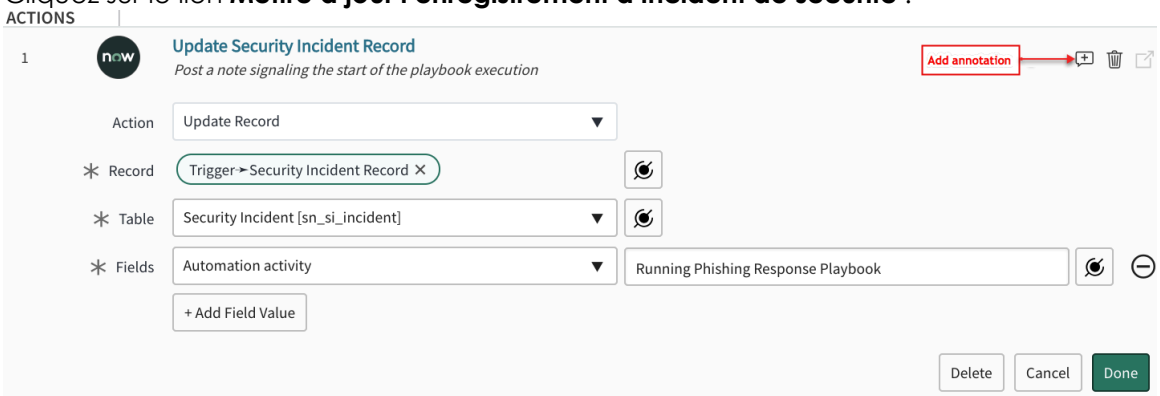
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans un premier temps, vous définissez ou définissez le déclencheur du flux. Spécifiez les conditions du déclencheur et la fréquence à laquelle vous souhaitez que le flux l'exécute.



Lorsque les conditions définies dans le flux (catégorie est hameçonnage et source est e-mail) sont remplies dans l'enregistrement d'incident, les tâches du flux d'hameçonnage automatisé commencent à s'exécuter séquentiellement. Vous pouvez modifier le déclencheur, ajouter des annotations, ajouter ou supprimer des conditions, etc.

5. Cliquez sur le lien **Mettre à jour l'enregistrement d'incident de sécurité** .

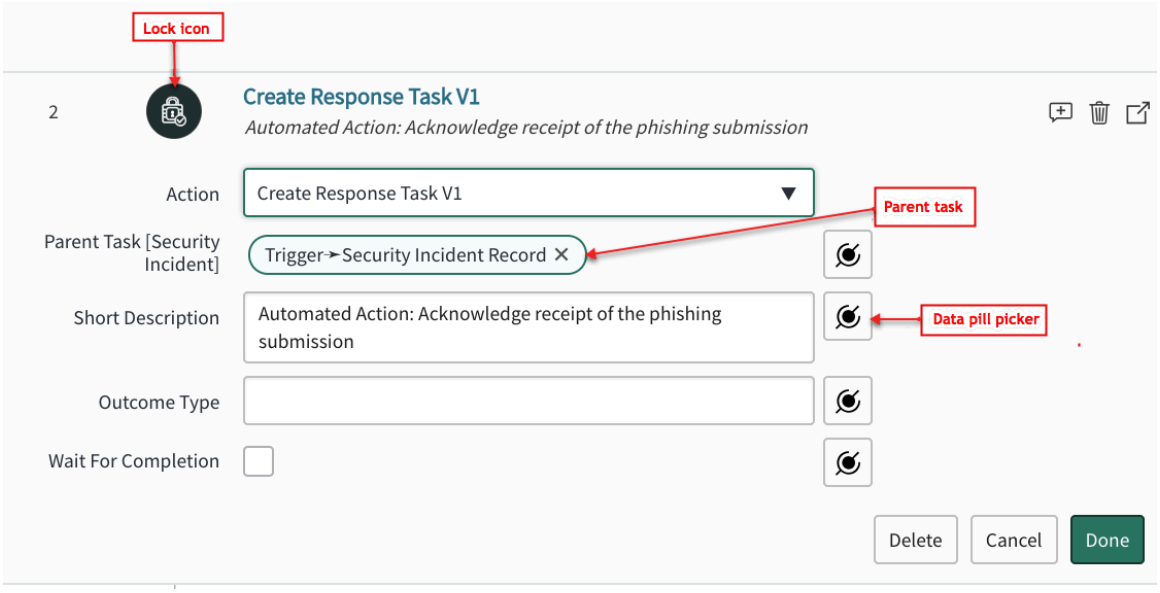


La mise à jour de l'enregistrement d'incident de sécurité est la première étape du flux. Cliquez sur l'icône pour ajouter une note à l'analyste de sécurité indiquant qu'un incident d'hameçonnage s'est produit et que le flux automatisé du playbook d'hameçonnage a commencé à s'exécuter.

6. Poursuivez avec l'étape 2 dans le flux et cliquez sur le lien **Créer une tâche de réponse** .

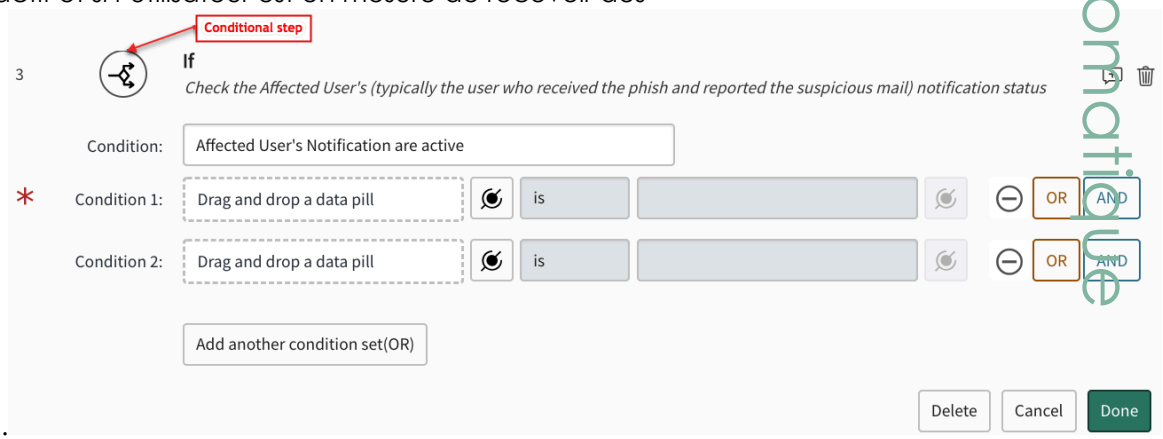
Dans cette étape, le flux crée une tâche de réponse automatisée pour accuser réception de l'incident à l'émetteur de l'incident ou à l'utilisateur affecté.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Notez que le champ **Tâche parente [Incident de sécurité]** fait référence à l'enregistrement parent associé à cette étape. Vous pouvez choisir n'importe quel enregistrement de référence à l'aide de l'icône de sélection de pastilles de données, de ou de faire glisser l'élément de référence pertinent à partir du panneau de droite. Remarquez l'icône de verrou . L'icône de verrou indique que cette étape ne nécessite aucune intervention de l'utilisateur.

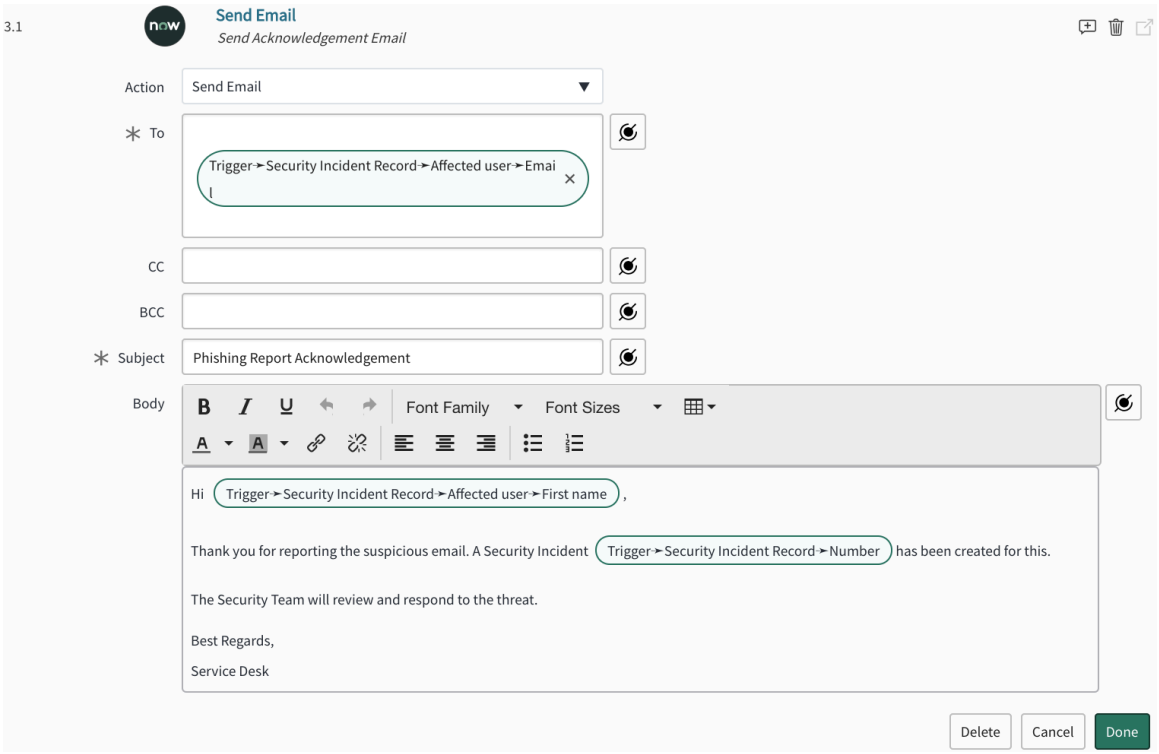
7. À l'étape 3, le flux collecte des détails supplémentaires sur l'utilisateur affecté (généralement, l'utilisateur qui a soumis l'incident) afin de s'assurer qu'il peut envoyer une notification avec succès.
Vous pouvez spécifier des conditions pour vérifier si l'état de l'utilisateur affecté est actif et si l'utilisateur est en mesure de recevoir des notifications.



Remarquez l'icône d'étape conditionnelle à l'étape 3. Le flux n'exécute l'étape suivante (3.1) que si les conditions spécifiées sont remplies.

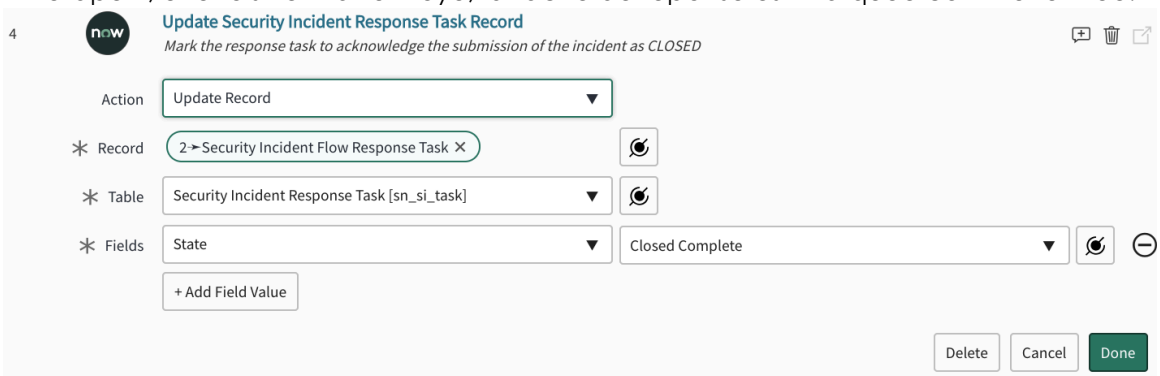
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

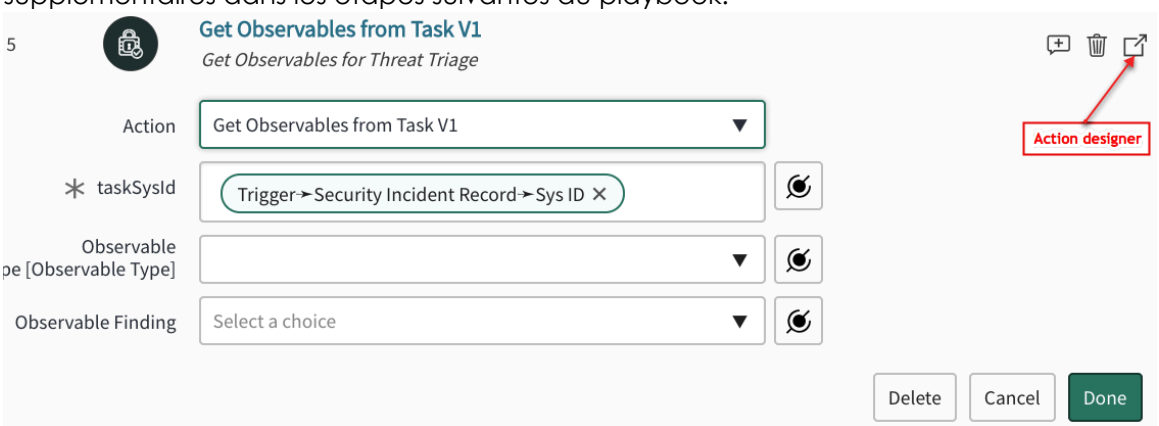


Lorsque les conditions définies à l'étape 3 sont remplies avec succès, l'e-mail est envoyé.

8. À l'étape 4, une fois l'e-mail envoyé, la tâche de réponse est marquée comme fermée.



9. À l'étape 5, tous les observables impliqués dans l'incident (tels que l'objet de l'e-mail, l'adresse e-mail à partir de laquelle l'e-mail d'hameçonnage a été envoyé, l'URL d'hameçonnage) ou les observables appartenant à une catégorie sélectionnée (hachage, fichier ou domaine) sont collectés pour effectuer des actions automatisées supplémentaires dans les étapes suivantes du playbook.



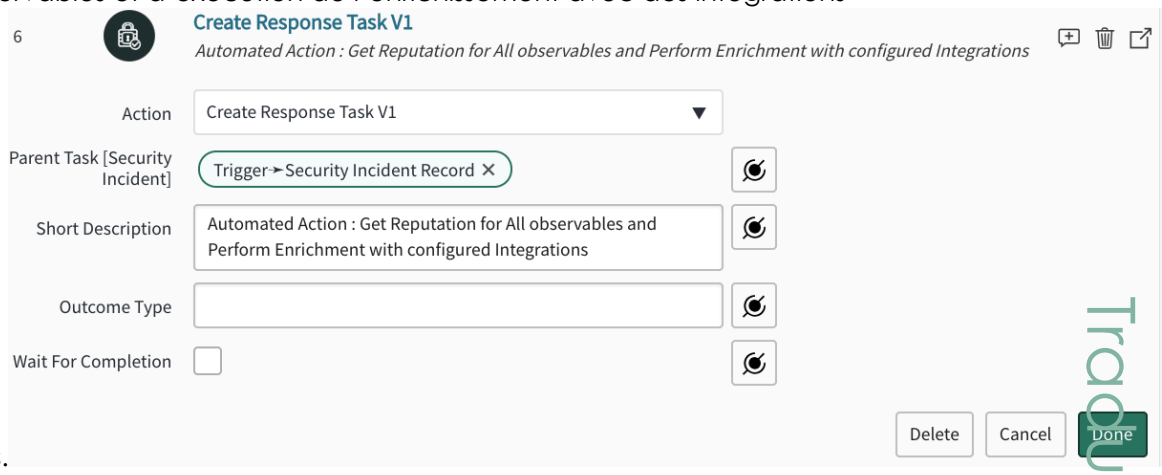
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cliquez sur l'icône du concepteur pour afficher une vue détaillée de l'action.

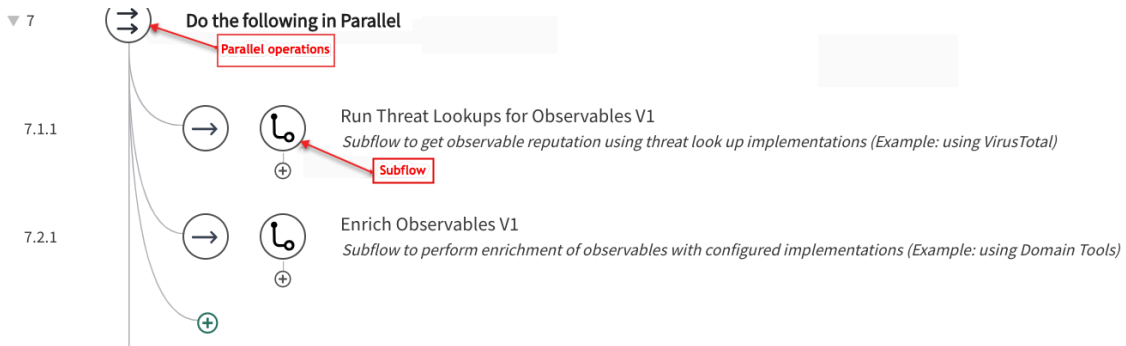
Pour afficher la page du Concepteur d'action , développez une étape dans le flux et cliquez sur l'icône du Concepteur d'action.

10. À l'étape 6, une tâche de réponse automatisée est créée.
Cette tâche capture le début du processus d'obtention de la réputation de tous les observables et d'exécution de l'enrichissement avec des intégrations configurées.



11. À l'étape 7, deux flux secondaires sont appelés :

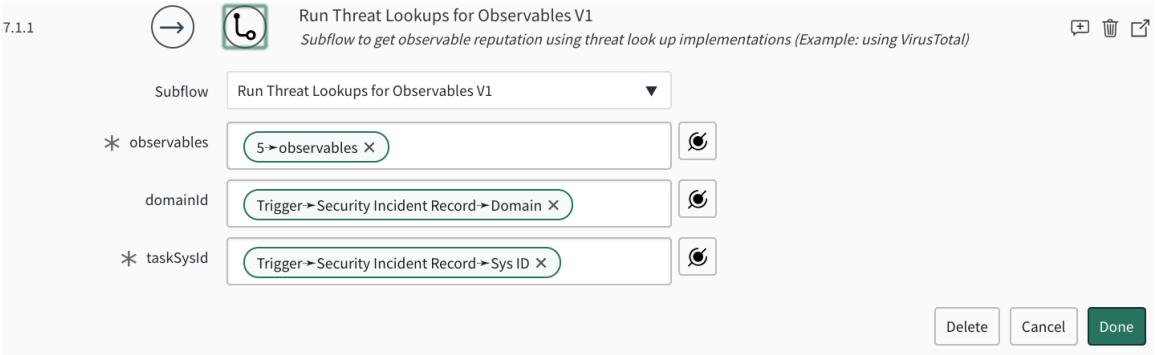
- Exécuter des recherches de menace pour les observables : ce flux secondaire est utilisé pour obtenir la réputation de tous les observables à l'aide d'implémentations de recherche de menace.
- Enrichir les observables : ce flux secondaire permet d'enrichir les observables avec les implémentations configurées.



Remarquez les icônes de cette tâche. L'icône indique que les deux tâches seront exécutées en parallèle et l'icône de flux secondaire indique que la tâche en cours d'exécution est un flux secondaire, comme indiqué ci-dessous :

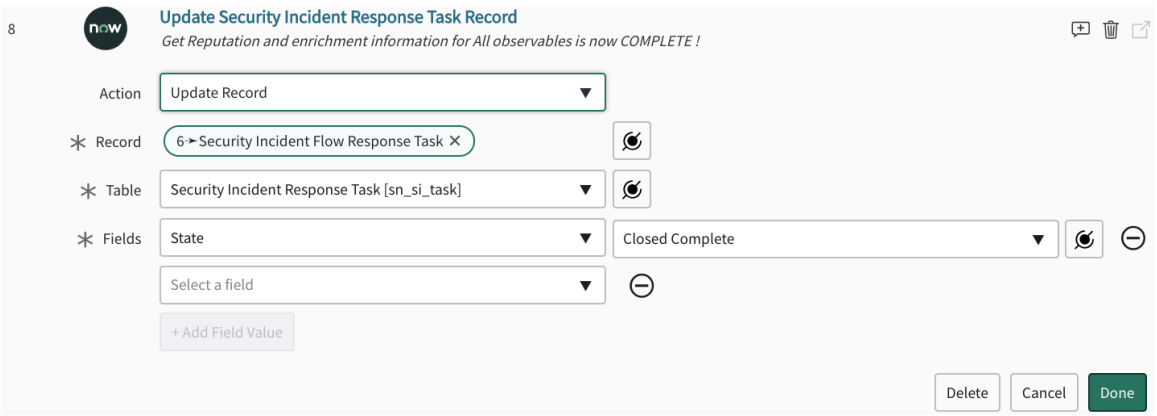
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

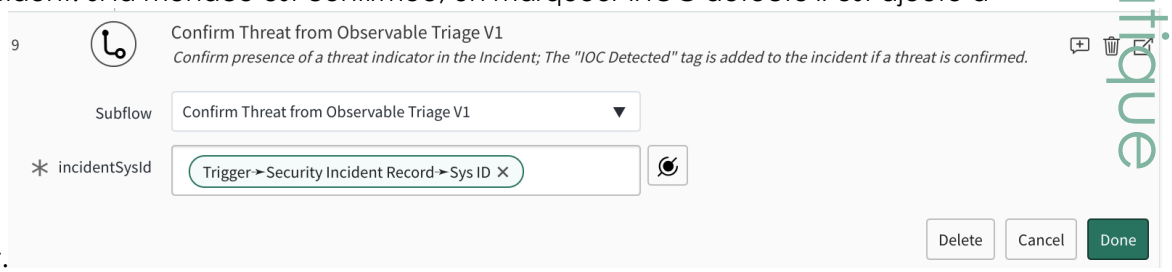


Notez le chiffre 5 dans le champ des observables. Cela indique que la recherche de menace sera exécutée sur les observables récupérés à l'étape 5. Ce flux secondaire appelle à son tour les workflows et les actions existants, comme indiqué dans le concepteur de flux secondaires.

12. À l'étape 8, une fois les flux secondaires terminés, la tâche de réponse est marquée comme fermée.



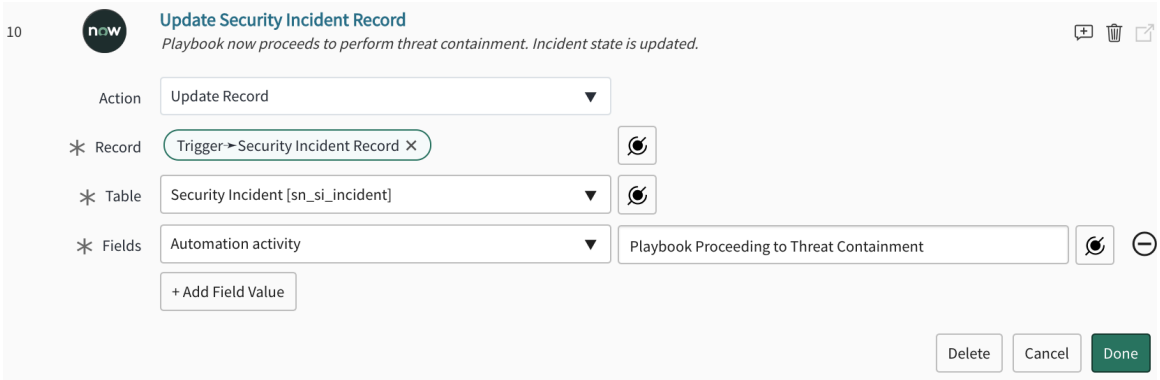
13. À l'étape 9, le flux secondaire Confirmer la menace à partir du triage des observables est appelé.
Ce flux secondaire est utilisé pour confirmer la présence d'un indicateur de menace dans l'incident. Si la menace est confirmée, un marqueur « IOC détecté » est ajouté à l'incident.



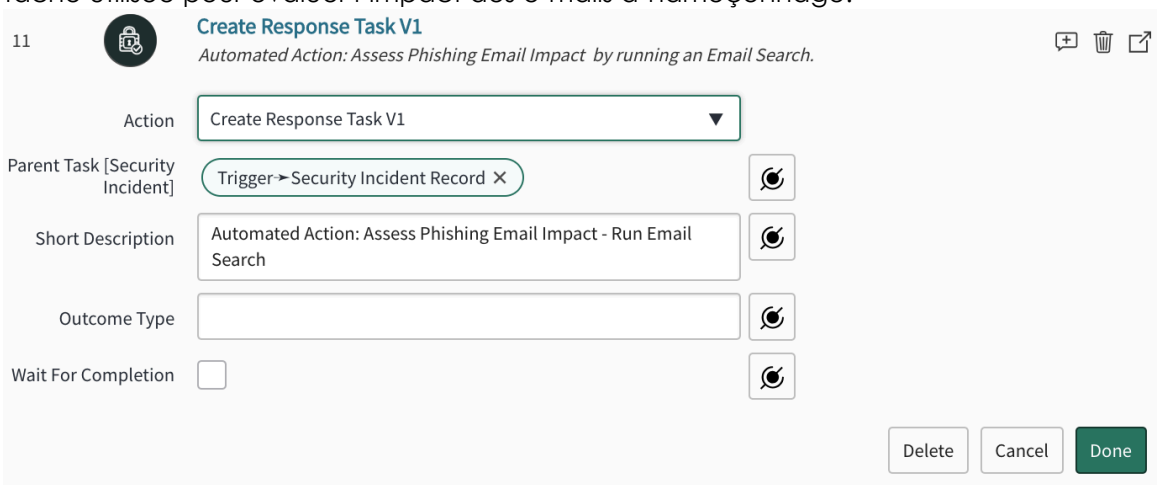
14. Lorsque la menace est confirmée, à l'étape 10, vous mettez à jour l'incident de sécurité et ajoutez une note indiquant que des tâches de maîtrise de la menace seront lancées.

Traduction automatique

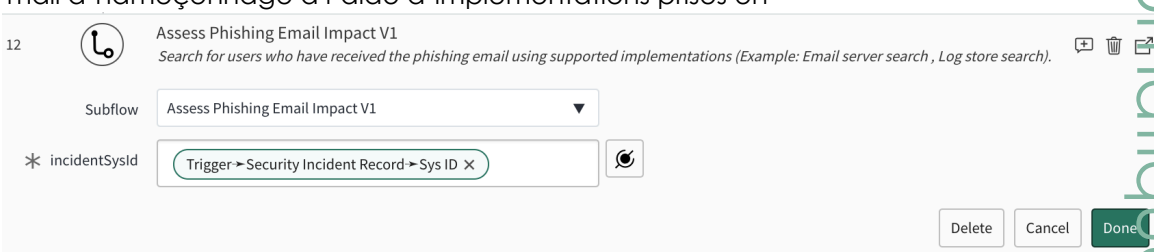
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



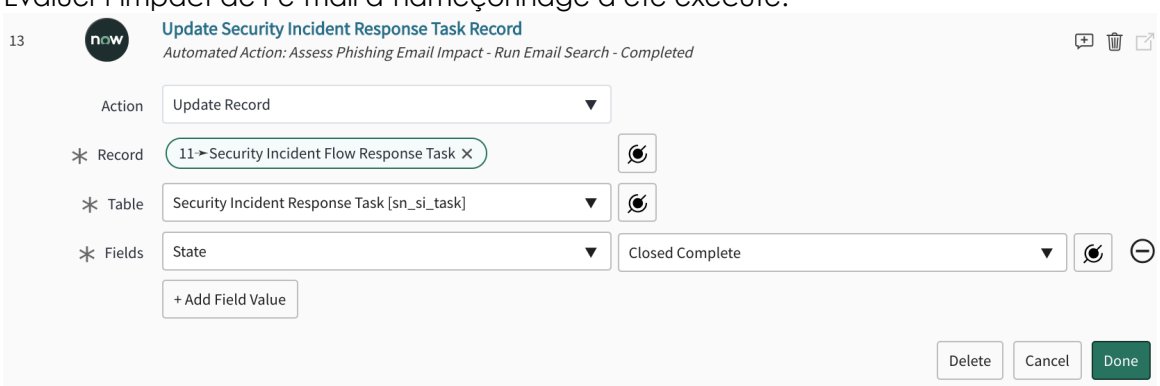
15. L'étape 11 est une tâche de réponse automatisée qui capture le début et la fin de la tâche utilisée pour évaluer l'impact des e-mails d'hameçonnage.



16. À l'étape 12, le flux secondaire Évaluer l'impact de l'e-mail d'hameçonnage est appelé. Ce flux secondaire est utilisé pour rechercher les utilisateurs qui ont reçu l'e-mail d'hameçonnage à l'aide d'implémentations prises en charge.



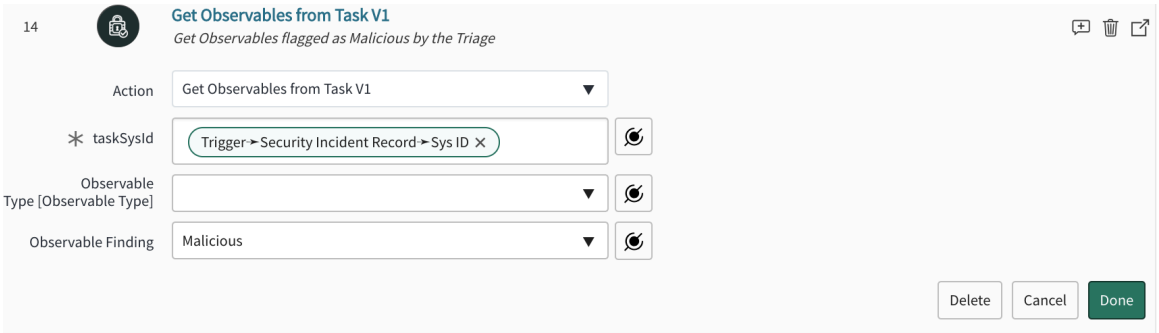
17. À l'étape 13, la tâche est marquée comme fermée pour indiquer que le flux secondaire Évaluer l'impact de l'e-mail d'hameçonnage a été exécuté.



18. L'étape 14 permet de récupérer tous les observables marqués comme malveillants.

Traduction automatique

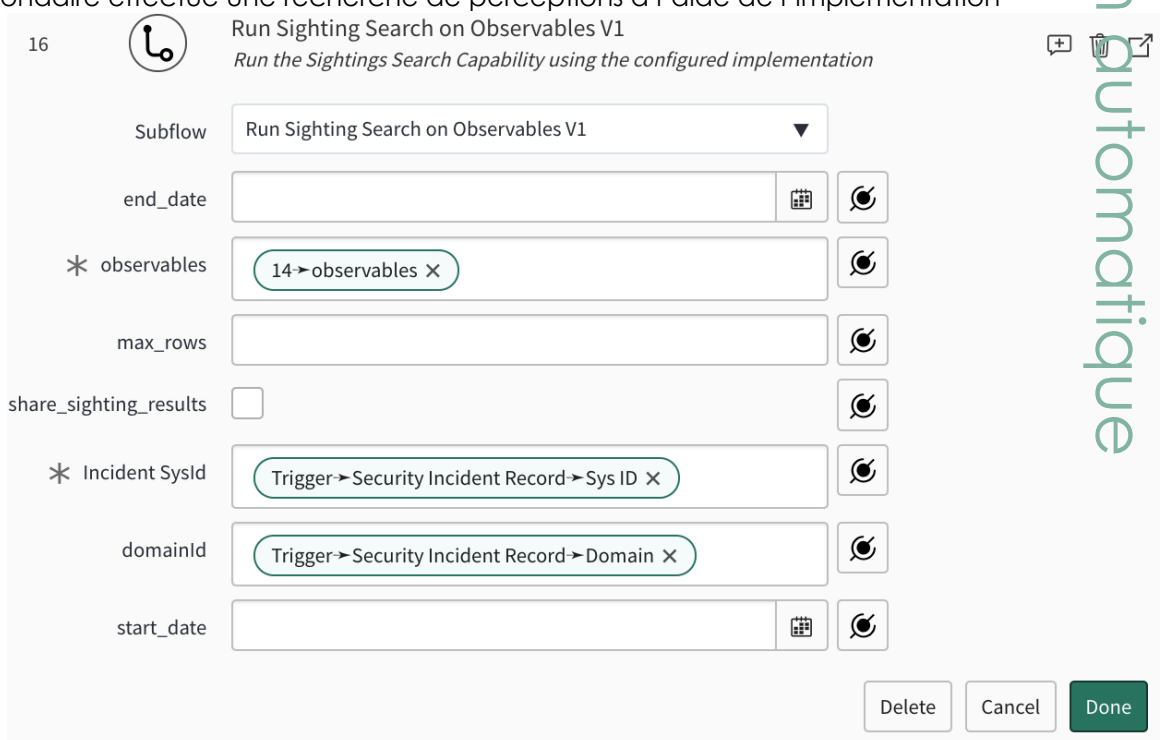
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



19. L'étape 15 est une tâche de réponse automatisée qui capture le début et la fin de la tâche de recherche de perception des observables.



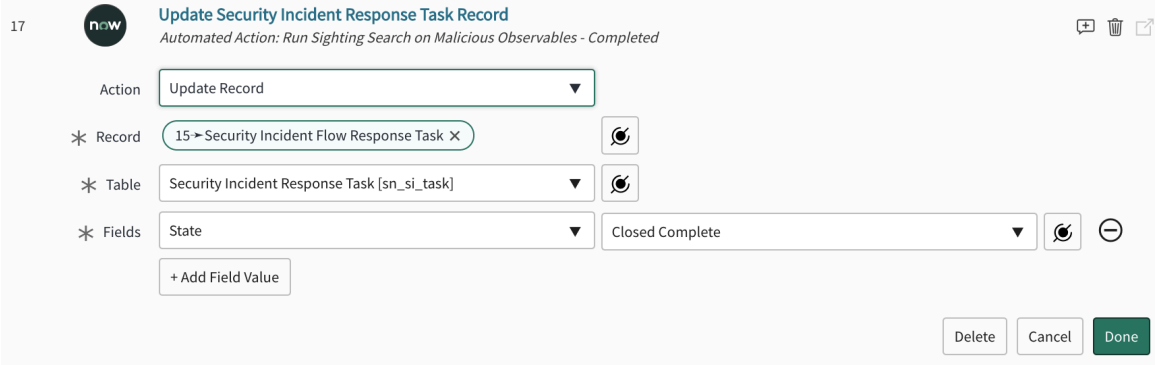
20. À l'étape 16, le flux secondaire Exécuter la recherche de perceptions sur les observables est appelé.
Ce flux secondaire effectue une recherche de perceptions à l'aide de l'implémentation



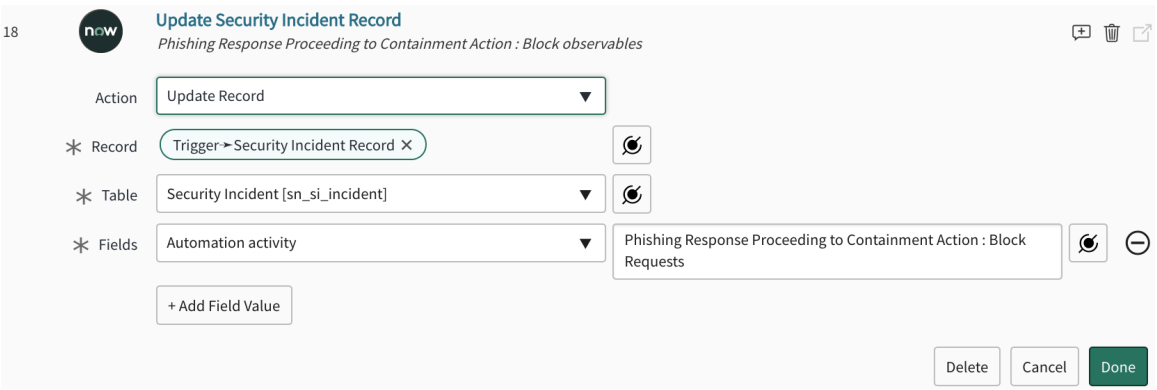
configurée.

21. À l'étape 17, la tâche est marquée comme fermée pour indiquer que le flux secondaire Exécuter la recherche de perceptions sur les observables a été terminé.

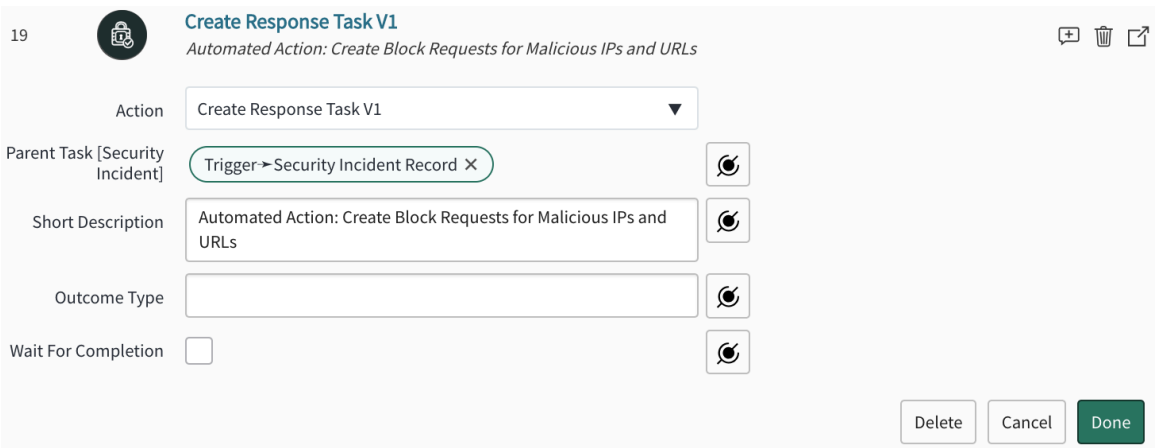
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



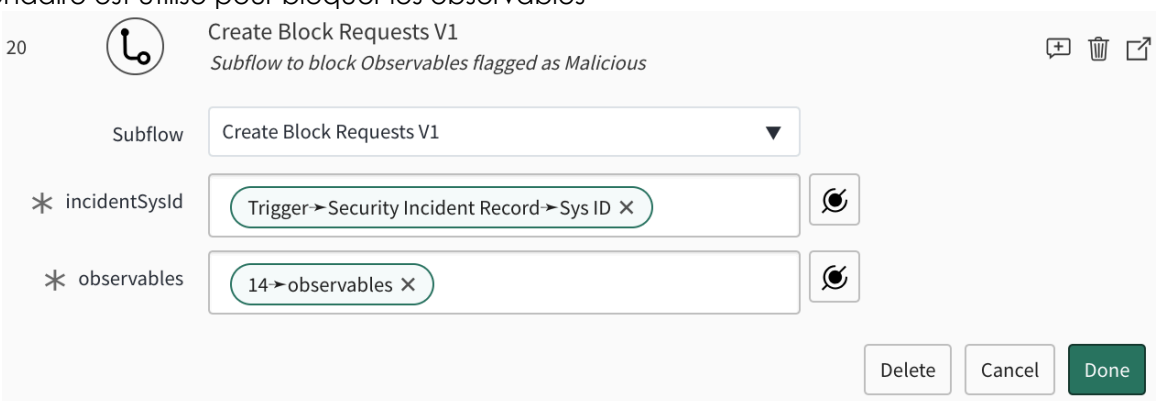
22. Une fois que vous avez identifié les observables malveillants, à l'étape 18, vous mettez à jour l'enregistrement d'incident de sécurité pour indiquer que les actions de confinement vont maintenant commencer.



23. L'étape 19 est une tâche de réponse automatisée qui capture le début et la fin de la tâche de demandes de bloc.



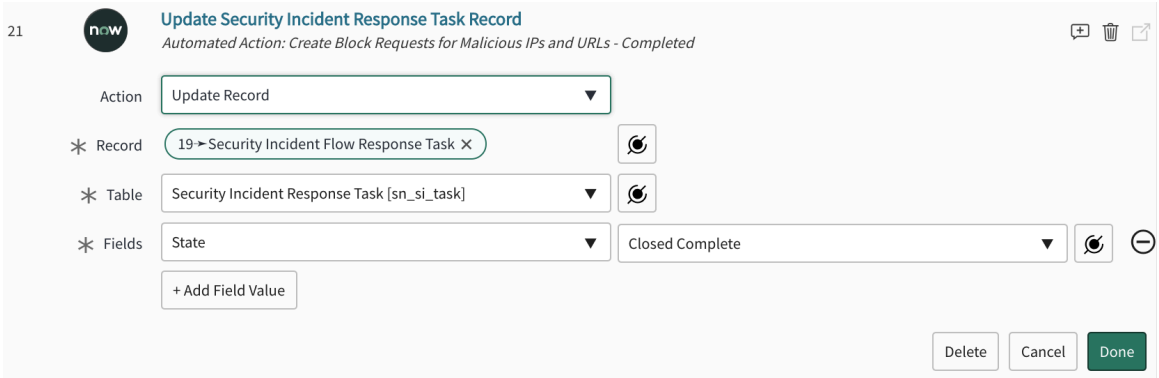
24. À l'étape 20, le flux secondaire Créer des demandes de bloc est appelé. Ce flux secondaire est utilisé pour bloquer les observables malveillants.



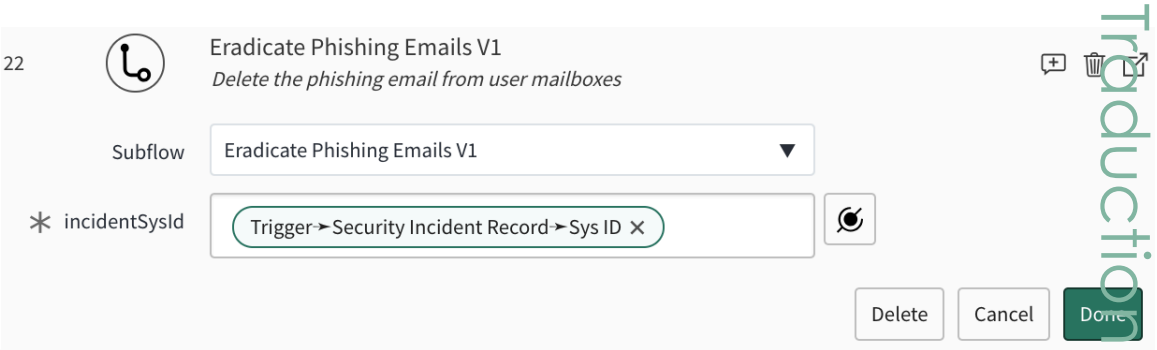
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

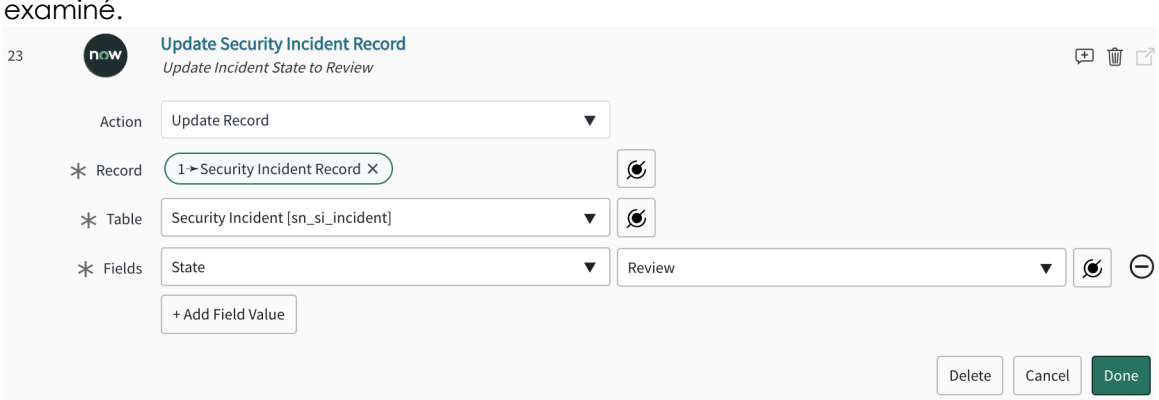
25. À l'étape 21, la tâche est marquée comme fermée pour indiquer que le flux secondaire Créer des demandes de bloc a été terminé.



26. À l'étape 22, le flux secondaire Éradiquer les e-mails d'hameçonnage est appelé. Ce flux secondaire est utilisé pour supprimer les e-mails d'hameçonnage des boîtes aux lettres des utilisateurs.



27. Une fois les e-mails d'hameçonnage supprimés, à l'étape 23, vous mettez à jour l'enregistrement d'incident de sécurité pour indiquer que l'état de l'incident doit être examiné.



28. À la dernière étape, le flux crée une tâche de réponse automatisée. Cette tâche permet d'envoyer un rappel à l'analyste de sécurité pour qu'il enregistre toutes les actions de réponse aux incidents pour des révisions futures.



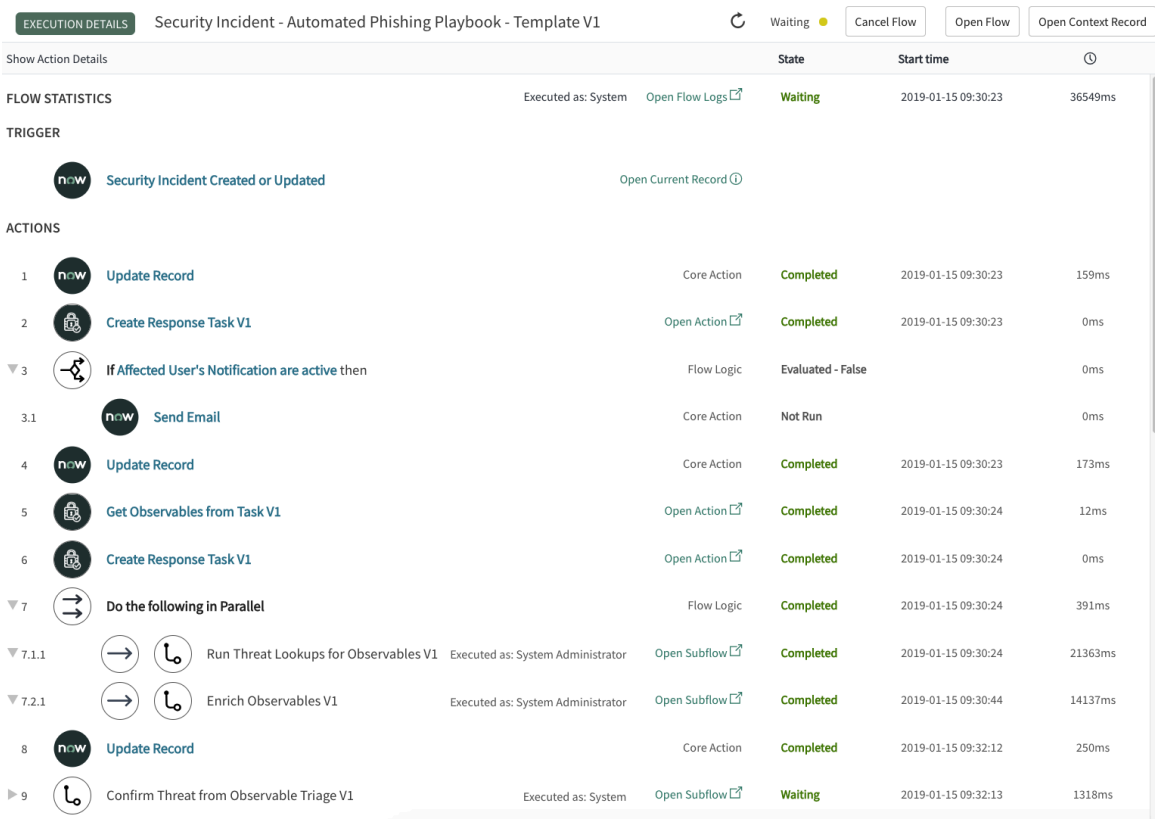
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Vous pouvez cliquer sur **Test** pour simuler les actions dans le flux avant de le publier. Après avoir testé le flux, cliquez sur **Activer** pour activer le flux et l'exécuter.

Cliquez sur **Exécutions** pour afficher les détails de l'exécution du flux.



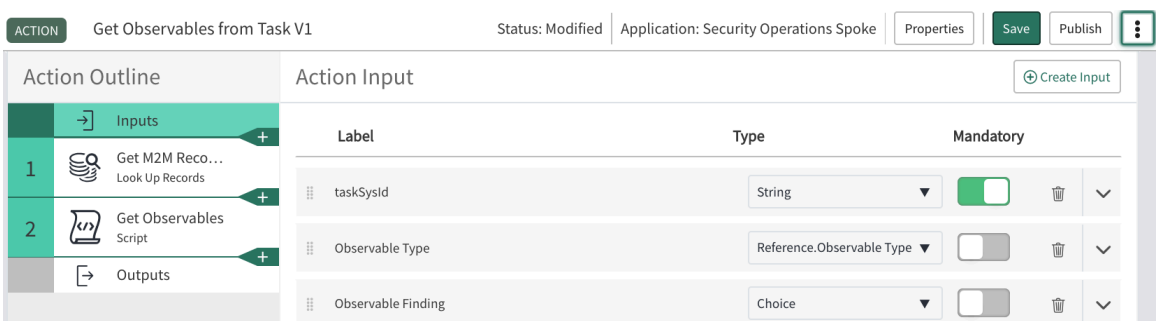
Afficher le flux du playbook de réponse d'hameçonnage automatisé Concepteur d'action

Vous pouvez explorer le concepteur d'action pour afficher des informations détaillées sur les actions effectuées pour une étape spécifique dans le flux du playbook de réponse d'hameçonnage automatisé.

Cette page décrit la page du Concepteur d'action pour l'étape Obtenir des observables à partir de la tâche. Cliquez sur une tâche dans le panneau Plan d'action pour afficher les détails.

Entrées d'action

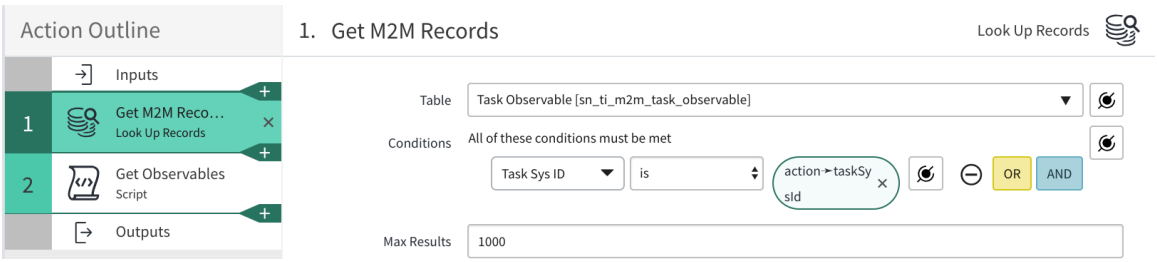
Cette section affiche des détails sur la façon dont l'action a été créée, y compris l'ID de l'incident, le type d'observable (hachage ou adresse IP) et le résultat de l'observable (e-mails malveillants uniquement).



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

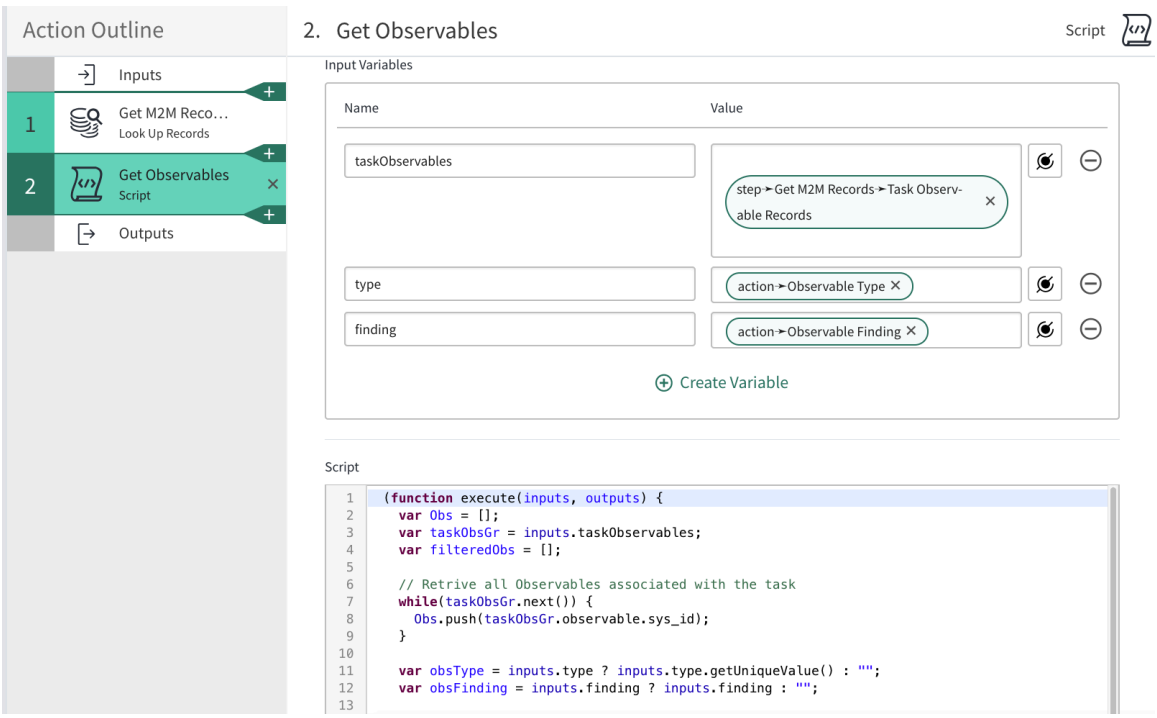
Obtenir les enregistrements N-N

Cette section affiche les conditions qui ont été définies pour rechercher des observables dans une table spécifiée.



Obtenir des observables

Cette section présente le script utilisé pour récupérer les observables en fonction des conditions de filtre spécifiées. Enfin, les observables répondant à ces critères et le nombre sont affichés.



Remarque : Toutes les actions définies dans ce flux sont réutilisables et modifiables en fonction de vos besoins.

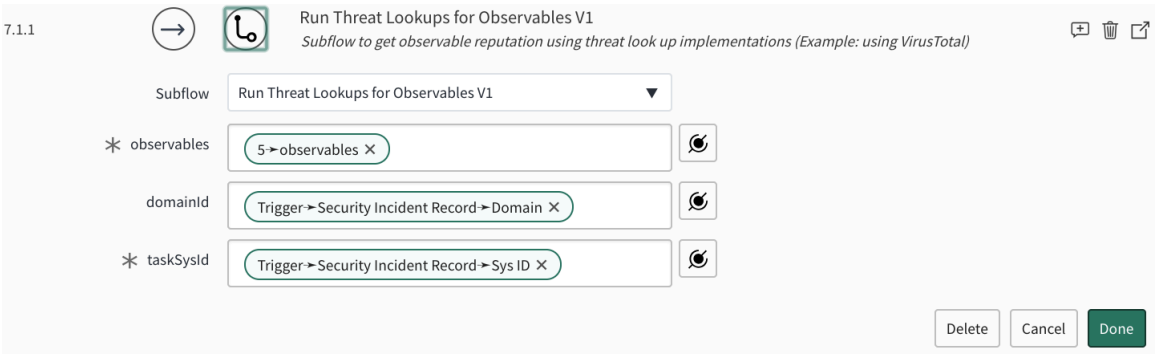
Afficher le playbook de réponse d'hameçonnage automatisé Concepteur de flux secondaires

Vous pouvez explorer le concepteur de flux secondaires pour afficher des informations détaillées sur le flux secondaire en cours d'exécution dans le cadre du flux du playbook de réponse d'hameçonnage automatisé.

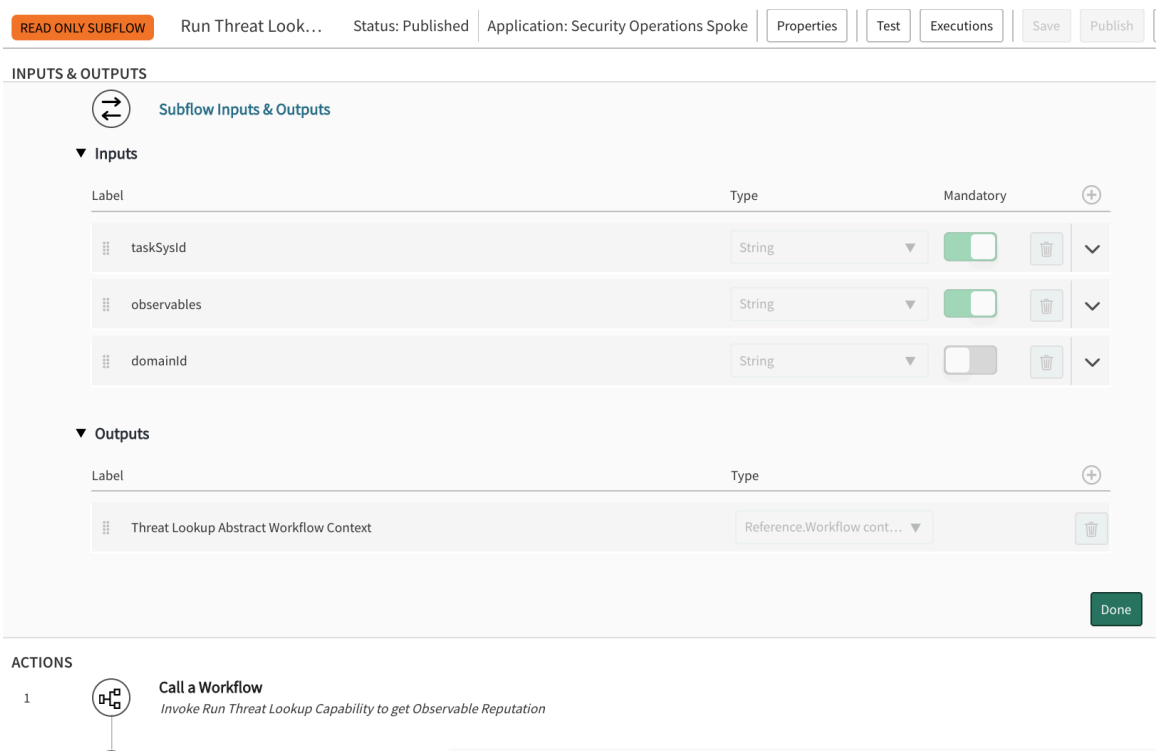
Vous pouvez lancer le concepteur de flux secondaires pour afficher les détails supplémentaires d'un flux secondaire. La page Concepteur de flux secondaires pour le flux secondaire Exécuter des recherches de menace pour les observables s'affiche ici. Cliquez sur l'icône du secondaires dans l'image ci-dessous pour afficher le concepteur de flux secondaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Dans la page Concepteur de flux secondaires, vous pouvez voir les entrées et sorties de ce flux secondaire, ainsi que les actions de workflow sous-jacentes en cours d'exécution.



Remarque : Ce flux secondaire est en lecture seule et ne peut pas être modifié. Vous pouvez ajouter ou supprimer des flux secondaires à l'étape, mais vous ne pouvez pas modifier le flux secondaire.

Playbook pour les programmes malveillants automatisés

Le Playbook de programme malveillant automatisé fournit une séquence d'étapes automatisées qui vous aide à résoudre les alertes de programme malveillant rapidement et efficacement.

Utilisez le flux du playbook de programme malveillant pour automatiser les étapes impliquées dans la gestion des alertes de programme malveillant provenant du point de terminaison ou du réseau. Le modèle de flux comprend des conditions de déclenchement, une séquence d'actions et des flux secondaires annotés à des fins de lisibilité.

Ces modèles contiennent une séquence d'actions réutilisables conçues pour répondre aux attaques de hameçonnage. Chaque flux dispose d'un déclencheur (condition), d'une séquence d'actions et de flux secondaires annotés pour plus de lisibilité. Pour accéder à ces flux, vous devez installer lespoke Security Operations et l'application Security Operations Palo Alto Networks - WildFire à partir du ServiceNow Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous devez activer ces modèles avant de pouvoir les utiliser.

Les flux et flux secondaires suivants sont inclus :

- Incident de sécurité - Automated Malware Playbook Modèle : ce modèle est conçu pour automatiser les réponses aux alertes de programme malveillant et contient une séquence d'actions, y compris un déclencheur.
- Incident de sécurité - Programme malveillant Modèle manuel : ce modèle est le workflow de réponse manuelle aux programmes malveillants qui est activé lorsque la catégorie est définie sur Activité du code malveillant.

Flux secondaires

- Confirmer la menace à partir de l'observable : vérifie si l'observable est malveillant et doit être traité.
- Définir la gravité de l'incident : définit l'état de gravité de l'incident.
- Playbook de rançongiciel : détermine s'il s'agit d'une attaque de rançongiciel.

Ces flux secondaires représentent un ensemble d'opérations réutilisables qui peuvent être utilisées dans plusieurs playbooks. Vous pouvez utiliser ces flux secondaires pour définir des modèles personnalisés (flux) en fonction de vos besoins.

Pour créer des modèles personnalisés (flux), suivez les instructions de la section Flux .

Exécuter le flux automatisé du playbook de programme malveillant

Utilisez ce flux pour automatiser les tâches dans le playbook afin d'analyser et de résoudre les attaques de programmes malveillants contre votre organisation.

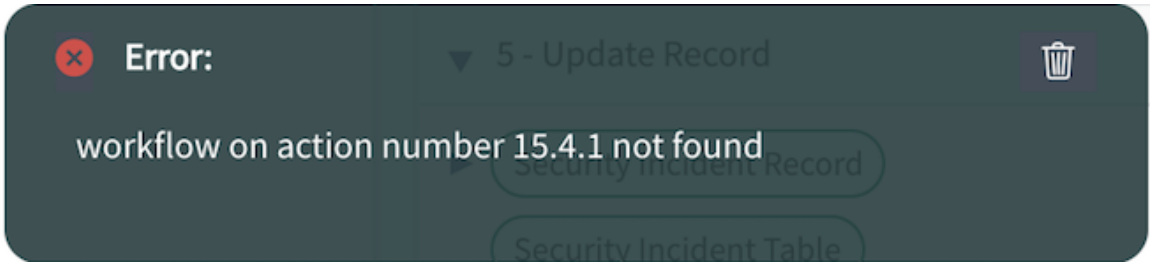
Avant de commencer

- Rôle requis : sn_si.admin, flow_designer et action_designer
- Installez et configurez les intégrations suivantes avec les informations d'identification correctes :
  - Palo Alto Networks WildFire pour les opérations de sécurité
  - Recherche de perception (Splunk)
  - Demandes de blocs
  - Recherche de menace
  - Enrichir les observables

  Vérifiez que ces intégrations fonctionnent correctement avant d'activer le modèle de playbook Incident de sécurité - Automated Malware.

- Application Security Operations Palo Alto Networks Wildfire : pour accéder au flux automatisé du playbook de logiciels malveillants, vous devez installer l'application Security Operations Spoke et Security Operations Palo Alto Networks - WildFire à partir du ServiceNow Store. Si l'application Security Operations Palo Alto Networks Wildfire n'est pas installée, vous verrez une erreur « workflow sur l'action numéro 15.4.1 introuvable » comme indiqué ci-dessous :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Si vous ne souhaitez pas installer cette application, supprimez les étapes **15.2, 15.3 et 15.4** du flux automatisé du playbook de programmes malveillants.

- Assurez-vous que les conditions suivantes sont remplies :
  - L'incident de sécurité a été affecté à un analyste de sécurité qui appartient au groupe d'approbation approprié.
  - L'analyste de sécurité qui gère l'incident doit avoir une adresse e-mail valide.
  - Les éléments de configuration et observables nécessaires ont été ajoutés à l'incident de sécurité.
- Pour **l'étape 21 (Demander l'approbation)**, modifiez le groupe **d'Affectation d'incident de sécurité** à votre groupe préféré.
- L'étape 21 du flux est une étape d'approbation de tâche obligatoire au cours de laquelle une demande d'approbation est envoyée à l'administrateur. Pour approuver la demande, l'administrateur doit accéder à la page Approbations de tâches et définir le champ État sur **Approuvé**. Si la tâche n'est pas approuvée, le concepteur de flux ne peut pas continuer et le processus se termine.

Pourquoi et quand exécuter cette tâche

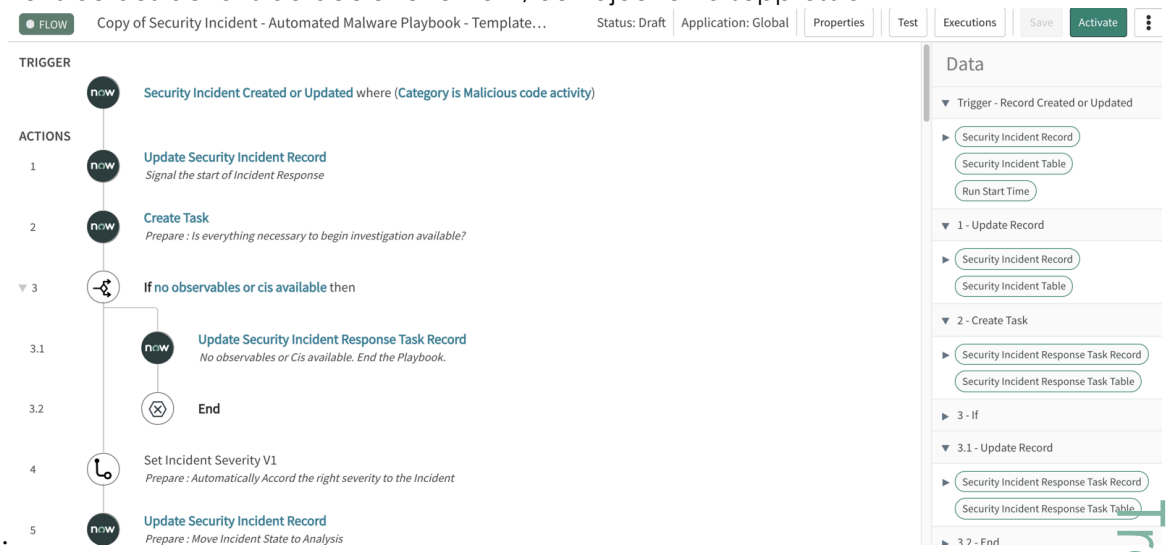
Lorsqu'une activité de code malveillant est détectée sur le réseau, un incident de sécurité est créé et le flux automatisé du playbook de programme malveillant est lancé. Vous pouvez utiliser les tâches définies dans le flux automatisé du playbook de programme malveillant pour trier, analyser, contenir et éradiquer la menace.

Procédure

1. Accédez à la **Tout** > **Concepteur de flux** > **Concepteur** pour afficher les flux disponibles avec le spoke Security Operations.
2. Cliquez sur le lien **Security Incident - Automated Malware Playbook Template VI (Incident de sécurité - Playbook de programme malveillant automatisé).**
3. Sur la page Flux, cliquez sur l'icône , faites une copie du flux et ouvrez-la pour votre utilisation.

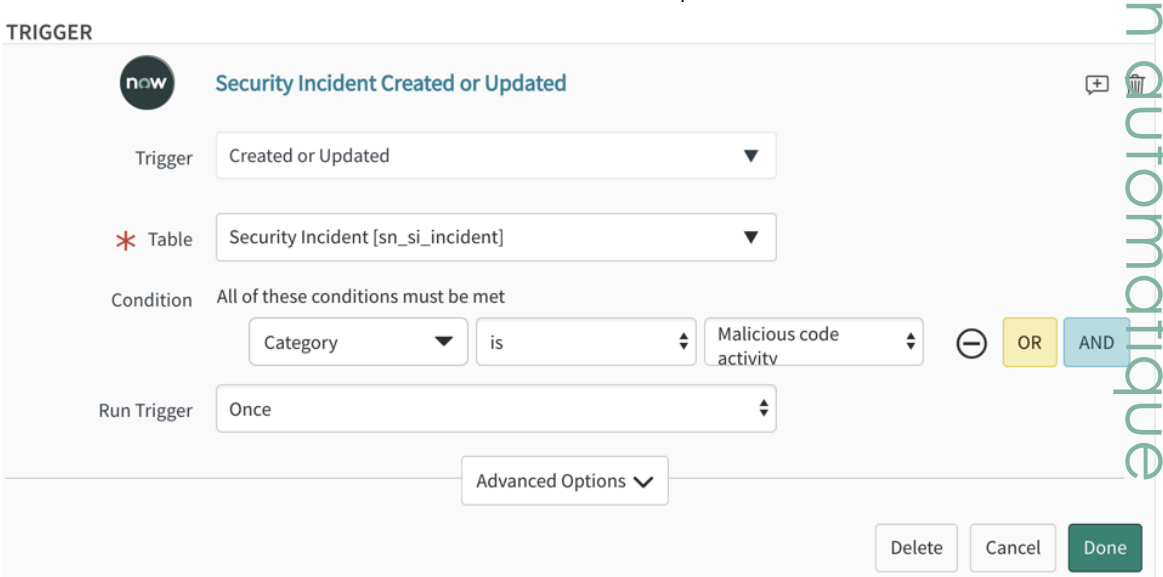
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez maintenant apporter des modifications à votre flux, telles que la modification des conditions ou des actions de déclenchement, ou l'ajout et la suppression d'actions.



Cela montre le déclencheur et les étapes qui seront exécutées avec le flux. Le panneau de droite montre le flux de données. Cliquez sur une icône pour développer l'étape et afficher les détails.

4. Cliquez sur l'icône **Déclencheur** .
Dans un premier temps, vous définissez ou définissez le déclencheur du flux. Spécifiez les conditions du déclencheur et de la tâche à exécuter lorsque les conditions sont remplies.

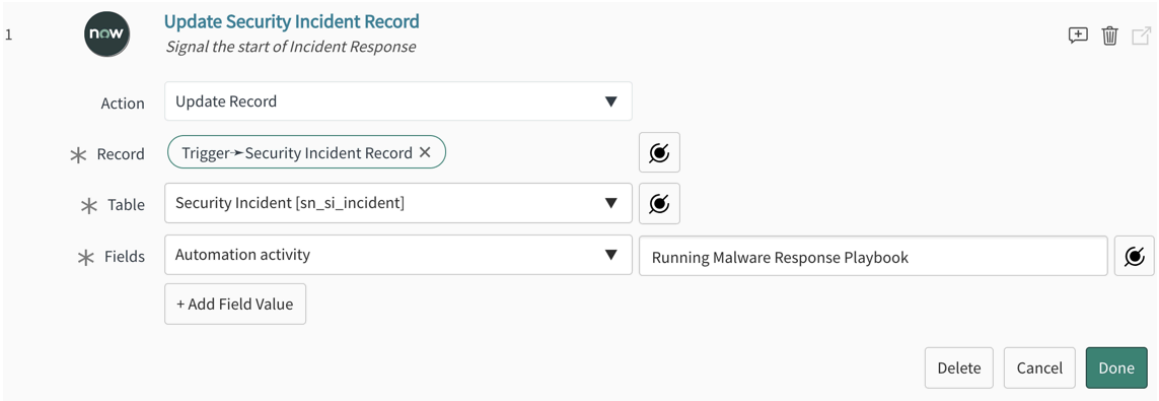


Lorsque la condition définie dans le flux (la catégorie est Activité de code malveillant) est remplie dans l'enregistrement d'incident, les tâches du flux d'hameçonnage automatisé commencent à s'exécuter séquentiellement. Vous pouvez modifier le déclencheur, ajouter des annotations, ajouter ou supprimer des conditions, etc.

5. La première étape du flux est **Mettre à jour l'enregistrement d'incident de sécurité**.

Traduction automatique

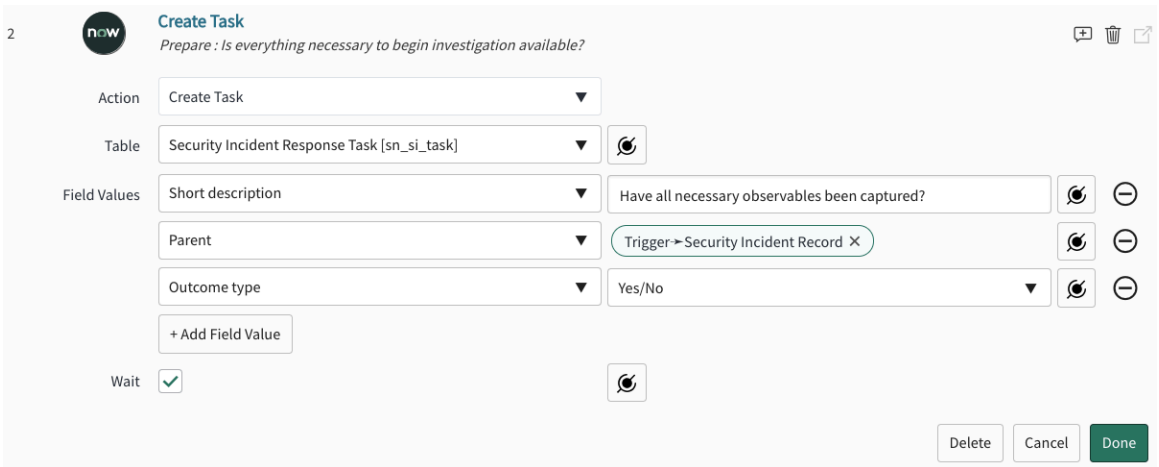
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cliquez sur le lien, puis cliquez sur l'icône d'annotation pour ajouter une note à l'analyste de sécurité indiquant qu'il y a eu une activité de code malveillant et que le flux automatisé du playbook de réponse aux programmes malveillants a commencé à s'exécuter.

6. Poursuivez avec l'étape 2 dans le flux et cliquez sur le lien **Créer une tâche** .

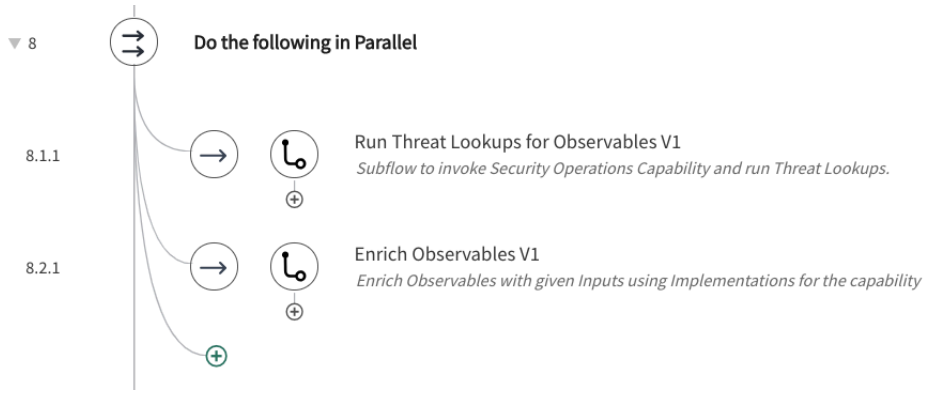
   Dans cette étape, une tâche de réponse automatisée est créée pour vérifier si tous les observables nécessaires ont été capturés et si l'enquête peut commencer.



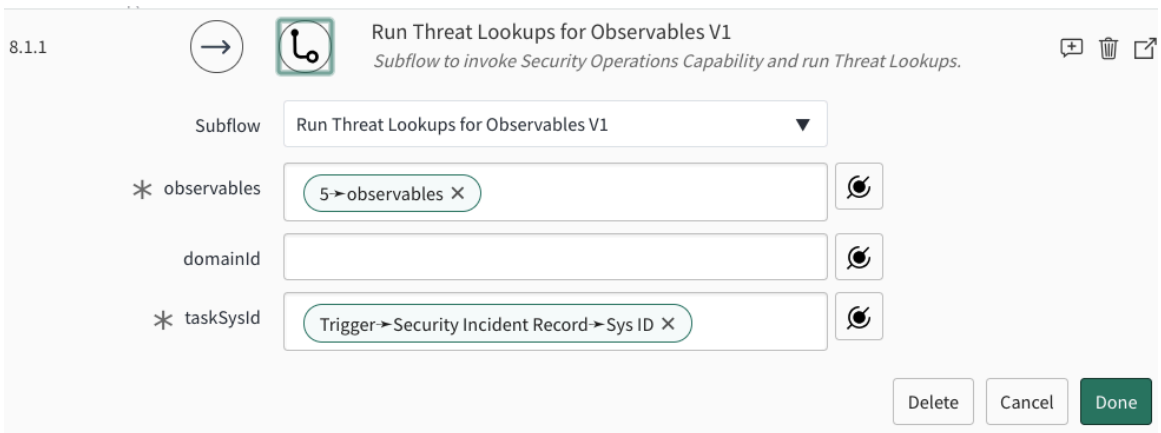
7. Si le type de résultat est **Non**, cela indique qu'aucun observable et CI n'est disponible pour lancer l'enquête.
   Mettez à jour l'enregistrement d'incident de sécurité pour indiquer que le playbook ne peut pas continuer.
8. Si le type de résultat est **Oui**, le flux secondaire Définir la gravité de l'incident affecte automatiquement la gravité correcte à l'incident de sécurité.
9. À l'étape suivante, l'enregistrement d'incident de sécurité est mis à jour.
10. À l'étape suivante, tous les observables impliqués dans l'incident ou dans une catégorie sélectionnée sont collectés pour effectuer des actions automatisées supplémentaires dans les étapes suivantes du playbook.
11. À l'étape suivante, une tâche de réponse automatisée est créée.
    Cette tâche capture le début du processus d'obtention de la réputation de tous les observables et d'exécution de l'enrichissement avec des intégrations configurées.
12. À l'étape 8, deux flux secondaires sont appelés :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Exécuter des recherches de menace pour les observables : ce flux secondaire est utilisé pour obtenir la réputation de tous les observables à l'aide d'implémentations de recherche de menace.
- Enrichir les observables : ce flux secondaire permet d'enrichir les observables avec les implémentations configurées.



Remarquez les icônes de cette tâche. L'icône indique que les deux tâches seront exécutées en parallèle et l'icône de flux secondaire indique que la tâche en cours d'exécution est un flux secondaire, comme indiqué ci-dessous :



Notez le chiffre 5 dans le champ des observables. Cela indique que la recherche de menace sera exécutée sur les observables récupérés à l'étape 5. Ce flux secondaire appelle à son tour les workflows et les actions existants.

13. À l'étape suivante, l'action Exécuter la recherche d'enregistrements est exécutée. Cette action est utilisée pour rechercher des enregistrements de contexte de workflow dans lesquels le workflow parent peut être l'un des suivants.
    - Contexte de workflow abstrait de la recherche de menace
    - Contexte de workflow abstrait d'enrichissement d'observable
14. À l'étape suivante, les résultats de réputation et d'enrichissement sont examinés tous les 8 enregistrements.
15. Passez en revue les étapes suivantes :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Mettre à jour l'enregistrement d'incident de sécurité : met à jour l'enregistrement d'incident de sécurité pour indiquer que les activités de recherche et d'enrichissement de réputation sont terminées.

b. Obtenir les observables à partir de la tâche : récupère tous les observables malveillants associés à l'incident de sécurité.

c. Créer une tâche : vérifie et confirme si les exécutions de triage automatisées ont réussi.

16. Si des observables ont été marqués comme malveillants :

a. Mettre à jour l'enregistrement d'incident de sécurité : publiez une note de travail indiquant qu'une menace a été détectée.

b. Créer une requête d'entrée à partir d'observables : si plus de dix observables ont été marqués comme malveillants, le flux secondaire Recherche de perception sur les observables (sur Splunk ou Carbon Black) est exécuté.

17. Si les observables ne sont pas marqués comme malveillants, le flux continue avec les étapes suivantes :

a. Mettre à jour l'enregistrement d'incident de sécurité : publier une note de travail indiquant qu'aucune menace n'a été détectée

b. Obtenir des observables à partir de la tâche : identifie tous les ID de hachage SHA256 de l'incident.

c. Rechercher les enregistrements d'observables : recherche les enregistrements qui répondent à ces critères.

18. Passez en revue les étapes suivantes :

a. Pour chaque observable malveillant, le workflow **Security Operations Palo Alto Networks - Get Wildfire Data Enrichment** est exécuté.

b. Examine les résultats de l'enquête pour voir s'ils sont satisfaisants.
Une tâche de réponse est créée pour vérifier si le programme malveillant suspecté est une attaque de rançongiciel. Si c'est le cas, le flux secondaire Playbook de rançongiciel est exécuté.

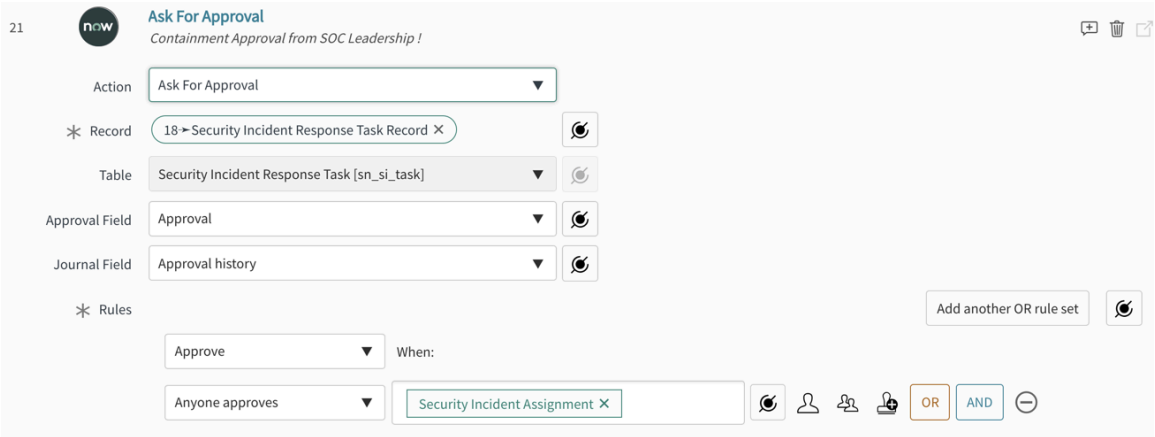
c. À l'étape suivante, un e-mail contenant un résumé de l'analyse et une demande d'approbation pour lancer les procédures de confinement est envoyé.

d. Une tâche est créée pour capturer les détails de l'approbation demandée.

e. L'étape suivante consiste à mettre à jour l'enregistrement d'incident de sécurité. Publiez une note de travail informant l'analyste de sécurité que la demande d'approbation a été effectuée.

f. Demande l'approbation de votre responsable SOC pour contenir les attaques de programme malveillant.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Lorsqu'une demande d'approbation est générée par le flux, la note de travail est mise à jour avec le message suivant :

`Une demande d'approbation a été effectuée pour <ID de tâche> en poursuivant le confinement.` Pour approuver cette tâche, en tant que gestionnaire SOC, procédez manuellement comme suit :

- Accédez à la page Approbations de tâches.
- La liste des approbations s'affiche. Cliquez sur l'< ID de tâche > à approuver.
- Changez l'état sur **Approuver** et enregistrez le <ID de tâche> mis à jour.

g. À l'étape suivante, l'enregistrement d'incident de sécurité est mis à jour pour suivre l'état d'approbation.

h. Ensuite, une tâche est créée pour initier les procédures de confinement.

i. Le flux secondaire Exécuter le flux secondaire Créer des demandes de bloc pour les observables malveillants est exécuté et un enregistrement d'incident est créé avec une demande de reconstruction de l'appareil infecté et de ses actifs.

j. Ensuite, une tâche est créée pour exécuter la recherche de perceptions afin de confirmer si l'environnement est sécurisé.
La recherche d'observations est répétée jusqu'à ce qu'aucune observation ne soit trouvée.

k. Ensuite, une tâche est créée pour indiquer que l'enregistrement d'incident de sécurité est prêt à être examiné.

l. Enfin, l'enregistrement est mis à jour et passé à l'étape Revue.

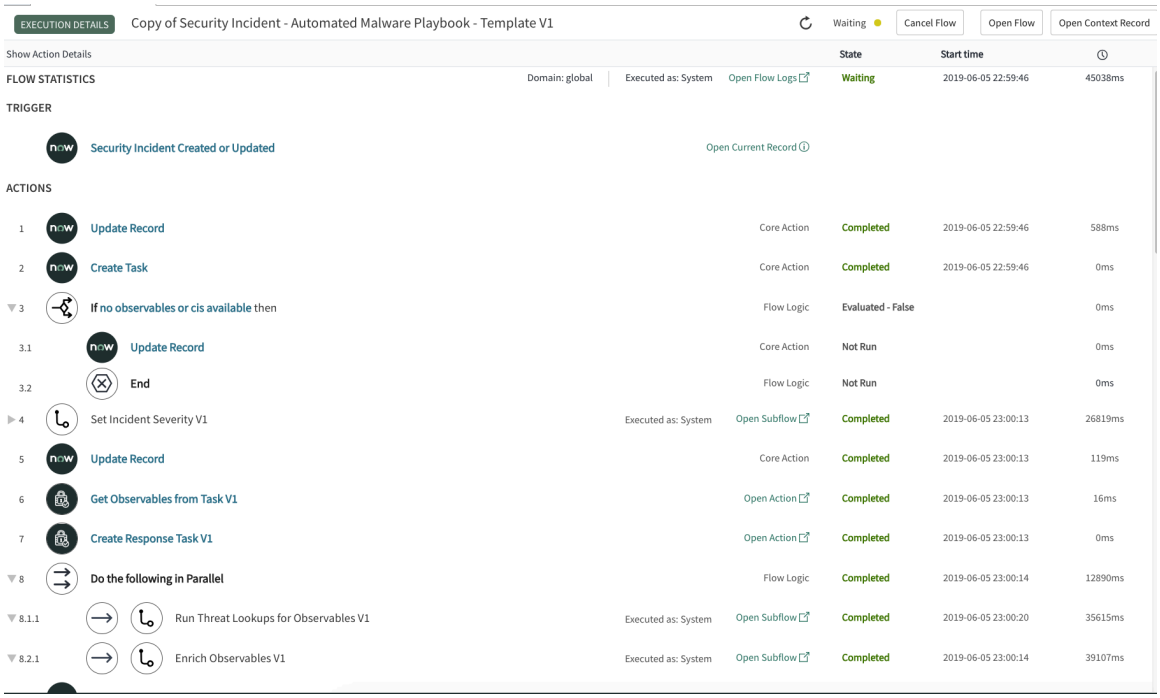
Que faire ensuite

Vous pouvez cliquer sur **Test** pour simuler les actions dans le flux avant sa publication. Après avoir testé le flux, cliquez sur **Activer** pour activer le flux afin qu'il puisse être exécuté.

Cliquez sur **Exécutions** pour afficher les détails de l'exécution du flux.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Playbook pour Échec de connexion manuelle

Lorsqu'un utilisateur effectue certaines tentatives de connexion infructueuses (conformément à la configuration de la carte SIM), un incident de sécurité est créé.

Ces tentatives de connexion infructueuses peuvent être des faux positifs ou des tentatives effectuées par des attaquants pour obtenir l'accès aux comptes de messagerie des utilisateurs. Dans de tels scénarios, le playbook Manuel d'échec de connexion peut fournir des conseils et aider à optimiser l'enquête sur les incidents de sécurité liés à l'échec de connexion.

Prérequis

Rôle requis :

- sn_si.admin
- flow_designer

Spoke : installer le spoke Security Operations (sn_sec_spoke)

Principales options

Le playbook Échec de la connexion couvre les options suivantes pour enquêter sur les incidents de sécurité :

1. Vérifie si l'utilisateur affecté est un utilisateur actif/inactif
2. Filtre les éléments observables sur la liste des éléments autorisés
3. Enrichit les observables
4. Effectue une recherche de menace automatisée.
5. Envoie un e-mail automatisé à l'utilisateur pour confirmer l'échec de la tentative de connexion.
6. Affecte des tâches à l'analyste pour examiner l'accès des utilisateurs
7. Identifie les observables malveillants et bloque les adresses IP et les URL.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Réinitialise le mot de passe utilisateur.
9. Met à jour l'état des incidents de sécurité
10. Affecte des tâches à un analyste de sécurité pour gérer l'examen post-incident.

Options requises

- Recherche de menace (Total virus, Hybrid Analysis)
- Enrichissement des observables (Whois, ReverseWhois)
- Recherche de perception (Splunk, QRadar)
- Blocage d'observables (CheckPoint, Palo Alto)

Pour plus d'informations, consultez le ServiceNow Store .

Expérience d'analyste de sécurité

Pour comprendre comment résoudre les menaces de sécurité étape par étape, reportez-vous à la section Résoudre les menaces de sécurité avec le playbook.

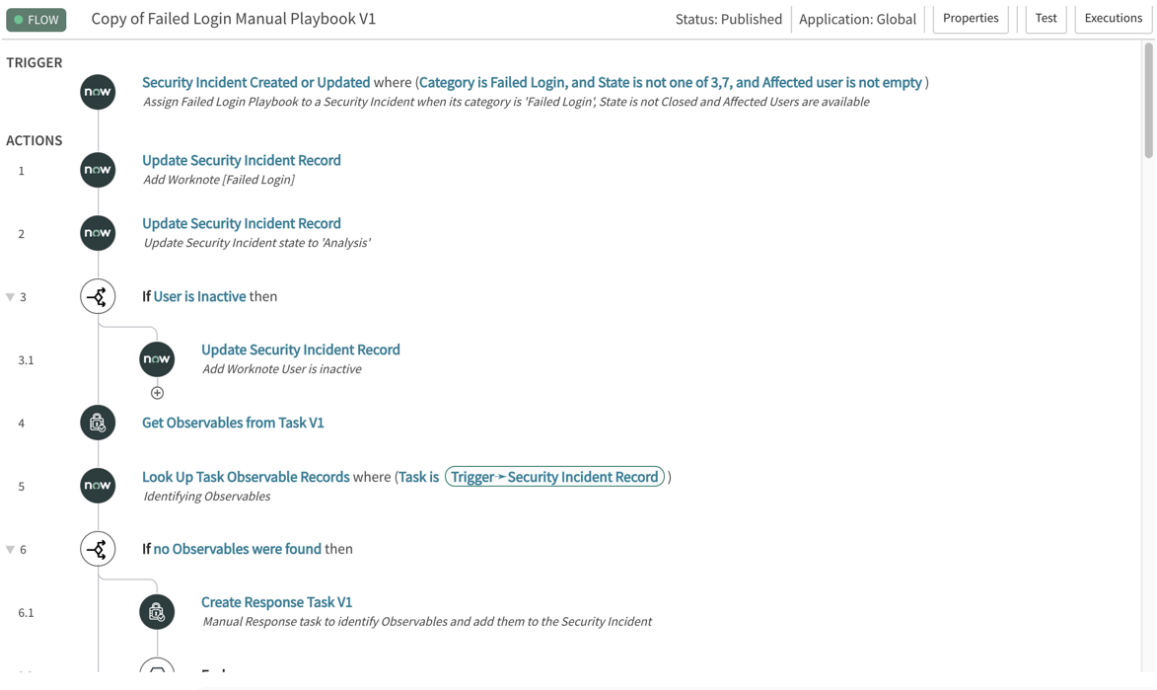
Utilisation du playbook en cas d'échec de connexion avec les options de Flow Designer

Mise en route

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Concepteur de flux** > **Concepteur** et cliquez sur le playbook **Échec de la connexion** .
3. Faites une copie des flux suivants pour copier le Playbook de connexion échouée et apportez les modifications nécessaires. (Il s'agit d'une étape facultative. Suivez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des modifications spécifiques au flux.
   - Échec de la connexion manuelle à Playbook V1
   - Échec de la connexion : analyser la réponse de l'utilisateur et mettre à jour la tâche de réponse V1
4. Apportez les modifications nécessaires en fonction de vos besoins. (Il s'agit d'une étape facultative. Suivez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des modifications spécifiques au flux.
5. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible avec le système de base.
   - Activez les flux copiés après avoir apporté des modifications en fonction de vos besoins.

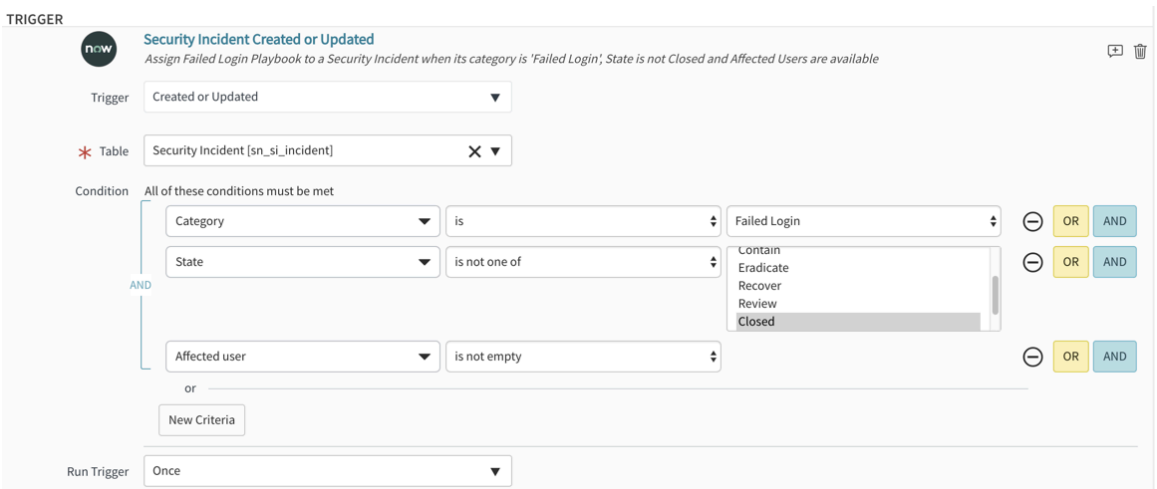
L'image suivante montre une copie du playbook Manuel d'échec de la connexion. Passez en revue les étapes ci-dessous pour mieux comprendre les différentes actions du playbook.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :

- La catégorie est Échec de la connexion
- A un ou plusieurs utilisateurs affectés
- L'incident de sécurité n'est ni fermé ni annulé

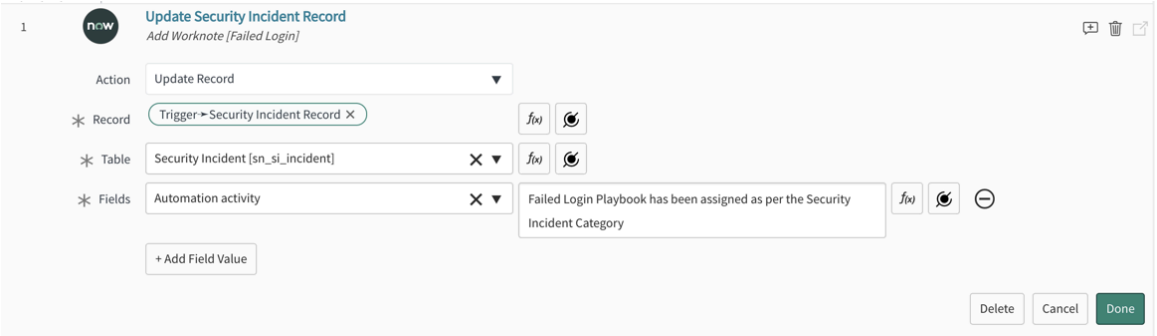


Les étapes suivantes vous guident à travers les actions, les tâches et les flux secondaires disponibles dans le playbook Échec de la connexion manuelle.

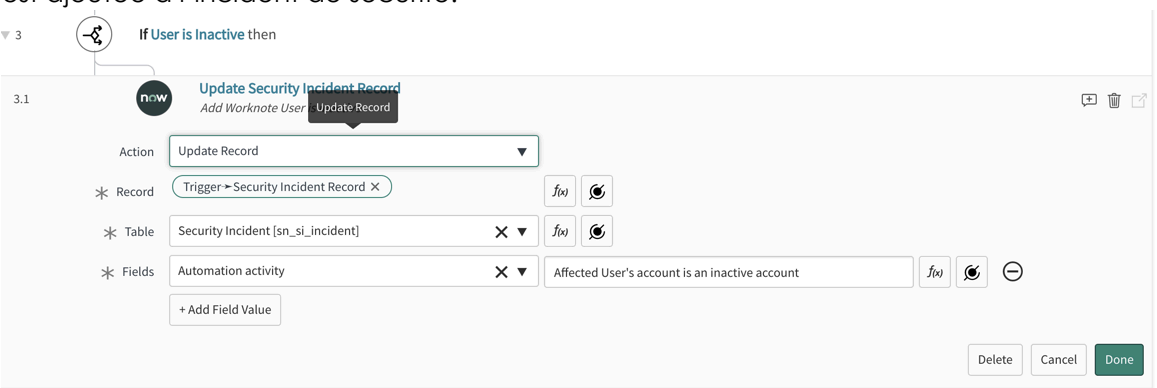
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Lorsque le playbook commence à s'exécuter, à l'étape 1, le playbook est automatiquement mis à jour avec une note de travail indiquant l'incident de sécurité avec la catégorie d'échec de connexion a été affectée.



2. À l'étape 2, le playbook est mis à jour et passé à l'état Analyse.
3. À l'étape 3, le playbook vérifie si l'utilisateur affecté est un utilisateur actif ou inactif. Si l'utilisateur est inactif, une note de travail indiquant que le compte d'utilisateur est inactif est ajoutée à l'incident de sécurité.



Remarque : À l'étape 3 du flux, le flux vérifie les utilisateurs inactifs dans la *table sn_si_incident* disponible dans ServiceNow. Cette étape est fournie à titre indicatif et doit être modifiée pour votre environnement spécifique. Si vous souhaitez utiliser cette fonctionnalité, nous vous recommandons d'avoir configuré une intégration Active Directory dans votre environnement. Vous pouvez vérifier auprès de votre intégration Active Directory pour trouver l'état de l'utilisateur et, en fonction de la réponse, vous pouvez concevoir les étapes suivantes pour votre playbook.

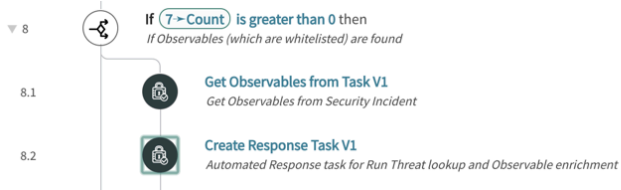
Si vous n'avez pas d'intégration Active Directory, remplacez cette étape par une tâche manuelle pour que l'analyste de sécurité travaille avec l'équipe informatique pour bloquer l'utilisateur et passer aux autres étapes du playbook.

4. À l'étape 4, les observables de l'incident de sécurité sont récupérés.
5. À l'étape 5, les observables sont identifiés.
6. Si aucun observable n'est trouvé, une tâche de réponse manuelle est créée à l'étape 6 et le flux se termine.

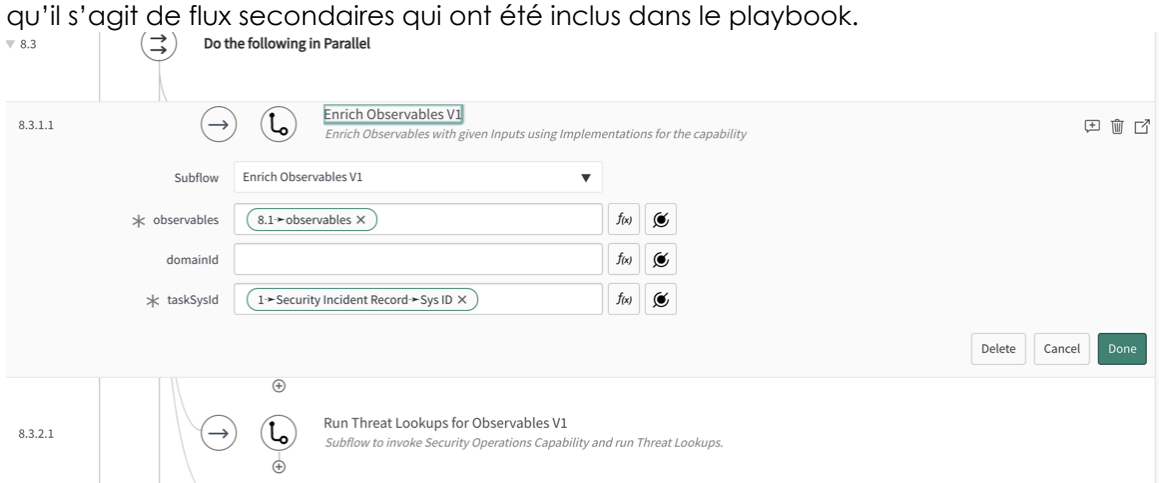
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Si des observables sont trouvés à l'étape 7, les observables qui ne figurent pas sur la liste d'autorisation sont identifiés.
8. Si au moins un des observables n'est pas autorisé dans la liste, les étapes suivantes sont exécutées :
   a. Les étapes 8.1 et 8.2 sont exécutées. Les observables sont récupérés et une tâche de réponse automatisée est lancée.



   b. Une fois la tâche automatisée créée, l'étape 8.3 (8.3.1.1 et 8.3.2.1) est exécutée et les intégrations Enrichir les observables et Recherche de menace sont exécutées. Notez qu'il s'agit de flux secondaires qui ont été inclus dans le playbook.



   c. À l'étape 8.4, une fois les intégrations terminées, l'enregistrement d'incident de sécurité est mis à jour.
   d. À l'étape 8.5, une nouvelle tâche de réponse est créée pour indiquer la prochaine tâche automatisée qui aura lieu.
   e. À l'étape 8.6, l'intégration de la recherche de perception sera exécutée sur les observables.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



f. Une fois le flux secondaire de recherche de perception terminé, à l'étape 8.7, l'incident de sécurité est mis à jour.

g. À l'étape 8.8, les observables sont vérifiés pour voir s'ils sont malveillants.

h. Si les observables ne sont pas malveillants et si le compte utilisateur est actif, un e-mail automatisé est envoyé à l'utilisateur pour reconfirmer les tentatives de connexion infructueuses. Une tâche de réponse manuelle est créée pour identifier les observables et les ajouter à l'incident de sécurité. Le playbook se termine alors à cette étape.

i. Si les observables sont malveillants, trois tâches de réponse sont créées :

i. Un e-mail automatisé est envoyé à l'utilisateur pour confirmer **(Oui ou Non)** les tentatives de connexion infructueuses. Si l'utilisateur répond Oui :

1. L'état de l'incident de sécurité est mis à jour à **Maîtriser**.

2. Un e-mail automatisé est envoyé à l'utilisateur pour réinitialiser le mot de passe.

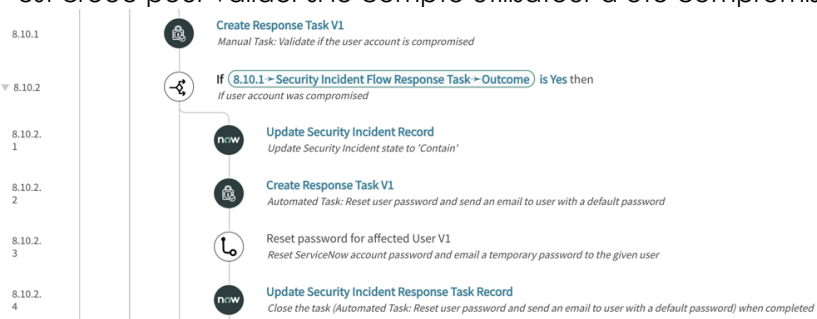
3. Le flux secondaire de réinitialisation du mot de passe est initié et un e-mail est envoyé à l'utilisateur lorsque la tâche est terminée.

Remarque : L'étape Réinitialiser le mot de passe est fournie à titre indicatif. Les étapes du flux réinitialisent le mot de passe du compte de l'utilisateur dans le système ServiceNow. Mais le processus de réinitialisation du mot de passe peut être différent en fonction de votre environnement. Vous pouvez vérifier avec votre intégration Active Directory pour réinitialiser automatiquement le mot de passe des utilisateurs. Si vous n'avez pas d'intégration Active Directory, remplacez cette étape par une tâche manuelle pour que l'analyste de sécurité travaille avec l'équipe informatique concernée pour réinitialiser le mot de passe des utilisateurs et passer aux autres étapes du playbook, une fois la tâche respective terminée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ii. Si l'utilisateur répond Non, un e-mail automatisé lui est envoyé pour reconfirmer la réponse. L'analyste de sécurité doit prendre manuellement les mesures appropriées.

iii. Si l'utilisateur ne répond pas à l'e-mail automatisé, l'analyste de sécurité doit mettre à jour manuellement l'incident de sécurité et fournir une réponse. Une tâche manuelle est créée pour valider si le compte utilisateur a été compromis.



9. À l'étape 8.10.3, l'état de l'incident de sécurité est mis à jour.
10. À l'étape 8.10.4, une tâche automatisée est créée pour vérifier si l'implémentation de l'aptitude Créer des demandes de bloc pour les adresses IP et URL malveillantes est disponible. Si l'implémentation de l'aptitude est disponible, le flux secondaire Créer des demandes de bloc est exécuté. Si ce n'est pas disponible, l'incident de sécurité est mis à jour et une note de travail est publiée pour indiquer que l'implémentation de l'aptitude n'est pas disponible.
11. À l'étape 9, l'incident de sécurité est mis à jour et l'état est défini sur **Révision**.
12. À l'étape 10, une tâche de réponse est créée pour que l'utilisateur termine l'examen post-incident avant de fermer la tâche.

Playbook pour l'automatisation des incidents de sécurité enfants

Les incidents de sécurité en double sont classés dans la catégorie des incidents de sécurité enfants et sont déployés sur les incidents de sécurité parents.

Le playbook d'automatisation des incidents de sécurité enfants permet de réduire le temps nécessaire pour enquêter et fermer les incidents de sécurité en double. Ce playbook déploie automatiquement des artefacts uniques spécifiques de l'incident de sécurité enfant (observables, utilisateurs affectés, CI) sur l'incident de sécurité parent.

Prérequis

Rôle requis :

- sn_si.admin
- flow_designer

Spoke : installer le spoke Security Operations (sn_sec_spoke)

Principales options

Le playbook d'automatisation enfant couvre les options suivantes :

1. Fait passer l'incident de sécurité à l'étape **Analyse** .
2. Élimine les doublons et ajoute (cumule) les utilisateurs et CI affectés à l'incident de sécurité parent.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Ajoute les observables de l'incident enfant à l'incident de sécurité parent.
4. Ferme ou annule l'incident de sécurité enfant lorsque l'incident de sécurité parent est fermé.

Options requises

Pour plus d'informations, consultez le ServiceNow Store .

Expérience d'analyste de sécurité

Pour comprendre comment résoudre les menaces de sécurité étape par étape, reportez-vous à la section Résoudre les menaces de sécurité avec le playbook.

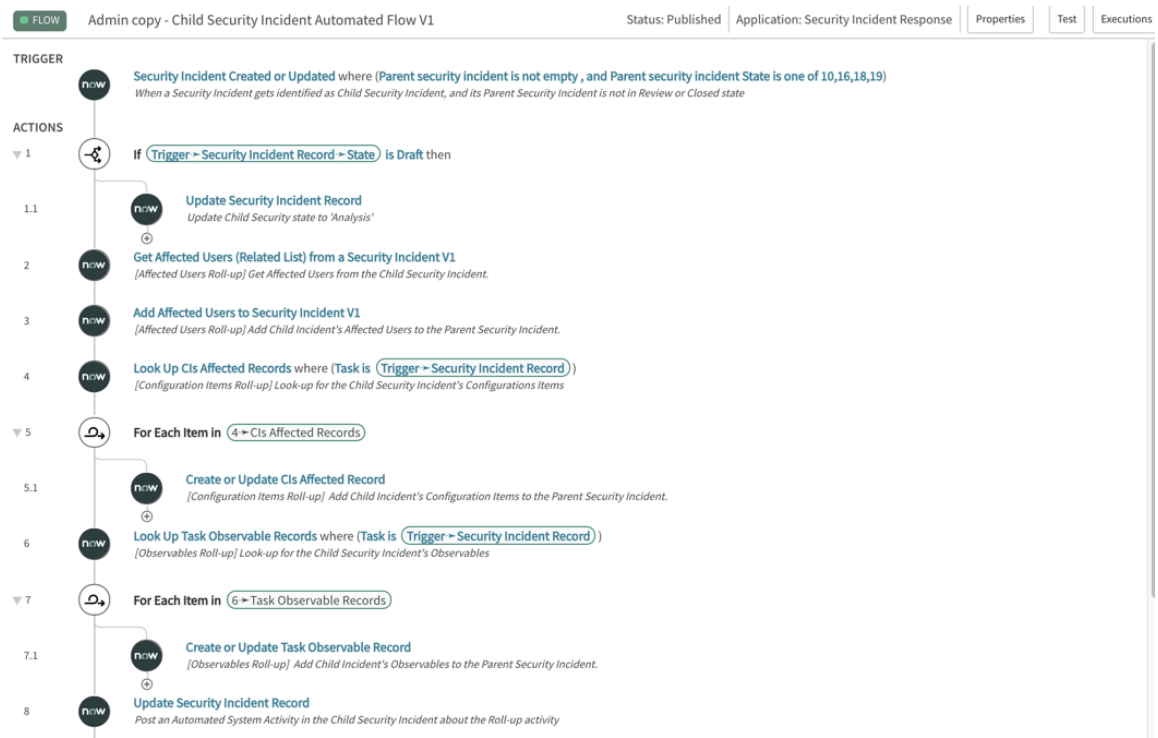
Meilleure compréhension du playbook d'automatisation des incidents de sécurité enfants avec les options de Flow Designer

Commencer

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Concepteur de flux** > **Concepteur** et cliquez sur le playbook Échec de la connexion.
3. Faites une copie du Playbook d'automatisation des incidents de sécurité enfants et apportez les modifications nécessaires. (Il s'agit d'une étape facultative. Suivez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des modifications spécifiques au flux.
4. Apportez les modifications nécessaires en fonction de vos besoins. (Il s'agit d'une étape facultative. Suivez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des modifications spécifiques au flux.
5. Activez le playbook.
   - Activez le flux principal pour utiliser le playbook disponible avec le système de base.
   - Activez le flux copié après avoir apporté des modifications en fonction de vos besoins.

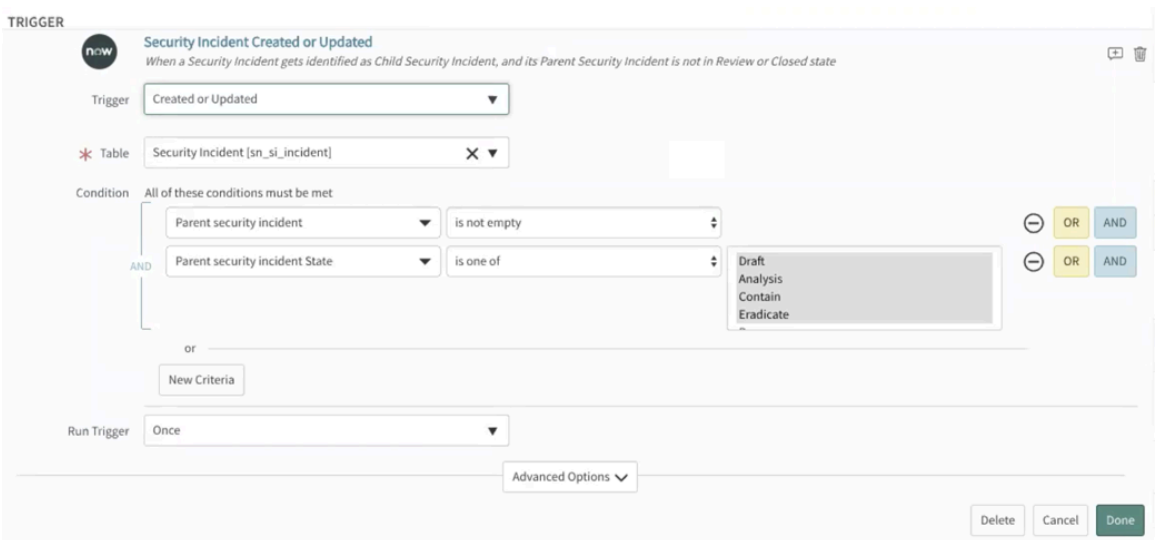
L'image suivante montre une copie du Playbook d'automatisation des incidents de sécurité enfants. Passez en revue les étapes ci-dessous pour mieux comprendre les différentes actions du playbook.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Ce playbook est déclenché lorsque :

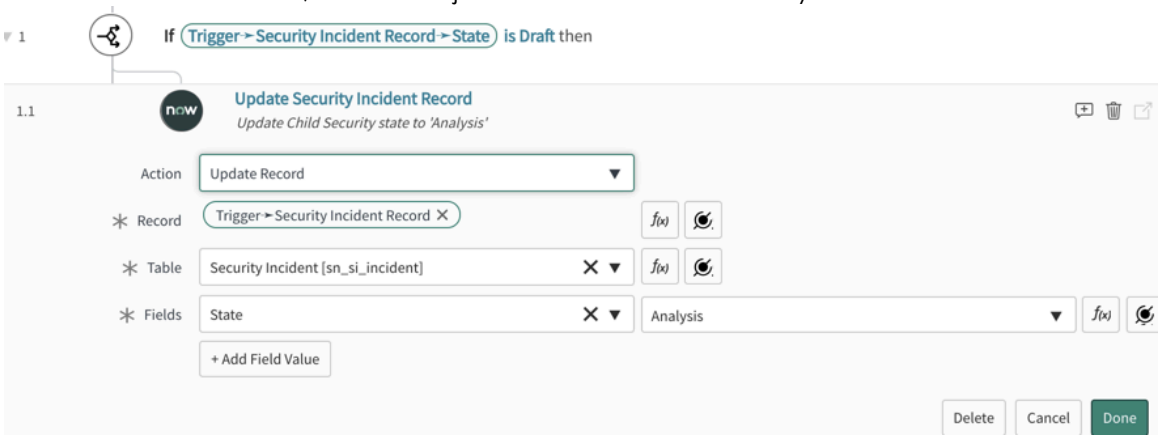
- Le champ d'incident de sécurité parent n'est pas vide.
- L'incident de sécurité parent est à l'état Brouillon, Analyse, Contenir ou Éradiquer.



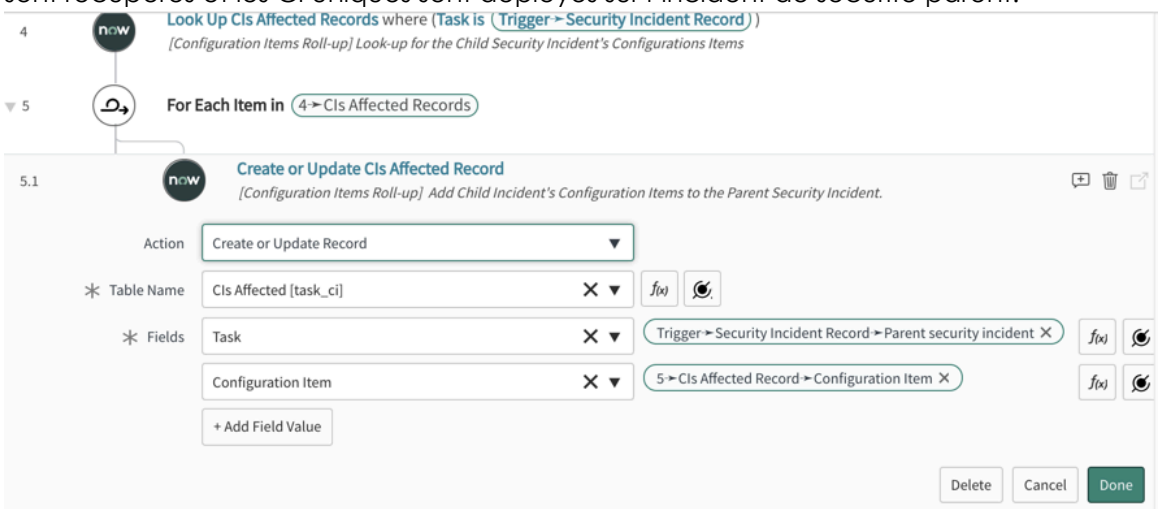
Les étapes suivantes vous guident à travers les actions et les tâches disponibles dans le Playbook d'automatisation des incidents de sécurité enfants.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

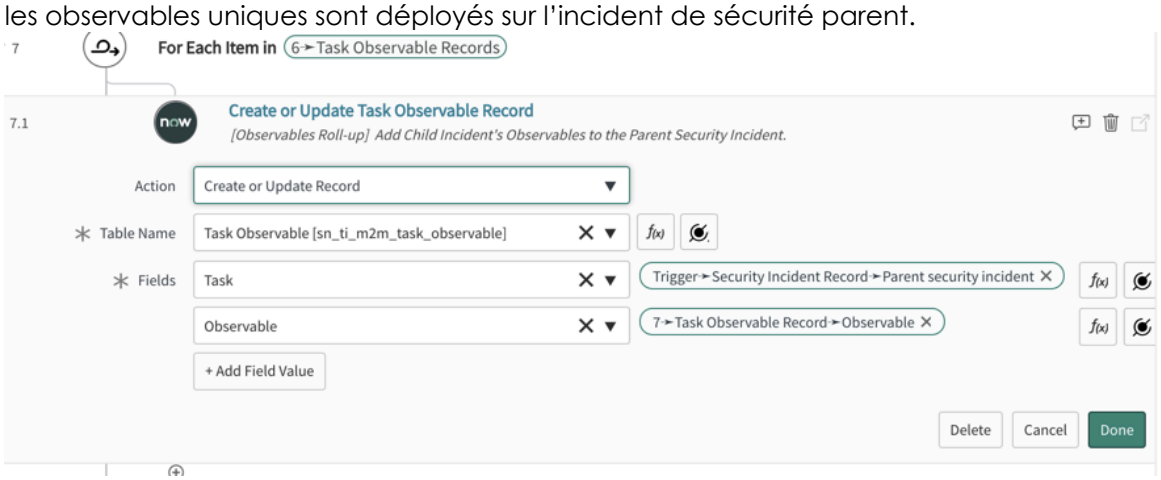
1. Lorsque le playbook commence à s'exécuter, à l'étape 1, si l'incident de sécurité se trouve à l'état Brouillon, il est mis à jour et défini sur l'état Analyse.



2. Aux étapes 2 et 3, les utilisateurs affectés par l'incident de sécurité sont récupérés et déployés sur l'incident de sécurité parent. Tous les utilisateurs en double sont éliminés.
3. Aux étapes 4 et 5, les éléments de configuration associés à l'incident de sécurité enfant sont récupérés et les CI uniques sont déployés sur l'incident de sécurité parent.



4. Aux étapes 6 et 7, les observables associés à l'incident de sécurité enfant sont récupérés et les observables uniques sont déployés sur l'incident de sécurité parent.



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Aux étapes 8 et 9, des notes de travail automatisées sont publiées sur les incidents de sécurité parents et enfants, indiquant que les utilisateurs, éléments de configuration et observables affectés ont été déployés de l'incident de sécurité enfant vers l'incident de sécurité parent.

Playbook pour Office 365 : fichier malveillant détecté

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les fichiers malveillants détectés dans Office 365.

Lorsque des fichiers malveillants sont détectés dans Office 365, vous pouvez utiliser le playbook 365 - Fichier malveillant détecté dans Concepteur de flux pour obtenir des conseils et aider à optimiser l'examen de ces fichiers malveillants.

Configurer le playbook Office Malicous Fichier détecté

Procédez comme suit pour configurer le playbook Fichier Malicous détecté Office.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

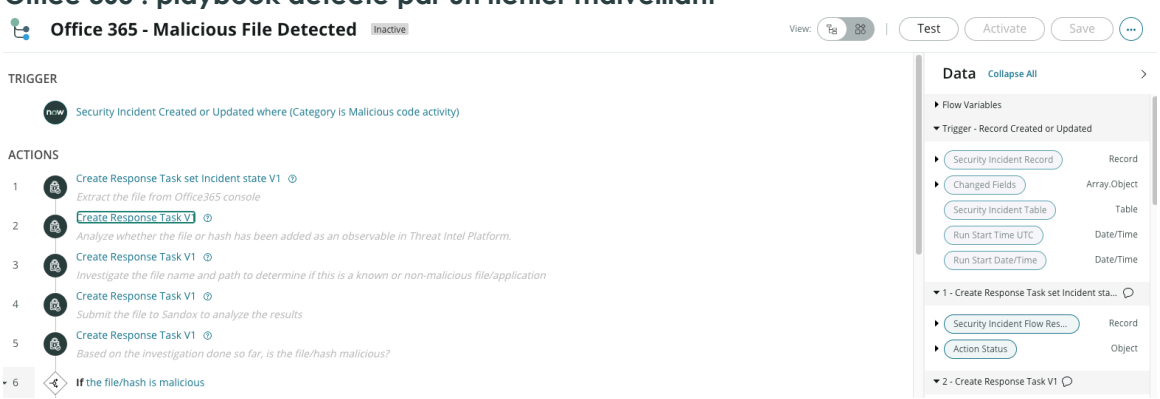
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **Office 365 - Fichier malveillant détecté.**
3. Facultatif : Vous pouvez créer une copie du flux de playbook Office 365 - Fichier malveillant détecté et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l'icône de  et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

Office 365 : playbook détecté par un fichier malveillant

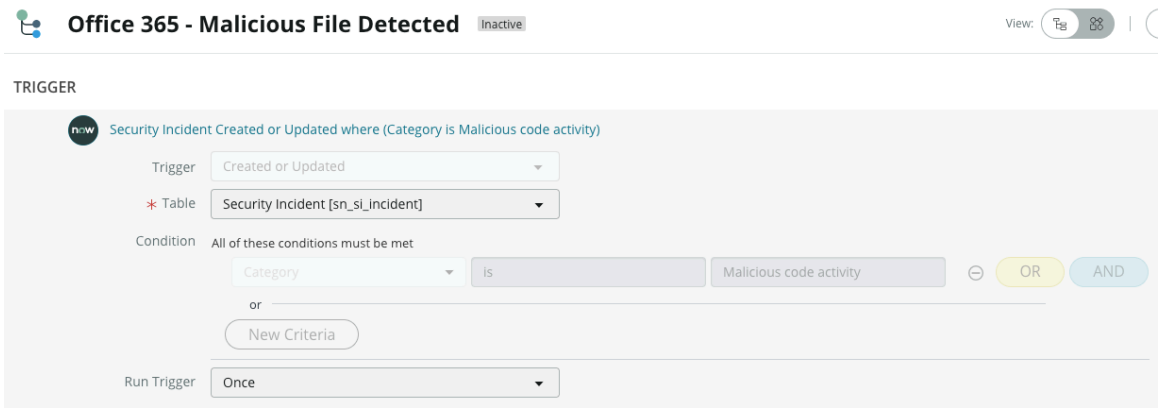


4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les modifications requises.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Activité de code malveillant**.



Utiliser le playbook Office 365 Fichier malveillant détecté

Utilisez ce playbook pour examiner les fichiers malveillants détectés dans Office 365. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le Playbook Office 365 Fichier malveillant détecté.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

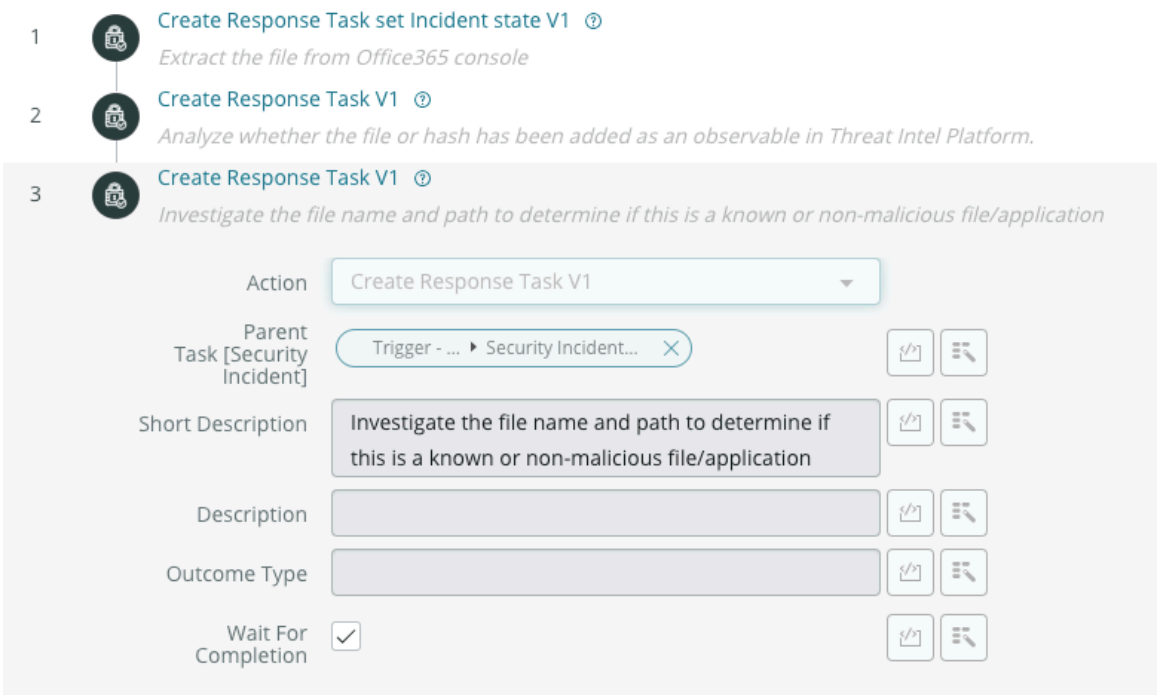
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez extraire le fichier malveillant de la console Office 365.
2. Dans l'action 2, vous devez analyser si le fichier ou le hachage a été ajouté en tant qu'observable dans la plateforme Threat Intel.
3. Dans l'action 3, vous devez examiner le nom et le chemin d'accès du fichier pour déterminer s'il s'agit d'un fichier/d'une application connu ou non malveillant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook Office 365 Fichier malveillant détecté



4. Dans l'action 4, vous devez soumettre le fichier à Sandbox pour analyser les résultats.
5. Dans l'action 5, sur la base de l'enquête effectuée jusqu'à présent, vous devez vérifier si le fichier ou le hachage est malveillant ou non.
   Si le fichier ou le hachage n'est pas malveillant, une tâche de réponse manuelle est créée dans l'action 5 et le flux se termine.
6. Dans l'action 6, si le fichier ou le hachage est malveillant, les actions 7 et 8 sont exécutées.
7. Dans Action 7, vous devez contacter l'utilisateur final pour obtenir une justification commerciale valable quant à la raison pour laquelle il a un fichier malveillant sur l'appareil.
   Si le fichier ou le hachage est malveillant, vous pouvez utiliser le modèle d'e-mail préexistant dans le playbook pour envoyer un e-mail à l'utilisateur final demandant des clarifications.
8. Dans l'action 8, vous devez vérifier si l'utilisateur final a fourni une justification commerciale valide ou non.
   Si l'utilisateur final a fourni une justification commerciale valide, une tâche de réponse manuelle est créée dans l'action 5 et le flux se termine.
9. Dans l'action 9, si l'utilisateur n'a pas fourni de justification commerciale valide, les actions 10, 11 et 12 sont exécutées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Dans l'action 10, puisqu'il n'y avait aucune justification commerciale valable, vous pouvez transmettre le fichier malveillant ou le hachage à l'équipe Threat Intelligence pour examen.
11. Dans l'action 11, vous devez exécuter le script Malware bytes scanner pour vérifier si le fichier ou le hachage est malveillant.
12. Dans l'action 12, vous devez effectuer une analyse médico-légale pour vérifier si le fichier ou le hachage est malveillant.
13. Dans l'action 13, une tâche de réponse est créée pour que l'utilisateur termine la revue post-incident avant de fermer la tâche.

Playbook pour la détection de répétition

Ce playbook vous aide à déterminer si la réponse aux incidents a été fournie dans un rapport de hameçonnage exact ou similaire dans le passé et fonctionne automatiquement sur le nouveau rapport de la même manière.

Le playbook Répéter la détection vérifie si l'incident d'hameçonnage nouvellement signalé ressemble à un incident passé. Lorsque la détection répétée est identifiée, l'incident de sécurité correspondant et les détails de résolution sont fournis à l'analyste, qui peut les utiliser sur l'incident nouvellement signalé, ce qui entraîne une remédiation rapide de l'incident de sécurité.

Configurer le playbook de détection de répétition

Procédez comme suit pour configurer le playbook Répéter la détection.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*). Vous pouvez modifier les propriétés système suivantes :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

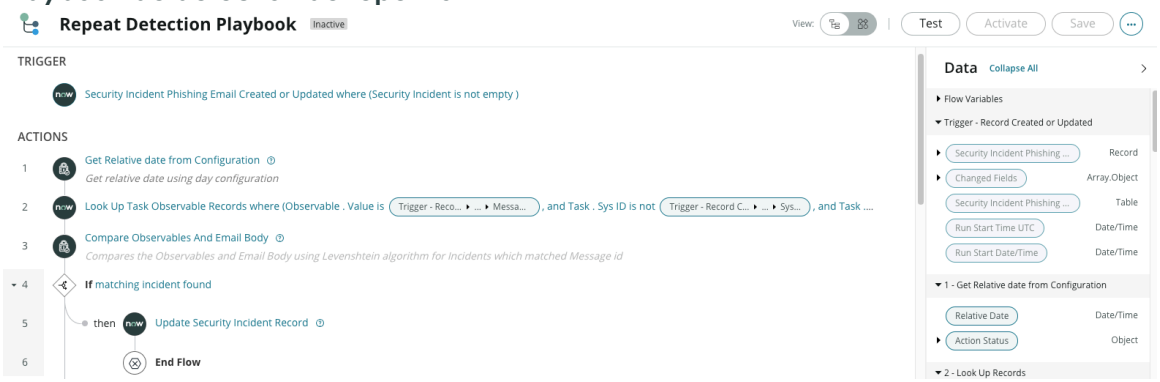
- *sn_sec_spoke.similarphish.earlyterminationscore*
- *sn_sec_spoke.similarphish.lookbackdays*
- *sn_sec_spoke.similarphish.maxcomparisonsize*
- *sn_sec_spoke.similarphish.minmatchscore*

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **Repeat Detection (Détection de répétition**).
3. Facultatif : Vous pouvez créer une copie du flux du playbook Répéter la détection et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l'icône de ••• et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

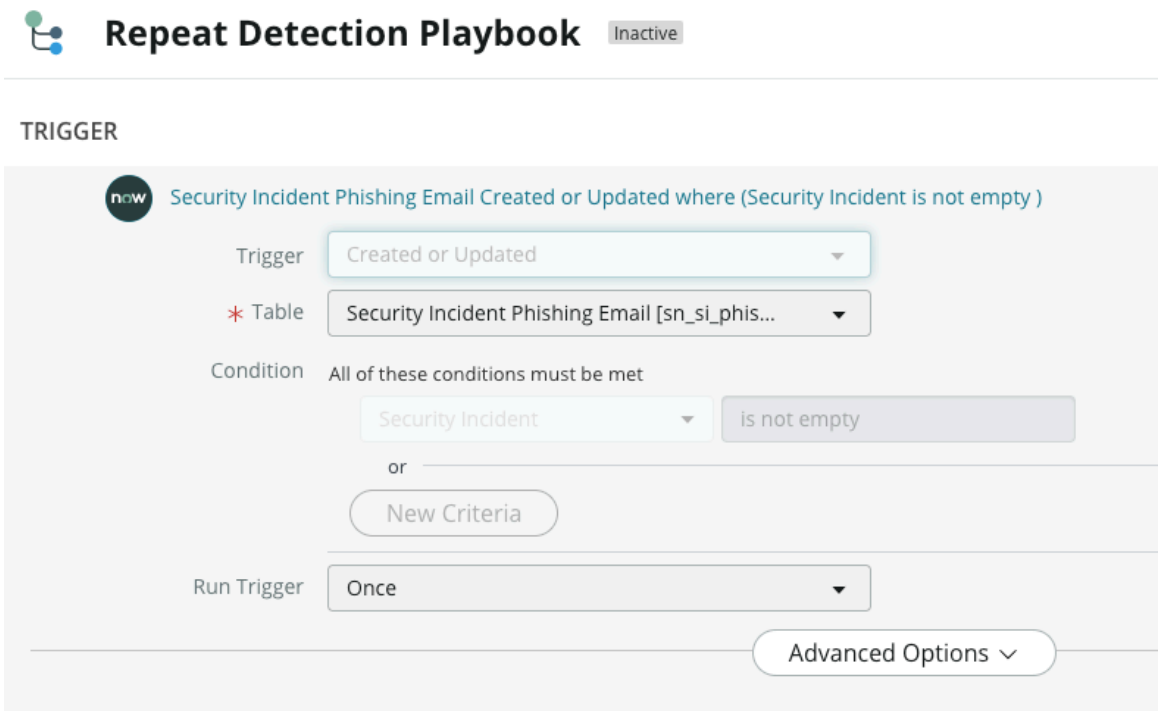
Playbook de détection de répétition



4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché lorsque **l'incident de sécurité n'est pas vide**.



Utiliser le playbook de détection de répétition

Utilisez ce playbook pour vérifier si la réponse aux incidents a été fournie dans un rapport de hameçonnage exact ou similaire dans le passé et si elle fonctionne automatiquement sur le nouveau rapport de la même manière. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Répéter la détection.

Avant de commencer

Rôle requis :

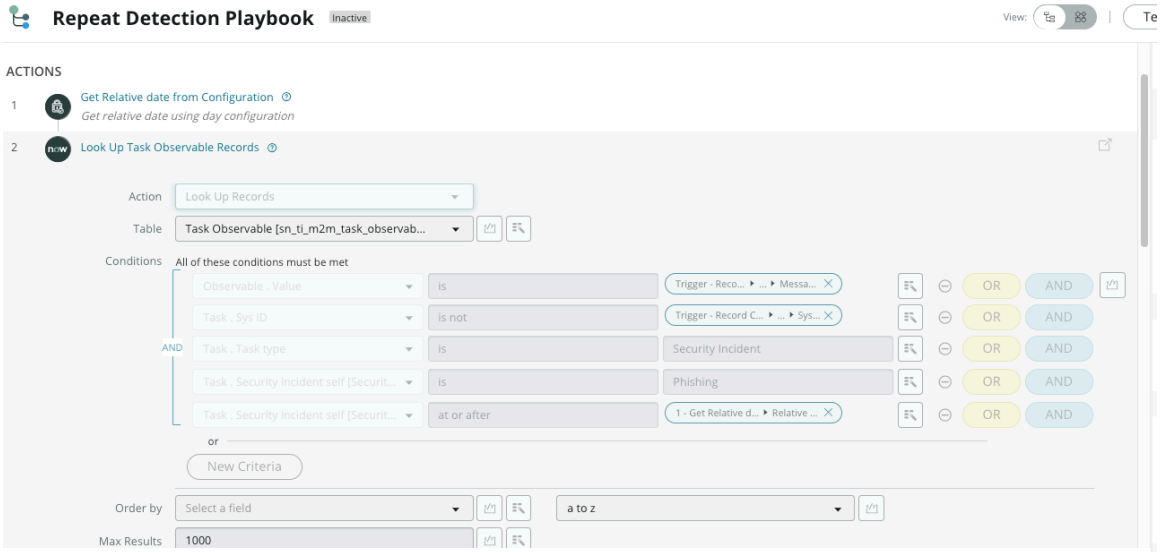
- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, le playbook récupère la date relative de l'incident de sécurité à l'aide de la configuration du jour.
2. Dans l'action 2, le playbook recherche les enregistrements d'observables de tâche sur la *table sn_ti_m2m_task_observable* qui correspondent à l'incident en fonction de l'ID de message.

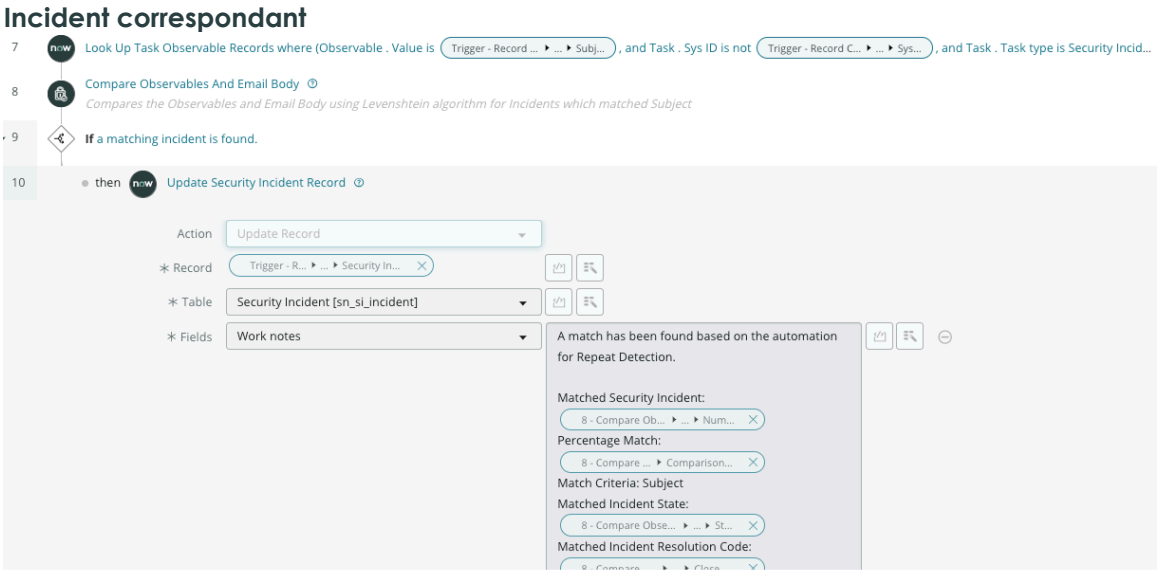
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de détection de répétition



3. Dans l'action 3, le playbook compare les observables de tâche et le corps de l'e-mail à l'aide de l'algorithme de Levenshtein pour les incidents qui correspondaient à l'ID de message.
4. Dans l'action 4, en fonction de l'enquête effectuée jusqu'à présent, le playbook vérifie si l'incident correspondant est détecté en fonction de l'ID de message ou non.
   Dans l'action 5, si l'incident correspondant est trouvé, le playbook met automatiquement à jour la note de travail indiquant qu'une correspondance a été trouvée en fonction de l'automatisation pour la détection répétée. Dans l'action 6, le flux se termine.
5. Si l'incident correspondant n'est pas trouvé, dans l'action 7, le playbook recherche les enregistrements d'observables de tâche sur la table *sn_ti_m2m_task_observable* qui correspondent à l'incident en fonction de l'objet.
6. Dans l'action 8, le playbook compare les observables de tâche et le corps de l'e-mail à l'aide de l'algorithme de Levenshtein pour les incidents qui correspondaient à l'objet.
7. Dans l'action 9, le playbook vérifie si l'incident correspondant est trouvé ou non.
   Dans l'action 10, si l'incident correspondant est trouvé, le playbook met automatiquement à jour la note de travail indiquant qu'une correspondance a été trouvée en fonction de l'automatisation pour la détection répétée. Dans l'action 11, le flux se termine.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Dans l'action 12, le playbook recherche les enregistrements observables de tâche sur la *table sn_ti_m2m_task_observable* qui correspondent à l'incident en fonction de l'adresse.
9. Dans l'action 13, le playbook compare les observables de tâche et le corps de l'e-mail à l'aide de l'algorithme de Levenshtein pour les incidents qui correspondaient à l'adresse.
10. Dans l'action 14, le playbook vérifie si l'incident correspondant est trouvé en fonction de l'adresse ou non.
    Dans l'action 15, si l'incident correspondant est trouvé, le playbook met automatiquement à jour la note de travail indiquant qu'une correspondance a été trouvée en fonction de l'automatisation pour la détection répétée. Dans l'action 16, le flux se termine.

Playbook pour les e-mails falsifiés (utilisant le même nom d'affichage)

Ce playbook fournit des étapes de rattrapage systématique pour enquêter sur les e-mails falsifiés, qui sont déclenchés lorsque des noms falsifiés pour des e-mails sont envoyés aux employés de l'organisation.

Configurer le playbook des e-mails falsifiés

Procédez comme suit pour configurer le playbook des e-mails usurpés.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

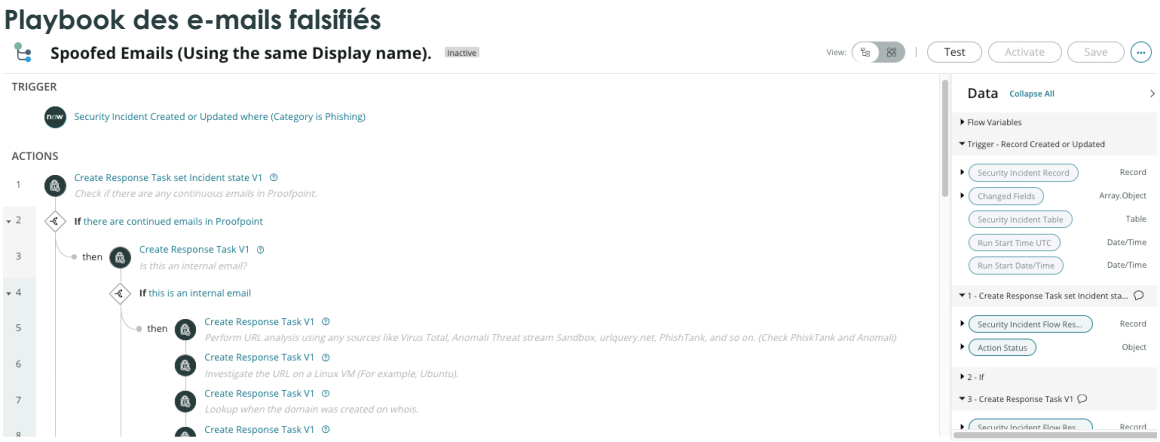
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **E-mails falsifiés (utilisant le même nom d'affichage).**
3. Facultatif : Vous pouvez créer une copie du flux du playbook Répéter la détection et apporter les modifications nécessaires.

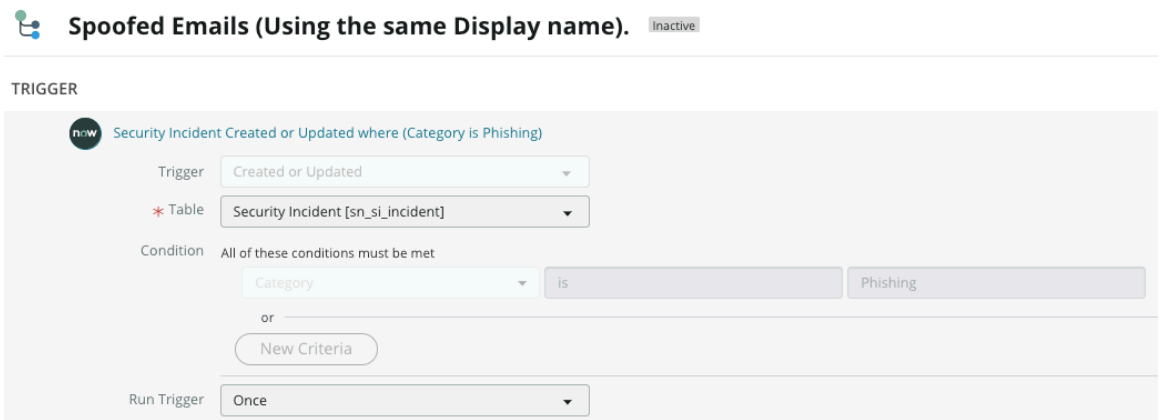
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour créer une copie du flux du playbook, cliquez sur l'icône de  et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.



4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Hameçonnage**.



Utiliser le playbook des e-mails falsifiés (utilisant le même nom d'affichage)

Utilisez ce playbook pour examiner les e-mails usurpés, qui sont déclenchés lorsque des noms falsifiés pour les e-mails sont envoyés aux employés de l'organisation. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le Playbook E-mails falsifiés (utilisant le même nom d'affichage).

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

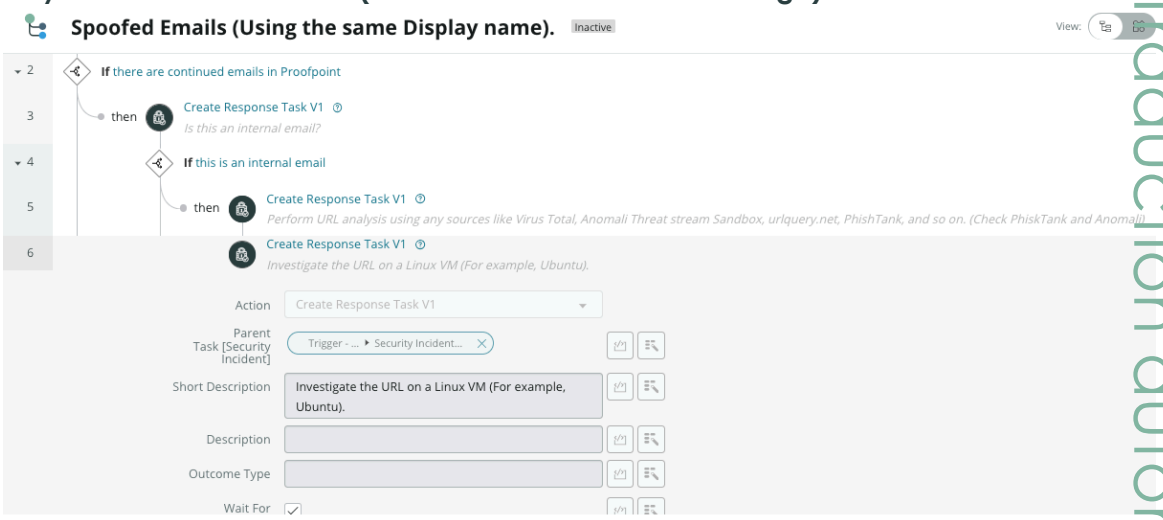
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez vérifier s'il existe des e-mails falsifiés continus dans Proofpoint.
2. Dans l'action 2, s'il y a des e-mails continus dans Proofpoint, vérifiez s'il s'agit d'un e-mail d'usurpation interne ou non.
3. Dans l'action 3, s'il s'agit d'un e-mail interne falsifié, effectuez les actions suivantes :

   a. Dans l'action 5, vous devez effectuer une analyse d'URL à l'aide de n'importe quelle source telle que Virus Total, Anomali Threat stream Sandbox, urlquery.net, PhishTank (par exemple, vérifiez PhiskTank et Anomali).

   b. Dans l'action 6, vous devez examiner l'URL sur une machine virtuelle Linux (par exemple, Ubuntu).

Playbook d'e-mails falsifiés (utilisant le même nom d'affichage)



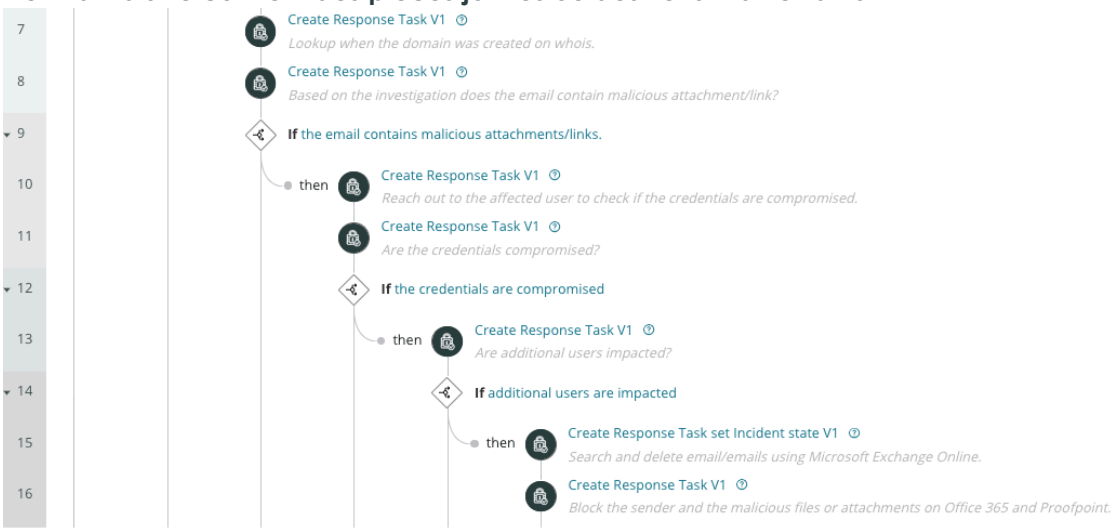
   c. Dans l'action 7, vous devez rechercher la date de création du domaine sur WHOIS. Recherchez les domaines récemment enregistrés (au cours de la dernière semaine) qui sont suspects et ont une forte probabilité d'attaques de phishing.

   d. Dans l'action 8, sur la base de l'enquête effectuée jusqu'à présent, vous devez vérifier si cet e-mail contient une pièce jointe ou un lien malveillant.
   Si cet e-mail ne contient pas de lien ou de pièce jointe malveillant, le flux s'arrête.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'e-mail falsifié contient des pièces jointes ou des liens malveillants



e. Dans Action 9, si l'e-mail contient des pièces jointes ou des liens malveillants, effectuez les actions suivantes.

i. Dans l'action 10, vous devez contacter l'utilisateur affecté pour vérifier si les informations d'identification sont compromises. Vous pouvez utiliser le modèle d'e-mail fourni pour contacter l'utilisateur affecté.

ii. Dans l'action 11, vous devez vérifier si les informations d'identification sont compromises en fonction de la réponse par e-mail. Si les informations d'identification n'ont pas été compromises, le flux s'arrête.

1. Dans l'action 12, si les informations d'identification sont compromises, dans l'action 13, vous devez vérifier si d'autres utilisateurs sont concernés. Si aucun utilisateur supplémentaire n'est impacté, le flux s'arrête.

2. Dans l'action 14, si des utilisateurs supplémentaires sont impactés, effectuez les actions suivantes :

a. Dans l'action 15, vous devez rechercher et supprimer des e-mails à l'aide de Microsoft Exchange Online.

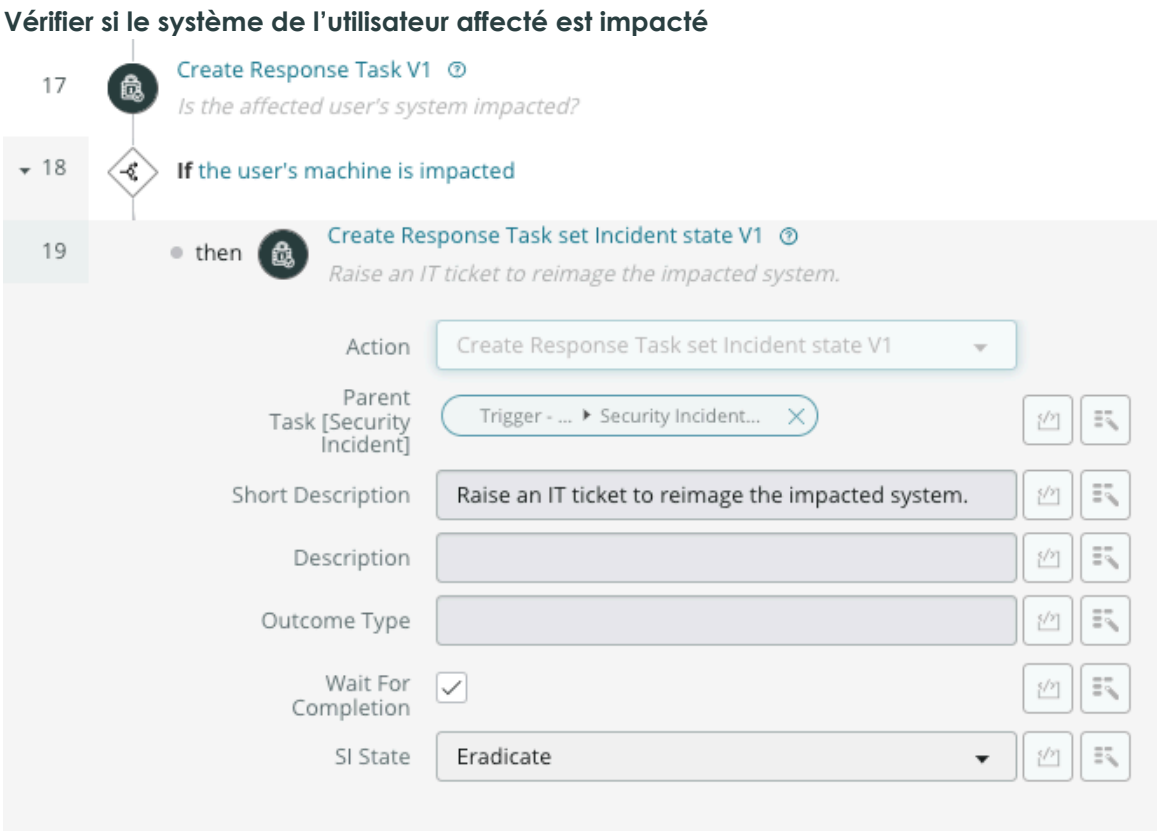
b. Dans Action 16, vous devez bloquer l'expéditeur et les fichiers ou pièces jointes malveillants sur Office 365 et Proofpoint.

4. Dans l'action 17, s'il ne s'agit pas d'un e-mail d'usurpation interne, vous devez vérifier si le système de l'utilisateur concerné est impacté.

5. Dans l'action 18, si le système de l'utilisateur est impacté, dans l'action 19, émettez un ticket informatique pour recréer l'image du système impacté.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Dans l'action 20, une tâche de réponse est créée pour vous permettre de terminer la revue post-incident avant de fermer la tâche.

Playbook pour Endpoint Detection

Ce playbook fournit des étapes de rattrapage systématiques pour examiner les alertes de programme malveillant déclenchées sur un hôte ou un point de terminaison (par exemple, une détection de fichier malveillant).

Lorsque des alertes CrowdStrike sont déclenchées sur un hôte ou un point de terminaison, vous pouvez utiliser le playbook Endpoint Detection dans Flow Designer pour obtenir des conseils et aider à optimiser l'enquête sur ces fichiers malveillants.

Configurer le playbook de détection d'un point de terminaison

Procédez comme suit pour configurer le playbook Détection d'un point de terminaison.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **Endpoint Detection** .

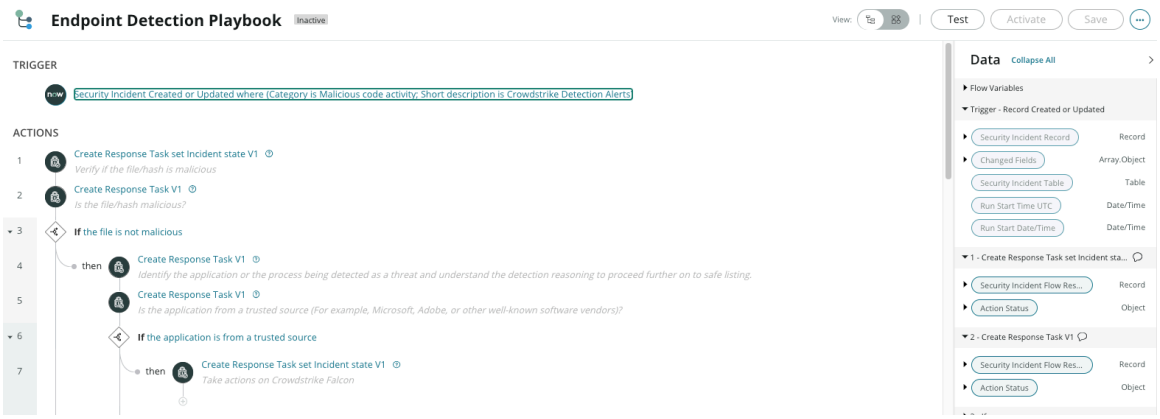
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

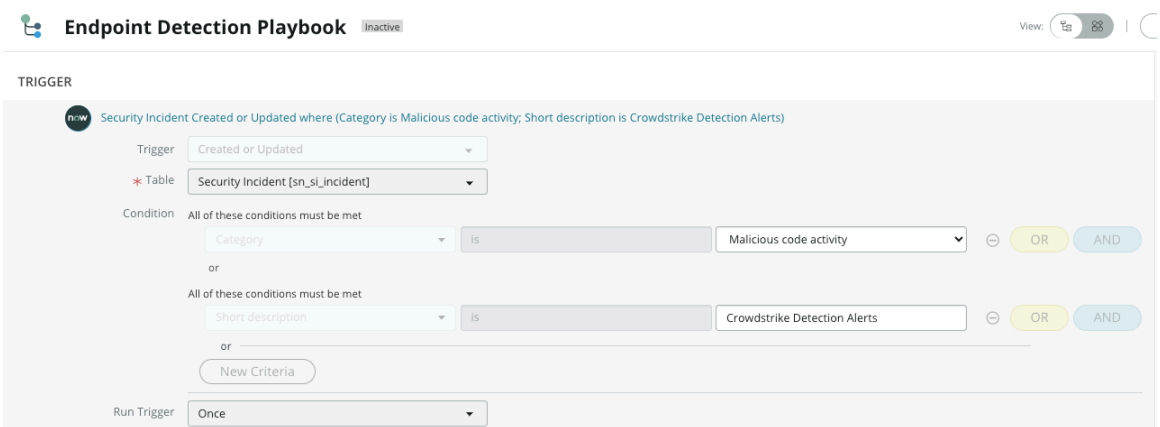
3. Facultatif : Vous pouvez créer une copie du flux de playbook de détection d'un point de terminaison et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l'icône de ••• et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

Playbook de détection d'un point de terminaison



4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :
   - **La catégorie** est **Activité de code malveillant**.
   - **La description courte** est **Alertes de détection CrowdStrike**.



Utiliser le playbook Endpoint Detection

Utilisez ce playbook pour examiner les alertes de programme malveillant déclenchées sur un hôte ou un point de terminaison. Les étapes suivantes vous donnent un aperçu des actions, des tâches et des flux secondaires disponibles dans le playbook de détection d'un point de terminaison.

Avant de commencer

Rôle requis :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez vérifier si le fichier ou le hachage est malveillant en analysant les résultats de la recherche de menace dans SIR et en recueillant des informations auprès de VirusTotal, WildFire, ThreatCrowd, entre autres.
2. Dans l'action 2, vous devez vérifier si le fichier ou le hachage est malveillant ou non.
3. Dans l'action 3, si le fichier ou le hachage est malveillant, effectuez les actions suivantes :

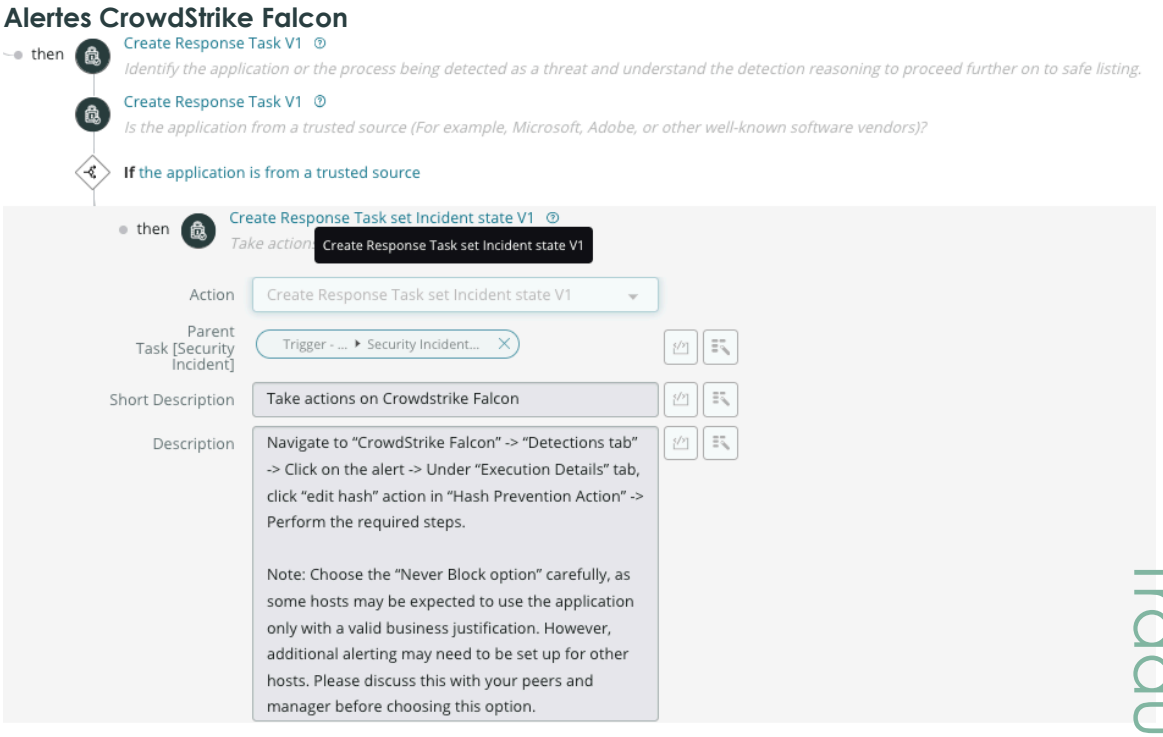
   a. Dans l'action 4, vous devez identifier l'application ou le processus détecté comme une menace et recueillir des informations sur le raisonnement de détection pour poursuivre vers la liste sécurisée.



   b. Dans l'action 5, vous devez vérifier si l'application provient d'une source fiable (par exemple, Microsoft, Adobe ou d'autres fournisseurs de logiciels bien connus).

   c. Dans Action 6, si l'application provient d'une source fiable, vous devez agir sur les alertes CrowdStrike Falcon.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Dans l'action 7, effectuez les actions suivantes :

i. Accédez à la **CrowdStrike Falcon** > **Détections** onglet.

ii. Cliquez sur l'alerte CrowdStrike Falcon.

iii. Sous l'onglet Détails de l'exécution, cliquez sur Modifier l'action **de hachage** dans l'action de prévention du hachage.

iv. Effectuez les étapes requises.

> **Remarque :** Choisissez l'option **Ne jamais bloquer** avec soin, car seuls certains hôtes peuvent être autorisés à utiliser l'application avec une justification commerciale valide. Toutefois, il peut être nécessaire de configurer des alertes supplémentaires pour d'autres hôtes.

e. Dans Action 8, si l'application ne provient pas d'une source fiable, vous devez choisir si vous souhaitez supprimer le fichier ou l'application de l'appareil localement.
Dans l'action 10, si vous souhaitez supprimer localement le fichier ou l'application de l'appareil, effectuez les actions suivantes :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Dans l'action 11, accédez à l'onglet **Fichiers en quarantaine** et filtrez le point de terminaison en recherchant le nom de l'appareil.

ii. Sélectionnez le fichier qui doit faire l'objet d'une levée locale, puis cliquez sur **Libérer**.

Remarque :

- Le fichier s'exécute toujours sur ce point de terminaison spécifique. Cependant, la détection et la mise en quarantaine continuent de se produire sur tous les autres hôtes.
- Pour libérer en bloc le fichier de quarantaine sur plusieurs hôtes, sélectionnez le nom et l'état de fichier appropriés. Cliquez sur **Sélectionner**, puis sélectionnez **Version**.

Dans l'action 12, si vous ne souhaitez pas supprimer localement le fichier ou l'application de l'appareil, vous pouvez rediriger l'utilisateur vers l'assistance informatique pour demander l'installation des applications approuvées.

4. Dans l'action 14, si le fichier ou le hachage n'est pas malveillant, effectuez les actions suivantes :

a. Dans l'action 15, vous devez déterminer si le fichier/hachage présente un risque élevé ou faible en fonction du rôle de l'utilisateur (service ou poste qui traite des informations sensibles), du type d'application (rançongiciel, rootkit...) et de l'impact de l'application (combien d'utilisateurs ont été impactés).

b. Dans l'action 16, s'il s'agit d'un fichier à haut risque, effectuez les actions suivantes :

i. Dans l'action 17, examinez les résultats avec l'équipe Threat Intel.

ii. Dans l'action 18, exécutez l'analyse d'octets de programme malveillant sur le fichier.

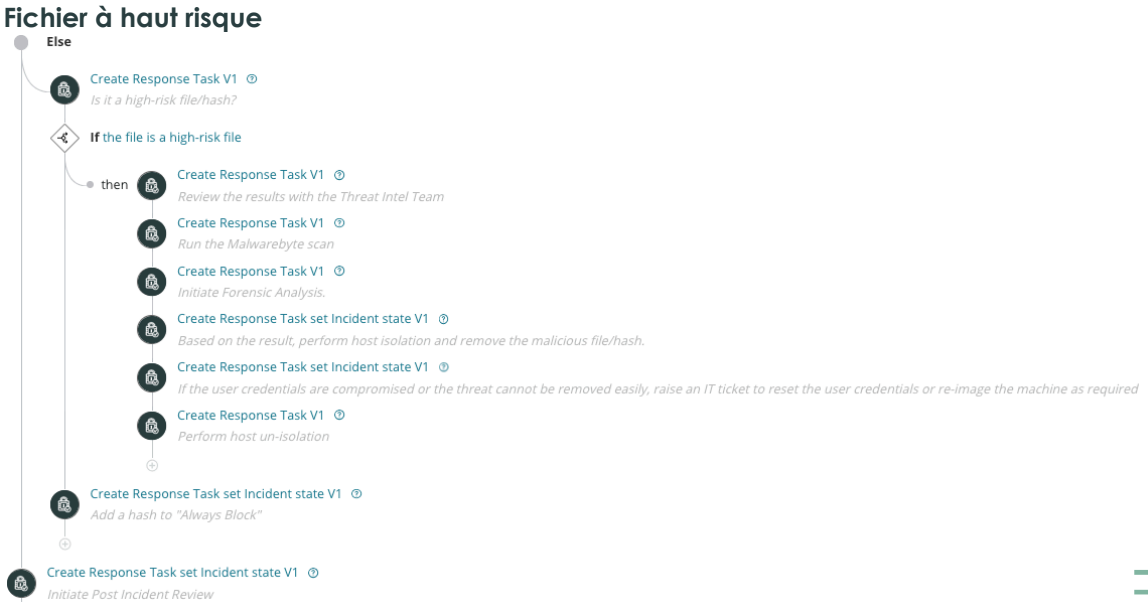
iii. Dans l'action 19, lancez l'analyse médico-légale.

iv. Dans l'action 20, en fonction du résultat de l'analyse médico-légale, procédez à l'isolement de l'hôte et supprimez le fichier/hachage malveillant.

v. Dans l'action 21, si les informations d'identification de l'utilisateur sont compromises ou si la menace ne peut pas être supprimée facilement, créez un ticket informatique pour réinitialiser les informations d'identification de l'utilisateur ou recréer l'image de la machine si nécessaire.

vi. Dans l'action 22, procédez à la désisolation de l'hôte.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Dans l'action 23, s'il ne s'agit pas d'un fichier à haut risque, effectuez les actions suivantes :

i. Accédez à la **CrowdStrike Falcon** > **Configurations** onglet.

ii. Depuis l'onglet Configurations, accédez à **Hachages de prévention** > > **Charger un hachage** > **Ajouter le hachage**.

iii. Choisissez le système d'exploitation requis, puis sélectionnez **Toujours bloquer**.

5. Dans l'action 24, une tâche de réponse est créée pour que l'utilisateur termine la revue post-incident avant de fermer la tâche.

Playbook pour une éventuelle pulvérisation de mot de passe

Ce playbook fournit des étapes de rattrapage systématiques pour examiner les alertes par pulvérisation de mot de passe déclenchées par plusieurs échecs de connexion (trop d'échecs d'authentification à partir de plusieurs adresses IP pour le même utilisateur).

Configurer le playbook Brouillard possible par pulvérisation de mot de passe

Procédez comme suit pour configurer le playbook Possible Password Spray.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.

2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **Possible Password Spray** .

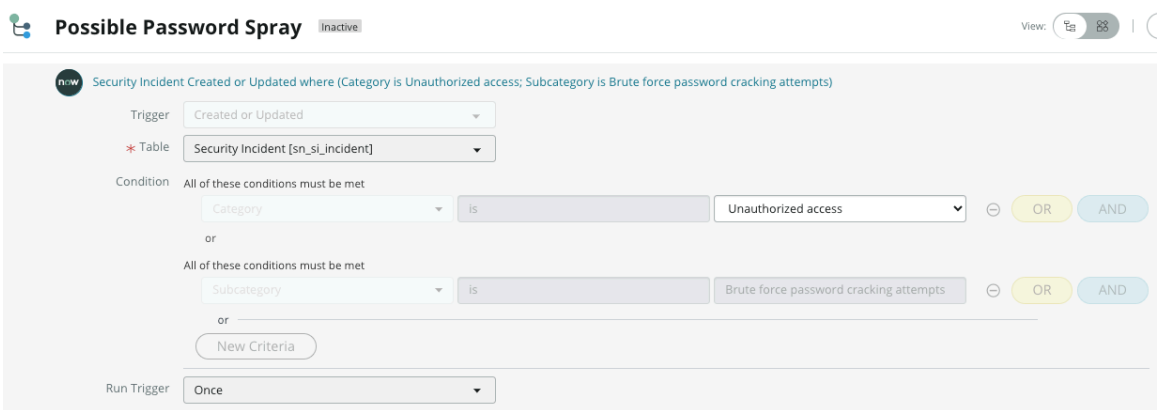
3. Facultatif : Vous pouvez créer une copie du flux de playbook Pulvérisation de mot de passe possible et apporter les modifications nécessaires.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour créer une copie du flux du playbook, cliquez sur l'icône de ••• et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.



4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :
   - **La catégorie** est **Accès non autorisé**.
   - **La sous-catégorie** comprend **les tentatives de craquage de mot de passe en force brute**.



Utiliser le playbook Possible Password Spray

Utilisez ce playbook pour examiner les alertes par pulvérisation de mot de passe déclenchées par plusieurs échecs de connexion (trop d'échecs d'authentification à partir de plusieurs adresses IP pour le même utilisateur). Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Brouillage possible de mot de passe.

Avant de commencer

Rôle requis :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

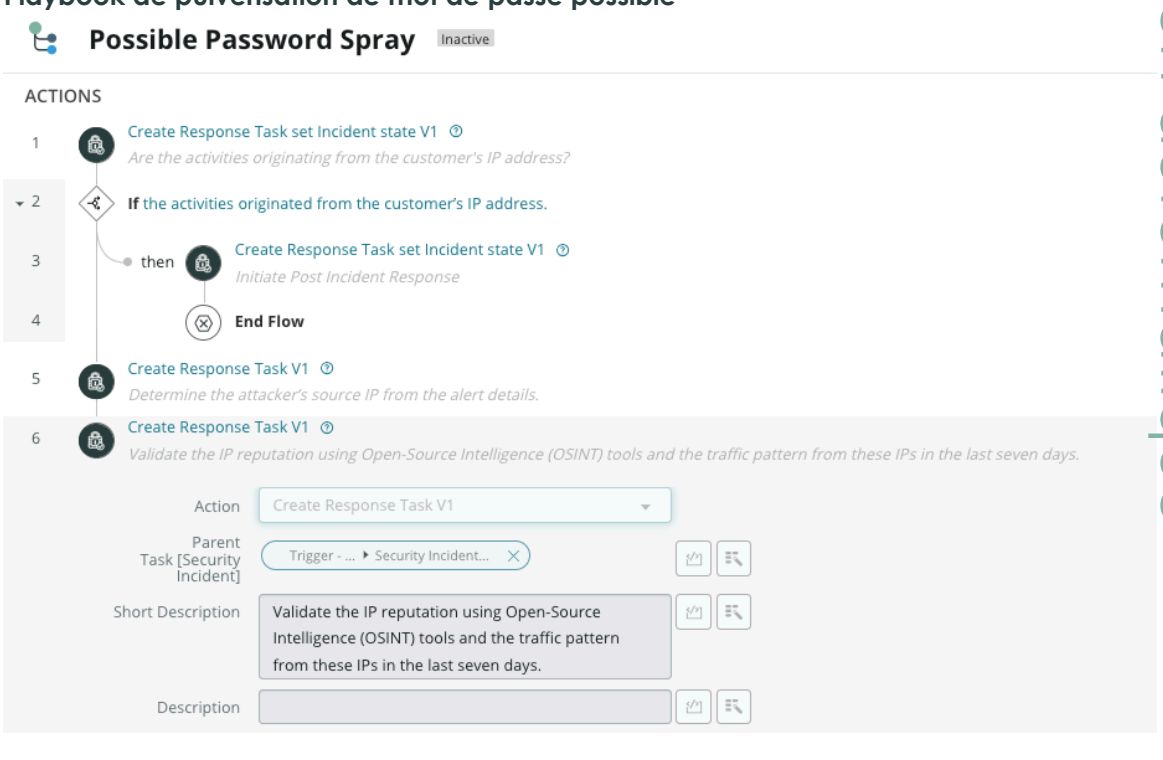
- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez vérifier si les activités proviennent de l'adresse IP du client.
   Identifiez les adresses IP effectuant l'attaque par pulvérisation de mot de passe. Par exemple, utilisez les TXID (ID de transaction) de l'alerte et comparez-les aux journaux F5.
2. Dans l'action 2, si les activités proviennent de l'adresse IP du client, effectuez les actions suivantes :
   a. Dans l'action 3, vous devez lancer un examen post-incident de l'attaque possible par pulvérisation de mot de passe.
   b. Dans l'action 4, le flux se termine.
3. Dans l'action 5, si les activités ne proviennent pas de l'adresse IP du client, déterminez l'adresse IP source de l'attaquant à partir des détails de l'alerte.
4. Dans l'action 6, vous devez valider la réputation IP à l'aide d'outils OSINT (Open-Source Intelligence) et le modèle de trafic de ces adresses IP au cours des sept derniers jours.

Playbook de pulvérisation de mot de passe possible



5. Dans l'action 7, vous devez identifier les noms d'utilisateur qui se sont connectés avec succès à l'aide de l'attaque Password Spray.
6. Dans l'action 8, vous devez identifier le nombre d'échecs de connexion et de modèles.
7. Dans l'action 9, vous devez identifier les indicateurs d'un vrai positif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

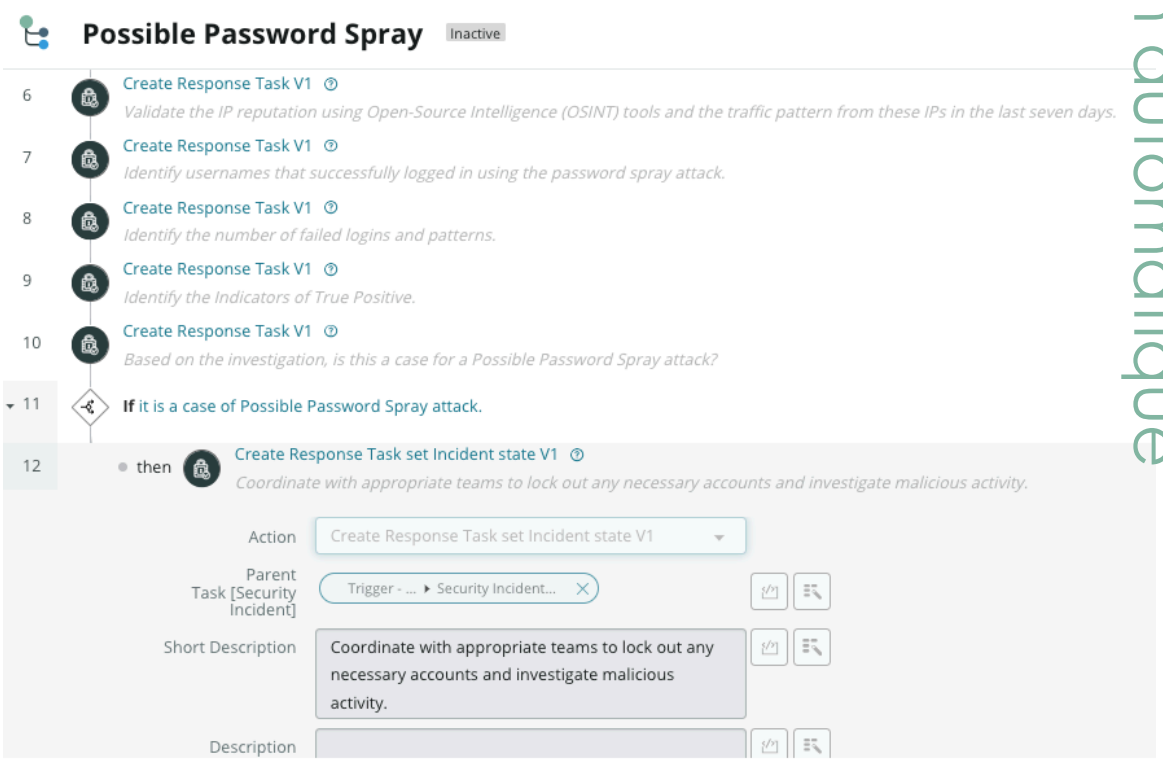
- Vérifiez le trafic provenant des adresses IP sources au cours des 60 derniers jours. Aucun trafic historique ne peut être une indication d'un vrai positif.
- Vérifiez les modèles de nom d'utilisateur présentant des échecs d'authentification et leur nombre. Plus le nombre est élevé, plus la probabilité qu'il s'agisse d'un vrai positif est élevée.
- Le nom d'utilisateur ressemble à une base de dictionnaire (de A à Z) et peut avoir des noms d'administrateur communs tels que admin, sysadmin, root, entre autres
- Le même nom d'utilisateur peut avoir des modèles différents dans l'attaque par pulvérisation, comme la même alerte peut avoir des échecs pour john.doe, johnd, jdoe, john_doe, jdoe7, etc., indiquant que les attaquants devinent le modèle de nom d'utilisateur en fonction des cas d'utilisation courants.
- Notez l'agent utilisateur et les URI des journaux F5 à l'étape ci-dessus, et voyez si les IOC sont liés aux alertes Red Condor. S'ils correspondent, alors c'est un véritable événement positif.

8. Dans l'action 10, sur la base de l'enquête effectuée jusqu'à présent, vous devez vérifier s'il s'agit d'un cas d'attaque possible par pulvérisation de mot de passe ou non.

9. Dans l'action 11, s'il s'agit d'une attaque par pulvérisation de mot de passe, effectuez les actions suivantes :

a. Dans l'action 12, vous devez vous coordonner avec les équipes appropriées pour verrouiller tous les comptes nécessaires et enquêter sur les activités malveillantes.

Playbook de pulvérisation de mot de passe possible



b. Dans l'action 13, vous devez lancer un examen post-incident de l'attaque possible par pulvérisation de mot de passe.

c. Dans l'action 14, le flux se termine.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Dans l'action 15, vous devez vérifier s'il ne s'agit pas d'un cas d'attaque possible par pulvérisation de mot de passe.
11. Dans l'action 16, s'il ne s'agit pas d'une attaque par pulvérisation de mot de passe, effectuez les actions suivantes :
    a. Dans l'action 17, vous devez documenter les résultats obtenus jusqu'à présent.
    b. Dans l'action 18, vous devez initier un examen post-incident de l'attaque possible par pulvérisation de mot de passe.
    c. Dans l'action 19, le flux se termine.
12. Dans l'action 20, vous devez consulter les pairs et le gestionnaire GIR pour obtenir des conseils.
13. Dans l'action 21, une tâche de réponse est créée pour terminer la revue post-incident avant de fermer la tâche.

Playbook pour T1003 : outils de détection de vidage des informations d'identification

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur un incident impliquant des activités de vidage d'identifiants.

Configurer le playbook T1003 - Détecter les outils de vidage des informations d'identification

Suivez les étapes suivantes pour configurer le playbook T1003 - Détecter les outils de vidage des informations d'identification.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **T1003 - Détecter les outils de vidage des informations d'identification** .
3. Facultatif : Vous pouvez créer une copie du flux de playbook T1003 - Détecter les outils de vidage des informations d'identification et y apporter les modifications nécessaires.

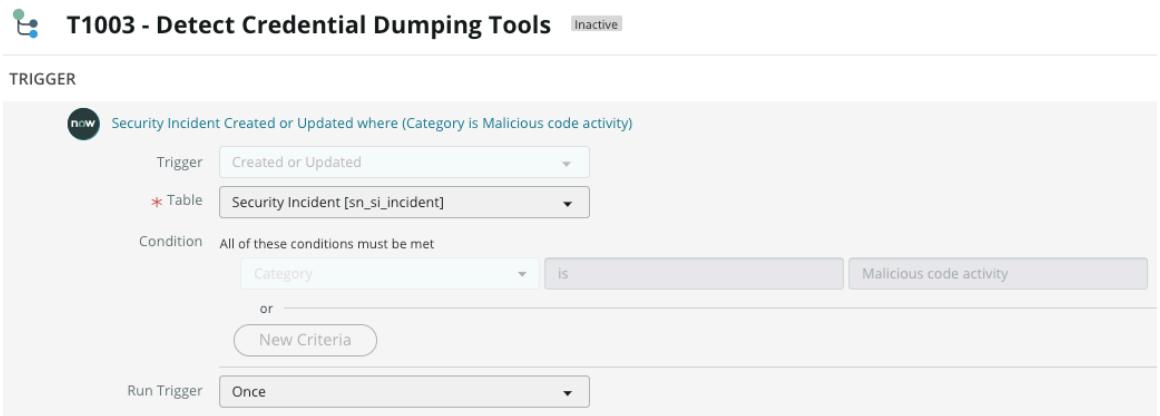
   Pour créer une copie du flux du playbook, cliquez sur l'icône de  et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Activité de code malveillant**.



Utiliser le playbook T1003 - Détecter les outils de vidage des informations d'identification

Utilisez ce playbook pour enquêter sur un incident impliquant des activités de vidage des informations d'identification. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le Playbook T1003 - Détecter les outils de vidage des informations d'identification.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

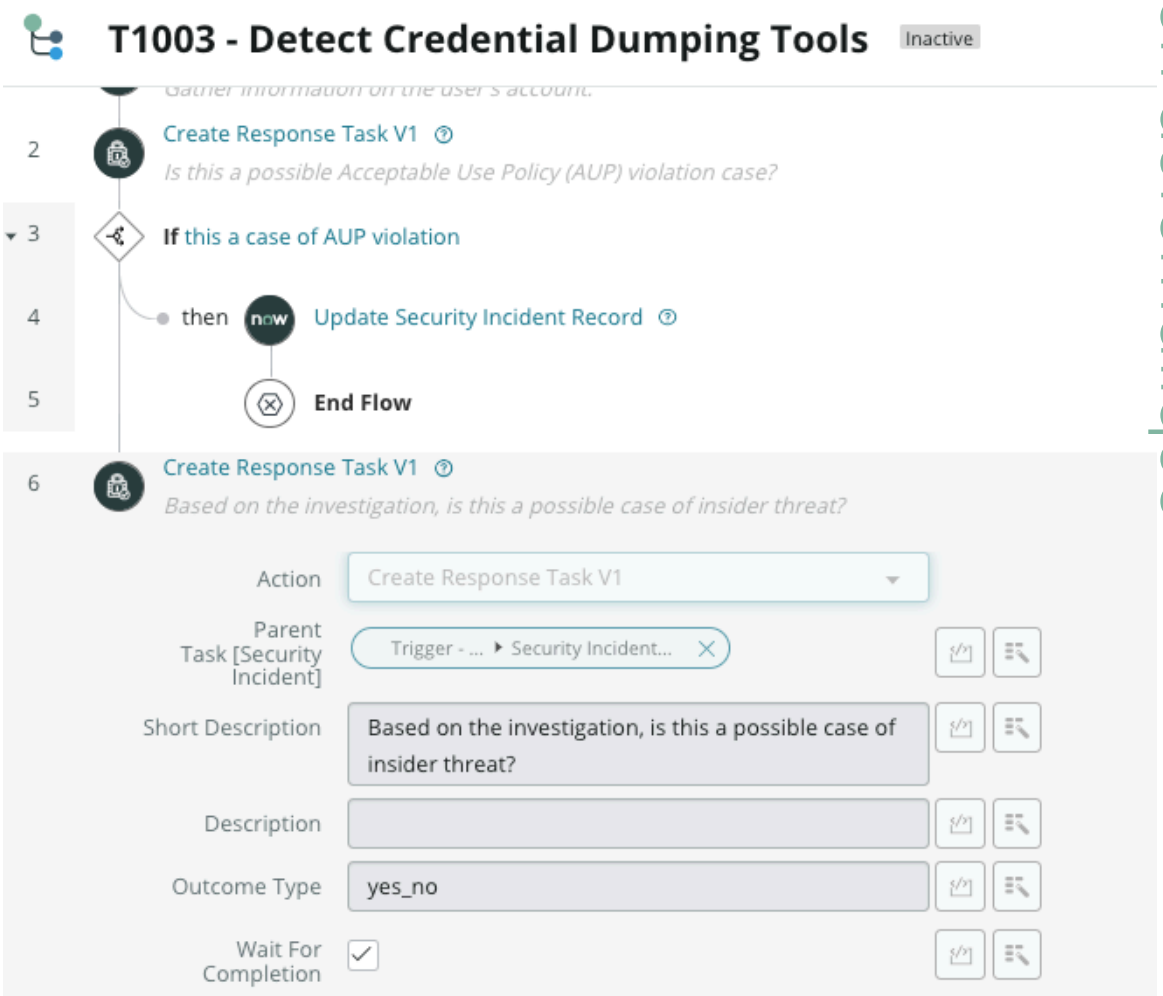
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez recueillir des informations sur le compte de l'utilisateur.
   - Vous devez vérifier l'activité de l'hôte pour rechercher toute activité suspecte.
   - Vous devez identifier le propriétaire du serveur/point de terminaison/machine virtuelle et capturer les données corrélées à l'outil.
   - Vous devez recueillir des informations sur les autres comptes de l'utilisateur.
2. Dans l'action 2, vous devez vérifier s'il s'agit d'un cas possible de violation de la politique d'utilisation acceptable (PUA).
   Vous pouvez procéder à un examen par les pairs avec les preuves recueillies et consulter votre gestionnaire d'incidents régional pour savoir s'il faut contacter l'utilisateur.
3. Dans l'action 3, s'il s'agit d'un cas de violation de la politique d'utilisation acceptable (PUA), effectuez les actions suivantes :
   a. Dans l'action 4, vous devez mettre à jour l'incident de sécurité pour indiquer qu'il s'agit d'un cas de violation de la PUA
   b. Dans l'action 5, le flux se termine.
4. Dans l'action 6, sur la base de l'enquête effectuée jusqu'à présent, vous devez vérifier s'il s'agit d'un cas possible de menace interne ou non.

T1003 : Playbook Détecter les outils de vidage des informations d'identification



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans l'action 7, s'il s'agit d'un cas de menace interne, effectuez les actions suivantes :

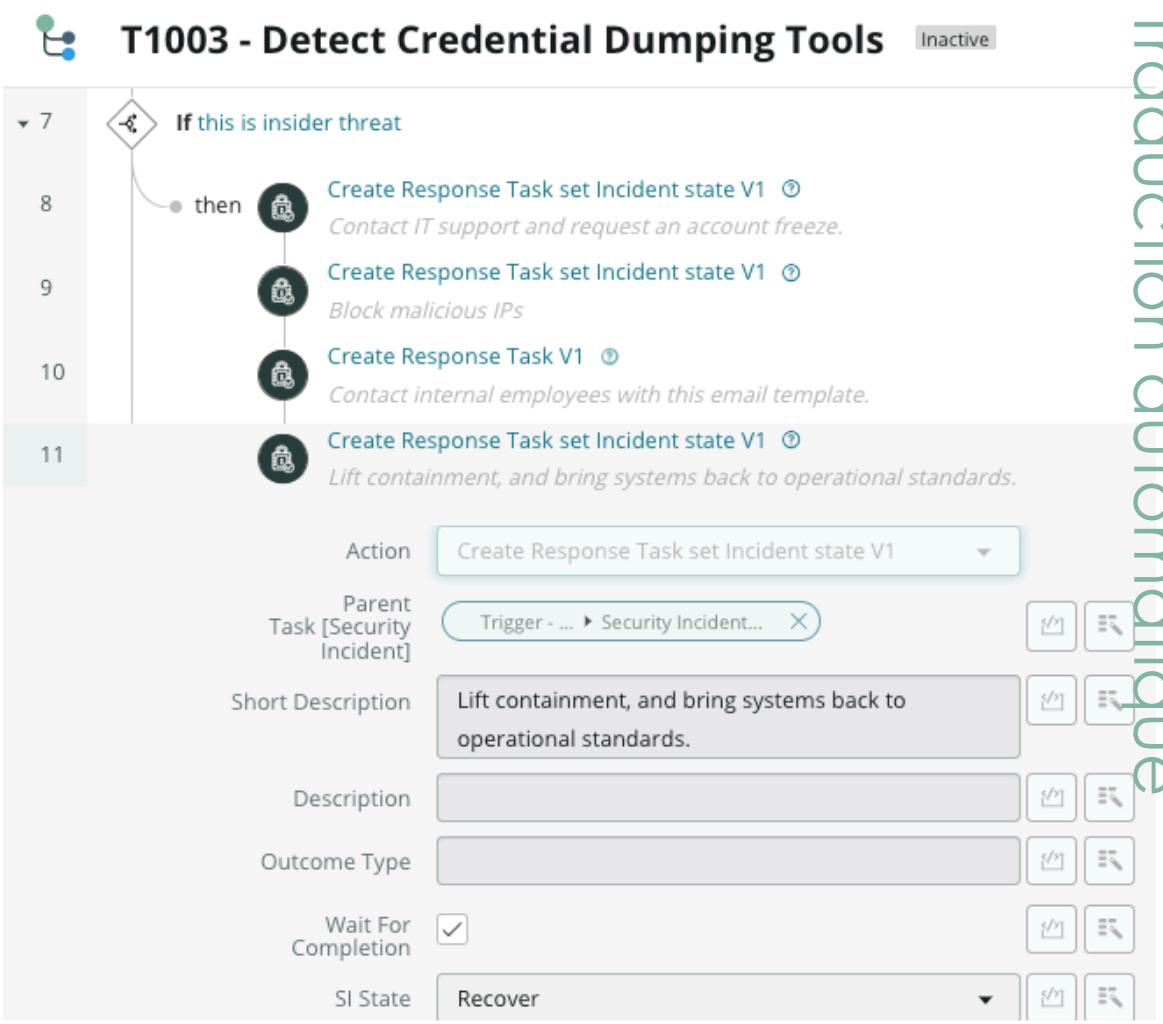
a. Dans l'action 8, vous devez contacter l'assistance informatique et demander un gel de compte.

b. Dans l'action 9, vous devez bloquer les adresses IP malveillantes.

c. Dans l'action 10, vous devez contacter les employés internes par e-mail.
Vous pouvez utiliser le modèle d'e-mail fourni pour contacter vos employés internes.

d. Dans l'action 11, vous devez lever le confinement et ramener les systèmes aux normes opérationnelles.
Le flux se termine.

Tâches d'intervention pour lever le confinement



6. Dans l'action 12, s'il ne s'agit pas d'une menace interne, dans l'action 13, vous devez effectuer un examen par les pairs pour déterminer si cela doit être ajouté à la liste d'exclusion.
Le flux se termine.

7. Dans l'action 14, une tâche de réponse est créée pour terminer la revue post-incident avant de fermer la tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook pour la détection d'usurpation de domaine de messagerie

Ce playbook facilite le tri précoce des soumissions de hameçonnage signalées par les utilisateurs en alertant l'analyste de la possibilité d'un domaine similaire dans l'adresse e-mail de l'hameçonnage.

Le playbook de détection d'usurpation de domaine d'e-mail recherche une correspondance de similarité entre le domaine de messagerie de l'expéditeur de l'hameçonnage et un nom de domaine approuvé existe dans le référentiel des observables. Lorsqu'une correspondance de domaine de messagerie de l'expéditeur usurpée a été identifiée par le playbook, les analystes sont alertés par une balise.

Le workflow est créé à partir d'un playbook existant, ce qui offre une approche cohérente et efficace pour l'examen des incidents. Chaque point de décision dans le playbook a été converti en une tâche axée sur les résultats et le flux change de direction en fonction du résultat de ces tâches.

Configurer le playbook de détection d'usurpation d'adresse e-mail

Suivez les étapes suivantes pour configurer le playbook de détection d'usurpation d'e-mail.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

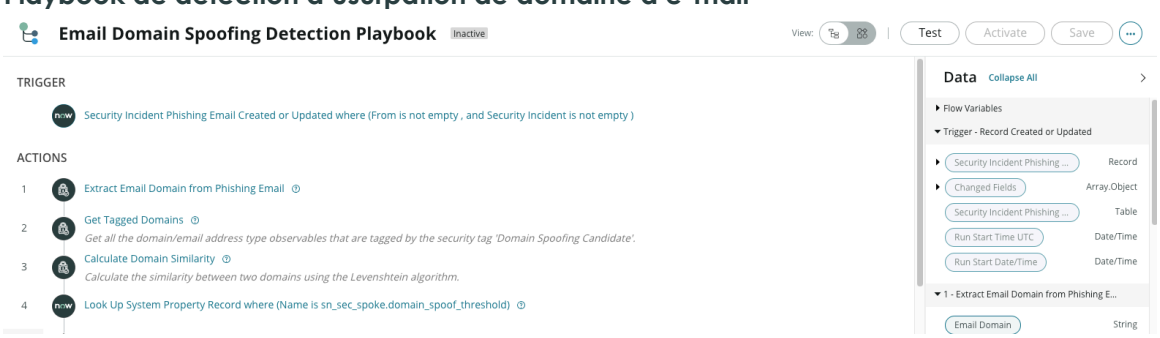
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le **playbook de détection d'usurpation de domaine de messagerie** .
3. Facultatif : Vous pouvez créer une copie du flux de playbook de détection d'usurpation de domaine de messagerie et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l'icône de ••• et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

Playbook de détection d'usurpation de domaine d'e-mail

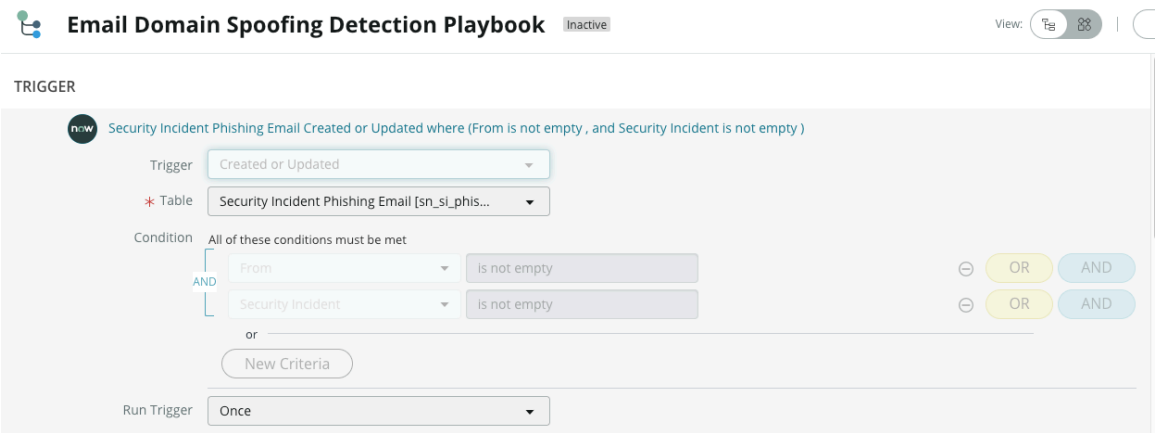


4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les modifications requises.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :
   - **De n'est** pas **vide**.
   - **L'incident de sécurité n'est** pas **vide**.



Utiliser le playbook de détection d'usurpation de domaine de messagerie

Utilisez ce playbook pour trouver une correspondance de similarité entre le domaine de messagerie de l'expéditeur de l'hameçonneur et un nom de domaine approuvé existe dans le référentiel des observables. Les étapes suivantes vous donnent un aperçu des actions, des tâches et des flux secondaires disponibles dans le playbook de détection d'usurpation de domaine de messagerie.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

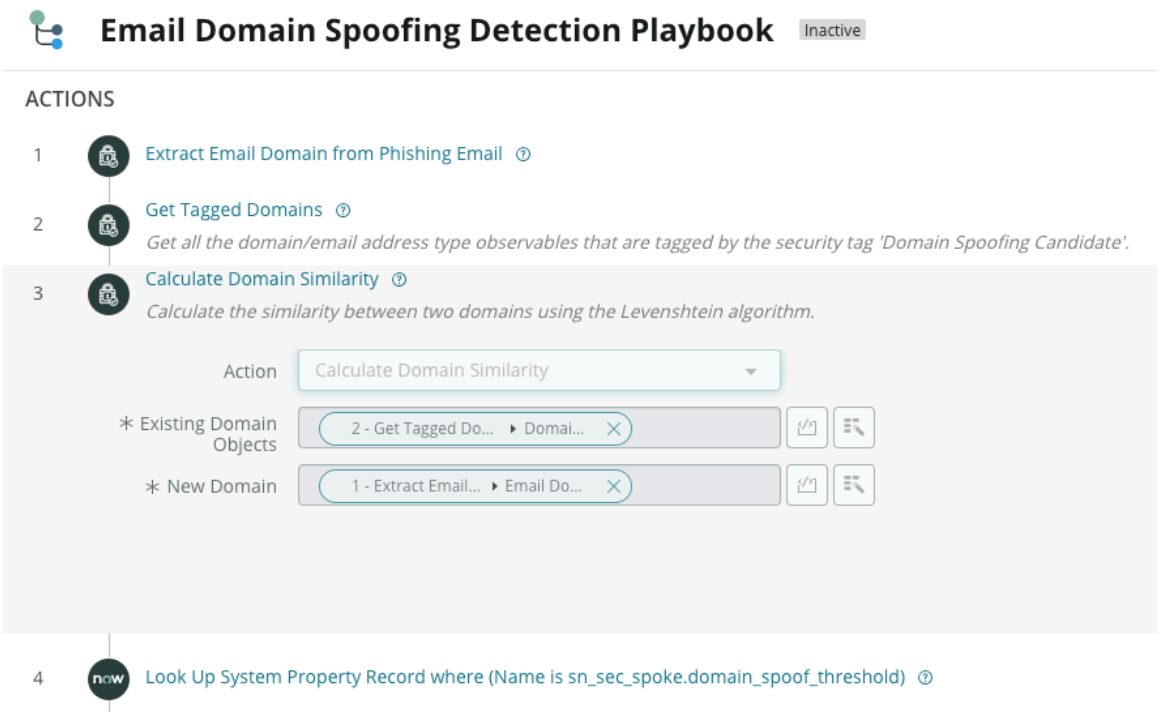
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, le playbook extrait le domaine d'e-mail de l'e-mail d'hameçonnage.
2. Dans l'action 2, le playbook récupère tous les observables de type domaine/adresse e-mail marqués par la balise de sécurité « Candidat d'usurpation de domaine ».
3. Dans l'action 3, le playbook calcule la similarité entre le domaine Get Tagged et le domaine Email à l'aide de l'algorithme de Levenshtein.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de détection d'usurpation de domaine d'e-mail



4. Dans l'action 4, le playbook recherche l'enregistrement Propriété système en fonction des conditions suivantes :
   - Le nom est sn_sec_spoke.domain_spoof_threshold, (OR)
   - Le nom va de a à z, et si plusieurs enregistrements sont trouvés, renvoyez uniquement le premier enregistrement.
5. Dans l'action 5, sur la base de l'enquête effectuée jusqu'à présent, le playbook vérifie si la similarité des deux domaines dépasse le seuil ou non.
   Si la similarité des deux domaines ne dépasse pas le seuil, une tâche de réponse manuelle est créée dans l'action 5 et le flux se termine. Si la similarité des deux domaines dépasse le seuil, les actions 6 et 7 sont exécutées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La similarité dépasse le seuil



6. Dans l'action 6, le playbook ajoute la balise de sécurité Usurpation de domaine de messagerie à l'incident de sécurité.
7. Dans l'action 7, le playbook ajoute un lien de note de travail au contexte à l'aide de l'option de script.
8. Dans l'action 8, le flux se termine.

Playbook pour le domaine squatté par typo

Ce playbook fournit des procédures systématiques pour enquêter sur les domaines mal orthographiés et collaborer avec le service juridique de l'organisation pour les retraits. Les domaines typosquattés sont des noms de domaine intentionnellement mal orthographiés qui ressemblent beaucoup aux domaines légitimes. Les attaquants profitent des fautes d'orthographe pour les diriger vers un site Web mal intentionné à des fins d'exploitation financière ou d'autres activités malveillantes.

Les domaines squattés par typo sont signalés à l'équipe des opérations de sécurité à partir de différentes sources, telles que les solutions de protection contre les risques numériques (Digital Shadows) et les plateformes de renseignements sur les menaces (Anomali Threatstream). Après la création d'un incident de sécurité, cette solution permet d'identifier si le domaine est effectivement un domaine squatté par typo. S'il s'agit d'un domaine squatté par une faute de frappe, l'analyste peut le signaler à l'équipe juridique afin que d'autres actions puissent être prises.

Le workflow est créé à partir d'un playbook existant, ce qui offre une approche cohérente et efficace pour l'examen des incidents. Chaque point de décision du playbook a été converti en une tâche axée sur les résultats, et le flux change de direction en fonction du résultat de ces tâches.

Configurer le playbook de domaine squatté par typo

Procédez comme suit pour configurer le playbook Domaine squatté par une faute de frappe.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **Domaine squatté par fautes de frappe** .
3. Facultatif : Vous pouvez créer une copie du flux du playbook de domaine squatté par typo et apporter les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, cliquez sur l'icône de ••• et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.



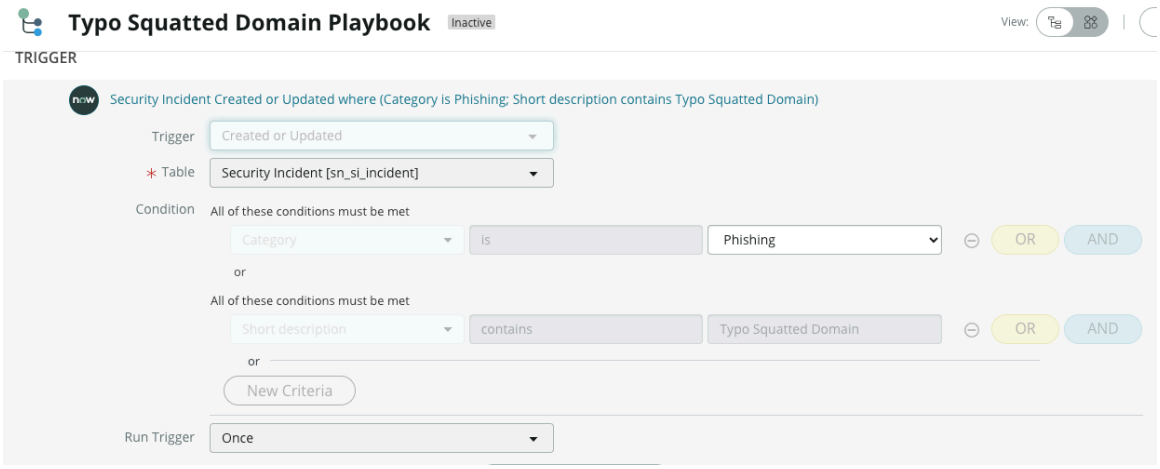
4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **La catégorie** est **Hameçonnage**.
- **La description courte** contient le **domaine squatté par typo**.



Utiliser le playbook de domaine squatté par typo

Utilisez ce playbook pour enquêter sur les domaines mal orthographiés et collaborer avec le service juridique de l'organisation pour les retraits. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Domaine squatté par typo.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

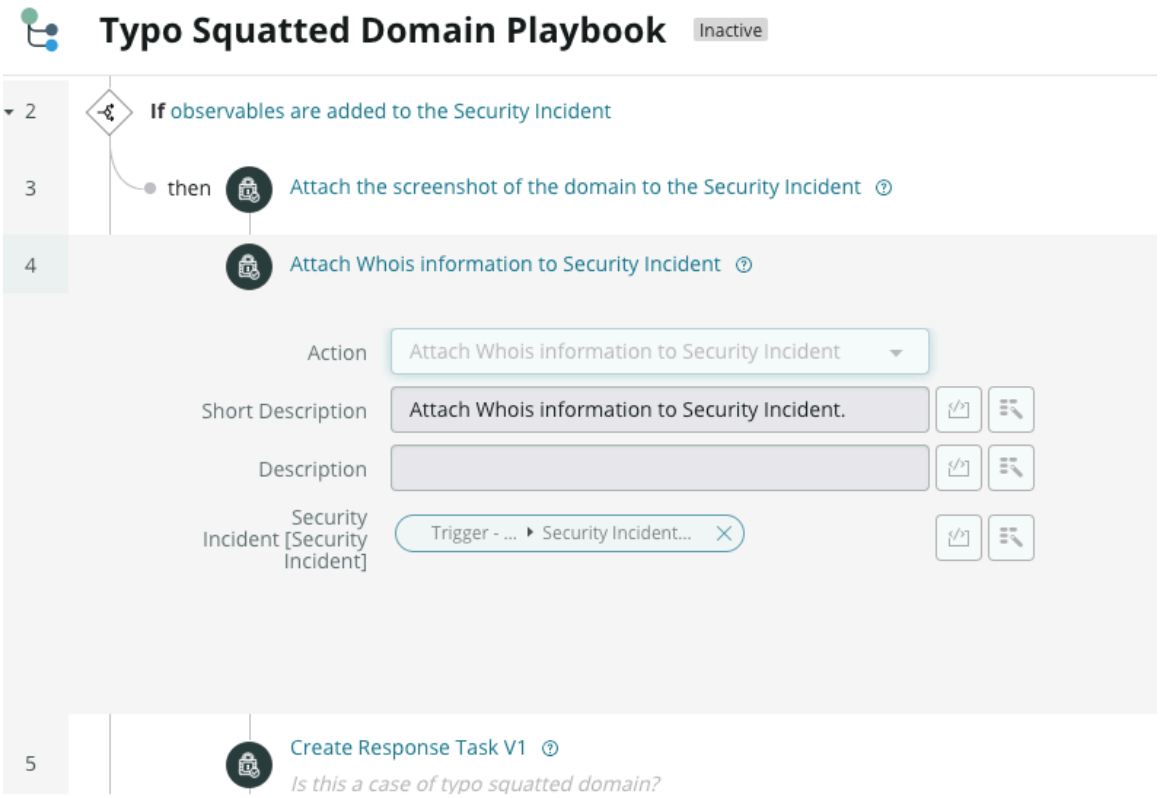
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez vérifier si les observables sont ajoutés à Security Incident Response (SIR).
   Si les observables ne sont pas ajoutés à SIR, veuillez ajouter les observables avant de poursuivre. Si les observables ne sont pas disponibles, l'action 10 est exécutée et l'incident de sécurité est clos.
2. Dans l'action 2, si les observables sont ajoutés à l'incident de sécurité, les actions suivantes sont exécutées.
3. Dans l'action 3, vous devez joindre la capture d'écran du domaine squatté par typo à l'incident de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Faute de frappe dans le playbook de domaine squatté



4. Dans l'action 4, vous devez joindre les informations d'identification à l'incident de sécurité.
5. Dans l'action 5, sur la base de l'enquête effectuée jusqu'à présent, le playbook vérifie s'il s'agit d'un cas de domaine squatté par typo ou non.
   S'il ne s'agit pas d'une faute de frappe dans le domaine, une tâche de réponse manuelle est créée dans l'action 5 et le flux se termine.
6. Dans l'action 6, s'il s'agit d'un domaine squatté par une faute de frappe, l'action 7 est exécutée.
7. Dans l'action 7, vous devez envoyer un e-mail et informer les équipes juridiques et autres équipes requises qu'il s'agit d'un cas de domaine squatté par coquille et prendre les mesures nécessaires pour l'éradiquer.
   S'il ne s'agit pas d'une faute de frappe dans le domaine, une tâche de réponse manuelle est créée dans l'action 5 et le flux se termine.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'une faute de frappe Domaine squatté



8. Dans l'action 9, une tâche de réponse est créée pour vous permettre de terminer la révision post-incident avant de fermer la tâche.

Playbook pour le reniflage d'informations d'identification

Ce playbook fournit les étapes de rattrapage du système pour enquêter sur un incident impliquant des activités de reniflage d'informations d'identification effectuées via la *sys_installation_exit* table dans une instance ServiceNow.

Le playbook de reniflage d'informations d'identification fournit un champ de script pour traiter les connexions à la base de données (base de données), l'authentification unique (SSO) et LDAP (protocole LDAP (protocole LDAP) à l'aide des enregistrements de la *sys_installation_exit* table. Ces champs de scripting privilégiés permettent l'écoute des demandes utilisateur et des paramètres des instances pendant la connexion, y compris les informations d'identification de l'utilisateur telles que le nom d'utilisateur et le mot de passe.

Un utilisateur malveillant peut créer un script pour écouter les demandes de l'utilisateur et enregistrer ces demandes sur l'instance. La *sys_installation_exit* table d'une instance définit les règles de traitement des activités de connexion et de déconnexion de tous les utilisateurs sur cette instance.

Configurer le playbook de reniflage d'informations d'identification

Suivez les étapes suivantes pour configurer le playbook de reniflage d'informations d'identification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

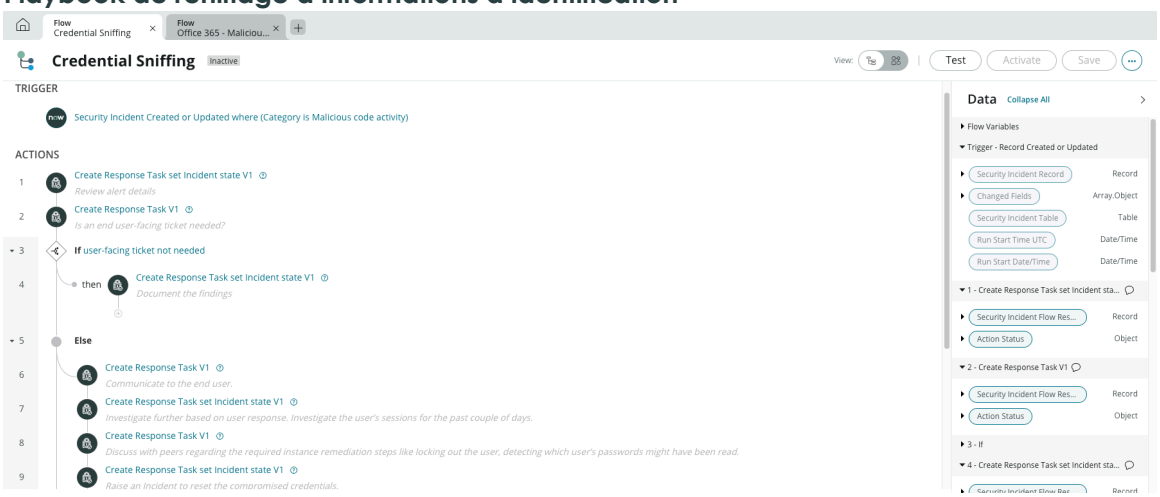
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **Reniflage d'informations d'identification** .
3. Facultatif : Créez une copie du flux de playbook de reniflage d'informations d'identification et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

Playbook de reniflage d'informations d'identification



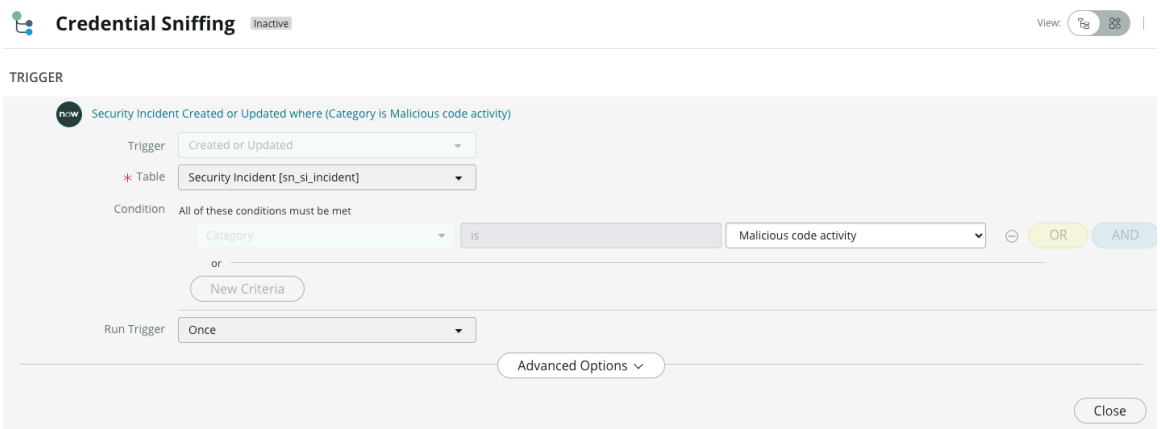
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Activité de code malveillant**.

Condition de déclenchement du Playbook de reniflage d'informations d'identification



Utiliser le playbook de reniflage d'informations d'identification

Utilisez ce playbook pour enquêter sur un incident impliquant des activités de reniflage d'informations d'identification effectuées via la *sys_installation_exit* table dans une instance ServiceNow. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Reniflage d'informations d'identification.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, examinez les détails d'alerte suivants.
   - Instance
   - ID de session
   - ID de transaction
   - _raw : fournit le script complet.

   Exemple de script :

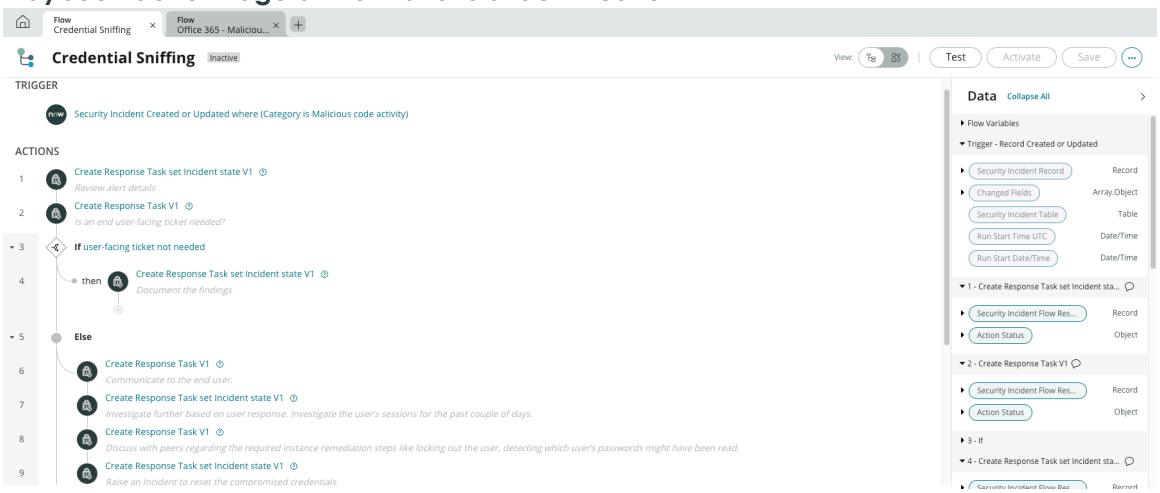
   ```
   Var pass= request.getParameter("user_password");
   Gs.log(pass);
   ```

2. Dans l'action 2, sur la base des données recueillies jusqu'à présent, vérifiez si un billet d'utilisateur final est requis pour cette alerte ou non.
3. Dans l'action 3, si l'alerte ne nécessite pas de ticket d'utilisateur final, dans l'action 4, documentez les résultats obtenus jusqu'à présent.
   Le flux se termine.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de reniflage d'informations d'identification



4. Dans l'action 5, si l'alerte nécessite un ticket d'utilisateur final, procédez comme suit :

a. Dans l'action 6, informez l'utilisateur final que l'alerte nécessite un ticket d'utilisateur final.

b. Dans l'action 7, examinez plus en détail en fonction de la réponse de l'utilisateur et des sessions de l'utilisateur au cours des deux derniers jours.

c. Dans l'action 8, discutez avec vos pairs des étapes de rattrapage de l'instance, comme le verrouillage de l'utilisateur et la détection des mots de passe de l'utilisateur qui ont peut-être été lus.

d. Dans l'action 9, soumettez un incident ou un ticket pour réinitialiser les informations d'identification de l'utilisateur compromis.

e. Dans l'action 10, lever le confinement et ramener les systèmes aux normes opérationnelles
Le flux se termine.

5. Dans l'action 11, terminez la vérification post-incident avant de fermer la tâche.

Playbook pour T1070 : journaux d'événements Windows effacés

Ce playbook fournit des étapes de rattrapage pour enquêter sur les incidents qui suivent les types d'événements pour lesquels l'utilisateur supprime les journaux de sécurité. Chaque fois que le journal de sécurité est effacé, les événements 517 et 1102 sont consignés, quel que soit l'état de la politique d'audit des événements système.

Cette alerte peut suivre les types d'événements suivants :

- **Événement 517** : Les champs Nom d'utilisateur principal et Nom d'utilisateur du client identifient l'utilisateur qui a effacé le journal. Le nom d'utilisateur principal correspond au système et le nom d'utilisateur client indique l'utilisateur qui a effacé le journal.
- **Événement 1102** : les champs Nom de compte et Nom de domaine identifient l'utilisateur qui a effacé le journal. L'ID de connexion vous permet d'effectuer une corrélation en arrière avec l'événement de connexion et d'autres événements enregistrés au cours de la même session de connexion.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer le T1070 : Journaux d'événements Windows effacés Playbook

Procédez comme suit pour configurer le playbook T1070 - Journaux d'événements Windows effacés.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **T1070 - Journaux d'événements Windows effacés** .
3. Facultatif : Créer une copie du flux de playbook T1070 - Journaux d'événements Windows effacé et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.



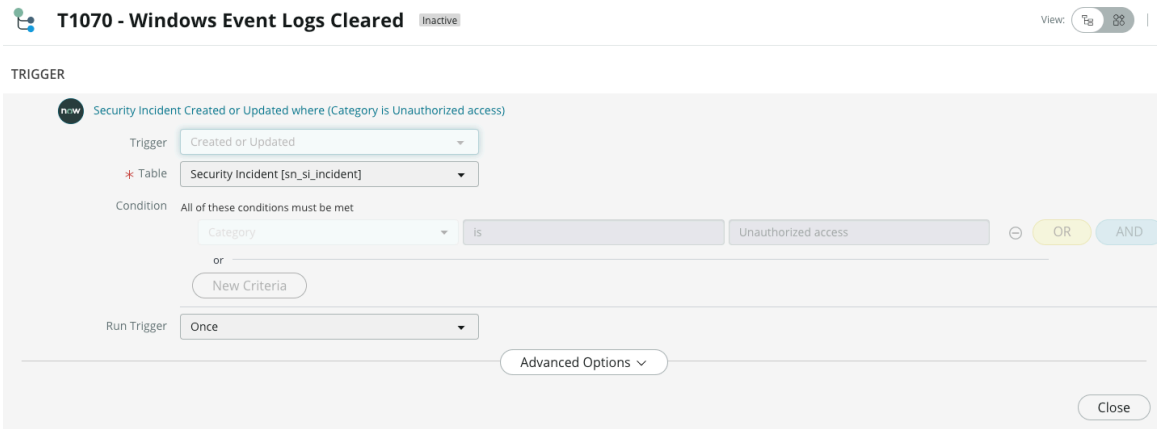
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Accès non autorisé**.

T1070 : les journaux d'événements Windows ont effacé la condition de déclenchement du Playbook



Utiliser le T1070 - Journaux d'événements Windows effacés Playbook

Utilisez ce playbook pour enquêter sur les incidents qui suivent les types d'événements pour lesquels l'utilisateur supprime les journaux de sécurité. Les étapes suivantes vous donnent un aperçu des actions, des tâches et des flux secondaires disponibles dans le T1070 : Playbook Journaux d'événements Windows effacés.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, obtenez les détails de l'utilisateur à partir de l'alerte.
2. Dans l'action 2, vérifiez si l'utilisateur a été identifié ou non.
3. Dans l'action 3, si l'utilisateur n'a pas été identifié, procédez comme suit :

   a. Dans l'action 4, vérifiez la CMDB (Configuration Management Database) pour les détails du propriétaire de l'hôte.

   b. Dans l'action 5, vérifiez si l'utilisateur a été identifié à partir de la CMDB ou non.

      Si l'utilisateur a été identifié à partir de la CMDB, une tâche de réponse manuelle est créée dans l'action 5 et le flux se termine.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Dans l'action 6, si l'utilisateur n'a pas été identifié à partir de la CMDB, procédez comme suit :

i. Dans l'action 7, créez un incident pour identifier le propriétaire du système et la personne qui a supprimé les journaux.

ii. Dans l'action 8, vérifiez si l'utilisateur a été identifié après avoir soumis un incident ou non.

Si l'utilisateur a été identifié après avoir soumis un incident, une tâche de réponse manuelle est créée dans l'action 8 et le flux se termine.

iii. Dans l'action 9, si l'utilisateur n'a pas été identifié après avoir soumis un incident, procédez comme suit :

1. Dans l'action 10, discutez du prochain plan d'action avec vos pairs.

2. Dans l'action 11, isolez le système hôte.

3. Dans l'action 12, supprimez tous les fichiers indésirables qui ont pu être créés et supprimez les comptes indésirables.

4. Dans l'action 13, levez le confinement et ramenez les systèmes aux normes opérationnelles.

5. Dans l'action 14, terminez la revue post-incident avant de fermer la tâche.

Dans l'action 15, le flux se termine.

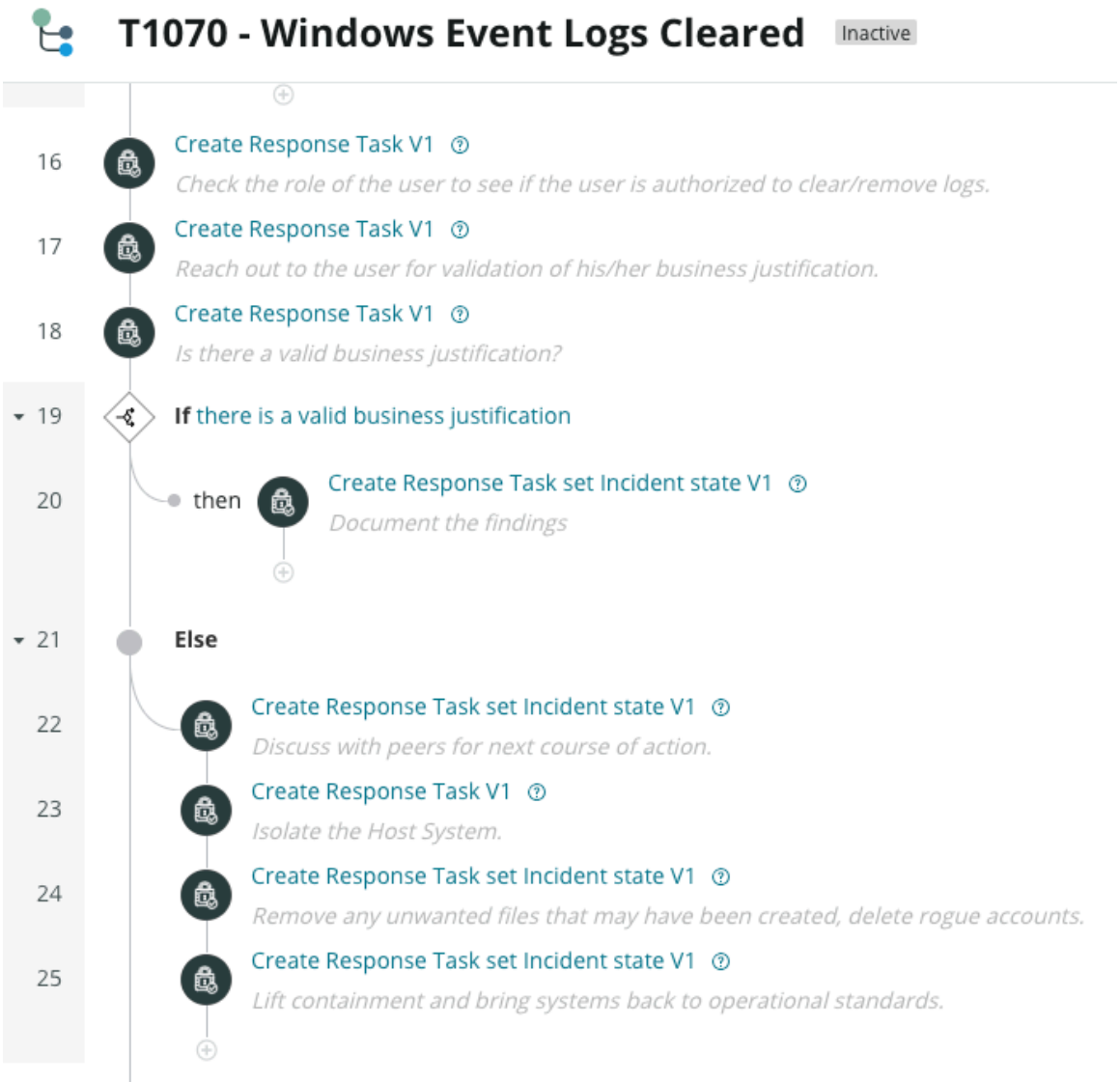
4. Dans l'action 16, si l'utilisateur a été identifié, vérifiez son rôle pour voir s'il est autorisé à effacer ou supprimer des journaux.

5. Dans l'action 17, contactez l'utilisateur pour valider sa justification commerciale. Vous pouvez utiliser le modèle d'e-mail fourni pour contacter l'utilisateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du T1070 : Playbook des journaux d'événements Windows effacés



Traduction automatique

6. Dans l'action 18, vérifiez si une justification commerciale valide est fournie ou non.
7. Dans l'action 19, s'il y avait une justification commerciale valide fournie, alors dans l'action 20, documentez les résultats jusqu'à présent.
   Le flux se termine.
8. Dans l'action 21, si aucune justification commerciale valide n'a été fournie, procédez comme suit :

   a. Dans l'action 22, discutez du prochain plan d'action avec vos pairs.

   b. Dans l'action 23, isolez le système hôte.

   c. Dans Action 24, supprimez tous les fichiers indésirables qui ont pu être créés et supprimez les comptes indésirables.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Dans l'action 25, lever le confinement et ramener les systèmes aux normes opérationnelles.
Le flux se termine.

9. Dans l'action 26, terminez la revue post-incident avant de fermer la tâche.

Playbook pour OSquery d'adresse externe dans le fichier /etc/hosts

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents qui indiquent qu'un nom d'hôte ou un domaine interne a été affecté à une adresse IP externe sur le DNS local (/etc/hosts) d'un serveur Linux.

Configurer la requête système d'exploitation de l'adresse externe dans le playbook de fichier /etc/hosts

Pour configurer la requête système d'exploitation d'adresse externe dans le playbook de fichier /etc/hosts, procédez comme suit.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

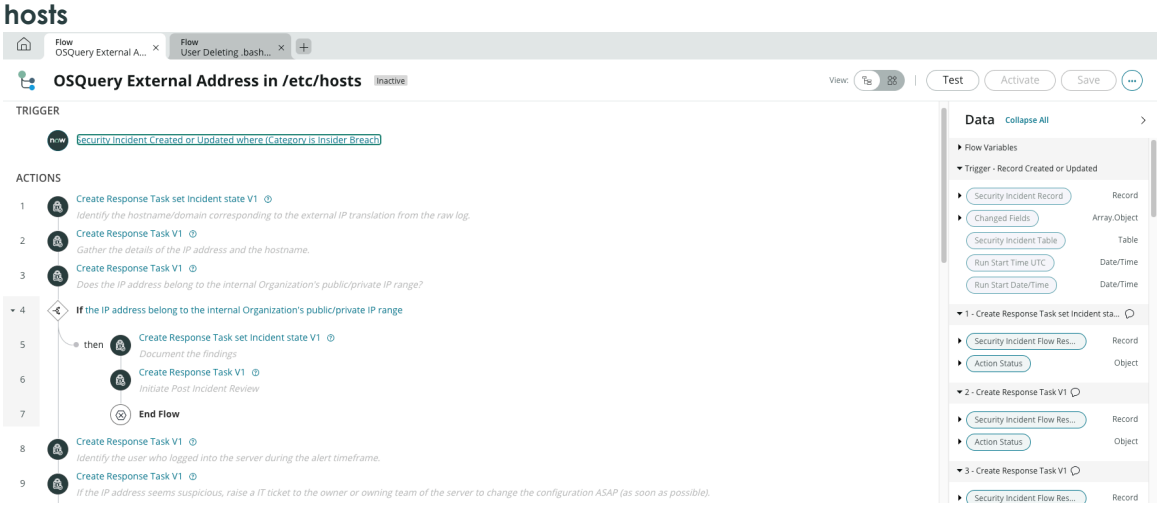
1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.

2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez **l'adresse externe OSquery dans le playbook /etc/hosts** .

3. Facultatif : Créez une copie de l'adresse externe OSquery dans le flux de playbook /etc/hosts et apportez les modifications nécessaires.

(Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

Requête système d'exploitation d'adresse externe dans le playbook /etc/hosts



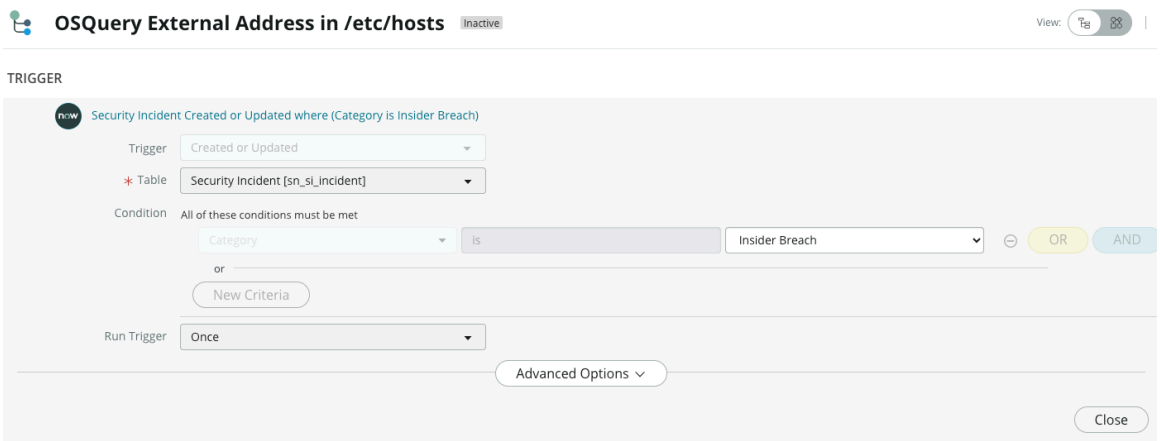
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Violation interne**.

Requête système d'exploitation d'adresse externe dans /etc/hosts condition de déclenchement du playbook



Utiliser l'OSquery de l'adresse externe dans le playbook de fichier /etc/hosts

Utilisez ce playbook pour examiner les incidents qui indiquent qu'un nom d'hôte ou un domaine interne a été affecté à une adresse IP externe sur le DNS local (/etc/hosts) d'un serveur Linux. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans l'OSquery d'adresse externe dans le playbook de fichier /etc/hosts.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

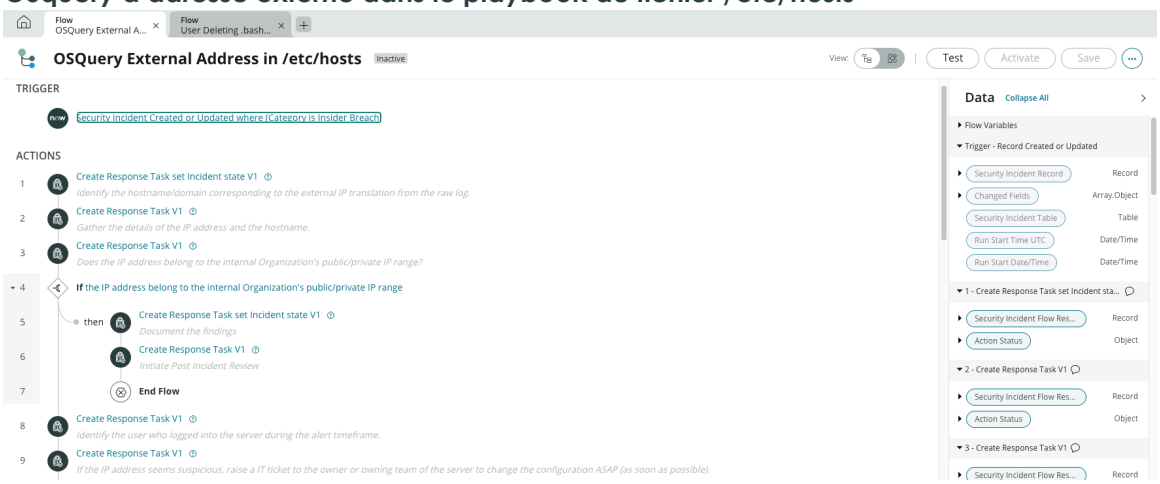
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, identifiez le nom d'hôte ou le nom de domaine correspondant à la traduction de l'adresse IP externe à partir du journal brut.
2. Dans l'action 2, rassemblez les détails de l'adresse IP et du nom d'hôte.
3. Dans l'action 3, vérifiez si cette adresse IP appartient ou non à la plage d'adresses IP publique/privée de l'organisation interne.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

OSquery d'adresse externe dans le playbook de fichier /etc/hosts



4. Dans l'action 4, si l'adresse IP appartient à la plage d'adresses IP publique/privée de l'organisation interne, procédez comme suit :

   a. Dans l'action 5, documentez les résultats obtenus jusqu'à présent.

   b. Dans l'action 6, lancez une revue post-incident.
   Dans l'action 7, après la revue post-incident, le flux se termine.

5. Si l'adresse IP n'appartient pas à la plage d'adresses IP publique/privée de l'organisation interne, identifiez l'utilisateur qui s'est connecté au serveur pendant la période de l'alerte dans Action 8.
6. Dans l'action 9, si l'adresse IP semble suspecte, soumettez un ticket informatique au propriétaire ou à l'équipe du serveur pour modifier la configuration dès que possible.
7. Dans l'action 10, vérifiez s'il y a eu une activité malveillante sur le serveur avant et après l'ajout de l'entrée DNS.
8. Dans l'action 11, vérifiez s'il y a des connexions à l'adresse IP externe à partir du serveur.
9. Dans l'action 12, documentez les résultats obtenus jusqu'à présent.
10. Dans l'action 13, vérifiez si les informations du propriétaire ou de l'équipe sont disponibles ou non.
11. Dans l'action 14, si des informations sur le propriétaire ou l'équipe sont disponibles, procédez comme suit :

    a. Dans l'action 15, contactez le propriétaire ou l'équipe du serveur pour voir s'ils reconnaissent l'activité.
    Vous pouvez utiliser le modèle d'e-mail fourni pour contacter le propriétaire ou l'équipe du serveur.

    b. Dans l'action 16, vérifiez si le propriétaire ou l'équipe a fourni une justification commerciale valide ou non.

    c. Dans l'action 17, si le propriétaire ou l'équipe fourni n'a pas fourni de justification commerciale valide, le flux s'arrête.
    Toutefois, si le propriétaire ou l'équipe a fourni une justification commerciale valide, procédez comme suit :

Traduction automatique

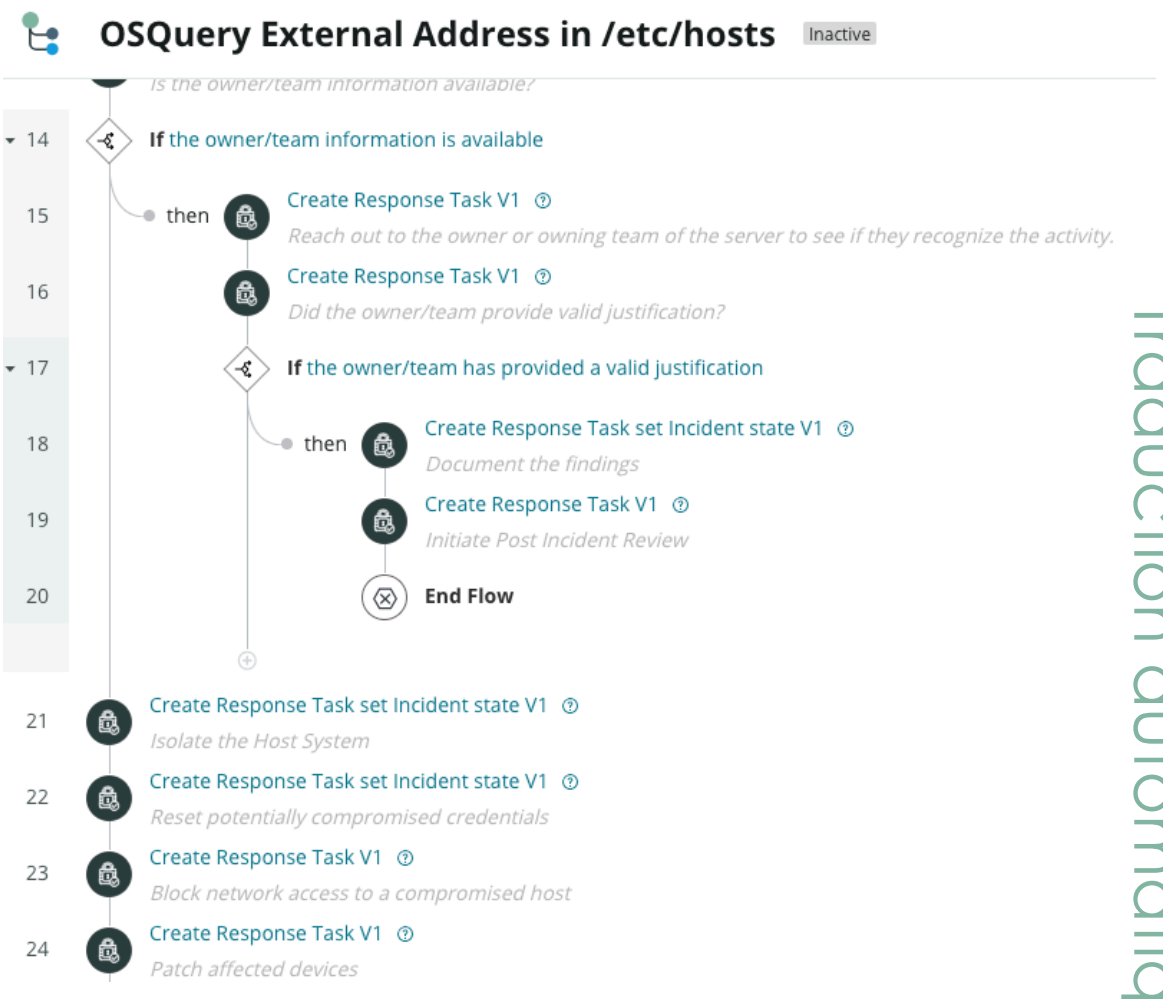
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Dans l'action 18, documentez les résultats obtenus jusqu'à présent.

ii. Dans l'action 19, lancez une revue post-incident.

Dans l'action 20, après la revue post-incident, le flux se termine.

Utilisation de l'osquery d'adresse externe dans le playbook de fichier /etc/hosts



12. Dans l'action 21, si les informations sur le propriétaire ou l'équipe ne sont pas disponibles, isolez le système hôte.
13. Dans l'action 22, réinitialisez les informations d'identification potentiellement compromises.
14. Dans l'action 23, bloquez l'accès réseau à l'hôte compromis.
15. Dans Action 24, corrigez les appareils concernés.
16. Dans l'action 25, lever le confinement et ramener les systèmes aux normes opérationnelles.
17. Dans l'action 26, terminez la revue post-incident avant de fermer la tâche.

Playbook pour la suppression de l'historique Bash par l'utilisateur : cloud

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents qui indiquent si quelqu'un essayait de supprimer le fichier d'historique bash (`.bash_history`) d'un serveur Linux.

Remarque : Vous devez atténuer cette alerte avec précaution, car elle est rarement déclenchée et indique potentiellement une menace interne.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer le playbook Historique Bash de suppression par l'utilisateur

Procédez comme suit pour configurer le playbook Historique Bash de suppression par l'utilisateur.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

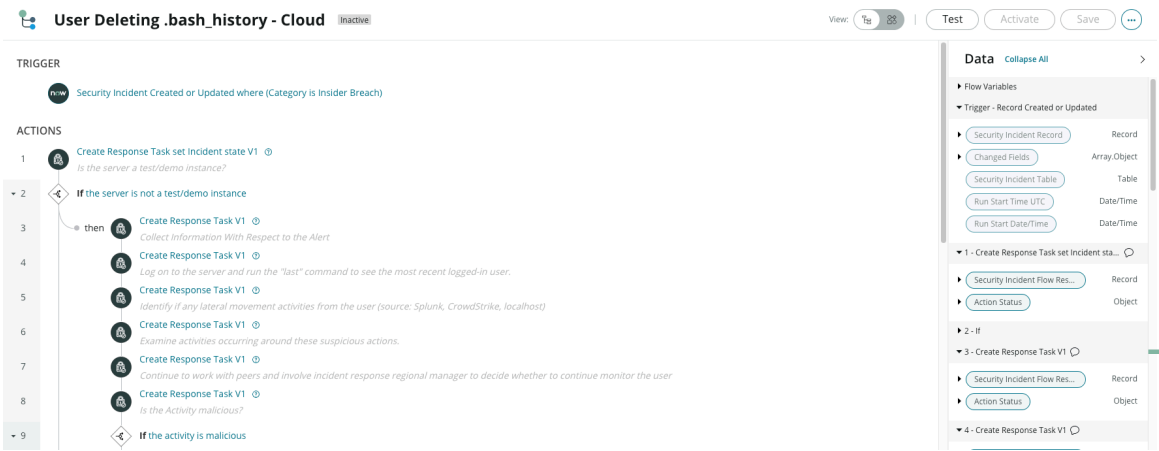
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le **playbook Suppression de l'utilisateur .bash_history - Cloud** .
3. Facultatif : Créez une copie du flux de playbook Suppression de l'utilisateur .bash_history - Cloud et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

Suppression par l'utilisateur de l'historique Bash : playbook dans le cloud



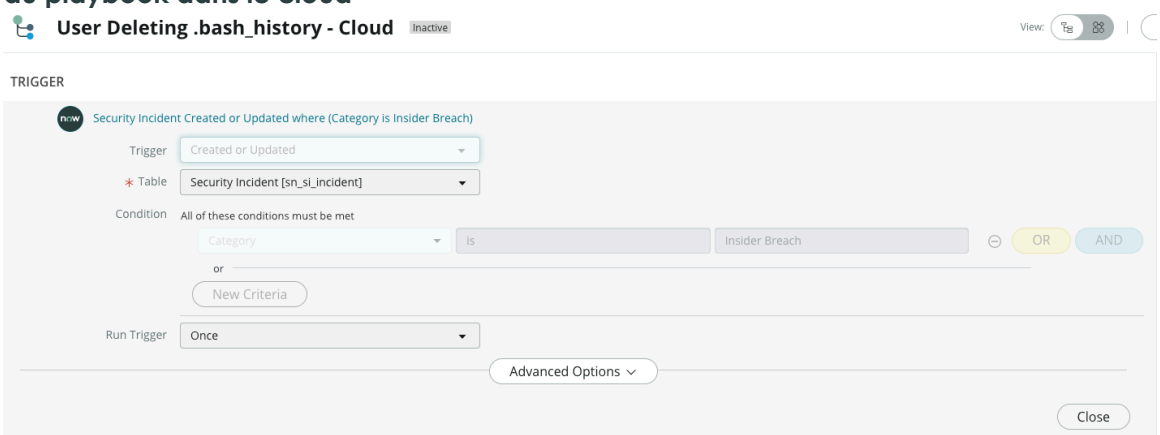
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Violation interne**.

Suppression par l'utilisateur de l'historique Bash : condition de déclenchement du playbook dans le cloud



Utiliser le playbook Historique Bash de suppression par l'utilisateur

Utilisez ce playbook pour enquêter sur les incidents qui indiquent si quelqu'un essayait de supprimer le fichier d'historique bash d'un serveur Linux. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires qui sont disponibles dans le playbook Suppression utilisateur de l'historique Bash (*.bash_history*).

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vérifiez si le serveur est une instance de test ou de démonstration.
2. Dans l'action 2, si le serveur n'est pas une instance de test ou de démonstration, procédez comme suit :

   a. Dans l'action 3, collectez les informations suivantes pour l'alerte :
      - Nom d'utilisateur
      - Adresse IP
      - Commandes malveillantes tentant de supprimer l'historique bash
      - Toutes les commandes exécutées par l'utilisateur, si elles sont disponibles dans les journaux CrowdStrike.

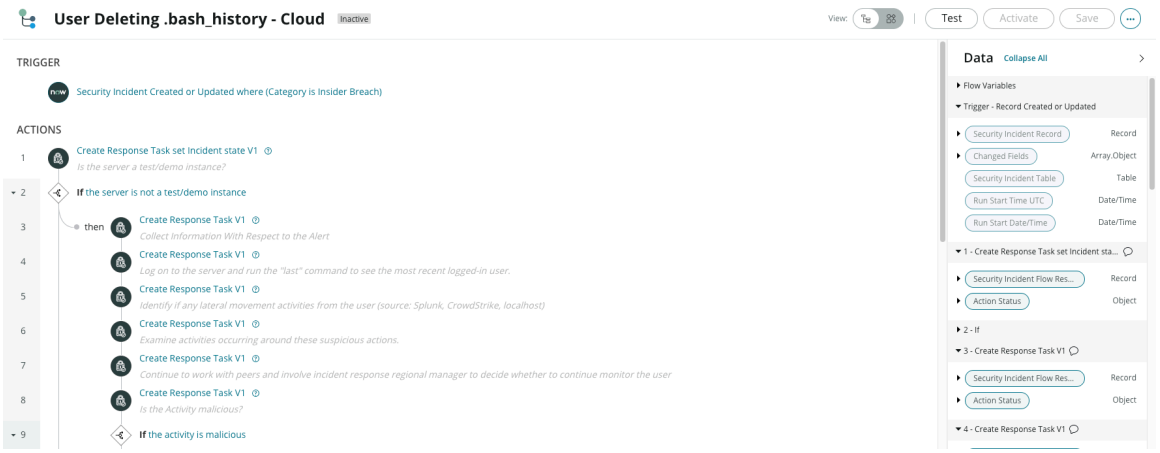
   b. Dans l'action 4, connectez-vous au serveur et exécutez la *dernière* commande pour afficher le dernier utilisateur connecté.

   c. Dans l'action 5, identifiez s'il y a eu des activités de mouvement latéral de la part de l'utilisateur (source : Splunk, CrowdStrike, localhost).

   d. Dans l'action 6, examinez les activités qui se déroulent autour de ces actions suspectes.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suppression par l'utilisateur du playbook d'historique Bash



e. Dans l'action 7, continuez à travailler avec vos pairs et impliquez le responsable régional de la réponse aux incidents dans la décision de continuer ou non à surveiller l'utilisateur.

f. Dans Action 8, déterminez si l'activité est malveillante ou non.

g. Dans l'action 9, si l'activité est malveillante, procédez comme suit :

i. Dans l'action 10, pendant l'enquête, contactez l'assistance informatique et demandez un gel de compte.

ii. Dans l'action 11, assurez-vous que l'instance est restaurée à un état normal exempt d'activités malveillantes.

iii. Dans l'action 12, lever le confinement et ramener les systèmes aux normes opérationnelles.

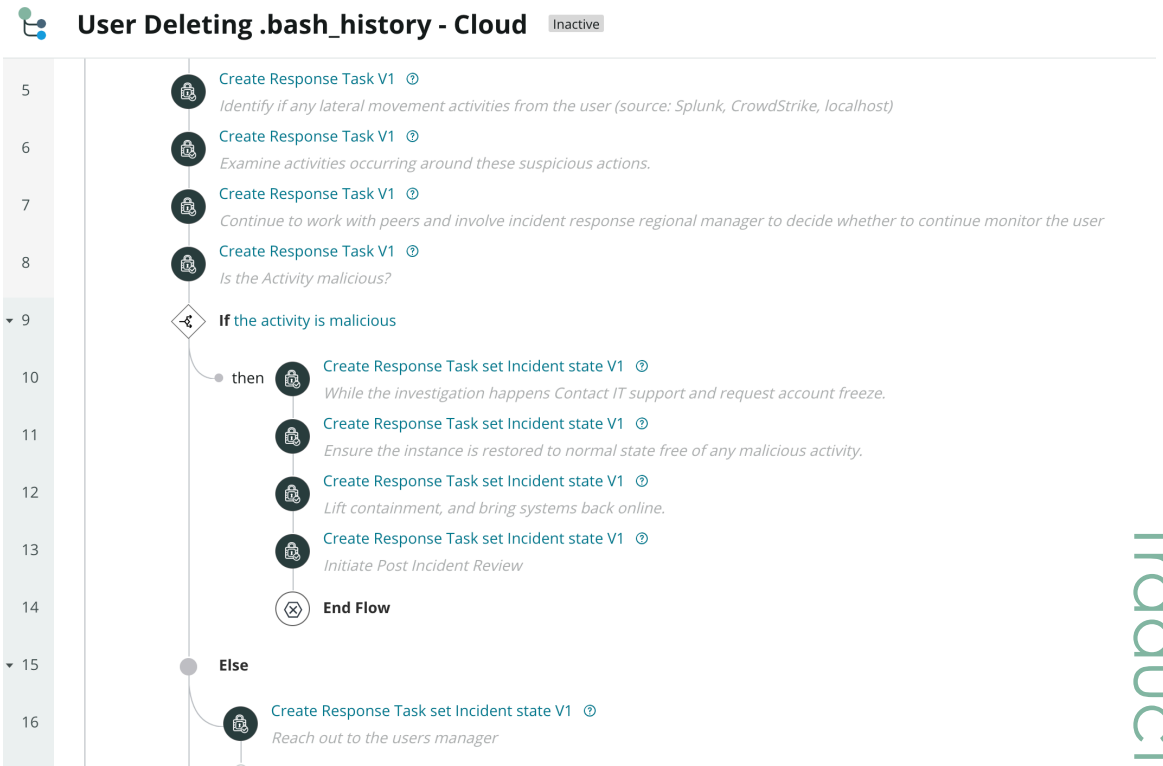
iv. Dans l'action 13, lancez une revue post-incident.

Dans l'action 14, après la revue post-incident, le flux se termine.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook Historique Bash de suppression par l'utilisateur



h. Dans l'Action 15, si l'activité n'est pas malveillante, contactez le responsable de l'utilisateur dans l'Action 16.
Vous pouvez utiliser le modèle d'e-mail fourni pour contacter le responsable de l'utilisateur et l'informer de l'approche recommandée.

3. Dans l'action 17, documentez les résultats obtenus jusqu'à présent.

4. Dans l'action 18, terminez la revue post-incident avant de fermer la tâche.

Playbook pour les tentatives réussies de VPN à partir des comptes de service : entreprise/cloud

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents qui suivent les tentatives de connexion réussies à partir de comptes de service via VPN. Les comptes de service ne sont pas censés avoir des événements de connexion à partir d'un VPN, et de tels événements pourraient être des indicateurs de force brute ou d'une éventuelle exposition des informations d'identification du compte.

Configurer les tentatives VPN réussies à partir du playbook des comptes de services

Suivez les étapes suivantes pour configurer les tentatives VPN réussies à partir du playbook Comptes de service.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Traduction automatique

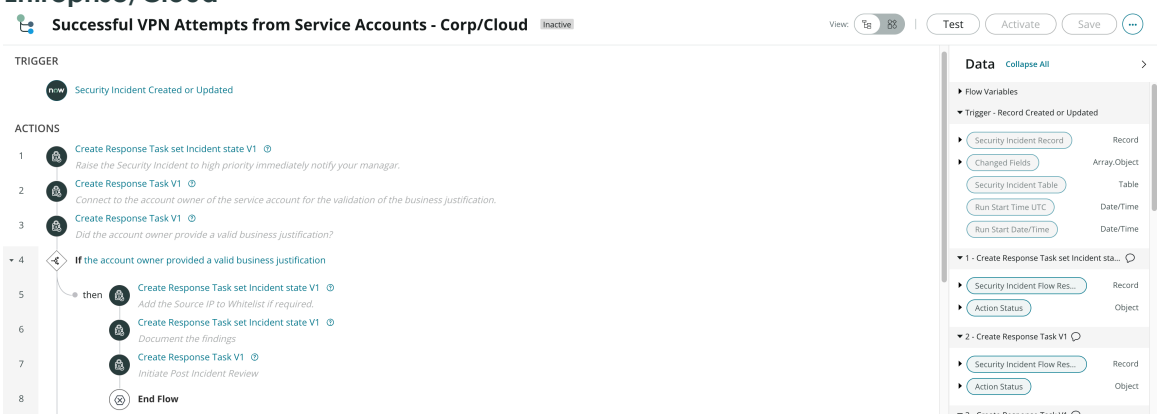
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez les **tentatives VPN réussies dans le playbook Comptes de services** .
3. Facultatif : Créez une copie des tentatives VPN réussies à partir du flux Playbook des comptes de service et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

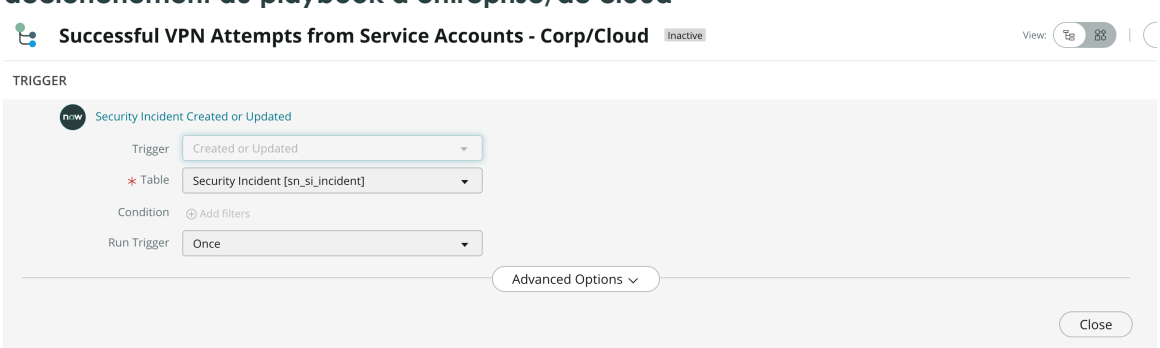
Tentatives VPN réussies à partir du playbook des comptes de service - Entreprise/Cloud



4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque l'incident de sécurité est créé ou mis à jour en fonction de vos conditions requises. Par exemple, lorsque **la catégorie** est **Violation interne**.

Tentatives VPN réussies à partir des comptes de service : condition de déclenchement du playbook d'entreprise/de cloud



Utiliser les tentatives VPN réussies à partir du playbook des comptes de service

Utilisez ce playbook pour enquêter sur les incidents qui suivent les tentatives de connexion réussies à partir de comptes de service via VPN. Les étapes suivantes vous donnent une

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

procédure pas à pas des actions, des tâches et des flux secondaires qui sont disponibles dans les tentatives VPN réussies à partir du playbook Comptes de services.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, augmentez l'incident de sécurité en haute priorité et informez immédiatement votre responsable.
2. Dans l'action 2, contactez le propriétaire du compte de service pour valider la justification commerciale.
   Vous pouvez utiliser le modèle d'e-mail fourni pour contacter le propriétaire du compte de service afin de valider la justification commerciale.
3. Dans l'action 3, vérifiez si le propriétaire du compte de service a fourni une justification commerciale valide.



4. Dans l'action 4, si le propriétaire du compte de service a fourni une justification commerciale valide, procédez comme suit :

   a. Dans l'action 5, ajoutez l'adresse IP source à la liste d'autorisation si nécessaire.

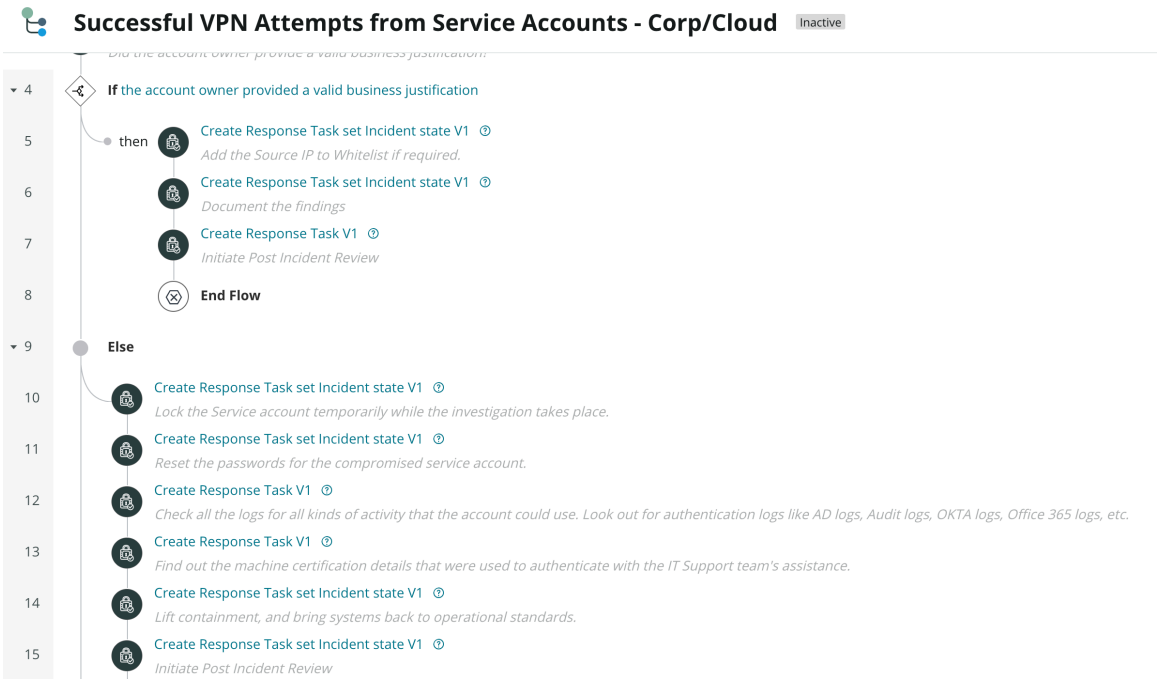
   b. Dans l'action 6, documentez les résultats obtenus jusqu'à présent.

   c. Dans l'action 7, lancez une révision post-incident.
   Dans l'action 8, après la revue post-incident, le flux se termine.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation des tentatives VPN réussies à partir du playbook Comptes de services - Entreprise/Cloud



5. Dans l'action 9, si le propriétaire du compte de service n'a pas fourni de justification commerciale valide, procédez comme suit :

a. Dans l'action 10, verrouillez temporairement le compte de service pendant que l'enquête est en cours.

b. Dans l'action 11, réinitialisez les mots de passe du compte de service compromis.

c. Dans l'action 12, vérifiez les journaux pour tous les types d'activités que le compte pourrait utiliser.
Recherchez les journaux d'authentification tels que les journaux Active Directory, les journaux d'audit, les journaux Okta, les journaux Office 365, etc.

d. Dans l'action 13, recherchez les détails de certification de la machine utilisés pour vous authentifier avec l'aide de l'équipe d'assistance informatique.

e. Dans l'action 14, lever le confinement et ramener les systèmes aux normes opérationnelles.

f. Dans l'action 15, terminez la revue post-incident avant de fermer la tâche.

Playbook pour tentative d'accès aux comptes désactivés

Ce playbook se déclenche lorsqu'un employé dont le compte est résilié, désactivé ou séparé tente de se connecter avec ses informations d'identification. L'état d'identité de l'utilisateur dans le point de navigation est généralement mis à jour pour être désactivé à la date de résiliation.

30 jours est le délai idéal à partir de la date d'arrêt pour qu'il soit mis à jour vers un état séparé. Vous pouvez utiliser la logique métier dans le point de navigation pour supprimer les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

comptes RSA et supprimer les appartenances à des groupes Active Directory (AD) après 30 jours.

Configurer le playbook de la tentative d'accès désactivé

Suivez les étapes suivantes pour configurer le playbook de tentative d'accès au compte désactivé.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **Compte désactivé pour tentative d'accès** .
3. Facultatif : Créez une copie du flux de playbook Compte désactivé de tentative d'accès et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.



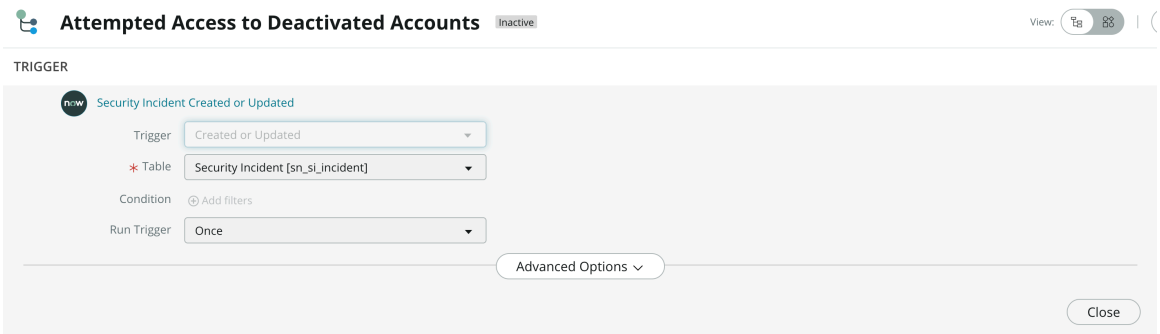
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché lorsque l'incident de sécurité est créé ou mis à jour en fonction de vos conditions requises. Par exemple, lorsque **la catégorie** est **Violation d'initié**

Tentative d'accès aux comptes désactivés Condition de déclenchement du Playbook



Utiliser le playbook de tentative d'accès aux comptes désactivés

Utilisez ce playbook lorsqu'un employé dont le compte est résilié, désactivé ou séparé tente de se connecter avec ses informations d'identification. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook de tentatives d'accès aux comptes désactivés.

Avant de commencer

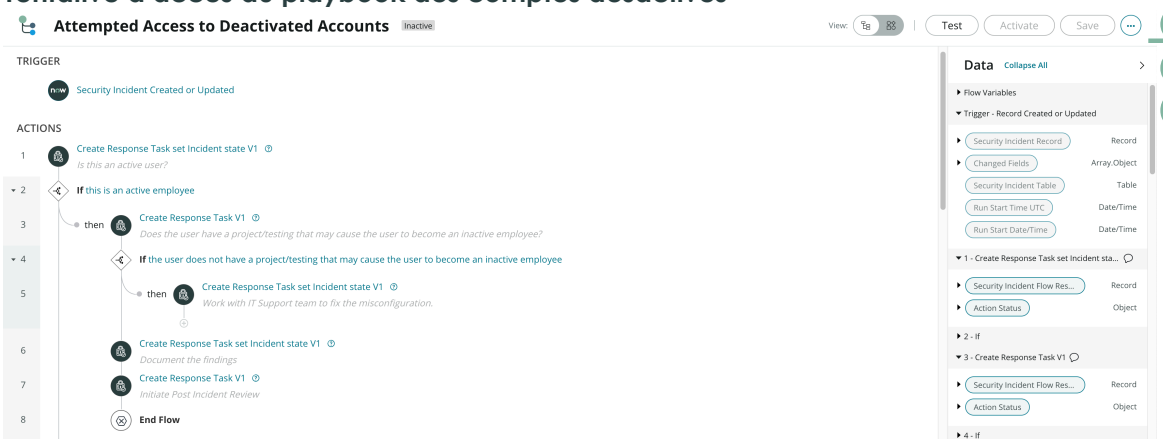
Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vérifiez si la tentative d'accès aux comptes désactivés a été effectuée par un utilisateur actif.
2. Dans l'action 2, vérifiez si la tentative d'accès aux comptes désactivés a été effectuée par un employé actif.

Tentative d'accès au playbook des comptes désactivés



3. Si la tentative d'accès aux comptes désactivés a été effectuée par un employé actif, procédez comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans l'action 3, vérifiez si l'utilisateur avait un projet ou un scénario de test qui l'a amené à devenir un employé inactif.

b. Dans l'action 4, si l'utilisateur n'a pas eu de projet ou de scénario de test qui l'a amené à devenir un employé inactif, travaillez avec l'équipe d'assistance informatique pour corriger l'erreur de configuration.
Le flux se termine.

c. Dans l'action 5, si l'utilisateur avait un projet ou un scénario de test qui l'a amené à devenir un employé inactif, procédez comme suit :

i. Dans l'action 6, documentez les résultats obtenus jusqu'à présent.

ii. Dans l'action 7, lancez une révision post-incident.

Dans l'action 8, après la revue post-incident, le flux se termine.

4. Dans l'action 9, si la tentative d'accès au compte désactivé n'a pas été effectuée par un employé actif, effectuez les étapes suivantes :

a. Dans l'action 10, vérifiez si l'utilisateur a réussi à se connecter.

b. Dans l'action 11, vérifiez quand l'employé a été licencié.

c. Dans l'action 12, examinez les événements survenus sur Splunk pour examiner les activités de l'utilisateur au cours de la période.

d. Dans l'action 13, sur la base de l'enquête menée jusqu'à présent, déterminez si l'utilisateur a exfiltré des données.

e. Dans l'action 14, si l'utilisateur n'a exfiltré aucune donnée, procédez comme suit :

i. Dans l'action 15, collaborez avec l'équipe d'assistance informatique pour mettre fin à toutes les sessions actives et désactiver les comptes.

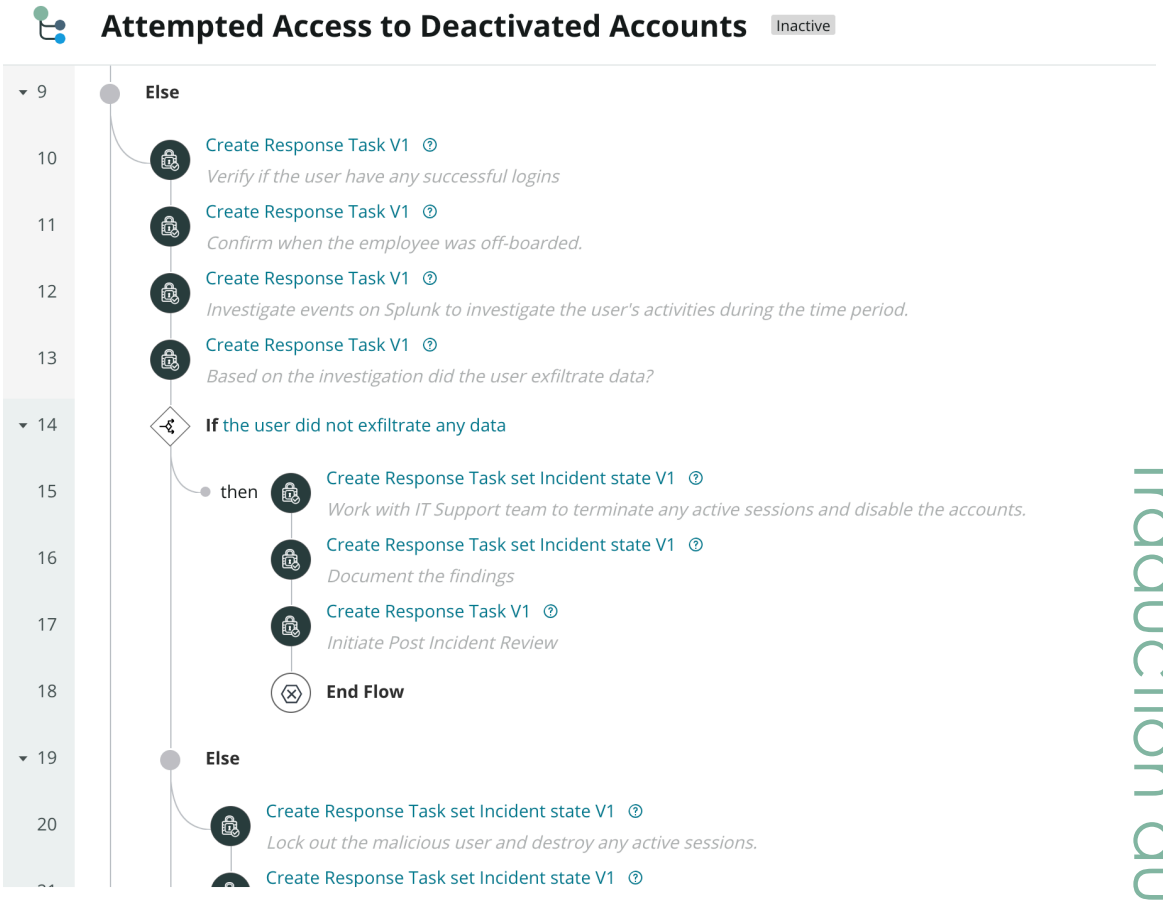
ii. Dans l'action 16, documentez les résultats obtenus jusqu'à présent.

iii. Dans l'action 17, lancez une révision post-incident.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'action 18, après la revue post-incident, le flux se termine.

Utilisation du playbook de tentative d'accès aux comptes désactivés



5. Dans l'action 19, si l'utilisateur a exfiltré des données, procédez comme suit :

a. Dans l'action 20, verrouillez l'utilisateur malveillant et détruisez toutes les sessions actives.

b. Dans Action 21, collaborez avec l'équipe d'assistance informatique pour désactiver tous les comptes.

c. Dans l'action 22, assurez-vous que les ressources sont restaurées à l'état normal et exemptes de toute activité malveillante.
Vous pouvez recréer une image des ressources si nécessaire.

d. Dans l'action 23, lever le confinement et ramener les systèmes aux normes opérationnelles.

e. Dans l'action 24, terminez la revue post-incident avant de fermer la tâche.

Playbook pour T1003 - Évasion défensive - Mimikatz DCShadow

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents soupçonnés d'être causés par Mimikatz DCShadow. DCShadow est une fonctionnalité de Mimikatz qui simule le comportement d'un contrôleur de domaine (un serveur contrôlant Active Directory) pour injecter ses propres données, en contournant la plupart des contrôles de sécurité standard (y compris les SIEM).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mimikatz DCShadow aide l'attaquant à établir un contrôleur de domaine (DC) non autorisé qui fait partie d'Active Directory (AD). Une fois enregistré, il peut agir comme un CD légitime et causer des dommages.

Configurer le playbook T1003 - Évasion défensive - Mimikatz DCShadow

Suivez les étapes suivantes pour configurer le playbook T1003 - Évasion défensive - Mimikatz DCShadow.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

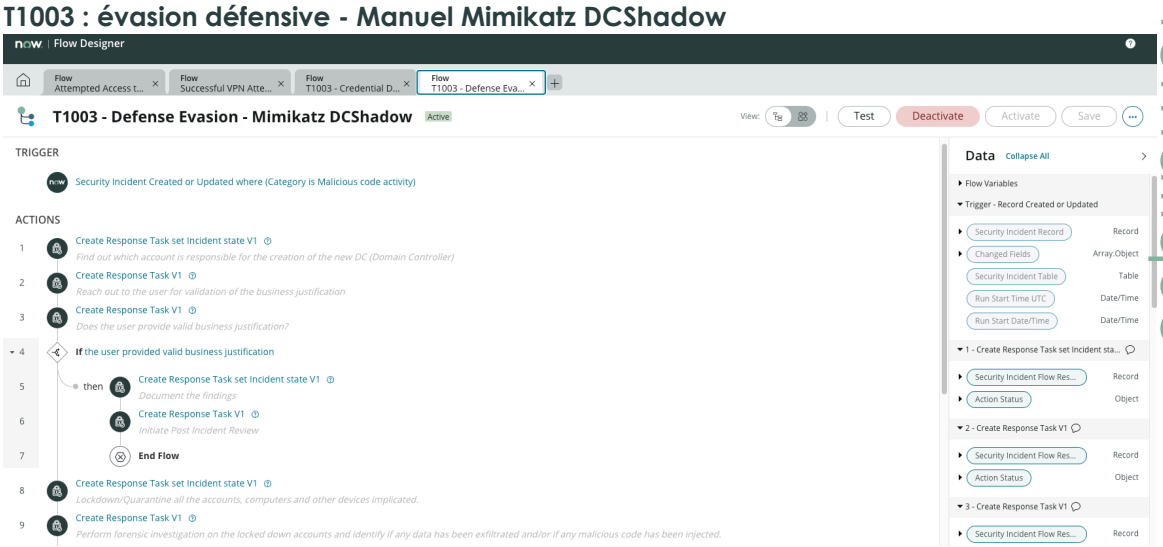
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **T1003 - Defense Evasion - Mimikatz DCShadow** .
3. Facultatif : Créez une copie du flux du playbook T1003 - Évasion de défense - Mimikatz DCShadow et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

T1003 : évasion défensive - Manuel Mimikatz DCShadow



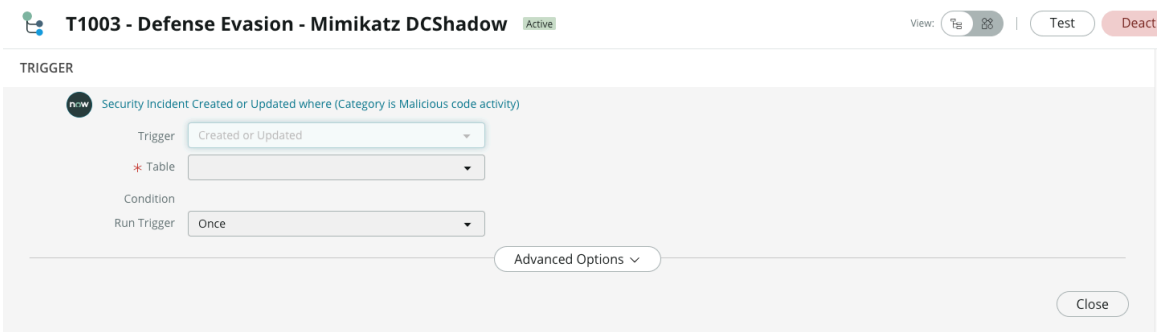
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Activité de code malveillant**.

T1003 : évasion défensive : condition de déclenchement du playbook Mimikatz DCShadow



Utiliser le playbook T1003 - Évasion défensive - Mimikatz DCShadow

Utilisez ce playbook pour enquêter sur les incidents de sécurité soupçonnés d'être causés par Mimikatz DCShadow. Les étapes suivantes vous donnent un aperçu des actions, des tâches et des flux secondaires disponibles dans le playbook T1003 - Évasion de défense - Mimikatz DCShadow.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

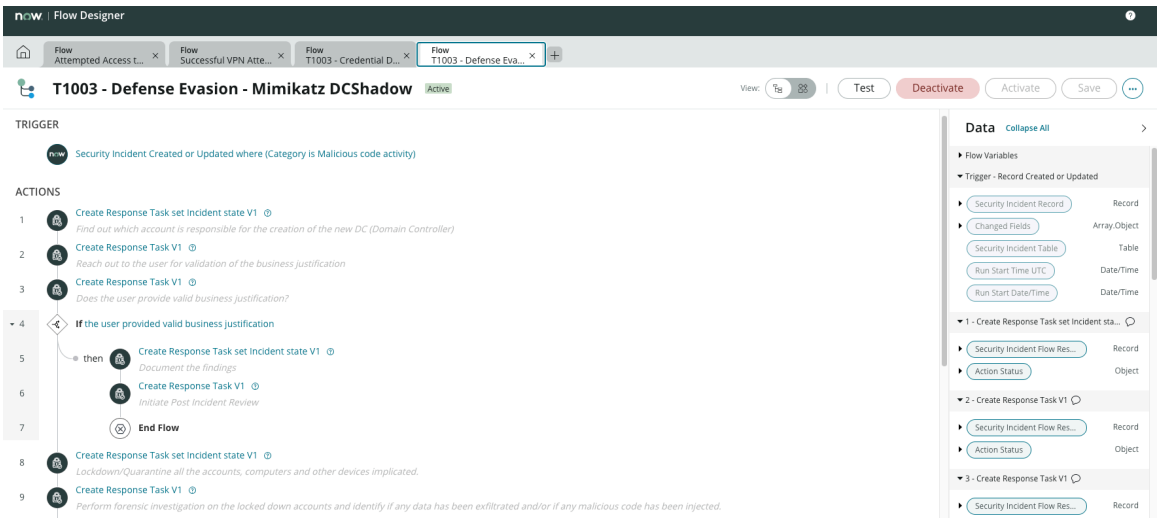
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, découvrez quel compte est responsable de la création du nouveau contrôleur de domaine (contrôleur de domaine).
2. Dans l'action 2, contactez l'utilisateur pour valider la justification commerciale. Vous pouvez utiliser le modèle d'e-mail fourni pour contacter l'utilisateur.
3. Dans l'action 3, vérifiez si l'utilisateur a fourni une justification commerciale valide.
4. Dans l'action 4, si l'utilisateur a fourni une justification commerciale valide, procédez comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

T1003 : évasion défensive - Manuel Mimikatz DCShadow

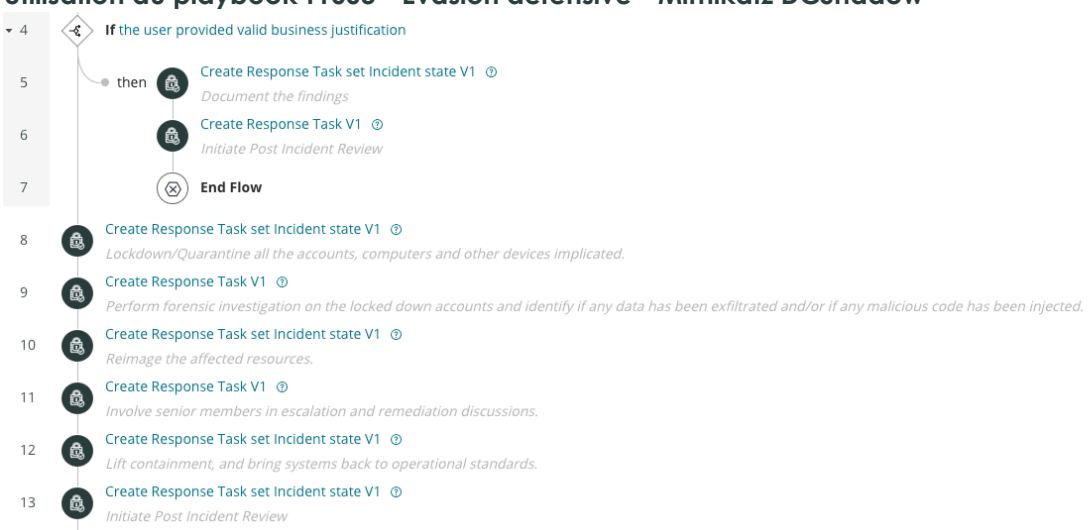


a. Dans l'action 5, documentez les résultats obtenus jusqu'à présent.

b. Dans l'action 6, lancez une revue post-incident.
Dans l'action 7, après la revue post-incident, le flux se termine.

5. Dans l'action 8, si l'utilisateur n'a pas fourni de justification commerciale valide, procédez comme suit :

Utilisation du playbook T1003 - Évasion défensive - Mimikatz DCShadow



a. Dans l'action 9, verrouillez ou mettez en quarantaine tous les comptes, ordinateurs et autres appareils concernés.

b. Dans l'action 10, effectuez une enquête médico-légale sur les comptes verrouillés et identifiez si des données ont été exfiltrées ou si un code malveillant a été injecté.

c. Dans l'action 11, recréez l'image des ressources affectées.

d. Dans l'action 12, lever le confinement et ramener les systèmes aux normes opérationnelles.

e. Dans l'action 13, terminez la revue post-incident avant de fermer la tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook pour T1003 : vidage des informations d'identification : Mimikatz DCSync

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents soupçonnés d'être causés par Mimikatz DCSync. Ce playbook se déclenche lorsque l'une des fonctions de Mimikatz *(lsadump ::d csync*) est utilisée. La fonction est généralement utilisée sur les contrôleurs de domaine (DC) attaqués.

Mimikatz est un outil de piratage populaire qui permet aux utilisateurs d'émettre des commandes qui aident à récupérer des données confidentielles du système attaqué. Les données confidentielles comprennent les mots de passe, leurs hachages et autres.

Remarque : Il s'agit d'une alerte haute-fidélité, qui est supposée être rarement déclenchée. Lorsqu'il se déclenche, vous devez en informer immédiatement un membre de l'équipe senior ou un gestionnaire.

Configurer le playbook T1003 - Vidage des informations d'identification - Mimikatz DCsync

Suivez les étapes suivantes pour configurer le playbook T1003 - Vidage des informations d'identification - Mimikatz DCsync.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

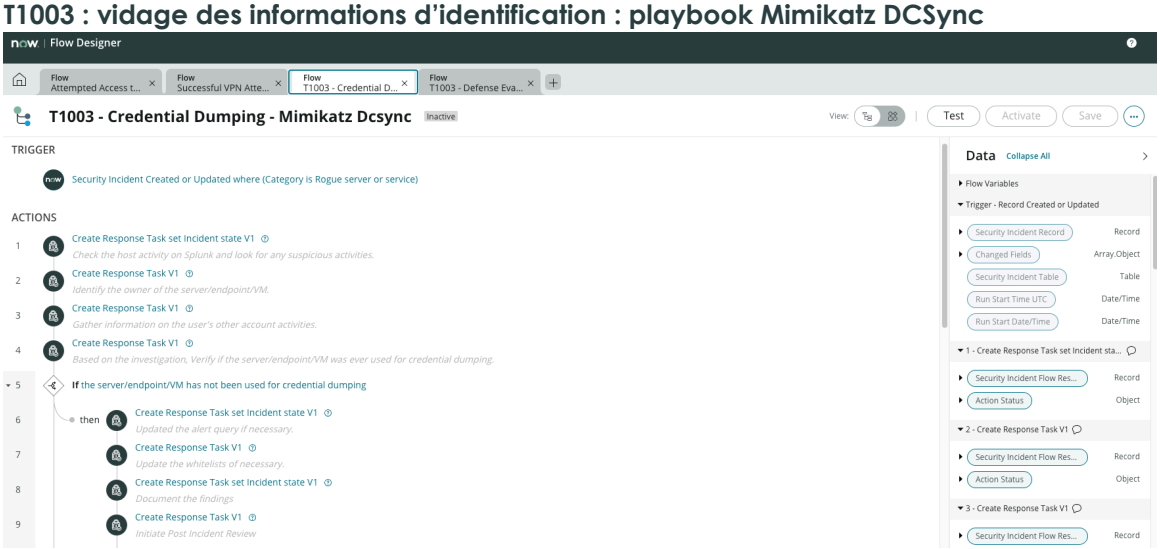
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **T1003 - Credential Dumping - Mimikatz DCsync** .
3. Facultatif : Créez une copie du flux de playbook T1003 - Vidage des informations d'identification - Mimikatz DCsync et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

T1003 : vidage des informations d'identification : playbook Mimikatz DCSync



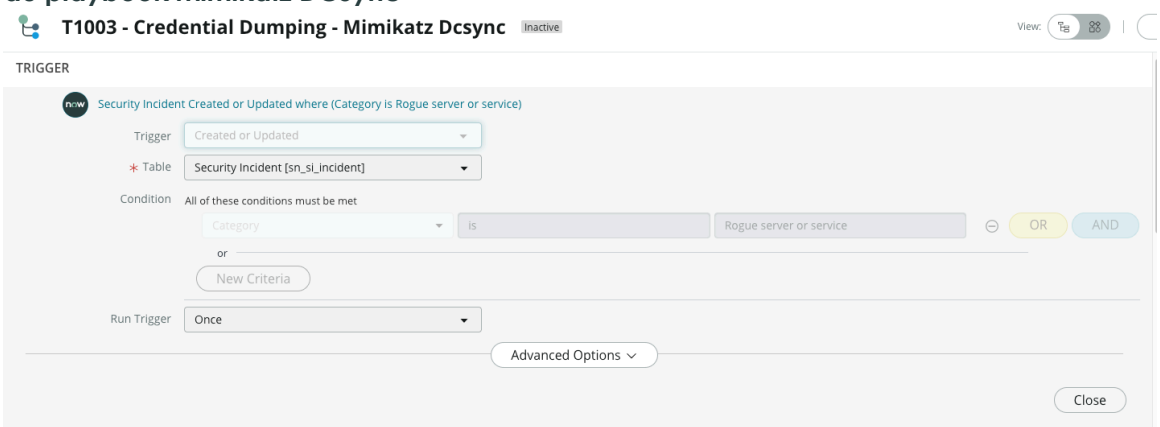
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Serveur ou service non autorisé**.

T1003 : vidage des informations d'identification : condition de déclenchement du playbook Mimikatz DCSync



Utiliser le playbook T1003 - Dumping des informations d'identification - Mimikatz DCsync

Utilisez ce playbook pour enquêter sur les incidents soupçonnés d'être causés par Mimikatz DCSync. Les étapes suivantes vous donnent un aperçu des actions, des tâches et des flux secondaires disponibles dans le playbook T1003 - Vidage des informations d'identification - Mimikatz DCsync.

Avant de commencer

Rôle requis :

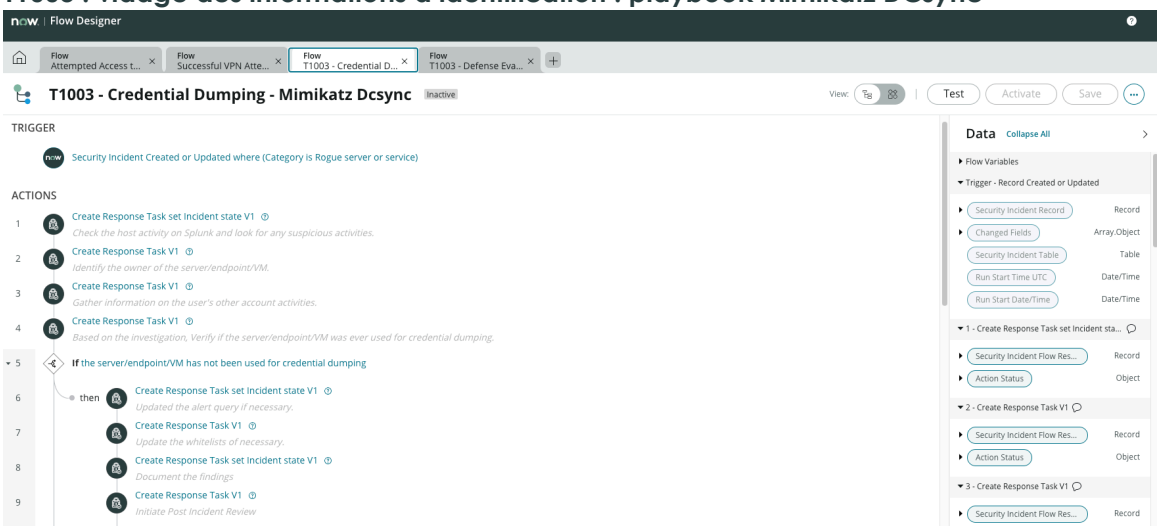
- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vérifiez l'activité de l'hôte sur Splunk et recherchez toute activité suspecte.
2. Dans l'action 2, identifiez le propriétaire du serveur/point de terminaison/machine virtuelle. Si l'utilisateur est en ligne, exécutez CrowdStrike EDR pour recueillir une meilleure portée des activités du système.
3. Dans l'action 3, recueillez des informations sur les autres activités du compte de l'utilisateur.
4. Dans l'action 4, en fonction de l'enquête, vérifiez si le serveur/point de terminaison/machine virtuelle a déjà été utilisé pour le vidage des informations d'identification.
5. Dans l'action 5, si le serveur/point de terminaison/machine virtuelle n'a pas été utilisé pour le vidage des informations d'identification, effectuez les actions suivantes :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

T1003 : vidage des informations d'identification : playbook Mimikatz DCsync



a. Dans l'action 6, mettez à jour la requête d'alerte si nécessaire.

b. Dans l'action 7, mettez à jour la liste d'autorisation si nécessaire.

c. Dans l'action 8, documentez les résultats obtenus jusqu'à présent.

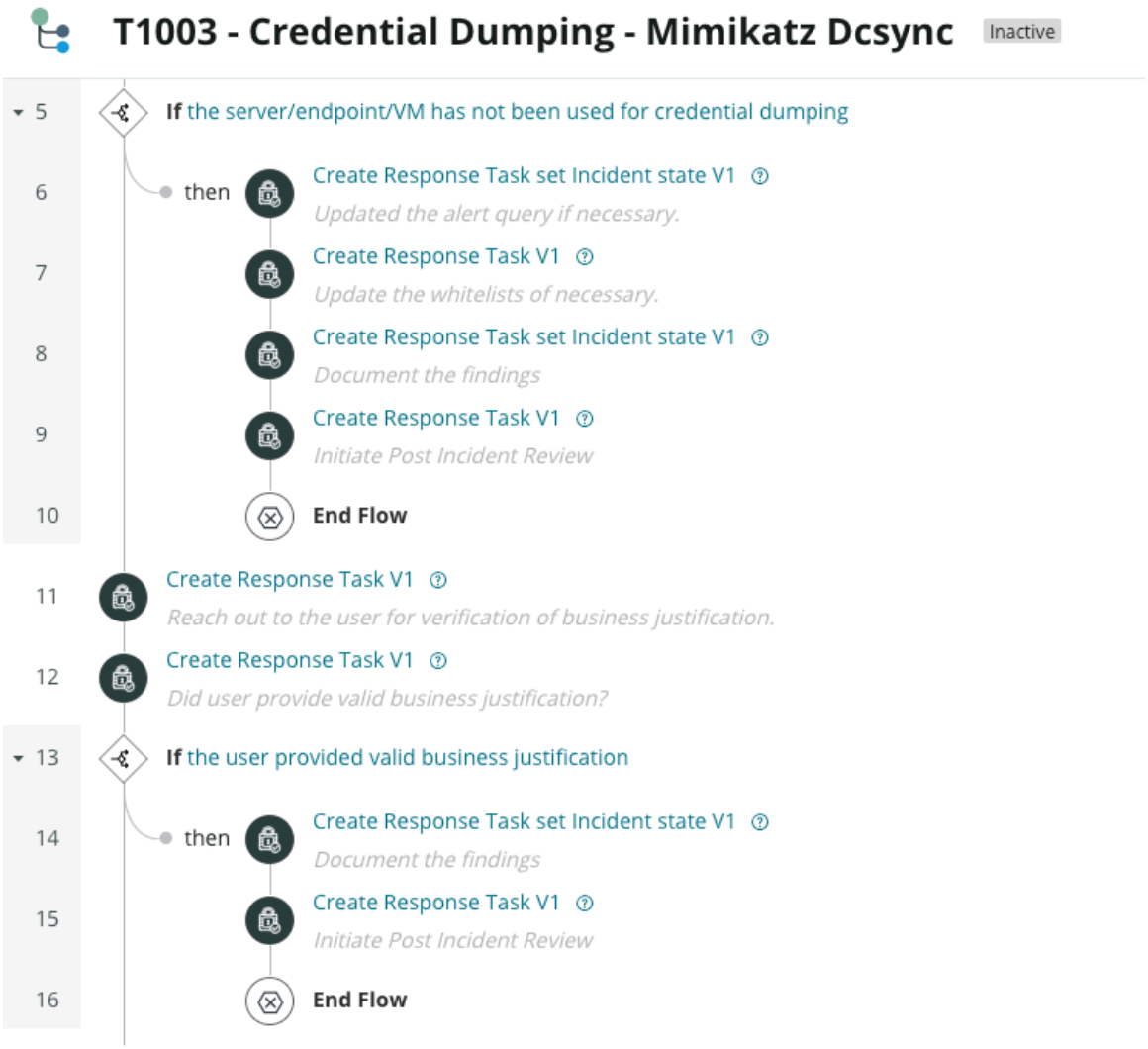
d. Dans l'action 9, lancez une revue post-incident.
Dans l'action 10, le flux se termine.

6. Si le serveur/point de terminaison/machine virtuelle a été utilisé pour le vidage des informations d'identification, contactez l'utilisateur dans l'action 11.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook T1003 - Dumping des informations d'identification - Mimikatz DCsync



7. Dans l'action 12, contactez l'utilisateur pour valider la justification commerciale.
8. Dans l'action 13, si l'utilisateur a fourni une justification commerciale valide, effectuez les actions suivantes :

   a. Dans l'action 14, documentez les résultats obtenus jusqu'à présent.

   b. Dans l'action 15, lancez une révision post-incident.
   Dans l'action 16, le flux se termine.

9. Si l'utilisateur n'a pas fourni de justification commerciale valide, mettez le système en quarantaine dans l'Action 17.
10. Dans Action 18, supprimez tous les fichiers indésirables qui ont pu être créés ou supprimés par les comptes malveillants.
11. Dans l'action 19, lever le confinement et ramener les systèmes aux normes opérationnelles.
12. Dans l'action 20, terminez la revue post-incident avant de fermer la tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Échecs de connexion utilisateur de Playbook for Okta à partir de plusieurs adresses IP

Ce playbook fournit des étapes de rattrapage systématique pour enquêter sur les incidents liés aux échecs de connexion de l'utilisateur sur Okta.

Le playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP fournit des instructions sur l'analyse de l'alerte lorsque des défaillances de compte ServiceNow sont observées sur Okta à partir de plusieurs adresses IP non ServiceNow. L'alerte associée à ce playbook vérifie les journaux Okta. Il déclenche une alerte en cas d'échec de connexion pour les ID d'utilisateur ServiceNow provenant de plus de trois plages d'adresses IP non-ServiceNow sur une durée d'une heure.

Configurer le playbook des échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP

Suivez les étapes suivantes pour configurer le playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

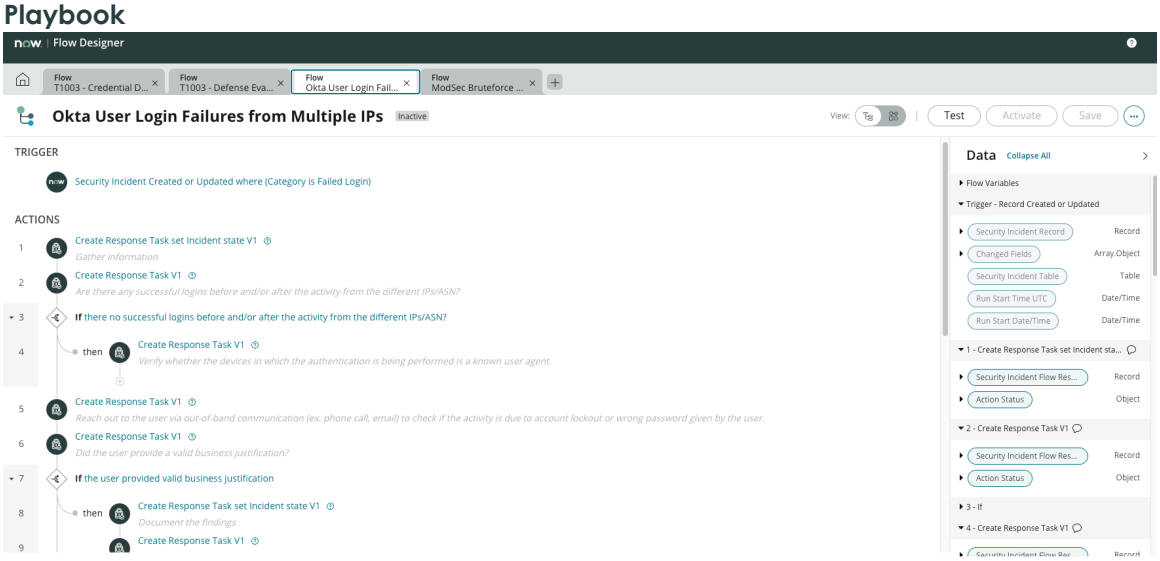
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP** .
3. Facultatif : Créez une copie du flux de playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP Playbook

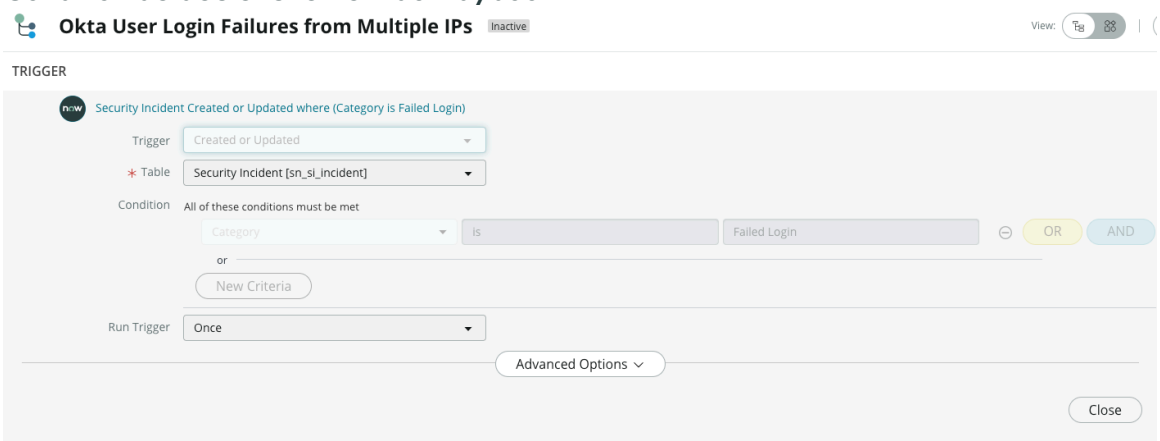


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Échec de connexion**.

Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP
Condition de déclenchement du Playbook



Utiliser le playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP

Utilisez ce playbook pour enquêter sur les incidents de sécurité liés aux échecs de connexion des utilisateurs sur Okta. Les étapes suivantes vous donnent un aperçu des actions, des tâches et des flux secondaires disponibles dans le playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP.

Avant de commencer

Rôle requis :

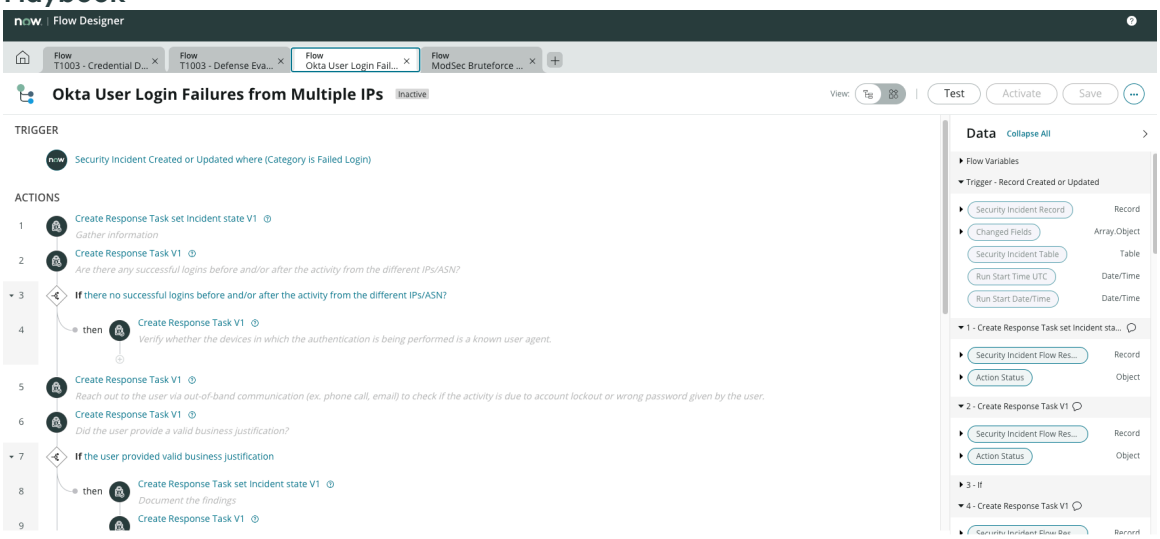
- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, effectuez les tâches suivantes :
   - Identifiez le compte utilisateur ciblé.
   - Vérifiez le sous-réseau IP et vérifiez s'ils appartiennent tous au même propriétaire de numéro de système autonome (ASN).
2. Dans l'action 2, vérifiez s'il y a eu des connexions réussies avant ou après l'activité à partir des différentes adresses IP/ASN.
3. Dans l'action 3, s'il n'y a pas eu de connexion réussie avant ou après l'activité à partir des différentes adresses IP/ASN, dans l'action 4, vérifiez si les appareils sur lesquels l'authentification est effectuée sont des agents utilisateur connus.
   Si les appareils sont authentifiés par des agents utilisateur connus, le flux s'arrête.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP Playbook



4. Dans l'action 5, en fonction de l'enquête, contactez l'utilisateur par le biais d'une communication hors bande (par exemple, appel téléphonique ou e-mail) pour vérifier si l'activité est due à un verrouillage du compte ou à un mot de passe incorrect fourni par l'utilisateur.
5. Dans l'action 6, vérifiez si l'utilisateur a fourni une justification commerciale valide.
6. Dans l'action 7, si l'utilisateur a fourni une justification commerciale valide, effectuez les tâches suivantes.

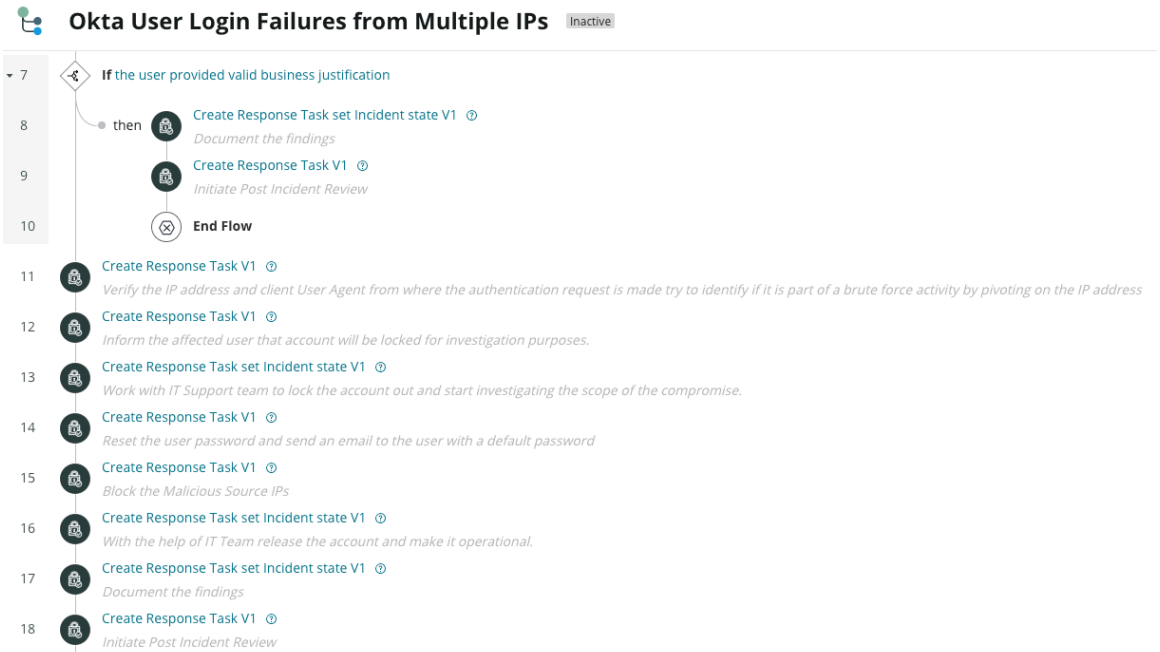
   a. Dans l'action 8, créez une tâche de réponse pour documenter les résultats obtenus jusqu'à présent.

   b. Dans l'action 9, créez une réponse pour lancer une révision post-incident.
   Dans l'action 10, le flux se termine.

7. Dans l'action 11, vérifiez l'adresse IP et l'agent utilisateur client à partir desquels la demande d'authentification est effectuée et essayez d'identifier si cela fait partie d'une activité de force brute en pivotant sur l'adresse IP.
8. Dans l'action 12, informez l'utilisateur concerné que le compte sera verrouillé à des fins d'enquête.
   Vous pouvez utiliser le modèle d'e-mail fourni pour informer l'utilisateur concerné.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP



9. Dans l'action 13, travaillez avec l'équipe d'assistance informatique pour verrouiller le compte et commencer à enquêter sur l'étendue de la compromission.
10. Dans l'action 14, réinitialisez le mot de passe utilisateur et envoyez un e-mail à l'utilisateur avec le mot de passe par défaut.
11. Dans l'action 15, bloquez les adresses IP sources malveillantes.
12. Dans l'action 16, demandez l'aide de l'équipe d'assistance informatique pour libérer le compte et le ramener aux normes opérationnelles.
13. Dans l'action 17, documentez les résultats obtenus jusqu'à présent.
14. Dans l'action 18, terminez la revue post-incident avant de fermer la tâche.

Playbook pour ModSec Attaque par force brute par rafale d'adresses IP

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents de tentatives par force brute sur les pages de connexion à partir de plusieurs adresses IP détectées par ModSec. Les conditions de l'événement peuvent être définies au niveau de la politique de sécurité Mod elle-même et déclenchent une alerte au niveau de Splunk lorsque l'événement est créé à l'heure de sécurité mod.

Ce playbook permet de détecter les nombres anormaux de trafic sur la page de connexion. Dans cet exemple, deux rafales successives de plus de 50 accès/minute doivent être effectuées à partir d'une adresse IP vers la page de connexion, ce qui indique une tentative de connexion par force brute.

Configurer le playbook ModSec Brute force by IP Burst

Procédez comme suit pour configurer le playbook ModSec Brute force by IP Burst.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

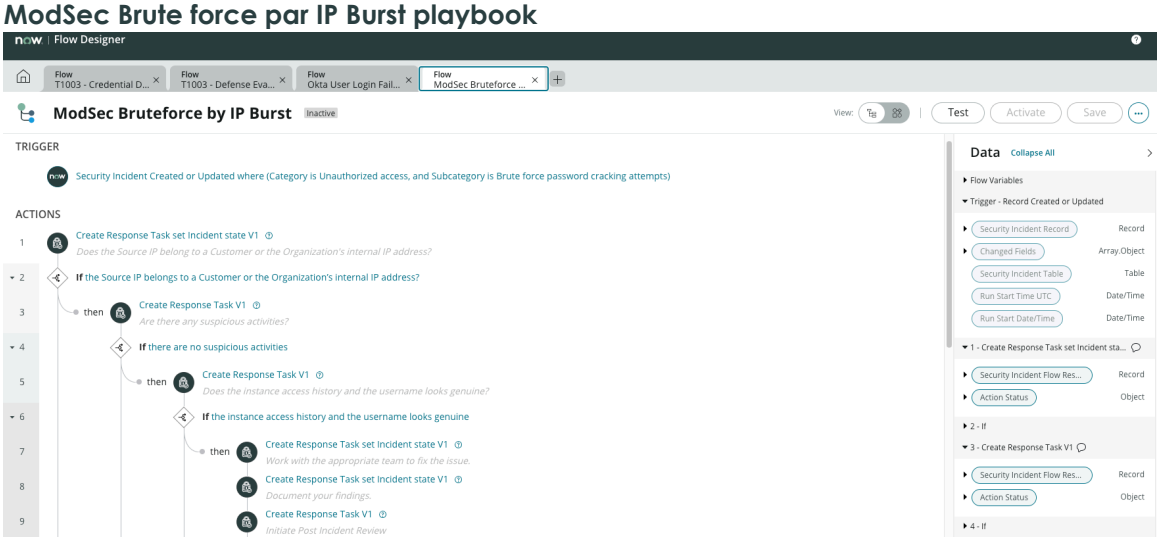
Assurez-vous d'avoir installé le spoke Security Operations (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tout** > **Concepteur de flux** et sélectionnez le playbook **ModSec Bruteforce by IP Burst** .
3. Facultatif : Créez une copie du flux de playbook ModSec Bruteforce by IP Burst et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de menu Actions supplémentaires ( supplémentaires), puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous envisagez de personnaliser ou d'apporter des changements spécifiques au flux.

ModSec Brute force par IP Burst playbook



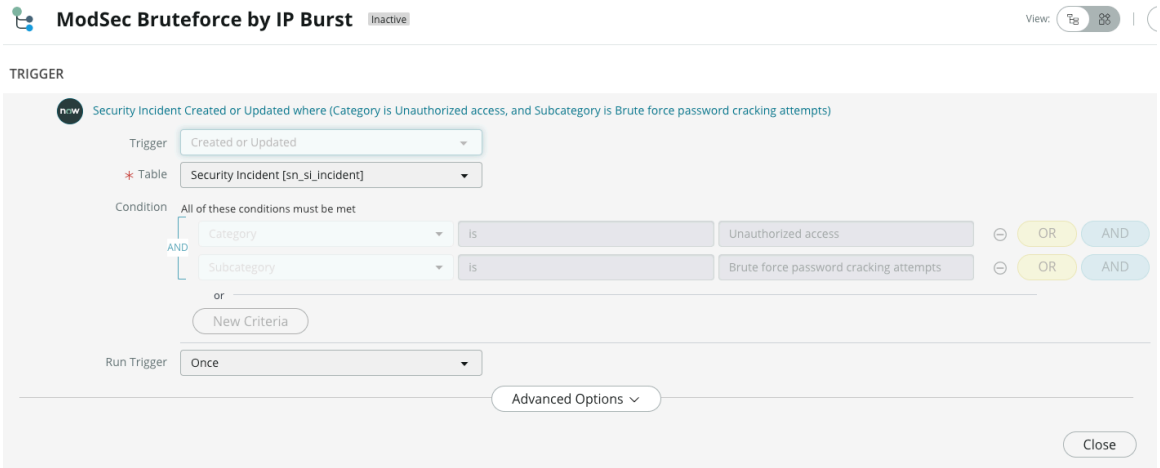
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les modifications requises.
5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **La catégorie** est **Accès non autorisé**.
- **La sous-catégorie** comprend **les tentatives de craquage de mot de passe en force brute**.

Force brute ModSec par condition de déclenchement du playbook en rafale d'adresses IP



Utiliser le playbook ModSec Brute force by IP Burst

Utilisez ce playbook pour enquêter sur les incidents de tentatives par force brute sur les pages de connexion à partir de plusieurs adresses IP détectées par ModSec. Les étapes suivantes vous donnent un aperçu des actions, des tâches et des flux secondaires disponibles dans le playbook ModSec Brute force by IP Burst.

Avant de commencer

Rôle requis :

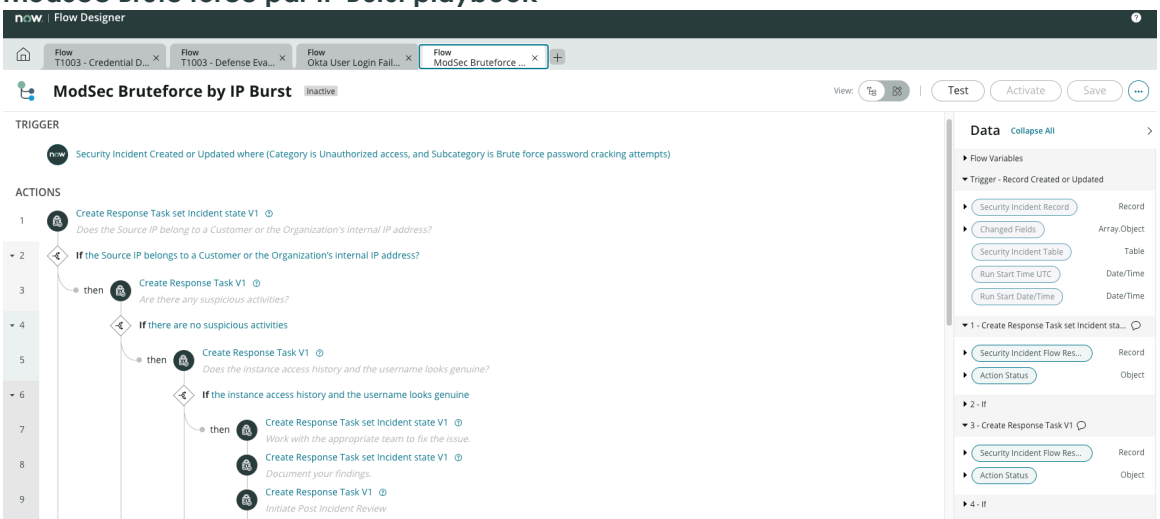
- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vérifiez si l'adresse IP source appartient à un client ou à l'adresse IP interne de l'organisation.
2. Dans l'action 2, si l'adresse IP source appartient à un client ou à l'adresse IP interne de l'entreprise, procédez comme suit :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ModSec Brute force par IP Burst playbook



a. Dans l'action 3, vérifiez s'il y a eu des activités suspectes.

- Vérifiez l'activité à partir de l'adresse IP source au cours des derniers jours. Si l'adresse IP avait un trafic négligeable, cela indique une attaque réelle.
- Vérifiez les noms d'utilisateur de pulvérisation. Par exemple, vérifiez si les noms d'utilisateur sont classés par ordre alphabétique.
- Recherchez les noms de compte génériques concernés. Par exemple, les noms de compte d'administrateur, d'administrateur système, de racine, d'administrateur et d'autres comptes d'application.

S'il n'y a aucune activité suspecte, le flux s'arrête.

b. Dans l'action 4, en cas d'activités suspectes, vérifiez dans l'action 5 si l'historique d'accès à l'instance et le nom d'utilisateur semblent authentiques.

Vérifiez les *Appnode* journaux pour voir s'il y a des signes de défaillance. Des événements d'échec SAML, SSO ou LDAP peuvent être dus à un problème opérationnel.

Si l'historique d'accès à l'instance et le nom d'utilisateur ne semblent pas authentiques, le flux s'arrête.

c. Dans l'action 6, si l'historique d'accès à l'instance et le nom d'utilisateur semblent authentiques, procédez comme suit :

i. Dans l'action 7, coordonnez-vous avec l'équipe appropriée pour résoudre le problème.

ii. Dans l'action 8, documentez les résultats obtenus jusqu'à présent.

iii. Dans l'action 9, terminez la vérification post-incident avant de fermer la tâche.

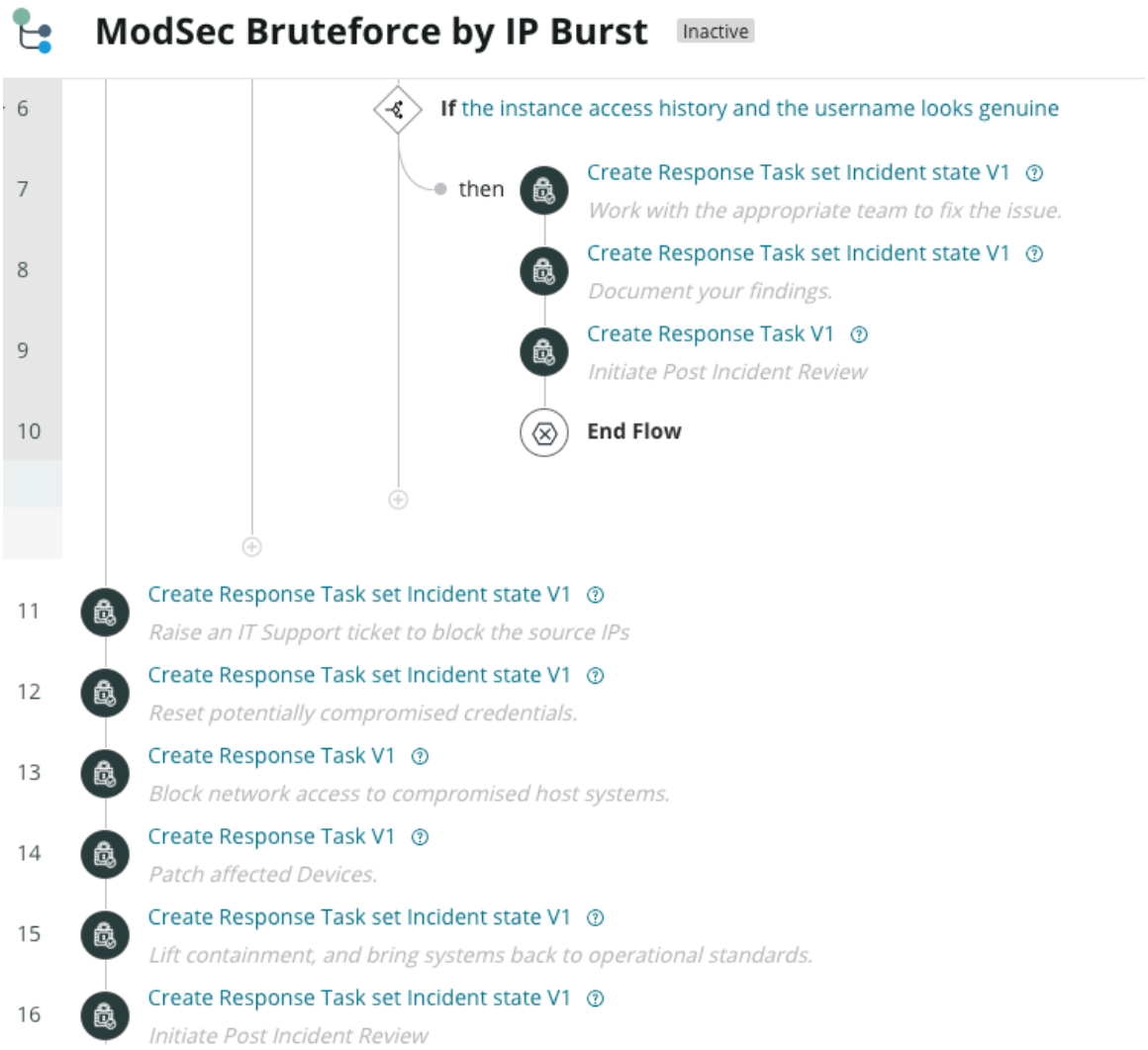
Dans l'action 10, le flux se termine.

3. Si l'adresse IP source n'appartient pas à un client ou à l'adresse IP interne de l'entreprise, émettez un ticket d'assistance informatique pour bloquer les adresses IP sources dans l'action 11.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook ModSec Brute force by IP Burst



4. Dans l'action 12, réinitialisez les informations d'identification potentiellement compromises.
5. Dans l'action 13, bloquez l'accès réseau aux systèmes hôtes compromis.
6. Dans Action 14, corrigez les appareils concernés.
7. Dans l'action 15, levez le confinement et ramenez les systèmes aux normes opérationnelles.
8. Dans l'action 16, terminez la vérification post-incident avant de fermer la tâche.

Actions du playbook Security Incident Response

Cette section décrit les actions fournies dans la bibliothèque d'actions de Concepteur de flux.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
Ajouter une balise de sécurité à l'incident de sécurité	Utilisez cette action pour ajouter automatiquement une balise de sécurité à l'aide de la logique Flow Designer.	Si le flux détecte un IOC, la balise **IOC détecté** peut être automatiquement ajoutée à l'aide de cette action. **Flux** :	• Entrée : incident de sécurité, balise de sécurité • Sortie : non applicable
Ajouter des observables à l'incident de sécurité	Utilisez cette action pour ajouter des observables à un incident de sécurité sélectionné. • Par défaut, la liste des observables est séparée par le délimiteur virgule (,) mais cela peut être modifié. Vous pouvez spécifier un autre caractère spécial comme délimiteur. Lors de l'ajout d'observables, le type (URL, adresse IP, hachage) est automatiquement défini. • Lorsque les observables sont ajoutés à l'incident de sécurité, le type (URL, adresse IP, hachage) est automatiquement défini. • Lorsque les observables sont ajoutés, l'option Filtrer les observables sur la liste d'autorisation identifie les observables de la liste d'autorisation et ne les ajoute pas à la liste connexe des observables de l'incident de sécurité. Une activité système		• Entrée : ◦ incident de sécurité ◦ observables ◦ délimiteur ◦ Filtrer les observables sur la liste d'autorisation et publier la note d'activité • Sortie : non applicable

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
	automatisée (réponse) est ajoutée pour indiquer que ces observables ont été supprimés.		
Obtenir les utilisateurs affectés (listes connexes) par plusieurs incidents de sécurité V1	Récupère tous les utilisateurs affectés répertoriés dans la liste connexe Utilisateurs affectés pour les incidents de sécurité spécifiés.	Vous pouvez avoir des incidents de sécurité parents avec plusieurs incidents de sécurité enfants. Utilisez cette action pour déployer les utilisateurs affectés de tous les incidents de sécurité enfants sur les incidents de sécurité parents correspondants. Seuls les utilisateurs affectés uniques sont déployés et tous les doublons sont éliminés.	• Entrée : incidents de sécurité • Sortie : ◦ Utilisateur affecté ◦ compter
Obtenir les utilisateurs affectés par plusieurs incidents de sécurité	Récupère l'utilisateur principal affecté pour l'incident de sécurité spécifié. Elle n'inclut pas les utilisateurs affectés de la liste connexe Utilisateurs affectés.	• Lors de l'enquête sur un incident de sécurité de hameçonnage, envoyez un e-mail aux principaux utilisateurs affectés (qui ont signalé l'incident d'hameçonnage) pour confirmer si l'un des utilisateurs a cliqué sur les liens malveillants contenus dans l'e-mail d'hameçonnage. • Mettez à jour la gravité ou le score de risque de l'incident de sécurité parent en fonction du nombre d'utilisateurs principaux affectés.	• Entrée : incidents de sécurité • Sortie : ◦ Utilisateurs affectés ◦ compter

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
Obtenir les utilisateurs affectés (liste connexe) à partir d'un incident de sécurité	Récupère tous les utilisateurs affectés répertoriés dans la liste connexe Utilisateurs affectés pour un incident de sécurité spécifié.		• Entrée : incidents de sécurité • Sortie : ◦ Utilisateurs affectés ◦ compter
Ajouter des utilisateurs affectés à un incident de sécurité	Ajoute tous les utilisateurs affectés à un incident de sécurité.	Supposons que vous ayez un incident de sécurité parent avec plusieurs incidents de sécurité enfants. Vous pouvez utiliser cette action pour déployer les utilisateurs affectés de tous les incidents de sécurité enfants sur l'incident de sécurité parent correspondant. Seuls les utilisateurs affectés uniques sont déployés et tous les doublons sont éliminés.	• Entrée : ◦ incident de sécurité ◦ utilisateur • Sortie : non applicable
Obtenir les éléments de configuration des utilisateurs affectés	Récupère les éléments de configuration (CI) de tous les utilisateurs affectés.	Dans les scénarios d'hameçonnage ou de programme malveillant, vous pouvez utiliser cette action pour mettre à jour la liste connexe des éléments de configuration (CI) affectés et examiner les CI. Vous pouvez ensuite mettre à jour la gravité ou le score de risque de l'incident de sécurité en fonction du nombre de CI identifiés.	• Entrée : users • Sortie : ◦ Éléments de configuration ◦ compter
Obtenir tous les incidents de sécurité enfants pour un incident de sécurité	Récupère tous les incidents de sécurité enfants liés à un incident de sécurité parent spécifique.	Exemple de scénario : utilisez cette action pour : • Mettre à jour l'état des incidents de sécurité enfants lorsque leur état	• Entrée : ◦ incident de sécurité ◦ État de l'incident • Sortie :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
		des incidents de sécurité parents correspondants est mis à jour. • Mettez à jour automatiquement la gravité ou le score de risque de l'incident de sécurité en fonction du nombre d'incidents de sécurité enfants.	◦ incident de sécurité enfant ◦ compter
Obtenir les éléments de configuration pour les observables (type adresse IP)	Récupère tous les éléments de configuration (CI) pour les observables de type adresse IP.	Un observable d'adresse IP peut être associé à un élément de configuration. Par exemple, l'adresse IP d'un serveur. Si vous utilisez cette action, vous pouvez récupérer des informations pour le serveur.	• Entrée : adresse IP de l'observable • Sortie : ◦ Éléments de configuration ◦ compter
Est un observable malveillant	Confirme la présence d'un ou de plusieurs observables malveillants dans un ensemble d'observables.	Une fois que la recherche des menaces est terminée et que vous avez identifié la présence d'observables malveillants, vous pouvez augmenter la gravité ou le score de risque d'un incident de sécurité.	• Entrée : incident de sécurité • Sortie : malveillant (vrai/faux)
Envoyer un e-mail pour confirmer l'interaction de l'utilisateur	Envoie un e-mail en réponse à une réponse de l'utilisateur.	Si un utilisateur tente plusieurs fois de se connecter à une application et qu'il échoue, cela entraîne un scénario d'échec de connexion. Dans ce cas, un e-mail est envoyé à l'utilisateur pour confirmer s'il a tenté de se connecter ou non. En fonction de la réponse de	

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
		l'utilisateur (Oui ou Non), différentes actions peuvent être entreprises. **Flux** : échec de la connexion manuelle Playbook	
Filtrer les éléments observables de la liste des éléments autorisés	Utilisez cette action pour autoriser la liste des observables à partir d'un ensemble donné d'observables.	Vous pouvez identifier certains observables qui peuvent être ignorés à partir d'un ensemble d'observables. Ces observables ne seront pas pris en compte lors de la résolution de l'incident de sécurité.	• Entrée : incident de sécurité • Sortie : ◦ Observables de la liste d'autorisation ◦ compter
Réinitialiser le mot de passe pour les utilisateurs concernés	Utilisez cette action pour réinitialiser le mot de passe pour les utilisateurs concernés.	Si un compte utilisateur a été piraté ou si un utilisateur demande la réinitialisation d'un mot de passe, un e-mail est envoyé à l'utilisateur pour réinitialiser le mot de passe. **Flux** : échec de la connexion manuelle au playbook.	
Obtenir le groupe d'utilisateurs pour l'utilisateur affecté	Récupère les détails du groupe d'utilisateurs des utilisateurs affectés.	Dans une organisation, si deux utilisateurs ou plus signalent des e-mails de hameçonnage, vous pouvez savoir à quel groupe ils appartiennent et identifier si d'autres utilisateurs ont été affectés	• Entrée : user • Sortie : ◦ Groupes d'utilisateurs ◦ compter

Rapports Security Incident Response

Les responsables de la sécurité peuvent identifier les zones de préoccupation à l'aide d'interfaces graphiques de haut niveau.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accéder à l'Explorateur Security Incident Response

Vous pouvez accéder au tableau de bord de l'Explorateur pour afficher l'activité Réponse aux incidents de sécurité des incidents de sécurité afin d'identifier instantanément les zones de préoccupation et de résoudre rapidement les problèmes.

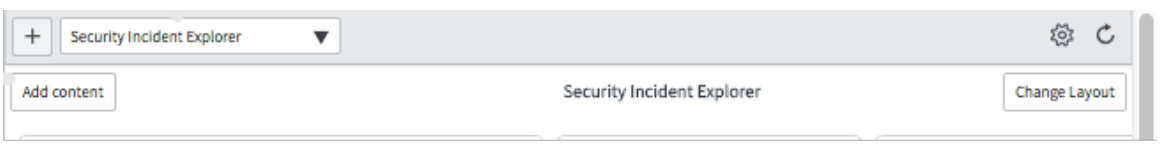
Avant de commencer

Rôles requis :

- sn_si.admin (pour écrire)
- sn_si_basic (lire)

Procédure

1. Accédez à la **Tout** > **Libre-service** > **Page d'accueil** ou accédez à **Libre-service** > **Tableaux de bord**.
2. Choisissez Explorateur des incidents de sécurité dans la liste des rapports.

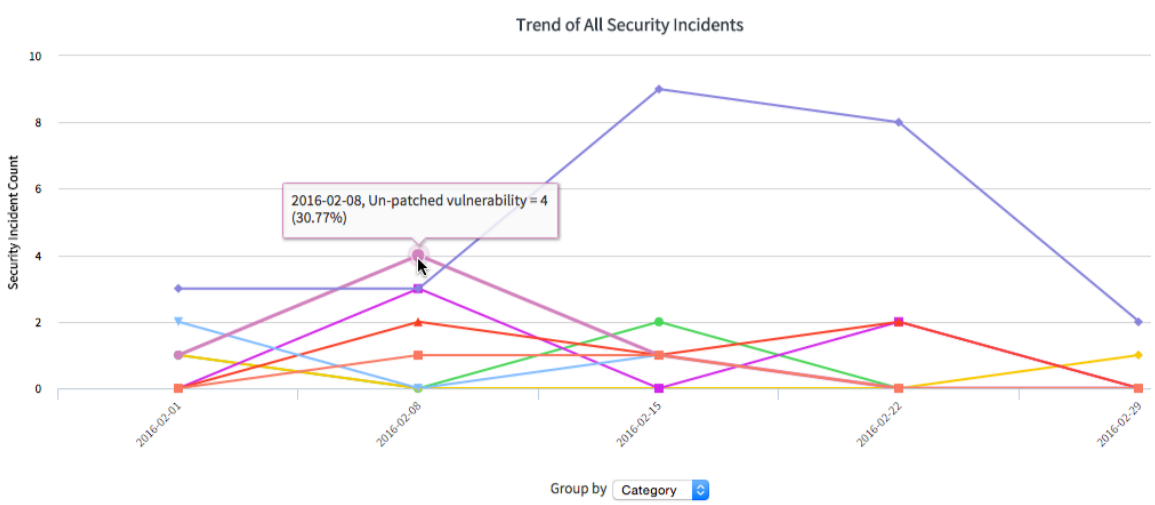


Réponse aux incidents de sécurité Vue d'ensemble

La Réponse aux incidents de sécurité vue d'ensemble fournit une vue de direction de l'activité des incidents de sécurité, en fournissant des tendances et des rapports, ainsi que des détails sur des données spécifiques.

Le module de vue d'ensemble affiche des informations sur l'incident de sécurité adaptées au rôle de l'utilisateur. Vous pouvez pointer sur n'importe quelle partie d'un graphique (barres, secteurs, point de données, carte thermique, etc.) pour afficher des données générales spécifiques à cette partie. Reportez-vous à l'image suivante. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

Tendance de tous les incidents de sécurité



Présentation du gestionnaire d'incidents de sécurité

Les utilisateurs ayant les rôles d'administrateur d'incident de sécurité et de gestionnaire d'incident de sécurité consultent la vue d'ensemble du gestionnaire d'incidents de sécurité. Il contient les rapports suivants dans le système de base.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports de vue d'ensemble de Security Incident Manager

Nom	Visuel	Description
Équipe Incidents de sécurité critique	Score unique	Nombre d'incidents de sécurité critiques affectés à l'équipe.
Équipe Incidents de sécurité élevée	Score unique	Nombre d'incidents de haute sécurité affectés à l'équipe.
SLA arrivant à expiration dans les 24 heures	Score unique	Nombre de SLA qui expirent dans les prochaines 24 heures.
Risque par rapport à la gravité	Carte thermique	Répartition des incidents de sécurité affectés à l'équipe par risque et gravité.
Incidents de sécurité par classe CI, 3 derniers mois	Histogramme	Nombre d'incidents de sécurité affectés à l'équipe par classe d'élément de configuration.
Tendance de tous les incidents de sécurité	Graphique de tendance	Trace le décompte du nombre d'incidents de sécurité reçus par catégorie ou priorité.
Incidents de sécurité liés aux accès non autorisés	Histogramme	Affiche les types de catégories d'incidents de sécurité reçues au fil du temps.
Délai moyen pour contenir	Score unique	Temps moyen nécessaire pour contenir tous les incidents de sécurité.
Délai moyen pour contenir critique	Score unique	Temps moyen nécessaire pour contenir tous les incidents de sécurité critiques.
Délai moyen d'identification	Score unique	Temps moyen nécessaire pour identifier tous les incidents de sécurité

Vue d'ensemble des analyses de sécurité

Les utilisateurs ayant le rôle d'analyste des incidents de sécurité voient la vue d'ensemble de l'analyste de sécurité. Il contient les rapports suivants dans le système de base.

Rapports de vue d'ensemble des analyses de sécurité

Nom	Visuel	Description
Mes tâches de priorité critique	Score unique	Nombre d'incidents de sécurité critiques qui me sont affectés.
Mes tâches de priorité élevée	Score unique	Le nombre d'incidents de haute sécurité qui me sont affectés.
Mes SLA arrivant à expiration dans les 24 heures	Score unique	Nombre de SLA qui me sont affectés et qui expirent dans les prochaines 24 heures.
Incidents de sécurité qui me sont affectés	Histogramme	Incidents de sécurité qui me sont affectés par état d'incident ou catégorie
Tâches qui me sont affectées par type	Histogramme	Tâches de sécurité (incidents, tâches ou demandes) qui me sont affectées par type ou priorité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports de vue d'ensemble des analyses de sécurité (suite)

Nom	Visuel	Description
Incidents de sécurité, demandes et tâches qui me sont affectées	Liste	Une liste de tous les incidents de sécurité, demandes de sécurité et tâches qui me sont affectés.
Emplacement de l'incident de sécurité	Carte	Emplacement régional des incidents de sécurité.
Nombre	Carte	Nombre d'incidents de sécurité par région.
Nombre min./max.	Barre du spectre de couleurs	Nombre minimal et maximal d'incidents de sécurité par région représentés par une barre du spectre de couleurs.
Pourcentage du nombre	Carte	Pourcentage du nombre total d'incidents par région.

Vue d'ensemble du CISO d'incident de sécurité avec l'analyse des incidents de sécurité activée

Lorsque le module d'extension est activé, les Analyse des incidents de sécurité utilisateurs ayant les rôles de CISO d'incident de sécurité et d'administrateur système voient la vue d'ensemble du CISO d'incident de sécurité. Les rapports CISO suivants sont fournis dans le système de base.

Rapports de vue d'ensemble du CISO d'incident de sécurité (avec l'analyse des incidents de sécurité activée)

Nom	Visuel	Description
Nouveaux incidents de sécurité de cette semaine	Score unique	Nombre de nouveaux incidents de sécurité reçus au cours de la semaine actuelle.
Incidents de sécurité fermés cette semaine	Score unique	Nombre d'incidents de sécurité fermés au cours de la semaine actuelle.
Nouveaux incidents de sécurité (sur 7 jours)	Score unique	Nombre d'incidents de sécurité ouverts au cours des 7 derniers jours.
Incidents de sécurité clôturés (sur 7 jours)	Score unique	Nombre d'incidents de sécurité fermés au cours des 7 derniers jours.
Incidents de sécurité nouveaux quotidiens par rapport aux incidents de sécurité fermés	Graphique de tendance	Nombres d'incidents de sécurité nouveaux et fermés au fil du temps par jour.
Nouveaux incidents de sécurité hebdomadaires par rapport aux incidents de sécurité clôturés	Graphique de tendance	Incidents de sécurité nouveaux et fermés au fil du temps par semaine.
Code de fermeture de l'incident de sécurité	Graphique de tendance	Nombre complet de codes de fermeture au fil du temps.
Impact opérationnel d'un incident de sécurité	Arborescence	Services d'entreprise avec incidents de sécurité avec regroupements disponibles par criticité opérationnelle.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports de vue d'ensemble du CISO d'incident de sécurité (avec l'analyse des incidents de sécurité activée) (suite)

Nom	Visuel	Description
Durée moyenne pour contenir (hebdomadaire)	Graphique de tendance	Temps moyen sur 7 jours nécessaire pour contenir un incident de sécurité au fil du temps.
Durée moyenne pour l'élimination (hebdomadaire)	Graphique de tendance	Délai moyen sur 7 jours nécessaire pour éradiquer un incident de sécurité au fil du temps.
Durée moyenne de création d'identité (hebdomadaire)	Graphique de tendance	Délai moyen sur 7 jours nécessaire pour identifier un incident de sécurité au fil du temps.
Emplacement de l'incident de sécurité	Carte	Emplacement régional des incidents de sécurité.
Nombre	Carte	Nombre d'incidents de sécurité par région.
Nombre min./max.	Barre du spectre de couleurs	Nombre minimal et maximal d'incidents de sécurité par région représentés par une barre du spectre de couleurs.
Pourcentage du nombre	Carte	Pourcentage du nombre total d'incidents par région.

Vue d'ensemble du CISO de l'incident de sécurité sans l'activation de l'analyse des incidents de sécurité

Lorsque le module d'extension n'est pas activé, les Analyse des incidents de sécurité utilisateurs ayant les rôles de CISO d'incident de sécurité et d'administrateur système voient la vue d'ensemble de génération de rapports du CISO d'incident de sécurité. Les rapports CISO suivants sont fournis dans le système de base.

Rapports de vue d'ensemble du CISO d'incident de sécurité (sans l'analyse des incidents de sécurité activée)

Nom	Visuel	Description
Nouveaux incidents de sécurité de cette semaine	Score unique	Nombre de nouveaux incidents de sécurité ouverts au cours de la semaine actuelle.
Incidents de sécurité fermés cette semaine	Score unique	Nombre d'incidents de sécurité fermés au cours de la semaine actuelle.
Nouveaux incidents de sécurité (sur 7 jours)	Score unique	Nombre d'incidents de sécurité ouverts au cours des 7 derniers jours.
Incidents de sécurité clôturés (sur 7 jours)	Score unique	Nombre d'incidents de sécurité fermés au cours des 7 derniers jours.
Nouveaux incidents de sécurité chaque semaine	Graphique de tendance	Les nouveaux incidents de sécurité s'ouvraient chaque semaine.
Incidents de sécurité fermés chaque semaine	Graphique de tendance	Les incidents de sécurité sont clôturés une fois par semaine.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports de vue d'ensemble du CISO d'incident de sécurité (sans l'analyse des incidents de sécurité activée) (suite)

Nom	Visuel	Description
Codes de fermeture des incidents de sécurité	Graphique de tendance	Codes de fermeture des incidents de sécurité au fil du temps.
Services d'entreprise avec incidents de sécurité - Impact sur l'entreprise	Arborescence	Services d'entreprise avec incidents de sécurité avec regroupements disponibles par criticité opérationnelle.
Délai moyen pour contenir	Score unique	Temps moyen nécessaire pour contenir tous les incidents de sécurité.
Délai moyen pour contenir critique	Score unique	Temps moyen nécessaire pour contenir tous les incidents de sécurité critiques.
Délai moyen d'identification	Score unique	Temps moyen nécessaire pour identifier tous les incidents de sécurité

Remarque : Le Réponse aux incidents de sécurité système de base inclut des solutions Performance Analytics pour afficher des tableaux de bord de bonnes pratiques préconfigurés. Les tableaux de bord présentent des mesures importantes pour analyser votre processus Security Incident Response, tels que les nouveaux incidents de sécurité ou l'âge moyen des incidents de sécurité ouverts. Pour plus d'informations et des instructions d'installation, voir Réponse aux incidents de sécurité Solutions Analyse de la plateforme et Reporting.

Carte des incidents de sécurité

La carte des incidents de sécurité fournit des données par emplacement géographique. La carte du monde est mise en évidence dans chaque zone dans laquelle un incident se produit. Lorsque le module d'extension Analyse des incidents de sécurité est activé, vous pouvez ajouter la carte des incidents de sécurité à la Réponse aux incidents de sécurité vue d'ensemble. Une fois qu'elle a été ajoutée, vous pouvez configurer la carte en modifiant les filtres de la carte.

Ajouter une carte à la vue d'ensemble Réponse aux incidents de sécurité

Vous pouvez ajouter la carte à la Réponse aux incidents de sécurité vue d'ensemble pour afficher les données d'incident de sécurité par emplacement géographique. Une carte vous permet d'explorer les informations sur les incidents de sécurité par emplacement.

Avant de commencer

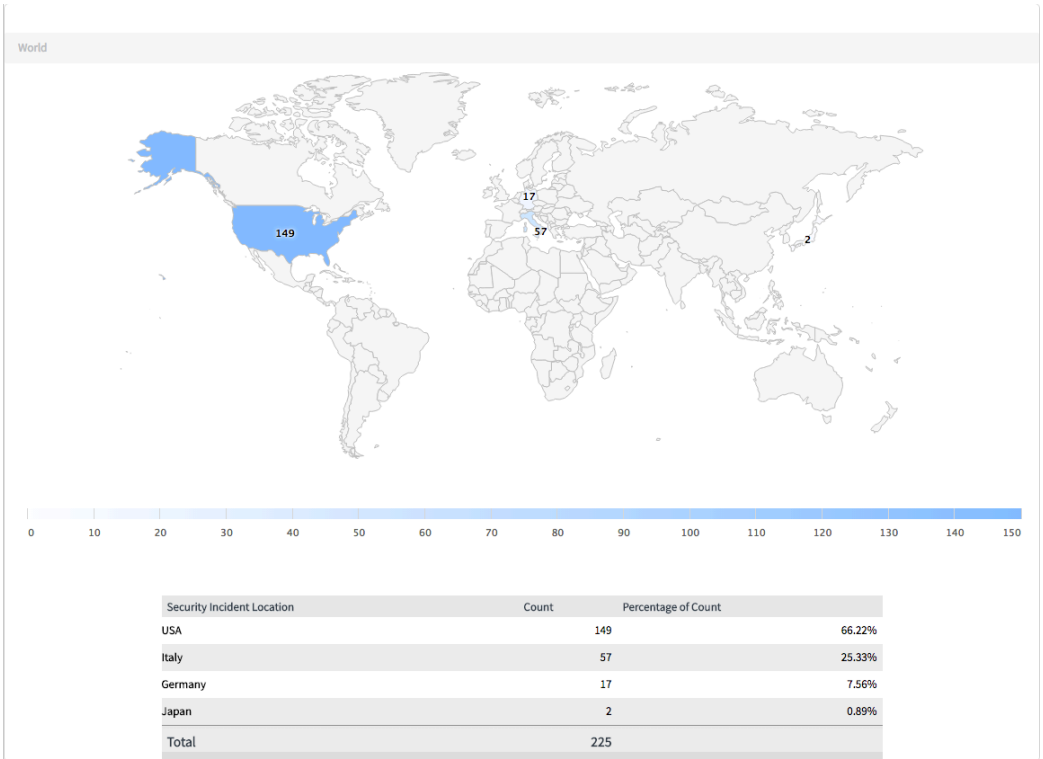
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Vue d'ensemble**.
2. Cliquez sur **Ajouter du contenu** dans le coin supérieur gauche de la page pour ouvrir le contrôle de sélection du widget.
3. Dans la première zone de sélection, cliquez sur **Rapports**.
4. Dans la deuxième zone de sélection, cliquez sur **Incident de sécurité**.
5. Dans la troisième zone de sélection, cliquez sur **la carte des incidents de sécurité**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. En bas de l'écran, cliquez sur l'emplacement de l'écran que vous souhaitez ajouter au rapport.
7. Fermez la zone **Ajouter du contenu** .

Modifier la carte des incidents de sécurité

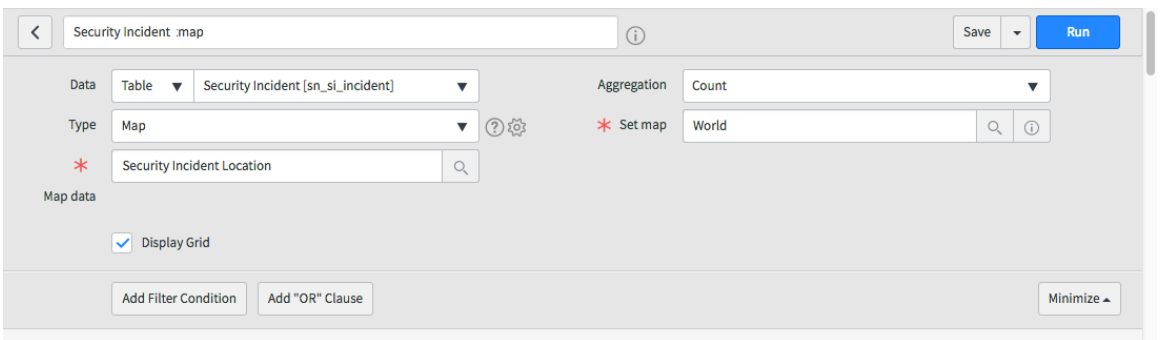
Les administrateurs du domaine global peuvent modifier la façon dont la carte des incidents de sécurité gère les incidents de sécurité à l'aide de filtres.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Rapports** > **Administration** > **Tout**.
2. Rechercher une **carte des incidents de sécurité**.
3. Cliquez sur **Modifier le rapport**.



4. Cliquez sur **Ajouter une condition de filtre** pour ajouter ou modifier des filtres.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Exécuter** pour afficher les changements appliqués.
6. Cliquez sur **Enregistrer**.

Arborescences des incidents de sécurité

Lorsque le module d'extension Analyse des incidents de sécurité est activé, vous pouvez ajouter les arborescences incident de sécurité - impact sur le service et incident de sécurité - en temps réel à la Réponse aux incidents de sécurité vue d'ensemble. Une fois ajoutées, vous pouvez configurer les arborescences en modifiant les catégories et les indicateurs des arborescences.

Ajouter des arborescences à la vue d'ensemble de Security Incident Response

Les arborescences affichent les données hiérarchiques (arborescentes) sous la forme d'un ensemble de rectangles imbriqués. Chaque branche de l'arbre reçoit un rectangle, qui est ensuite carrelé avec des rectangles plus petits représentant des sous-branches. Les arborescences vous permettent d'afficher les informations sur les incidents de sécurité de manière dynamique et intéressante.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Vue d'ensemble**.
2. Cliquez sur **Ajouter du contenu** dans le coin supérieur gauche de la page pour ouvrir le contrôle de sélection du widget.
3. Dans la première zone de sélection, cliquez sur **Treemap**.
4. Dans la deuxième zone de sélection, sélectionnez l'arborescence à insérer dans la liste suivante :
   - Incident de sécurité - Impact sur le service
   - Incident de sécurité : en temps réel
   - Incident de sécurité - Impact sur l'entreprise
   - Importance de la vulnérabilité

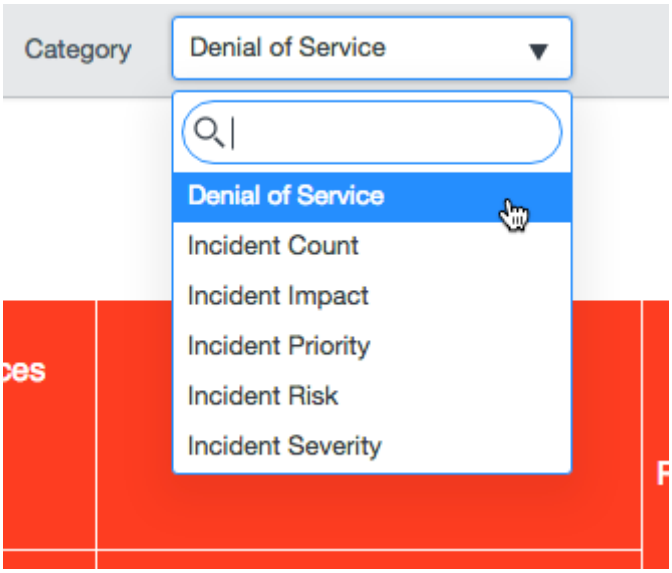
   Remarque : L'arborescence Impact sur l'entreprise s'affiche par défaut sur la page d'accueil Réponse aux incidents de sécurité . Les arborescences Impact sur le service et Temps réel nécessitent que le module d'extension Analyse des incidents de sécurité soit activé.

5. Dans la troisième zone de sélection, sélectionnez le niveau de granularité des informations que vous souhaitez récupérer pour l'arborescence sélectionnée.

   Remarque : Pour l'arborescence Incident de sécurité - Impact du service, sélectionnez **Incident de sécurité** dans la troisième zone de sélection. Cette sélection fournit une liste déroulante avec plusieurs catégories de données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. En bas de l'écran, cliquez sur l'emplacement de l'écran où vous souhaitez ajouter la jauge.
7. Fermez la zone **Ajouter du contenu** .

Créer ou mettre à jour une catégorie d'arborescence

Vous pouvez modifier les catégories prédéfinies pour les arborescences des incidents de sécurité ou créer des catégories selon les besoins.

Avant de commencer

Rôle requis : sn_si.admin

Les arborescences utilisent Analyse des performances comme source de données. Le module Analyse des performances nécessite un module d'extension distinct.

Pourquoi et quand exécuter cette tâche

Dans le système de base, des catégories d'arborescence telles que le risque d'incident, le déni de service et la gravité de l'incident sont incluses. Vous pouvez modifier ces catégories ou en définir d'autres selon vos besoins.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Administration**et ouvrez la définition de l'arborescence pour laquelle vous souhaitez configurer des catégories :
   - **Définition de reporting sur la criticité des services**
   - **Définition en temps réel**
2. Facultatif : Modifiez le nom de la définition de l'arborescence.
   Dans le système de base, le nom par défaut de la définition de l'arborescence **d'impact du service est Incident de sécurité**. Le nom par défaut de la définition de l'arborescence en temps réel est **Incident de sécurité - Temps réel**.
3. À moins que vous n'utilisiez une arborescence personnalisée, ne modifiez pas la valeur **du groupe d'indicateurs PA** .
4. Pour désactiver la définition de l'arborescence, décochez la case **Actif** .
   Si, par exemple, vous désactivez la catégorie Déni de service dans le tableau de bord d'impact sur le système, cette catégorie d'arborescence n'est pas disponible.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans la liste connexe des **catégories de l'arborescence** , sélectionnez une catégorie à modifier ou cliquez sur **Nouveau** pour créer une nouvelle catégorie.
6. Renseignez les champs.

Formulaire Catégorie d'arborescence

Champ	Description
Nom	Nom affiché pour la catégorie dans la liste **Catégories** au-dessus de l'arborescence.
Ordre	Ordre dans lequel la catégorie apparaît dans la liste **Catégories** au-dessus de l'arborescence.
Arborescence	Nom de l'arborescence qui utilise cette catégorie.
Couleur	Couleur affichée pour cette catégorie dans l'arborescence.
Actif	Sélectionnez cette option pour activer cette catégorie.
Description	Description de la catégorie.
Visible par tous les rôles	Sélectionnez cette option pour rendre cette catégorie visible à tous les utilisateurs, quel que soit leur rôle.
Rôles	Si vous n'avez pas coché la case **Visible par tous les rôles** , sélectionnez les rôles pouvant afficher cette catégorie.

7. Cliquez sur **Envoyer** ou **Mettre à jour**.

Créer ou mettre à jour un indicateur d'arborescence

Vous pouvez modifier les indicateurs prédéfinis pour une catégorie d'arborescence ou créer de nouveaux indicateurs. Pour chaque indicateur, vous pouvez configurer sa source de données et spécifier comment les listes d'incidents de sécurité sont ouvertes à partir des arborescences affichées avec l'indicateur.

Avant de commencer

Rôle requis : sn_si.admin

Les arborescences utilisent Analyse des performances comme source de données. Le module Analyse des performances nécessite un module d'extension distinct.

Procédure

1. Ouvrez la définition de l'arborescence pour laquelle vous souhaitez configurer les indicateurs.

Définition de l'arborescence	Action
Arborescence de l'impact du service	Accédez à la **Incident de sécurité** > **Administration** > **Définition de l'impact sur le service**.
Arborescence en temps réel	Accédez à la **Incident de sécurité** > **Administration** > **Définition en temps réel**.

2. Dans la liste connexe **des catégories d'arborescence** , sélectionnez la catégorie pour laquelle vous souhaitez configurer des indicateurs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans la liste connexe aux **indicateurs d'arborescence** , sélectionnez un indicateur à modifier ou cliquez sur **Nouveau** pour créer un indicateur.
4. Renseignez les champs.

Formulaire Indicateur d'arborescence

Champ	Description
Nom	Nom affiché pour l'indicateur dans la liste **Indicateurs** du tableau de bord d'impact sur le service.
Description brève	Description affichée pour l'indicateur dans la liste **Indicateurs** au-dessus de l'arborescence.
Limite du résultat	Nombre maximal de résultats autorisés. La limite supérieure est 100.
Précision du résultat	Nombre de chiffres à afficher après la décimale. Ce champ s'affiche uniquement pour la définition de l'arborescence en temps réel.
Actif	Case à cocher pour activer cet indicateur.
Catégorie	Nom de catégorie saisi sur l'écran précédent.
Direction	Indique si la mosaïque de l'arborescence est réduite ou agrandie. Ce champ s'affiche uniquement pour la définition de l'arborescence en temps réel.
Unité	L'unité de mesure à utiliser pour la mesure. ce champ est affiché pour la définition en temps réel uniquement.
Intervalle d'actualisation automatique	Fréquence d'actualisation de l'arborescence.
Ordre	Ordre dans lequel l'indicateur apparaît dans la liste **Indicateurs** au-dessus de l'arborescence.

5. Cliquez sur l'onglet Configuration de la **source de données** et configurez l'une des options de source de données suivantes pour l'indicateur.

Option	Action
Analyse des performances	Sélectionnez **Analyse des performances** dans le champ **Source de données** , puis saisissez les entrées suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Action
	◦ **Indicateur:** Indicateur utilisé pour regrouper les données PA. ◦ **Répartition par défaut :** Répartition par défaut utilisée pour diviser l'indicateur PA sélectionné en plusieurs parties.
Script personnalisé	Sélectionnez **Script personnalisé** dans le champ **Source de données** . Utilisez ensuite l'éditeur HTML pour personnaliser le script selon vos besoins. Le résultat de l'exécution du script doit être un tableau pour que les informations s'affichent dans l'arborescence.
Conditions de la requête	Sélectionnez **Condition de requête** dans le champ **Source de données** , puis entrez les champs suivants : ◦ **Table de requêtes :** Table de base à interroger. ◦ **Type d'agrégat :** Type d'agrégat (SOMME, NOMBRE, AVG, MIN, MAX) à utiliser. ◦ **Champ d'agrégat :** Champ à utiliser par la requête. ◦ **Grouper par :** Champ permettant de trier les données interrogées. **Remarque :** Pour améliorer la requête, cliquez sur **Ajouter une condition de filtre** et **Ajouter une clause « OU »**.

6. Cliquez sur l'onglet **Clic de renvoi** et spécifiez comment les listes d'incidents de sécurité sont ouvertes à partir de l'arborescence.
   a. Dans le champ Type de navigation dans les **URL par clic** , indiquez si vous souhaitez que la liste des incidents de sécurité s'ouvre dans une nouvelle fenêtre, dans la même fenêtre ou dans une boîte de dialogue.
   b. Facultatif : Dans le champ **Script d'URL par clic** , modifiez l'exemple de script si nécessaire.
7. Cliquez sur **Envoyer** ou **Mettre à jour**.

Ajouter des graphiques d'importance de la vulnérabilité à une vue d'ensemble

Si le module d'extension est activé, vous pouvez ajouter des graphiques de définition de l'importance de la Réponse aux vulnérabilités vulnérabilité et d'autres visualisations à la vue d'ensemble.

Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la page Vue d'ensemble à laquelle vous souhaitez ajouter la jauge d'importance de la vulnérabilité.
2. Cliquez sur **Ajouter du contenu** dans le coin supérieur gauche de la page pour ouvrir le contrôle de sélection du widget.
3. Dans les trois cases de sélection, effectuez les sélections en fonction de la jauge (arborescence ou rapport de score) que vous souhaitez ajouter :
   - Pour ajouter l'arborescence de l'importance de la vulnérabilité, effectuez les sélections suivantes :
     - Arborescence
     - Importance de la vulnérabilité
     - Importance de la vulnérabilité
   - Pour ajouter le rapport de score d'importance de la vulnérabilité, effectuez les sélections suivantes :
     - Analyse des performances
     - Score
     - Services avec une vulnérabilité importante
4. Cliquez sur l'emplacement de l'écran où vous souhaitez ajouter la jauge.
5. Fermez la zone **Ajouter du contenu** .

Gestion des incidents de sécurité majeurs

L'application ServiceNow® Gestion des incidents de sécurité majeurs suit la progression de Incident de sécurité majeur (MSI) depuis la découverte jusqu'à l'analyse, en passant par la proposition, la promotion et le lien des incidents de sécurité, et la fermeture.

Gestion des incidents de sécurité majeurs

Explorer	Configurer	Intégrer
Découvrez comment les analystes, les administrateurs et les gestionnaires utilisent la gestion des incidents de sécurité majeurs (MSIM)	Planifier et configurer votre implémentation	Étendre les options MSIM en les intégrant à d'autres Microsoft applications

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Administrer	Utiliser	Rapports d'état
Tâches d'administration sur le balisage des enregistrements d'incidents et la configuration des étiquettes	Proposer, promouvoir, lier et rejeter des enregistrements d'incidents de sécurité majeurs via la gestion de l'espace de travail	Surveillez les tâches liées aux incidents et améliorez les processus grâce à des mesures, des graphiques de tendances et des rapports
Options supplémentaires		
Configurer les informations pour déployer les enregistrements		

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Demander une application Opérations de sécurité dans l'App Store

Si vous êtes un nouveau Opérations de sécurité client à partir d'un Rome jour ou d'une autre, visitez le ServiceNow Store pour afficher les applications disponibles et des informations sur la façon de soumettre des demandes à la boutique.

Plus de ressources

Visitez le Gestion des incidents de sécurité majeurs forum sur le ServiceNow Community.

Explorer la gestion des incidents de sécurité majeurs

Explorez Gestion des incidents de sécurité majeurs pour comprendre le fonctionnement de l'application en termes de suivi des incidents de sécurité critiques de priorité élevée, qui sont identifiés comme une menace pour l'organisation.

Utilisez cette section pour découvrir les principales fonctionnalités et les différents rôles impliqués dans le traitement des enregistrements d'incidents de sécurité majeurs. Cette section vous aide également à comprendre comment démarrer avec l'application, les conditions préalables et les modules d'extension requis pour travailler avec l'application.

Gestion des incidents de sécurité majeurs

Suivez et gérez diverses activités qui font généralement partie de la résolution d'un incident de sécurité majeur via Gestion des incidents de sécurité majeurs. Grâce à un espace de travail intuitif, les gestionnaires d'incidents et les personnes travaillant sur un incident peuvent

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

proposer et promouvoir des incidents en incidents majeurs, suivre les activités des incidents de sécurité majeurs et collaborer facilement avec leurs collègues.

Vue d'ensemble

Les principales options de gestion des incidents de sécurité fonctionnent conjointement avec les capacités existantes du produit Security Incident Response. Cela inclut la possibilité pour un analyste de sécurité d'escalader un incident de sécurité standard en un incident de sécurité majeur, de sorte que les nouvelles options du produit soient disponibles pour prendre en charge le processus de correction.

Après l'installation sur votre ServiceNow instance, un analyste des incidents de sécurité peut :

- Proposez un incident de sécurité au candidat à un incident de sécurité majeur afin de lancer un processus d'examen sur la nécessité de créer un incident de sécurité majeur.
- Promouvoir directement un incident de sécurité en un incident de sécurité majeur sans avoir besoin d'un processus d'examen supplémentaire.
- Rejeter un incident de sécurité proposé en tant qu'incident de sécurité majeur (MSI).
- Liez un incident de sécurité en tant qu'incident enfant à l'incident de sécurité majeur (MSI) afin que tous les incidents de sécurité puissent être traités.

Fonctionnalités principales

Gestion des incidents de sécurité majeurs (MSIM) améliore le processus de remédiation des incidents de sécurité majeurs avec les fonctionnalités suivantes :

- Espace de travail dédié à la gestion des incidents de sécurité majeurs, conçu pour le rôle d'utilisateur gestionnaire des incidents de sécurité majeurs.
- Organisez les tâches de réponse pour plusieurs incidents de sécurité « enfants ».
- Automatisez la création de dossiers de collaboration et de canaux de communication par messagerie instantanée après la création d'un incident de sécurité majeur, ainsi que l'archivage dans le cadre de la fermeture de l'incident.
- Composant d'explorateur de fichiers permettant d'organiser et de suivre la collecte d'artefacts (fichiers) liés à l'incident de sécurité majeur via une Microsoft SharePoint intégration.
- Gestionnaire de canal de messagerie instantanée et composants de flux d'activité pour gérer les communications entre plusieurs groupes de sécurité, informatiques et fonctionnels via une Microsoft Teams intégration.

Composants de l'espace de travail

Le Gestion des incidents de sécurité majeurs produit contient plusieurs nouveaux composants d'espace de travail et de nouvelles pages d'interface utilisateur qui fournissent les fonctionnalités principales :

- Espace de travail dédié à la gestion des incidents de sécurité majeurs, spécialement conçu pour le rôle d'utilisateur gestionnaire des incidents de sécurité majeurs.
- Organisez les tâches de réponse pour plusieurs incidents de sécurité enfants.
- Automatisez la création de dossiers de collaboration et de canaux de communication par messagerie instantanée après la création d'un incident de sécurité majeur, ainsi que l'archivage dans le cadre de la fermeture de l'incident.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Composant d'explorateur de fichiers permettant d'organiser et de suivre la collecte d'artefacts (fichiers) liés à l'incident de sécurité majeur via une Microsoft SharePoint intégration.
- Gestionnaire de canal de messagerie instantanée et composants de flux d'activité pour gérer les communications entre plusieurs groupes de sécurité, informatiques et fonctionnels via une Microsoft Teams intégration.

Versions prises en charge de Major Security Incident Management

Gestion des incidents de sécurité majeurs (MSIM) nécessite Now Platform® Version Rome.

Cette fonctionnalité prend en charge Microsoft Teams, qui est un espace de travail centré sur la messagerie instantanée dans la Microsoft Office 365 suite. Auparavant Microsoft Teams , il s'agissait d'une installation distincte des Microsoft Office 365 applications.

Versions prises en charge Now Platform

Cette fonctionnalité est prise en charge à partir Rome des versions ultérieures.

Les applications suivantes Opérations de sécurité sont les modules d'extension standard Réponse aux incidents de sécurité qui seront probablement installés pour la plupart des utilisateurs s'ils utilisent déjà Réponse aux incidents de sécurité (SIR). Si ce n'est pas le cas, vous devez l'installer et l'activer à partir de ServiceNow Store. Installez puis activez une application à la fois dans l'ordre mentionné pour assurer une installation fluide :

1. Réponse aux incidents de sécurité: com.snc.si_dep est le module d'extension dépendant. L'installation de ce module d'extension active les autres applications Security Operations.
2. Cadre de travail de Security Integration
3. Security Support Common
4. Security Support Common Orchestration

Introduction à MSIM

Passez en revue les informations suivantes avant de commencer à utiliser Gestion des incidents de sécurité majeurs.

Rôle requis : sn_msi.workspace_admin.

Pour faciliter l'installation et la configuration de l'application Gestion des incidents de sécurité majeurs , vous devrez peut-être vérifier si les modules d'extension suivants sont activés.

Important : Un ensemble de mises à jour (KB1289784) est disponible dans le Guide de démarrage rapide de la Gestion des incidents de sécurité majeurs Pour faciliter la configuration des utilisateurs, vous devez importer l'ensemble de mises à jour une fois que vous avez terminé l'installation de l'application. Suivez la procédure décrite dans le Guide de démarrage rapide (étape 2) sous la section Pièces justificatives de l'application MSIM, disponible sur ServiceNow Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prérequis

Tâche	Description
Avant de commencer avec l'application, assurez-vous que vous disposez des modules d'extension dépendants requis.	Dans un premier temps, installez : • Programme d'installation de ServiceNow IntegrationHub (com.glide.hub.integrations) • ServiceNow® Hub d'intégration Runtime (com.glide.hub.integration.runtime). • ServiceNow® Hub d'intégration Action Step - REST (com.glide.hub.action_step.rest) • ServiceNow® Hub d'intégration Modèle d'action : flux de données (com.glide.hub.action_type.datastream) • ServiceNow® Hub d'intégration Concepteur de flux : entrées dynamiques (com.glide.hub.dynamic_inputs) **Remarque :** Si vous ne disposez pas des privilèges nécessaires pour l'un des modules d'extension répertoriés ServiceNow® Hub d'intégration , créez un ticket de support afin d'installer ces applications prérequises.
Vérifiez que vous disposez de l'accès requis pour installer Microsoft SharePoint le spoke et Microsoft Teams Graph le spoke. **Remarque :** Les applications dépendantes primaires répertoriées ci-dessus sont les principales applications dépendantes avec lesquelles démarrer Gestion des incidents de sécurité majeurs.	Avant d'installer Microsoft SharePoint le spoke et Microsoft Teams Graph le spoke, assurez-vous de disposer de l'accès ServiceNow Hub d'intégration requis aux applications. **Remarque :** Microsoft SharePoint Le spoke et Microsoft Teams Graph le spoke sont des applications dépendantes des ServiceNow® Hub d'intégration applications.

Liste de vérification pour MSIM la configuration

Avant d'utiliser l'application ServiceNow® Gestion des incidents de sécurité majeurs (MSIM), téléchargez-la à partir du ServiceNow® Storefichier .

Suivez votre progression dans l'installation, l'installation et la configuration à partir de la table suivante.

Remarque : Les rôles affectés à Gestion des incidents de sécurité majeurs l'application sont répertoriés dans les sections suivantes. Pour plus d'informations, reportez-vous à la section Gestion des incidents de sécurité majeurs rôles.

Utilisez la liste de vérification suivante pour vous guider dans les étapes de bout en bout d'installation et de configuration Gestion des incidents de sécurité majeurs de l'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification

Tâche de configuration	Description
Vérifiez que l'application Gestion des incidents de sécurité majeurs est installée et activée à partir du ServiceNow® Store.	Gestion des incidents de sécurité majeurs La version 1.1.1 est disponible sur ServiceNow® Store. Suivez ces instructions : le téléchargement d'une application à partir de ServiceNow Store.
Vérifiez que les applications suivantes sont installées dans l'ordre donné.	Les applications suivantes sont installées par défaut après l'installation Gestion des incidents de sécurité majeurs de l'application dans la version actuelle de l'application : • File Explorer Core pour Security Operations v1.1.1 • Microsoft SharePoint File Explorer Connecteur pour Opérations de sécurité v1.1.1 • File Explorer Composant pour Opérations de sécurité v1.0.0 • Microsoft Teams Connecteur de messagerie instantanée pour Security Operations v1.0.0 • Messagerie instantanée principale pour Opérations de sécurité v1.0.0 • Incident de sécurité majeur Réponse v1.1.1 • Carte EVAM de la messagerie instantanée de collaboration pour MSIM l'espace de travail v1.0.0 (cette application est configurée uniquement pour les visualisations de l'interface utilisateur en arrière-plan de l'application pour Gestion des incidents de sécurité majeurs l'espace de travail) • Composant de l'interface utilisateur de l'organisateur de tâche pour Gestion des incidents de sécurité majeurs workspace 1.0.0 • Réponse aux incidents de sécurité v12.8.1
Vérifiez que les rôles d'utilisateur sont affectés comme Incident de sécurité majeur il convient.	Les rôles suivants sont impliqués tout au long du cycle de vie de l'incident du processus de Incident de sécurité majeur rattrapage :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	• Administrateur MSI [sn_msi.workspace_admin] • Gestionnaire MSI [sn_msi.workspace_manager] • Répondeur MSI [sn_msi.workspace_responder Pour en savoir plus sur chaque rôle, reportez-vous à Gestion des incidents de sécurité majeurs rôles.
Vérifiez que vous avez correctement configuré Microsoft SharePoint la configuration v1.0.0.	Microsoft SharePoint Gère les sites, les dossiers, les fichiers, les groupes et les utilisateurs dans Microsoft SharePoint. Ajoutez Microsoft SharePoint des données à votre ServiceNow® instance. Pour ce faire, vous devez configurer des connexions Graph et Rest. Pour plus d'informations, consultez la documentation duspoke Microsoft SharePoint v1.1.2 sur la configuration des connexions REST et Graph. Établissez une connexion Graph et REST pour vous connecter à votre ServiceNow® instance à partir de Microsoft SharePoint.
Vérifiez que vous avez créé un Microsoft SharePoint site pour créer une bibliothèque de documents.	Créez un Microsoft SharePoint site, si nécessaire, ou vous pouvez utiliser un site existant pour créer notre bibliothèque de documents.
Vérifiez que vous avez créé une bibliothèque de documents sous le Microsoft SharePoint site.	Créez une bibliothèque de documents dédiée sous un site nouveau ou existant Microsoft SharePoint .
Vérifiez que les autorisations requises sont fournies aux utilisateurs et affectées aux groupes d'utilisateurs requis dans le Microsoft SharePoint.	Gérez l'accès du site à différents utilisateurs et groupes d'utilisateurs Microsoft SharePoint .
Vérifiez que vous avez créé et configuré Microsoft SharePoint Drive ainsi que les paramètres de configuration nécessaires.	Pour vérifier les configurations des lecteurs, configurez Microsoft SharePoint le connecteur de l'explorateur de fichiers, les dossiers et les actions de fichier et les modèles de dossiers :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	• Configurer le lecteur de référentiel de l'explorateur de fichiers: créer une connexion à partir de l'instance Microsoft SharePoint de destination ServiceNow® . • Configurer les paramètres d'action de fichier et de dossier: configurez et contrôlez les actions individuelles de dossier et de fichier affichées dans le composant de l'explorateur de fichiers. • Créer des modèles de dossier: configurer pour créer des dossiers uniques pour différents types d'incidents de sécurité majeurs.
Vérifiez que vous avez établi une connexion à l'application Connecteur de messagerie instantanée Microsoft Teams.	Pour établir la connexion de l'application Microsoft Teams Chat Connector avec ServiceNow® l'instance, suivez la procédure expliquée ici : Établir une connexion MS Teams Graph sur Now Platform.
Vérifiez que vous avez configuré Microsoft Teams avec Now Platform® l'instance et créé des configurations de connexions et d'informations d'identification.	Pour vérifier Microsoft Teams la configuration avec ServiceNow® l'instance, suivez la procédure comme expliqué ici : • Établir une connexion MS Teams Graph sur Now Platform • Créer un modèle de canal de messagerie instantanée
Vérifiez que les paramètres de configuration de l'Administration des incidents de sécurité majeurs sont corrects.	En tant qu'administrateur MSI, vous devez être en mesure de : • Déterminez si les analystes de sécurité peuvent proposer et promouvoir l'incident et lier d'autres incidents de sécurité. • Activez ou désactivez les notifications lorsqu'un incident est proposé ou promu. Possibilité de modifier les messages du modèle par défaut. • Configurez les balises de sécurité qui apparaissent sur l'interface d'analyse de la sécurité pour différencier les incidents qui ont été proposés en tant que candidat à l'incident de sécurité majeur ou promus en incident de sécurité majeur.
Vérifiez que les paramètres Administration des incidents de sécurité majeurs - Notifications sont corrects.	En tant qu'administrateur MSI, déclenchez des notifications par e-mail lorsqu'un incident de sécurité est proposé et envoyez à tous les utilisateurs et groupes

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	configurés dans la liste de notifications. Pour plus d'informations, consultez Définir les préférences de notification pour MSIM.

Gestion des incidents de sécurité majeurs rôles

Affectez des rôles pour vous assurer que les utilisateurs peuvent effectuer toutes les actions nécessaires dans l'application MSIM.

Rôles pour Gestion des incidents majeurs

Type de rôle	Rôle	Description
Administrateur MSI	sn_msi.workspace_admin	Puis-je installer, configurer Gestion des incidents majeurs et configurer les applications dépendantes telles que File Explorer (FE), Microsoft Teams et la configuration de canal de messagerie instantanée, la configuration de l'espace de travail et la configuration de MSI Administration : configurations et notifications. Comment configurer : • Composant de l'explorateur de fichiers (FE) : ◦ Configurez le référentiel de fichiers. ◦ Configurez les actions de fichier et de dossier, qui sont fournies dans le composant Explorateur de fichiers de l'onglet Collaboration de l'espace de travail Major Security Incident Management. ◦ Créez les dossiers racines et les sous-dossiers, et fournissez l'accès aux sous-dossiers. • Gestion des canaux de messagerie instantanée

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles pour Gestion des incidents majeurs (suite)

Type de rôle	Rôle	Description
		◦ Activez et configurez Microsoft Teams en validant la Microsoft Teams connexion. ◦ Créez des équipes de messagerie instantanée et des canaux de messagerie instantanée, puis ajoutez des utilisateurs et affectez-les à différents groupes d'utilisateurs. • Administration de MSI : ◦ Configurations : configurez les actions des analystes de sécurité, les notifications envoyées lorsque des incidents sont proposés et promus, et affichez les balises pour les incidents de sécurité. ◦ Notifications : automatisez le processus de notification par e-mail et les notifications de l'utilisateur lorsqu'un incident de sécurité est proposé ou promu comme incident de sécurité majeur.
Gestionnaire MSI	sn_msi.workspace_manager	• Affichez l'accès à la page des paramètres de configuration de la gestion des incidents de sécurité majeurs. Ne peut modifier aucun des paramètres de configuration. • Affichez et modifiez les données d'enregistrement d'incident dans les onglets **Détails**, **Collaboration** et **Organisateur de tâche** de l'espace Gestion des incidents majeurs de travail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles pour Gestion des incidents majeurs (suite)

Type de rôle	Rôle	Description
		• Promouvez l'incident de sécurité en incident de sécurité majeur. • Configurez les actions de fichiers et de dossiers disponibles dans le composant Explorateur de fichiers de l'onglet **Collaboration** de l'espace Gestion des incidents majeurs de travail. • Lier et dissocier des enregistrements supplémentaires aux incidents de sécurité majeurs à partir de l'espace de travail.
Répondeur MSI	sn_msi.workspace_responder	• Rôle facultatif permettant d'afficher, de modifier et de répondre aux incidents de sécurité majeurs dans **Détails** et **Tâches** onglets de l'espace Gestion des incidents majeurs de travail. • Lier et dissocier des enregistrements supplémentaires aux incidents de sécurité majeurs à partir de l'espace de travail.

Traduction automatique

Intégrant Gestion des incidents de sécurité majeurs

Étendez les options de l'instance Gestion des incidents de sécurité majeurs et connectez-vous avec elle Now Platform en l'intégrant aux Microsoft applications.

Important : Un ensemble de mises à jour (KB1289784) est disponible dans le Guide de démarrage rapide de la Gestion des incidents de sécurité majeurs Pour faciliter la configuration des utilisateurs, vous devez importer l'ensemble de mises à jour une fois que vous avez terminé l'installation de l'application. Suivez la procédure décrite dans le Guide de démarrage rapide (étape 2) sous la section Pièces justificatives de l'application MSIM, disponible sur ServiceNow Store.

Configurer la bibliothèque de Microsoft SharePoint documents

Passez en revue la configuration requise qui doit être effectuée dans le Microsoft SharePoint.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Vérifiez que la procédure de configuration suivante est terminée.

Rôle requis : Administrateur système, sn_msi.workspace_admin

Procédure

1. Créez une nouvelle bibliothèque de documents sous un site nouveau ou existant Microsoft SharePoint et utilisez ce même site lors de la configuration du référentiel de Gestion des incidents de sécurité majeurs fichiers.
2. Enregistrez une application Microsoft pour établir une connexion et communiquer à Microsoft SharePoint l'aide de l'API Microsoft SharePoint REST.
   L'enregistrement de l'application établit une connexion entre l'application et Microsoft.
   Pour plus d'informations, voir Configurer l'accès par application uniquement à SharePoint sur docs.microsoft.com portail.

   Il y a deux façons d'enregistrer une demande auprès Microsoft SharePointde :

   a. Octroi de l'accès via l'application Azure AD uniquement

   b. Octroi de l'accès à l'aide de Microsoft SharePoint Application uniquement

   Important : L'octroi de l'accès à l'aide d'une Microsoft SharePoint application uniquement est une approche héritée, mais très pertinente et facile à configurer.

   Utilisez l'ID client et le secret client générés à partir de l'étape ci-dessus lors de la configuration d'une connexion REST pour le connecteur de l'explorateur Microsoft SharePoint de fichiers.
3. Enregistrez une application supplémentaire pour Microsoft communiquer à Microsoft SharePoint l'aide des API Microsoft Graph.
   Pour plus d'informations, consultez Enregistrer une application auprès de Microsoft Identity Platform **Enregistrer une nouvelle application sur Azure avec l'instance Now Platform**

   a. Connectez-vous au portail Azure à l'aide de votre Microsoft compte.

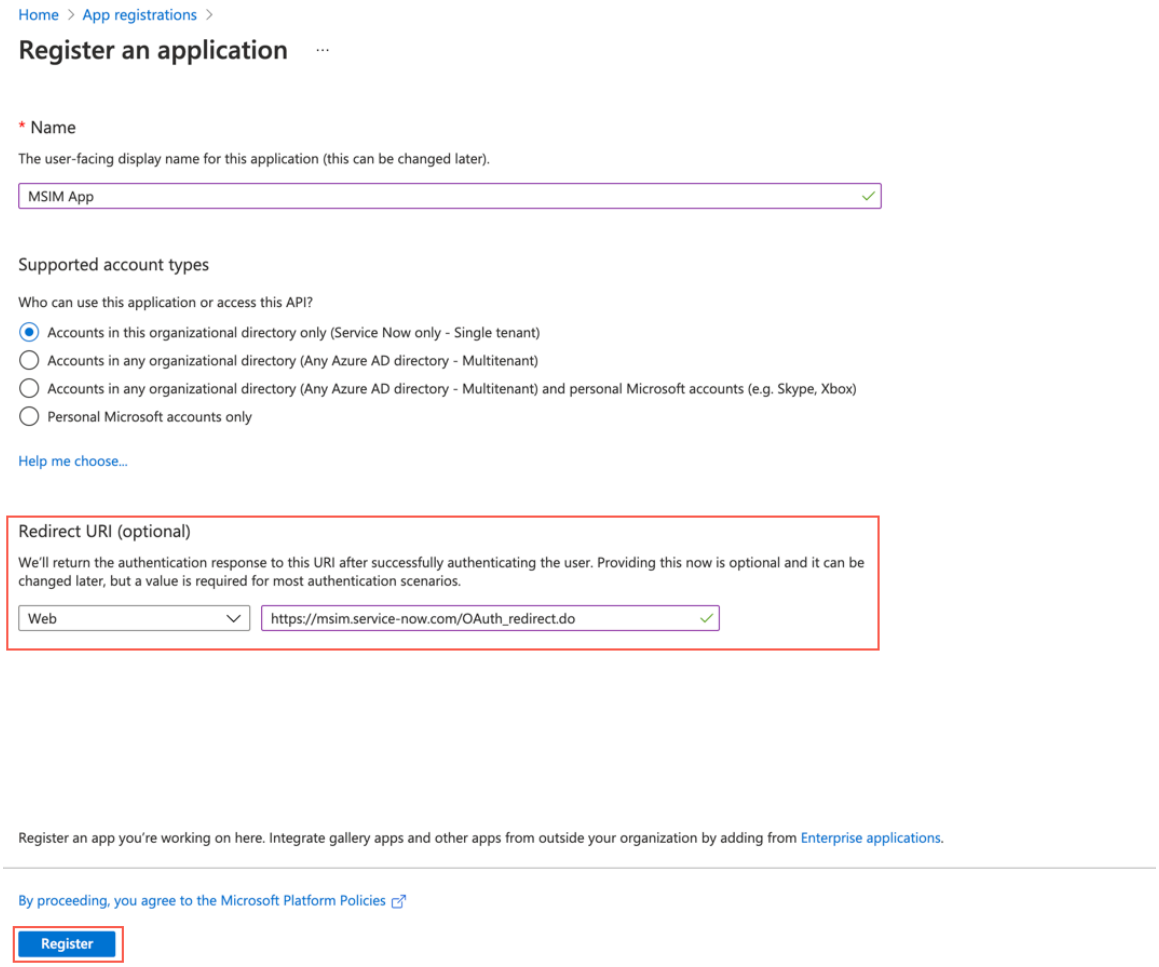
   b. Suivez les instructions décrites sur le portail Microsoft.

   c. Fournissez l'URL Now Platform® de redirection d'instance dans le champ URL de redirection autorisée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, `msim.service-now.com/OAuth_redirect.do`



d. **S'inscrire** l'application.

e. Accédez à la section **Certificats et secrets** et créez un nouveau secret client.

> **Remarque :** Vous pouvez également charger un certificat client et vous assurer de copier et de stocker la valeur d'empreinte générée.

f. Copiez et stockez le secret client généré quelque part, car il est requis lors de la configuration du registre d'application OAuth sur ServiceNow® l'instance.

4. Sous **Autorisations d'API**, ajoutez l'autorisation Microsoft Graph :

a. Cliquez sur **Ajouter une autorisation**.

b. Sélectionnez **Microsoft Graph**.

c. Sélectionnez **les autorisations déléguées**.

d. Dans la liste **Sites** , sélectionnez **l'autorisation Sites.ReadWrite.All** .

e. Dans la liste **Utilisateur** , sélectionnez **User.Read** permission.

f. Cliquez sur **Ajouter des autorisations**.

5. Sous **Autorisations d'API**, ajoutez l'autorisation SharePoint :

a. Cliquez sur **Ajouter une autorisation**.

b. Sélectionnez **SharePoint**.

Traduction automatique

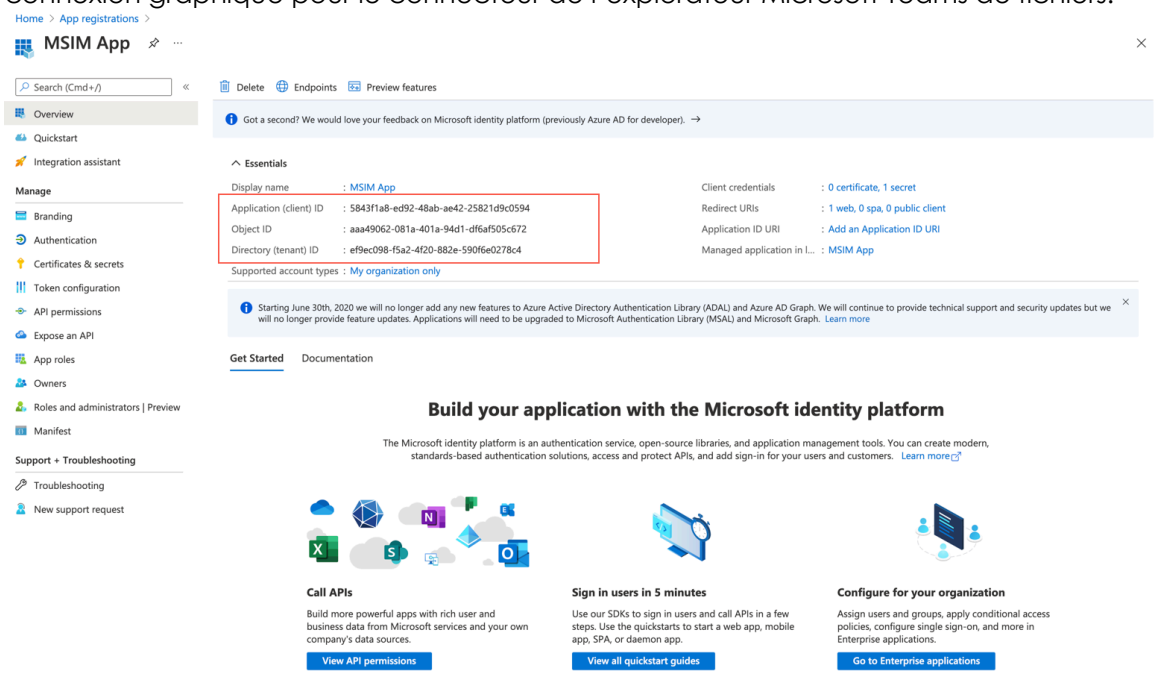
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Sélectionnez **Autorisations de l'application**.

d. Dans la liste **Sites** , sélectionnez l'autorisation **Sites.FullControl.All** .

e. Cliquez sur **Ajouter des autorisations**.

6. Après avoir ajouté des autorisations, cliquez sur **Accorder le consentement de l'administrateur**.
7. Utilisez les mêmes valeurs d'ID client et de secret client générées à partir de ce registre d'application (disponible dans la section Vue d'ensemble) lors de la configuration de la connexion graphique pour le connecteur de l'explorateur Microsoft Teams de fichiers.



Établir des connexions Graph et REST sur Now Platform

Configurez les connexions Graph et REST sur Now Platform l'instance avec laquelle communiquer Microsoft SharePoint.

Intégrez l'instance Now Platform et Microsoft SharePoint en créant une application OAuth personnalisée dans Microsoft SharePoint pour authentifier les demandes Now Platform.

Configurer la connexion REST pour MS SharePoint

Configurez la connexion REST sur Now Platform l'instance avec laquelle communiquer Microsoft SharePoint.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Configurez un nouvel enregistrement de locataire et sélectionnez **MicrosoftSharePointOnline** comme enregistrement d'alias.
   Pour plus d'informations, voir Définir les locataires Microsoft SharePoint .
2. Pour configurer l'alias de connexion et d'informations d'identification **MicrosoftSharePointOnline** , Configurer l'enregistrement de connexion Microsoft SharePoint Online .
3. Sélectionnez l'enregistrement du locataire créé à l'étape 2 ci-dessus comme suit : **Connexion REST** tout en remplissant le formulaire **Configuration du référentiel de fichiers** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la connexion graphique pour MS SharePoint

Configurez la connexion Graph sur Now Platform l'instance avec laquelle communiquer Microsoft SharePoint.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Pour configurer l'alias de connexion et d'informations d'identification Graph à l'aide d'un secret client, reportez-vous à la section Configurer l'enregistrement de connexion Microsoft SharePoint Online .
   Suivez les étapes ci-dessous pour configurer la connexion Graph et l'alias d'informations d'identification à l'aide du certificat client.

   Remarque : Par défaut, le fournisseur JWT, la clé JWT et le certificat, qui sont configurés dans la connexion REST précédente, sont utilisés ici dans cette procédure. Pour plus d'informations, consultez Configurer la connexion REST pour MS SharePoint.

   a. Accédez à la **Tout** > **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.

   b. Ouvrez l'enregistrement, **MicrosoftSharePointGraph**.

   c. Cliquez sur le lien **connexe Créer une nouvelle connexion et de nouvelles informations d'identification** .

   d. Renseignez les informations suivantes sur le formulaire.

Champ	Description
Nom de l'entité OAuth	Nom permettant d'identifier l'enregistrement du registre d'application OAuth.
ID client OAuth	ID client
Secret client OAuth	Vous pouvez saisir n'importe quelle valeur. **Remarque :** Ce n'est pas important car vous utiliserez l'authentification basée sur certificat.
URL d'autorisation OAuth	URL d'autorisation au format suivant : `https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/authorize ?response_mode=query`
URL du jeton OAuth	URL du jeton au format suivant : `https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token`
URL de révocation du jeton	URL de révocation du jeton au format suivant : `https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token`.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL de redirection OAuth	ServiceNow URL de redirection au format suivant : `https://empipaas.service-now.com/oauth_redirect.do`

Remarque : Vous pouvez modifier les valeurs par défaut selon vos besoins.

e. Cliquez sur **Créer et obtenir un jeton OAuth**.
Un message d'erreur s'affiche avec 401 - non autorisé.

f. Rechargez le formulaire et ouvrez l'enregistrement dans la liste connexe **Connexions** .

g. Saisissez la valeur **d'empreinte** codée Base64 dans l'attribut **Valeur d'empreinte codée** dans la section **Attributs** .

Remarque : La valeur **Empreinte** est une valeur hexadécimale. Vous pouvez utiliser un outil de conversion hexadécimal vers Base64 (hexadécimal vers Base64) pour encoder la valeur **d'empreinte digitale** en une valeur Base64.

h. Accédez à la **OAuth système** > **Registre d'application**.

i. Ouvrez l'enregistrement portant le même nom que **le nom de l'entité OAuth**, qui est l'étape d de cette même procédure.

j. Remplacez le script d'API OAuth par : **OAuthUtilJWTFESPGraph**

k. Accédez à la **Connexions et informations d'identification** > **Informations d'identification**.

l. Ouvrez l'enregistrement : **Informations d'identification Microsoft SharePoint Graph**.

m. Cliquez sur **Obtenir un jeton OAuth** dans la section Liens connexes.

2. Mettez à jour le périmètre de l'entité OAuth.

a. Accédez à la **OAuth système** > **Registre d'application**.

b. Ouvrez l'enregistrement du registre d'application OAuth généré à partir de l'étape 1.

c. Sélectionnez la liste connexe **Périmètres des entités OAuth** .

d. Remplacez le champ **du champ d'application OAuth** par la valeur **offline_access** suivante :

```
https://graph.microsoft.com/Sites.ReadWrite.All
```

Remarque : Vous pouvez ignorer l'étape 2 et passer à l'étape suivante, si vous ajoutez un certificat client.

3. Configurez un nouvel enregistrement de locataire et sélectionnez l'enregistrement d'alias tel que créé à l'étape 1.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations, voir Définir les locataires Microsoft SharePoint .

4. Sélectionnez l'enregistrement du locataire créé à l'étape 3 comme suit : **Connexion graphique** tout en remplissant le formulaire Configuration du référentiel de fichiers.

Établir une connexion MS Teams Graph sur Now Platform

Intégrez Now Platform l'instance et Microsoft Teams le compte en établissant une Microsoft Teams Graph connexion.

Avant de commencer

Si vous le souhaitez, vous pouvez utiliser la même application que celle que vous avez créée pour SharePoint afin d'établir la connexion Microsoft Teams Graph.

Rôle requis : admin, admin Azure

Enregistrer une nouvelle application sur Azure pour Microsoft Teams Graph Connection

Procédure

1. Connectez-vous au portail Azure à l'aide de votre Microsoft compte.
2. Accédez à la **Azure Services** > **Enregistrement de l'application** > **Nouvel enregistrement**.
3. Saisissez le nom de l'application.
   Par exemple, Microsoft Teams Graph.
4. Sélectionnez l'option **Types de comptes pris en charge** respectifs qui s'applique à votre organisation.
   Par exemple, sélectionnez **l'option Comptes dans cet annuaire d'organisation uniquement (ServiceNow uniquement - locataire unique).**

   Remarque : Pour plus d'informations sur les types de comptes pris en charge, consultez Enregistrer une application auprès de Microsoft Identity Platform .

5. Sélectionnez le type **Web** dans la liste déroulante sous l'URL de redirection.
6. Entrez Now Platform l'URL de redirection d'instance dans le champ URL de redirection autorisée.
   Par exemple, https://<<InstanceName>>.service-now.com/oauth_redirect.do
7. Cliquez sur **Enregistrer** pour enregistrer votre nouvelle application et assurez-vous que la page s'affiche avec la section **Vue d'ensemble** .

Utilisation de certificats pour l'authentification

Demander un jeton d'accès avec un certificat d'informations d'identification.

Avant de commencer

1. Vous pouvez utiliser un certificat autosigné ou un certificat délivré par l'autorité de certification. Vous pouvez créer un certificat auto-signé en exécutant le script PowerShell comme indiqué dansConfiguration d'une application Azure AD pour un accès uniquement à l'application . Le script génère deux fichiers : . PFX et . Fichier de la Régie.

   Remarque : Assurez-vous de connaître le mot de passe utilisé pour chiffrer la clé privée afin de générer le fichier . PFX et . Fichier de la Régie.

2. Utilisez le fichier . PFX pour créer un fichier Java Key Store (JKS).

   Remarque : Assurez-vous de connaître le mot de passe utilisé pour générer le fichier JKS à partir du fichier . Fichier PFX.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

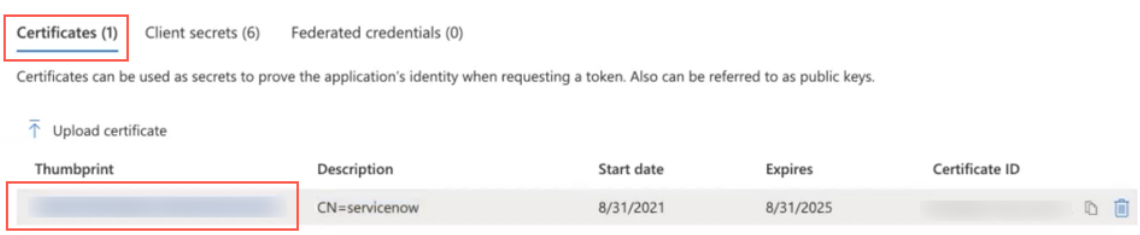
Rôle requis : administrateur

Procédure

1. Accédez aux **inscriptions des applications sur le** portail Azure AD.
2. Cliquez sur **Certificats et secrets** dans la section **Gérer** .
3. Dans l'onglet **Certificats** , cliquez sur **Télécharger le certificat**.
4. Renseignez ces valeurs sur le formulaire.

Champ	Description
Chargez un certificat (clé publique) avec l'un des types de fichiers suivants : .cer, .pem, .crt	. CER que vous avez généré à l'aide du script PowerShell.
Description	Description du certificat.

5. Cliquez sur **Ajouter**.
   Le certificat est téléchargé et ses détails s'affichent sous l'onglet **Certificats** .
6. Copiez la valeur **d'empreinte** du certificat chargé.
   La valeur **Empreinte** est une valeur hexadécimale.



7. Encodez la valeur **d'empreinte en** une valeur Base64 et enregistrez la valeur pour une utilisation ultérieure.

> **Remarque :** Vous pouvez utiliser un outil de conversion hexadécimal en base64 (hexadécimal en base64) pour coder la valeur **d'empreinte digitale** en valeur Base64.

Joindre un certificat Java Key Store pour MS Teams

Activez l'authentification du jeton JWT Bearer Grant en joignant un certificat Java Key Store (JKS) valide.

Avant de commencer

Connectez-vous à votre instance ServiceNow pour effectuer la procédure suivante.

- Certificat de magasin de clés Java valide
- Rôle requis : administrateur

Procédure

1. Accédez à la **Définition du système** > **Certificats**.
2. Ouvrez l'enregistrement **Certificat du connecteur Microsoft Teams**.
   Assurez-vous d'utiliser l'enregistrement par défaut **Microsoft Teams Connector Certificate** uniquement.
3. Saisissez le mot de passe associé au fichier JKS dans **Mot de passe du magasin de clés**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur l'icône Pièces jointes (icône) et joignez le certificat JKS que vous avez généré.
   Pour plus d'informations, consultez Configurer l'application OAuth dans Microsoft Azure .
5. Cliquez sur **Valider les banques/certificats**.
6. Cliquez sur **Mettre à jour**.

Configurer la clé de signature JWT pour MS Teams

Créez une clé de signature JSON Web Token (JWT) à affecter à votre certificat Java Key Store.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **OAuth système** > **Clés JWT**.
2. Ouvrez l'enregistrement **Microsoft Teams Connector JWT**.
3. Entrez le mot de passe utilisé pour chiffrer la clé privée afin de générer le fichier . PFX et . CER dans **Signature avec le mot de passe de clé**.
4. Cliquez sur **Mettre à jour**.

Configurer le fournisseur JWT pour MS Teams

Ajoutez un fournisseur JSON Web Token (JWT) à votre instance ServiceNow.

Avant de commencer

- Copiez et enregistrez la valeur de **l'ID (client) de l'application (client)** et de **l'ID (locataire)** de l'application que vous aviez enregistrée dans le portail Azure.



- Rôle requis : administrateur

Procédure

1. Accédez à la **OAuth système** > **Fournisseurs JWT**.
2. Ouvrez l'enregistrement **Connecteur MS Teams Fournisseur JWT**.
3. Entrez les valeurs pour **iss**, **sub** et **aud** dans la liste connexe Réclamations standard.

Champ	Valeur
Aud	URL Microsoft Online au format suivant : `https://login.microsoftonline.com/<tenant-id>/oauth2/token`. Remplacez `<tenant-id>` par la valeur **d'ID (locataire) du répertoire** de votre application avait enregistré dans le portail Azure.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Iss	**ID de l'application (client) de** l'application que vous aviez enregistrée dans le portail Azure.
sub	**ID de l'application (client) de** l'application que vous aviez enregistrée dans le portail Azure.

4. Cliquez sur **Mettre à jour**.

Établir une connexion à l'aide de certificats

Établissez une connexion entre les applications Microsoft Teams Graph nouvellement créées à l'aide de certificats.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.
2. Ouvrez **le spoke Microsoft Teams**.
3. Modifier la valeur du champ **Modèle de configuration : Modèle de code d'autorisation du connecteur MSIM Microsoft Teams et enregistrez** le formulaire.

   Remarque : Ce modèle contient l'autorisation d'API déléguée requise pour l'intégration MSTeams.

4. Dans la section Liens connexes, cliquez sur Créer une **nouvelle connexion et de nouvelles informations d'identification**.

Nom	N'importe quel nom unique.
URL de connexion	URL de connexion. Par exemple, https://graph.microsoft.com
Version de l'API	Version de l'API. Par exemple, v1.0
URL d'autorisation	https://login.microsoftonline.com/<<ID locataire>/oauth2/v2.0/authorize
URL de jeton	https://login.microsoftonline.com/<<ID locataire>/oauth2/v2.0/token
URL de révocation du jeton	https://login.microsoftonline.com/<<ID locataire>/oauth2/v2.0/revoquer
ID client OAuth	ID client.
Secret client OAuth	Vous pouvez saisir n'importe quelle valeur. **Remarque :** Ce n'est pas important car vous utiliserez l'authentification basée sur certificat.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Créer et obtenir un jeton OAuth**.
   Un message d'erreur s'affiche avec 401 - non autorisé.
6. Rechargez le formulaire et ouvrez l'enregistrement dans la liste connexe Connexions.
7. Saisissez la valeur **d'empreinte** codée Base64 dans l'attribut **Empreinte du certificat codé** dans la section **Attributs** .

> **Remarque :** La valeur Empreinte est une valeur hexadécimale. Vous pouvez utiliser un outil de conversion hexadécimal vers Base64 (hexadécimal vers Base64) pour encoder la valeur d'empreinte digitale en une valeur Base64.

8. Accédez à la **OAuth système** > **Registre d'application**
9. **Ouvrez l'enregistrement du code d'autorisation du connecteur MSIM Microsoft Teams**.
10. Modifiez le script de l'API OAuth : **OAuthUtilJWTMSTeamsConnector**.
11. Accédez à la **Connexions et informations d'identification** > **Informations d'identification**.
12. Ouvrez l'enregistrement **Informations d'identification du connecteur Microsoft Teams MSIM**.
13. Dans Liens connexes, cliquez sur Obtenir un **jeton OAuth**.
    En cas de réussite, les autorisations d'API suivantes sont ajoutées à l'application Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Traduction automatique

Utilisation de la valeur Secret client

Utilisez la valeur du secret client pour configurer l'enregistrement du registre d'application Graph.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez aux **inscriptions des applications sur le** portail Azure AD.
2. Cliquez sur **Certificats et secrets** dans la section **Gérer** .
3. Cliquez sur **Nouveau secret client**.
4. Copiez et notez le secret client créé dans le champ **Valeur** .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Établir une connexion à l'aide du secret client

Établissez une connexion entre l'application Microsoft Teams Graph nouvellement créée et l'instance Now Platform .

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.
2. Ouvrez **le spoke Microsoft Teams**.
3. Modifier la valeur du champ **Modèle de configuration : Modèle de code d'autorisation du connecteur MSIM Microsoft Teams et enregistrez** le formulaire.

   Remarque : Ce modèle contient l'autorisation d'API déléguée requise pour l'intégration MSTeams.

4. Dans la section Liens connexes, cliquez sur Créer une **nouvelle connexion et de nouvelles informations d'identification**.

Nom	N'importe quel nom unique.
URL de connexion	URL de connexion. Par exemple, https://graph.microsoft.com
Version de l'API	Version de l'API. Par exemple, v1.0
URL d'autorisation	https://login.microsoftonline.com/<<ID locataire>/oauth2/v2.0/authorize
URL de jeton	https://login.microsoftonline.com/<<ID locataire>/oauth2/v2.0/token
URL de révocation du jeton	https://login.microsoftonline.com/<<ID locataire>/oauth2/v2.0/revoquer
ID client OAuth	ID client.
Secret client OAuth	Secret client.

5. Cliquez sur **Créer et obtenir un jeton OAuth**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En cas de réussite, les autorisations d'API suivantes sont ajoutées à l'application Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				•••
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now •••
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now •••
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now •••
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now •••
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now •••
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now •••
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now •••
openid	Delegated	Sign users in	No	Granted for Service Now •••
Team.Create	Delegated	Create teams	No	Granted for Service Now •••
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now •••
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now •••
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now •••
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now •••

Activer le connecteur de messagerie instantanée MS Teams pour l'utilisateur de Graph Spoke MS Teams

Si vous êtes un utilisateur existant, suivez la procédure de cette section pour activer le connecteur de messagerie instantanée Microsoft Teams.

Avant de commencer

Rôle requis : administrateur

Procédure

Si vous êtes un utilisateur existant de Microsoft Teams Graph Spoke, suivez les étapes ci-dessous :

- Accédez à votre application inscrite sur le portail Azure, qui est utilisé par Microsoft Teams Graph Spoke.
- Accédez à la section **Autorisations d'API** pour configurer les autorisations d'API requises.
- Cliquez sur **Ajouter une autorisation**.
- Sélectionnez **Microsoft Graph**.
- Pour utiliser l'application Microsoft Teams Connector, vous devez ajouter deux autres autorisations déléguées à votre application à partir du portail Azure : « ChannelMember.ReadWrite.All » et « TeamMember.ReadWrite.All ».
- Après avoir ajouté les autorisations requises ci-dessus, cliquez sur **Accorder le consentement de l'administrateur**.

Configurer MS Teams sur l'instance Now Platform pour un utilisateur existant :

- Accédez aux **alias de connexion et d'informations d'identification**.
- Sélectionnez l'enregistrement du **spoke Microsoft Teams** comme illustré dans l'image ci-dessous.
- Sélectionnez l'enregistrement d'informations d'identification associé au spoke Microsoft Teams.
- Cliquez sur **Obtenir le jeton OAuth**. Un message de confirmation s'affiche pour indiquer que le jeton d'actualisation OAuth est disponible.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En tant qu'utilisateur existant, vous avez maintenant terminé l'intégration de l'application de connecteur de messagerie instantanée Microsoft Teams à l'API Microsoft Teams Graph.

Gestion des incidents de sécurité majeurs Intégration de la téléconférence

Avec Gestion des incidents de sécurité majeurs l'intégration des téléconférences, vous pouvez collaborer avec vos clients et vos homologues agents pour résoudre les problèmes des clients à l'aide des options de partage d'écran et de vidéo dans Microsoft Teamsou Cisco WebexZoom à partir de l'application MSIM.

L'intégration Gestion des incidents de sécurité majeurs Téléconférence vous permet d'intégrer le canal de communication de conférence au canal de Notification communication en gérant et en initiant un , Cisco Webexou Zoom une Microsoft Teamsréunion directement à partir de l'applicationGestion des incidents de sécurité majeurs.

En tant que gestionnaire MSI, vous pouvez utiliser l'intégration de la téléconférence MSIM pour lancer Microsoft Teamsdes Cisco WebexZoom réunions. Intégrez la Gestion des incidents de sécurité majeurs téléconférence avec les fournisseurs de services tiers comme canal de communication pour rencontrer les personnes concernées afin de résoudre les incidents de sécurité majeurs.

Fonctionnalités principales

L'intégration Incident de sécurité majeur de la téléconférence de gestion fournit les fonctionnalités clés suivantes :

- Les gestionnaires MSI peuvent lancer une téléconférence ou une Microsoft TeamsCisco WebexZoom téléconférence directement à partir de l'incident de sécurité majeur.
- Invitez d'autres participants à l'appel.
- Affichez les enregistrements d'appels et les détails de la messagerie instantanée.
- Envoie des invitations aux participants par e-mail et Microsoft Teams par messagerie instantanée.

Commencer une téléconférence

Démarrez une téléconférence à partir d'une tâche ou d'une sécurité majeure en invitant un ou plusieurs utilisateurs à rejoindre une téléconférence. La téléconférence commence uniquement lorsqu'au moins deux participants y participent.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Assurez-vous d'avoir effectué les actions suivantes sur l'instance ServiceNow® :

- Installez et activez le module d'extension Notification (com.snc.notify).
- Composants de l'interface utilisateur installés pour l'application Notification Configurable Workspaces.
- Installez et activez le module d'extension Tableau visuel des tâches (com.devsnc.snb_vtb).

Pour plus d'informations, consultez Demander un Centre d'intégration .

Pourquoi et quand exécuter cette tâche

Les participants à l'appel peuvent inclure les éléments suivants :

- Utilisateurs auxquels des responsabilités spécifiques ont été affectées.
- Contacts ponctuels ou à la demande
- Autres contacts de tiers

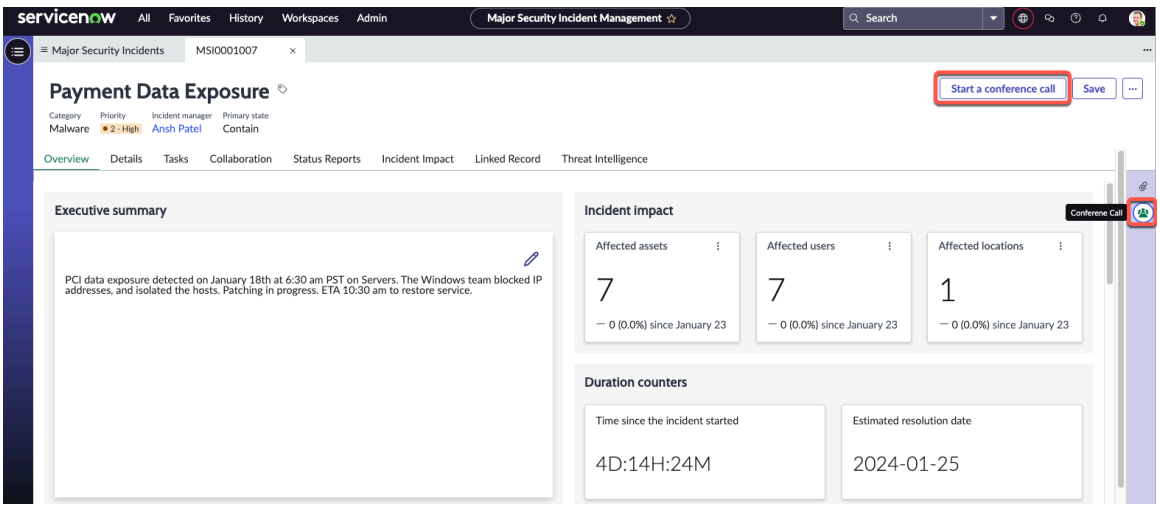
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste Incidents de sécurité majeurs, sélectionnez un incident de sécurité majeur.
3. Sélectionnez l'action **Démarrer une téléconférence** .
4. Vous pouvez également démarrer une téléconférence en sélectionnant l'icône dans le menu contextuel de droite et en sélectionnant l'icône +.
   La fenêtre contextuelle Démarrer la téléconférence s'affiche.

Téléconférence MSIM



5. Dans le champ Pont de conférence, choisissez un **pont de conférence** à partir duquel vous souhaitez vous connecter.
   Par exemple, Microsoft Team, Zoom ou Cisco Webex.
6. Dans le champ Titre, indiquez un titre décrivant le motif de la téléconférence.
7. Dans le champ Ajouter des participants, sélectionnez les participants à la téléconférence. Vous pouvez utiliser l'option de recherche pour trouver et ajouter les participants requis ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations de participants à ajouter à la téléconférence.

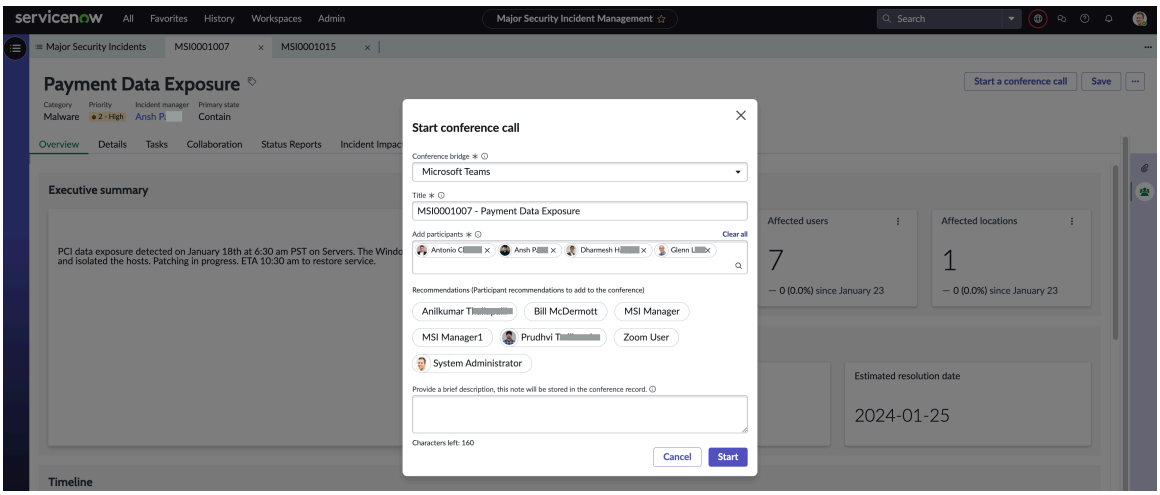
   L'utilisateur (hôte) qui lance la téléconférence est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste **Recommandations** .

> **Remarque :** Assurez-vous que les participants que vous sélectionnez ont une adresse e-mail valide.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commencer une téléconférence



8. Après avoir sélectionné les participants, décrivez brièvement le motif pour lequel vous démarrez la téléconférence dans le champ Description.
   La description que vous fournissez sera ajoutée à l'enregistrement de la conférence.
9. Une fois la liste des participants finalisée, sélectionnez **Démarrer**.
   La téléconférence commence dans le pont de conférence sélectionné. Tous les participants sont informés par e-mail, et ils sont également informés via le pont de conférence respectif qui a été sélectionné.
10. Sélectionnez l'option **Cliquer ici** en haut de l'incident de sécurité majeur pour rejoindre la téléconférence.
    Les participants peuvent utiliser le lien de la notification par e-mail ou la notification du pont de conférence sélectionné pour rejoindre l'appel.
11. Ouvrez l'incident de sécurité majeur associé pour afficher les détails de la téléconférence. Lorsque le dernier participant quitte la conférence, la téléconférence se termine ou sélectionnez **Terminer l'appel** pour mettre fin à la téléconférence.

Ajouter des participants à une téléconférence

Ajoutez des participants à une téléconférence à l'aide de l'option de recherche de la fenêtre contextuelle **Démarrer la téléconférence** pour trouver et ajouter les participants requis. Vous pouvez également ajouter des participants en sélectionnant les participants dans la liste Recommandations, qui fournit des recommandations de participants à ajouter à la téléconférence.

Avant de commencer
Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche
L'utilisateur (hôte) qui lance la téléconférence est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste Recommandations.

Les participants à l'appel peuvent inclure les éléments suivants :

- Utilisateurs auxquels des responsabilités spécifiques ont été affectées.
- Contacts ponctuels ou à la demande
- Autres contacts de tiers

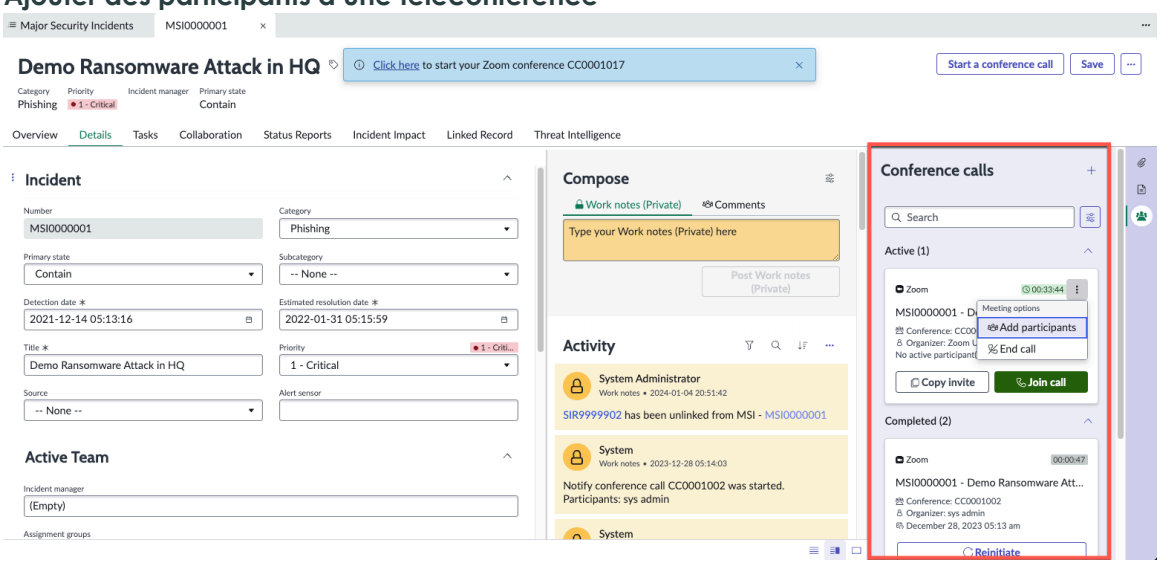
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez l'incident de sécurité majeur que vous tentez de résoudre lors de la téléconférence.
3. Sélectionnez l'icône dans le menu contextuel de droite pour afficher les détails des téléconférences.
   Cela inclut des détails tels que le nom du pont de conférence, le nom de l'organisateur, la date, l'heure, la durée de l'appel, les participants actifs et inactifs.
4. Sélectionnez en regard de la téléconférence active et sélectionnez l'option **Ajouter des participants** .

Ajouter des participants à une téléconférence



5. Vous pouvez utiliser l'option de recherche pour trouver et ajouter les participants requis ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations de participants à ajouter à la téléconférence.
6. Après avoir sélectionné les participants, décrivez brièvement le motif pour lequel vous démarrez la téléconférence dans le champ Description.
   Tous les participants sont informés par e-mail, et ils sont également informés via le pont de conférence respectif qui a été sélectionné. Les participants peuvent utiliser le lien de la notification par e-mail ou la notification du pont de conférence sélectionné pour rejoindre l'appel.
7. Vous pouvez également ajouter des participants en sélectionnant l'option **Copier l'invitation** dans la section Téléconférences du menu contextuel de droite, et vous pouvez partager avec les participants requis.

Désactiver le micro de participants à une téléconférence

En tant que responsable MSI ou hôte de téléconférence, vous avez la possibilité de désactiver le micro d'un participant particulier ou de tous les participants à la téléconférence.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Avant de commencer cette procédure, vérifiez qu'il existe une téléconférence active avec un ou plusieurs participants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez l'incident de sécurité majeur que vous tentez de résoudre lors de la téléconférence.
3. Sélectionnez l'icône dans le menu contextuel de droite pour afficher les détails des téléconférences.
4. Sélectionnez **Rejoindre l'appel** sur le pont de conférence actif.
5. Après avoir rejoint la téléconférence, sélectionnez un participant dont vous souhaitez couper le micro, puis sélectionnez **Désactiver le micro** sur le pont de conférence.
6. Pour désactiver le son de tous les participants à la téléconférence, sélectionnez **Participants** dans les commandes de la réunion, puis sélectionnez **Désactiver tous les micros**.

Afficher les détails de la téléconférence

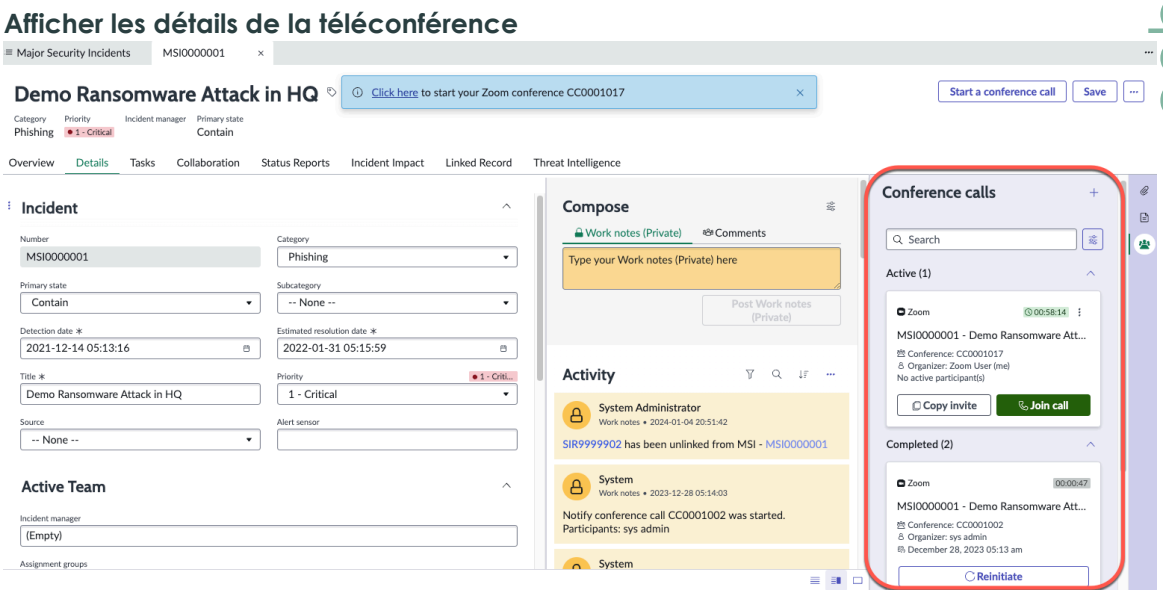
Les téléconférences sont répertoriées en tant qu'activités système dans la section Activité de l'incident de sécurité majeur et également répertoriées dans la liste connexe Téléconférences. Vous pouvez afficher des détails tels que le nom du pont de conférence, le nom de l'organisateur, la date, l'heure, la durée de l'appel, les participants actifs et inactifs.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez l'incident de sécurité majeur que vous tentez de résoudre lors de la téléconférence.
3. Sélectionnez l'icône dans le menu contextuel de droite pour afficher les détails des téléconférences.
   Cela inclut des détails tels que le nom du pont de conférence, le nom de l'organisateur, la date, l'heure, la durée de l'appel, les participants actifs et inactifs.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Vous pouvez utiliser l'option de recherche pour rechercher une téléconférence particulière.
   Il peut y avoir plusieurs appels pour le même incident de sécurité majeur.
5. Pour ajouter des participants à une téléconférence, sélectionnez Options de la ⋮ en regard de la téléconférence téléphonique active et sélectionnez l'option **Ajouter des participants** .
6. Vous pouvez également ajouter des participants en utilisant l'option **Copier l'invitation** et en partageant le lien avec les participants requis.
7. Pour participer à une téléconférence, accédez à la section Actif et sélectionnez l'option **Rejoindre l'appel** de la téléconférence requise.
8. Pour mettre fin à une téléconférence, sélectionnez Options de la ⋮ en regard de la téléconférence active et sélectionnez l'option **Fin de l'appel** .
9. Pour redémarrer une téléconférence, accédez à la section Terminé et sélectionnez l'option **Réinitialiser** de la téléconférence requise.

Intégrer les téléconférences MSIM à Microsoft Teams

L'intégration Téléconférence Microsoft Teams vous permet de gérer et d'initier une Microsoft Teams téléconférence directement à partir d'un incident de sécurité majeur.

Fonctionnalités principales

- Démarrez et terminez Microsoft Teams les téléconférences directement à partir d'incidents de sécurité majeurs ou une tâche à partir de la console de sécurité principale.
- Gérez une téléconférence en ajoutant ou en supprimant des Microsoft Teams participants.

Prérequis

Vérifiez que vous avez installé les modules d'extension suivants Hub d'intégration sur votre ServiceNow instance.

- Notification Module d'extension (com.snc.notify)
- Microsoft Teams Module d'extension Spoke de communication (sn_msteams_com_spk).
- Module d'extension Azure Active Directory User Mapping (sn_now_azure).
- Notification Composants de l'interface utilisateur pour les espaces de travail configurables

Pour plus d'informations, consultez Demander un Centre d'intégration .

Configuration

- Pour configurer l'intégration de la téléconférence Microsoft Teams MSIM à l'aide de l'application préconfigurée, reportez-vous à la section Intégrer l'application prépubliée du connecteur Notification à Microsoft Teams .
- Pour configurer l'intégration de la téléconférence Microsoft Teams MSIM à l'aide de l'application autoconfigurée, reportez-vous à la section Intégrerl'application autoconfigurée du connecteur Notification à Microsoft Teams .

Utiliser l'intégration de la téléconférence Microsoft Teams MSIM

Les étapes suivantes vous expliquent comment gérer et initier une Microsoft Teams téléconférence directement à partir d'un incident de sécurité majeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

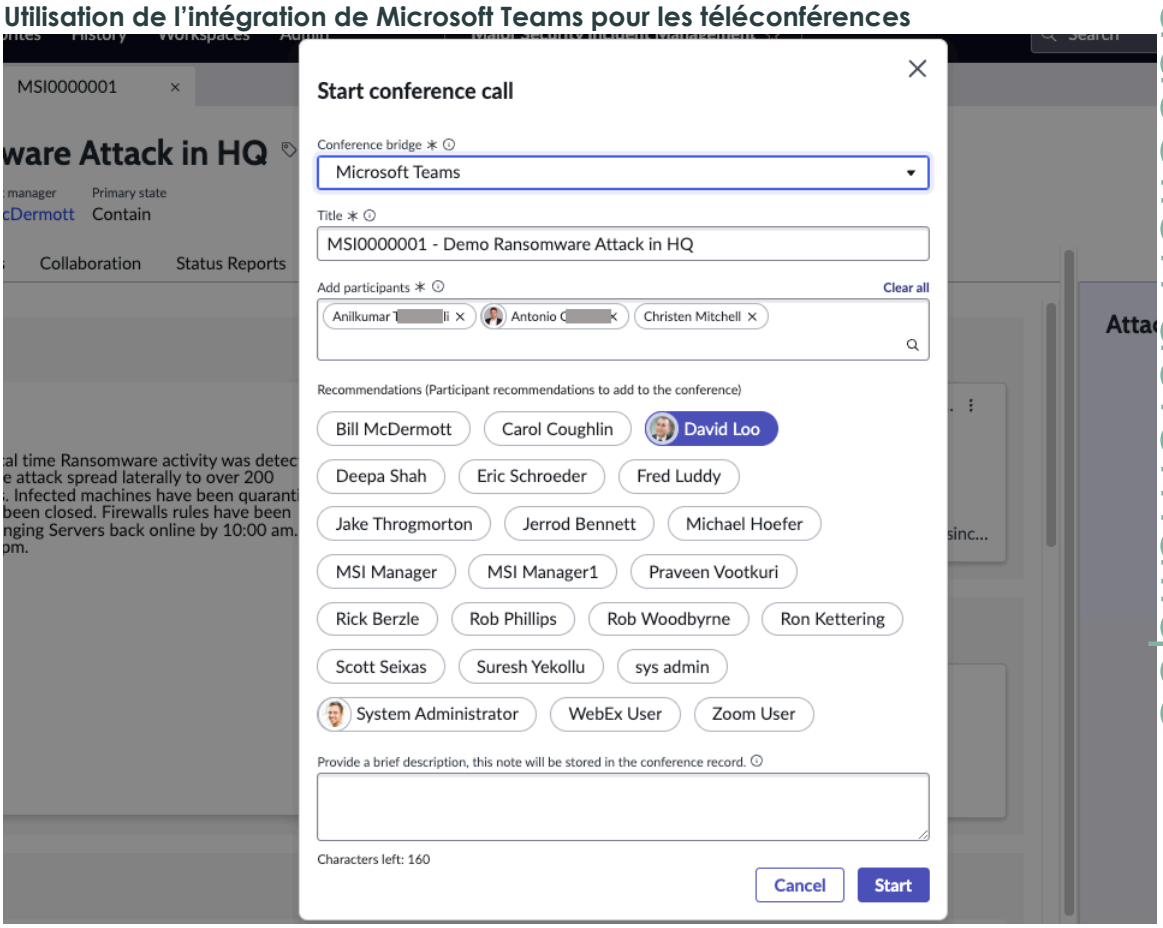
Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste Incidents de sécurité majeurs, sélectionnez un incident de sécurité majeur.
3. Sélectionnez l'action **Démarrer une téléconférence** .
4. Vous pouvez également démarrer une téléconférence en sélectionnant l'icône dans le menu contextuel de droite et en sélectionnant l'icône +.
   La fenêtre contextuelle Démarrer la téléconférence s'affiche.
5. Choisissez **Microsoft Teams** comme pont de conférence à partir duquel vous souhaitez vous connecter.
6. Dans le champ Titre, indiquez un titre décrivant le motif de la téléconférence Microsoft Teams.

Utilisation de l'intégration de Microsoft Teams pour les téléconférences



7. Dans le champ Ajouter des participants, sélectionnez les participants à la téléconférence Microsoft Teams.
   Vous pouvez utiliser l'option de recherche pour trouver et ajouter les participants requis ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations de participants à ajouter à la téléconférence Microsoft Teams.

   L'utilisateur (hôte) qui lance la téléconférence Microsoft Teams est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste **Recommandations** .

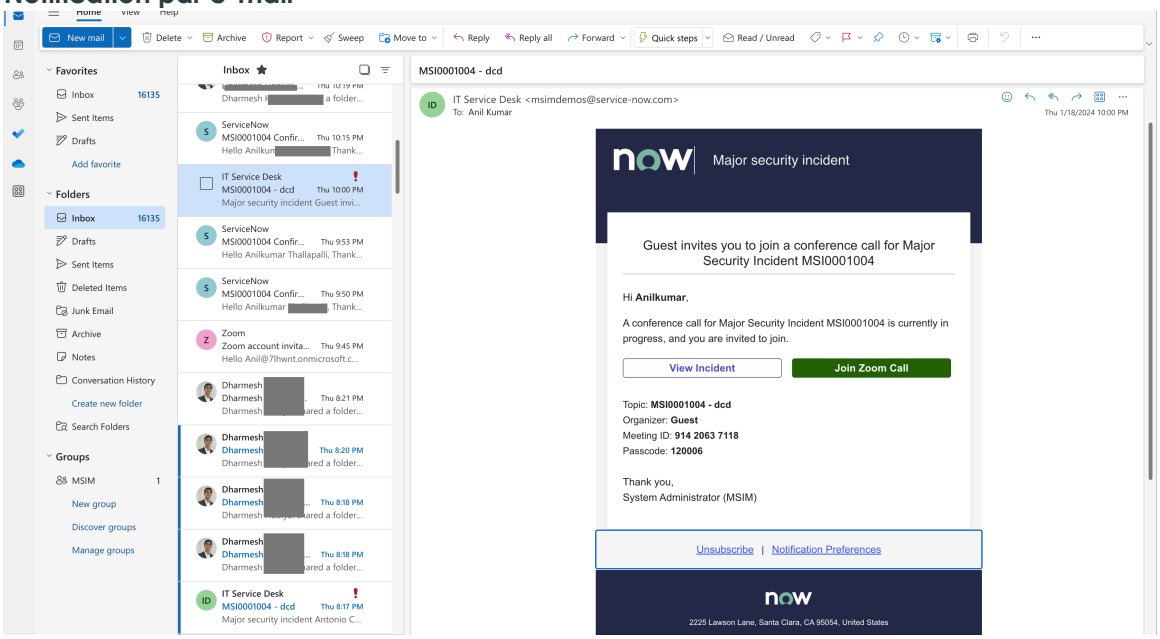
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Assurez-vous que les participants que vous sélectionnez ont une adresse e-mail valide.

8. Après avoir sélectionné les participants, décrivez brièvement le motif pour lequel vous démarrez la téléconférence dans le champ Description.
   La description que vous fournissez sera ajoutée à l'enregistrement de la conférence.
9. Une fois la liste des participants finalisée, sélectionnez **Démarrer**.
   La téléconférence démarre dans l'application Microsoft Teams. Tous les participants sont informés par e-mail à partir de l'application MSIM et l'autre notification est envoyée via un bot sur l'application Microsoft Teams.
10. Sélectionnez l'option **Cliquez ici** au-dessus de l'incident de sécurité majeur pour rejoindre la téléconférence sur l'application Microsoft Teams.
    Les participants peuvent utiliser le lien de la notification par e-mail MSIM ou la notification de l'application Microsoft Teams pour rejoindre l'appel.

Notification par e-mail



11. Ouvrez l'incident de sécurité majeur associé dans l'espace de travail MSIM pour afficher les détails de la téléconférence.

    Lorsque le dernier participant quitte l'appel, la téléconférence se termine ou sélectionnez **Terminer l'appel** dans la section Téléconférence pour terminer la téléconférence.

Intégrer les téléconférences MSIM à Zoom

L'intégration Téléconférence Zoom vous permet de gérer et d'initier une Zoom téléconférence directement à partir d'un incident de sécurité majeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalités principales

- Démarrez et terminez Zoom les réunions directement à partir de n'importe quel enregistrement de tâche, tel qu'un incident de sécurité majeur, un changement ou même à partir de la console d'incident majeur.
- Gérez les Zoom réunions en ajoutant ou en supprimant des participants.
- Suivez et rapportez les détails de la réunion, tels que la durée de la réunion et les participants, pour une analyse plus approfondie.

Prérequis

Vérifiez que vous avez installé les modules d'extension suivants Hub d'intégration sur votre ServiceNow instance.

- Notification Module d'extension (com.snc.notify)
- Zoom Spoke (sn_zoom_spoke)
- Notification Agrandir (sn_notify_zoom)
- Notification Composants de l'interface utilisateur pour les espaces de travail configurables

Pour plus d'informations, consultez Demander un Centre d'intégration .

Configuration

Pour configurer l'intégration de la téléconférence Zoom MSIM à l'aide du canal de communication, reportez-vous à la Notification section Configurer le connecteur Zoom de Notification dans Notification .

Utiliser l'intégration de la téléconférence Zoom MSIM

Les étapes suivantes vous expliquent comment gérer et initier une Zoom téléconférence directement à partir d'un incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

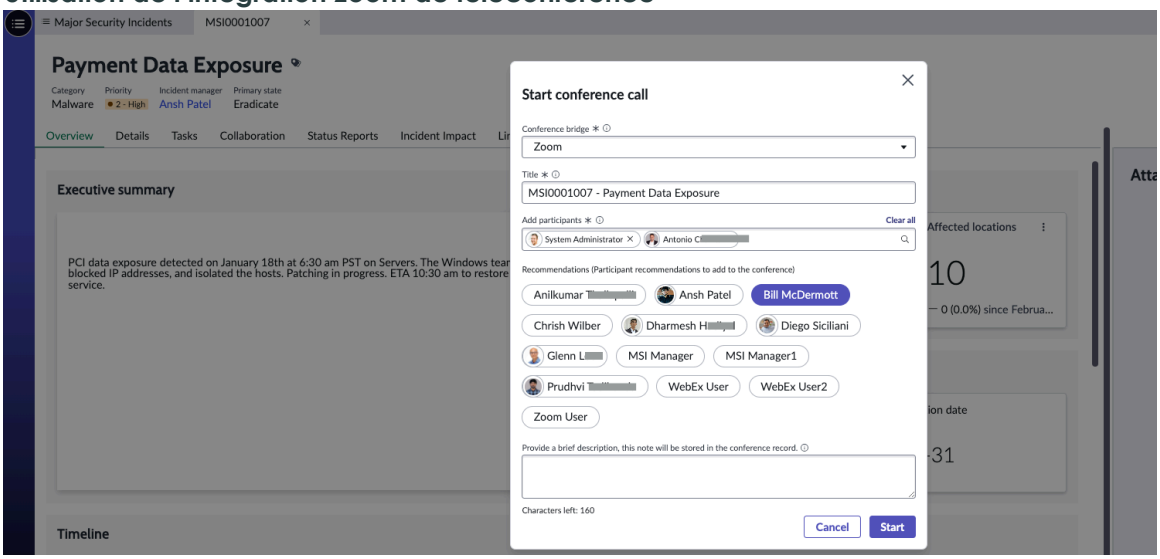
Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste Incidents de sécurité majeurs, sélectionnez un incident de sécurité majeur.
3. Cliquez sur l'action **Démarrer une téléconférence** .
4. Vous pouvez également démarrer une téléconférence en cliquant sur l'icône dans le menu contextuel de droite et en sélectionnant l'icône +.
   La fenêtre contextuelle Démarrer la téléconférence s'affiche.
5. Choisissez **Zoom** comme pont de conférence à partir duquel vous souhaitez vous connecter.
6. Dans le champ Titre, indiquez un titre décrivant le motif de la téléconférence Zoom.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation de l'intégration Zoom de téléconférence



7. Dans le champ Ajouter des participants, sélectionnez les participants à la téléconférence Zoom.
   Vous pouvez utiliser l'option de recherche pour trouver et ajouter les participants requis ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations de participants à ajouter à la téléconférence Zoom.

   L'utilisateur (hôte) qui lance la téléconférence Zoom est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste **Recommandations** .

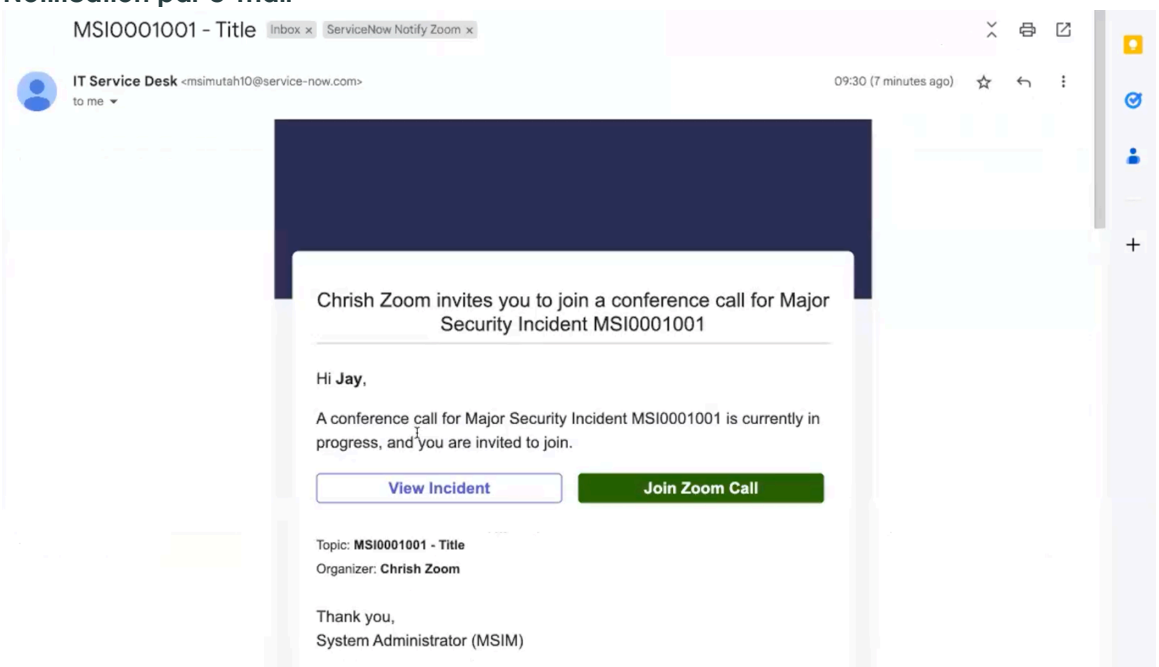
   Remarque : Assurez-vous que les participants que vous sélectionnez ont une adresse e-mail valide.

8. Après avoir sélectionné les participants, décrivez brièvement le motif pour lequel vous démarrez la téléconférence dans le champ Description.
   La description que vous fournissez sera ajoutée à l'enregistrement de la conférence.
9. Une fois la liste des participants finalisée, cliquez sur **Démarrer**.
   La téléconférence commence dans l'application Zoom. Tous les participants sont informés par le biais de deux e-mails, un e-mail est envoyé aux participants à partir de l'application MSIM et l'autre e-mail est envoyé à partir du pont de conférence Zoom.
10. Sélectionnez l'option **Cliquez ici** en haut de l'incident de sécurité majeur pour rejoindre la téléconférence sur l'application Zoom.
    Les participants peuvent utiliser le lien de la notification par e-mail MSIM ou la notification de l'application Zoom pour se joindre à l'appel.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notification par e-mail



11. Ouvrez l'incident de sécurité majeur associé dans l'espace de travail MSIM pour afficher les détails de la téléconférence.

    Lorsque le dernier participant quitte l'appel, la téléconférence se termine ou sélectionnez **Terminer l'appel** dans la section Téléconférence pour terminer la téléconférence.

    Si la téléconférence a été enregistrée, l'enregistrement sera disponible dans la section Téléconférence de l'incident de sécurité majeur associé après un certain temps.

Intégrer les téléconférences MSIM à Cisco Webex

L'intégration de la téléconférence Cisco Webex MSIM vous permet de gérer et d'initier une Cisco Webex téléconférence directement à partir d'un incident de sécurité majeur.

Fonctionnalités principales

- Démarrer et terminer Cisco Webex les réunions directement à partir d'incidents de sécurité majeurs.
- Gérez une réunion en ajoutant ou en supprimant des Cisco Webex participants.

Prérequis

Vérifiez que vous avez installé les modules d'extension suivants Hub d'intégration sur votre ServiceNow instance.

- Notification Module d'extension (com.snc.notify)
- Notification Cisco Webex Connecteur (sn_notify_webex)
- Cisco Webex Spoke Teams (sn_cisco_teams_spk)
- Notification Composants de l'interface utilisateur pour les espaces de travail configurables

Pour plus d'informations, consultez Demander un Centre d'intégration .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration

Pour configurer l'intégration de la téléconférence Cisco Webex MSIM à l'aide du canal de communication, reportez-vous à la Notification section Configurer Notification Cisco le connecteur Webex .

Utiliser l'intégration des téléconférences Cisco Webex

Les étapes suivantes vous expliquent comment gérer et initier une Cisco Webex téléconférence directement à partir d'un incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

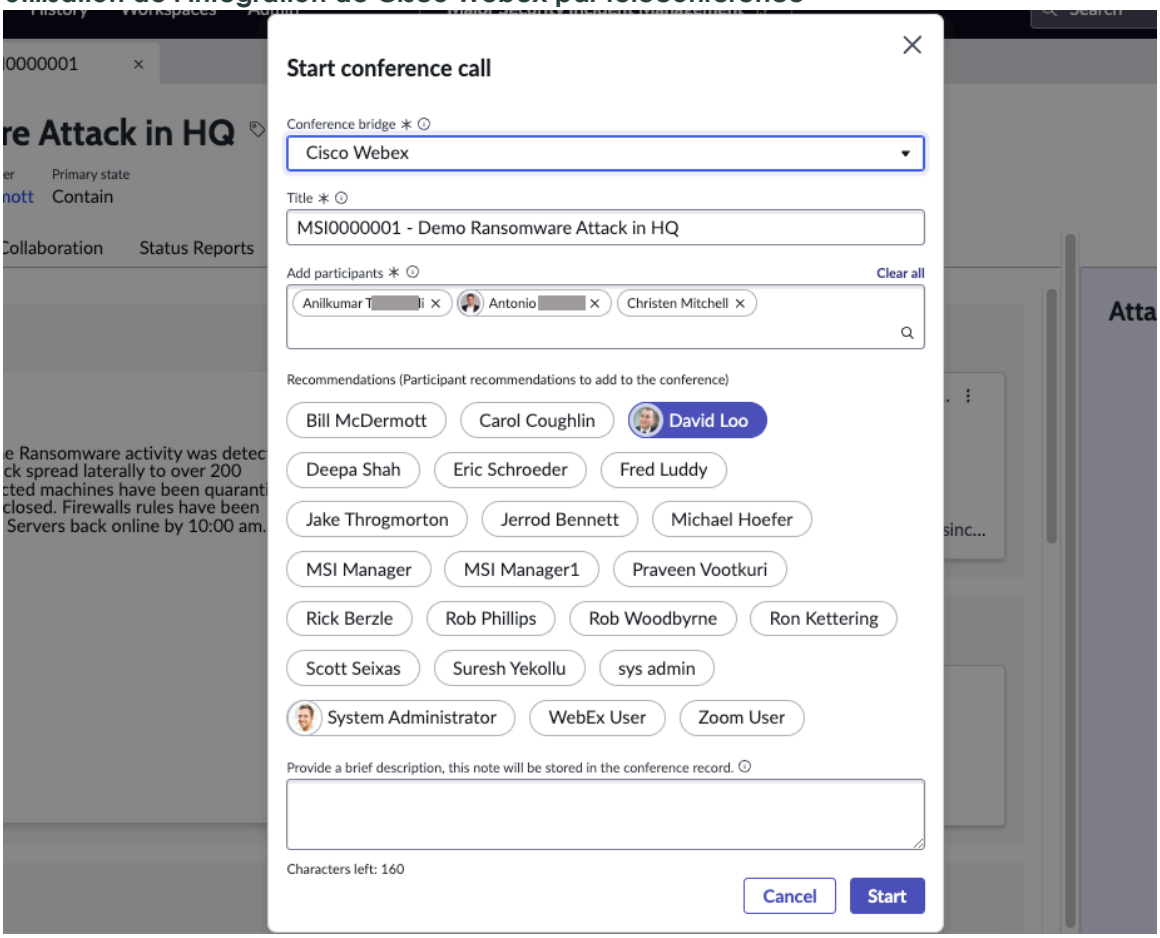
Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste Incidents de sécurité majeurs, sélectionnez un incident de sécurité majeur.
3. Sélectionnez l'action **Démarrer une téléconférence** .
4. Vous pouvez également démarrer une téléconférence en sélectionnant l'icône dans le menu contextuel de droite et en sélectionnant l'icône +.
   La fenêtre contextuelle Démarrer la téléconférence s'affiche.
5. Choisissez **Cisco Webex** comme pont de conférence à partir duquel vous souhaitez vous connecter.
6. Dans le champ Titre, fournissez un titre qui décrit le motif de la téléconférence Cisco Webex.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation de l'intégration de Cisco Webex par téléconférence



7. Dans le champ Ajouter des participants, sélectionnez les participants à la téléconférence Cisco Webex.
   Vous pouvez utiliser l'option de recherche pour trouver et ajouter les participants requis ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations de participants à ajouter à la téléconférence Cisco Webex.

   L'utilisateur (hôte) qui lance la téléconférence Cisco Webex est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste **Recommandations** .

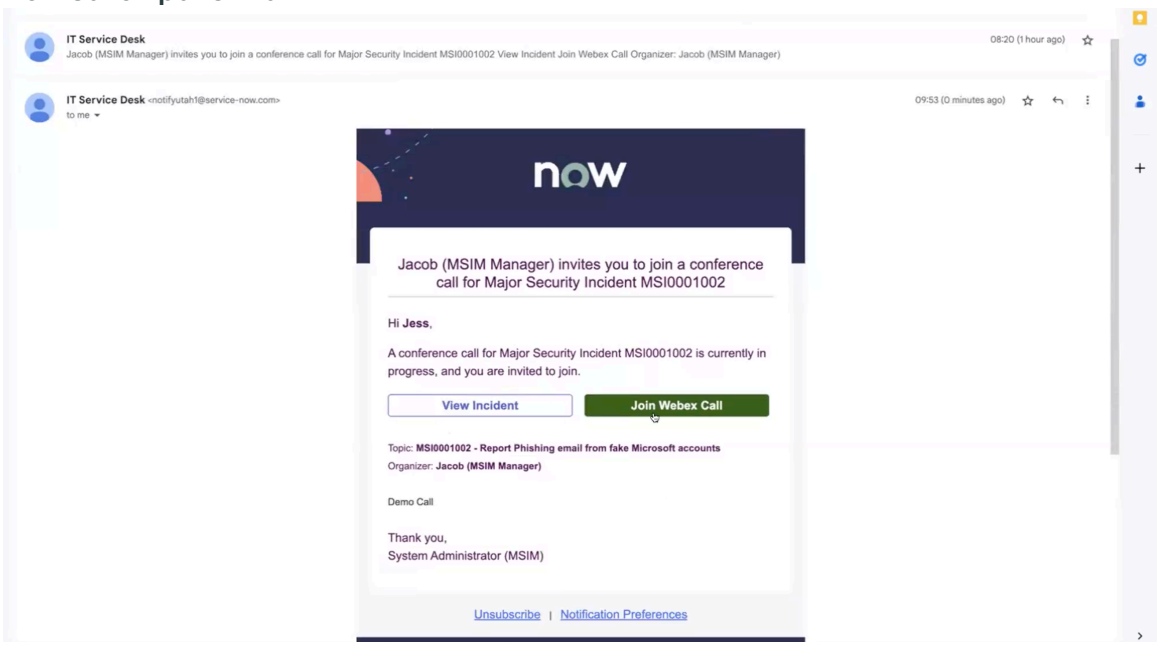
   Remarque : Assurez-vous que les participants que vous sélectionnez ont une adresse e-mail valide.

8. Après avoir sélectionné les participants, décrivez brièvement le motif pour lequel vous démarrez la téléconférence dans le champ Description.
   La description que vous fournissez sera ajoutée à l'enregistrement de la conférence.
9. Une fois la liste des participants finalisée, sélectionnez **Démarrer**.
   La téléconférence commence dans l'application Cisco Webex. Tous les participants sont informés par le biais de deux e-mails, un e-mail est envoyé aux participants à partir de l'application MSIM et l'autre e-mail est envoyé à partir du pont de conférence Cisco Webex.
10. Sélectionnez l'option **Cliquez ici** au-dessus de l'incident de sécurité majeur pour rejoindre la téléconférence sur l'application Cisco Webex.
    Les participants peuvent utiliser le lien de la notification par e-mail MSIM ou la notification de l'application Cisco Webex pour rejoindre l'appel.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notification par e-mail



11. Ouvrez l'incident de sécurité majeur associé dans l'espace de travail MSIM pour afficher les détails de la téléconférence.

    Lorsque le dernier participant quitte l'appel, la téléconférence se termine ou sélectionnez **Terminer l'appel** dans la section Téléconférence pour terminer la téléconférence.

    Si la téléconférence a été enregistrée, l'enregistrement sera disponible dans la section Téléconférence de l'incident de sécurité majeur associé après un certain temps.

Configurer Gestion des incidents de sécurité majeurs

Installez et configurez Gestion des incidents de sécurité majeurs l'application.

Important :

- Pour démarrer rapidement avec Gestion des incidents de sécurité majeurs la configuration, vous pouvez consulter le Guide de démarrage rapide de la Gestion des incidents de sécurité majeurs (MSIM) sur le ServiceNow Store.
- Après l'installation de l'application Gestion des incidents de sécurité majeurs , assurez-vous d'importer l'ensemble de mises à jour dans KB1289784 de charger les fichiers partiellement préconfigurés.

Utilisez cette section pour apprendre à configurer les configurations nécessaires requises pour travailler avec Incident de sécurité majeur des enregistrements en intégrant avec d'autres applications externes Microsoft afin d'établir des connexions avec ServiceNow l'instance.

Configurer le composant de l'explorateur de fichiers

Le composant de l'espace de travail de l'explorateur de fichiers organise et suit la collecte d'artefacts (fichiers) liés à un incident de sécurité majeur. Il est conçu pour prendre en charge l'intégration avec n'importe quel fournisseur d'hébergement de fichiers tiers, par exemple Microsoft SharePoint dans l'espace Gestion des incidents de sécurité majeurs de travail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- File Explorer Composant : fournit une interface utilisateur graphique pour afficher le système de fichiers et permet aux utilisateurs d'effectuer des opérations sur les fichiers.
- File Explorer Core : fournit une couche d'abstraction qui permet au composant de l'explorateur de fichiers d'afficher le système de fichiers et d'effectuer diverses opérations sur les fichiers sans rien savoir du connecteur sous-jacent utilisé pour communiquer avec des référentiels externes.
- File Explorer Microsoft SharePoint Application Connecteur : fournit les modules d'implémentation nécessaires pour suivre et extraire les métadonnées des fichiers/dossiers à partir d'une Microsoft SharePoint bibliothèque de documents et effectuer des opérations sur les fichiers.

Le File Explorer composant Core fournit une infrastructure de base requise pour que les différentes applications de connecteur de partage de fichiers définissent ses propriétés de connexion.

Vous devez installer et configurer le lecteur de référentiel de fichiers et le fournisseur de référentiel de fichiers en ajoutant les propriétés de connexion pour extraire les métadonnées des fichiers à partir d'un emplacement de fournisseur d'hébergement de fichiers.

Pour cette version actuelle du , ces instructions incluent la configuration et l'abonnement à une récupération des métadonnées de fichier telles que les mises à jour de fichiers et de File Explorerdossiers, les Microsoft SharePoint opérations sur les fichiers et l'activité des fichiers de journalisation. Une bibliothèque de documents désignée Microsoft SharePoint et une configuration de lecteur connexe seront nécessaires pour créer des dossiers individuels spécifiques à un incident de sécurité majeur.

File Explorer permet également des applications de connecteur telles que Microsoft SharePoint. Vous pouvez utiliser cet exemple pour configurer ses implémentations d'opérations de fichiers telles que **Télécharger** ou **Renommer** les actions de dossier et de fichier seront activées dans le composant de l'espace de travail de l'explorateur de fichiers. Ces actions sont activées et exécutées à l'aide des sous-flux intégrés du concepteur de flux. Pour plus d'informations, reportez-vous à la section Paramètres d'action de fichier et de dossier.

File Explorer La configuration comprend la configuration suivante :

- Configurer le lecteur de référentiel de l'explorateur de fichiers
- Configurer les paramètres d'action de fichier et de dossier
- Créer des modèles de dossier

Introduction à l'Explorateur de fichiers

Passez en revue les informations suivantes avant de commencer à travailler avec File Explorer le composant.

Passez en revue les informations suivantes avant de commencer à établir la connexion avec Microsoft SharePoint, en créant des actions de dossier et de fichier et en créant des modèles de dossier pour le composant de l'explorateur de fichiers.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prérequis

Nom	Description
Microsoft SharePoint spoke, version 2.0.2 pour ServiceNow® IntegrationHub.	Utilisez **sn_sp_spoke** ID de module d'extension pour rechercher et installer Microsoft SharePoint un spoke. L'installation de ce module d'extension fournit des flux et des actions pour automatiser la collaboration, la gestion des documents et les droits d'accès des utilisateurs dans Microsoft SharePoint.
Composant de l'explorateur de fichiers v1.1.0	Utilisez **sn_file_explorer** ID de module d'extension pour rechercher et installer le composant de l'explorateur de fichiers v1.1.0 L'installation de ce module d'extension fournit une interface utilisateur graphique pour parcourir le système de fichiers, qui est disponible dans le noyau de l'explorateur de fichiers.
Explorateur de fichiers Core for Security Operations v1.1.1	Utilisez **sn_fe** ID de module d'extension pour rechercher et installer File Explorer Core. L'installation de ce module d'extension fournit une infrastructure de base à intégrer à n'importe quel fournisseur d'hébergement de fichiers tiers.
Microsoft SharePoint Connecteur de l'explorateur de fichiers pour Security Operations v1.1.1	Utilisez **sn_fe_sharepoint** ID de module d'extension pour rechercher et installer Microsoft SharePoint le connecteur de l'explorateur de fichiers. L'installation de ce module d'extension gérera les fichiers/dossiers à l'aide de l'explorateur Microsoft SharePoint de fichiers.

Configurer le lecteur de référentiel de l'explorateur de fichiers

Le Microsoft SharePoint connecteur fournit diverses fonctionnalités à implémenter dans Microsoft SharePoint les fonctionnalités de l'explorateur de fichiers en gérant et en suivant les métadonnées du fichier.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tout** > **Incident de sécurité majeur** > **Explorateur de fichiers** > **Configuration du référentiel de fichier**.
2. Renseignez les champs suivants comme décrit dans la table suivante :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description de champ
Nom	Nom de l'enregistrement du référentiel de fichiers qui identifie l'utilisation. Par exemple, MSIM.
Fournisseur	Nom du fournisseur tiers, fournisseur de référentiel d'hébergement de fichiers. Par exemple,Microsoft SharePoint.
Propriétés	
Chemin d'accès à l'URL du site	Entrez une URL avec un chemin d'accès Microsoft SharePoint de site spécifique. Fournir uniquement le chemin d'accès relatif au site et une URL de site complète peut ne pas être nécessaire. Par exemple, Sites/MSIM.
Nom de la bibliothèque de documents	Créez une bibliothèque de documents sous le Microsoft SharePoint site et fournissez le même nom de bibliothèque de documents ici. Il s'agit de la même bibliothèque de documents que celle que vous avez créée dans la configuration du lecteur de Microsoft SharePoint connecteur.
Connexion graphique	Sélectionnez l'enregistrement de locataire du graphique de l'explorateur de fichiers. Pour plus d'informations sur la configuration de la connexion du locataire, voir Spoke Microsoft SharePoint .
Connexion REST	Sélectionnez l'enregistrement de locataire REST de l'Explorateur de fichiers. Pour plus d'informations sur la configuration de la connexion du locataire, voir Spoke Microsoft SharePoint .

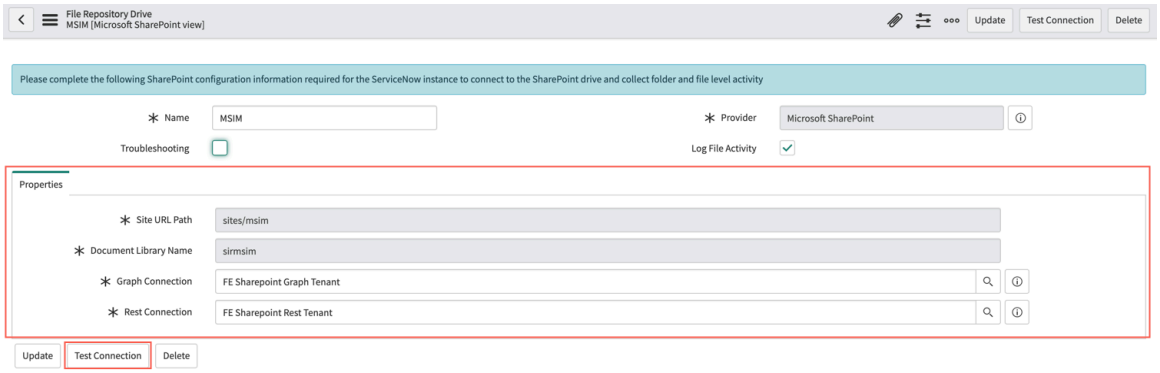
3. Sélectionnez **Enregistrer**.
4. Cliquer sur **Test de la connexion** pour tester la connexion et valider les propriétés de configuration du lecteur de référentiel de fichiers.

   Remarque : Avant **d'activer** le référentiel de fichiers, assurez-vous que la bibliothèque de documents correspondante ne Microsoft SharePoint contient pas de données de dossier ou de fichier.

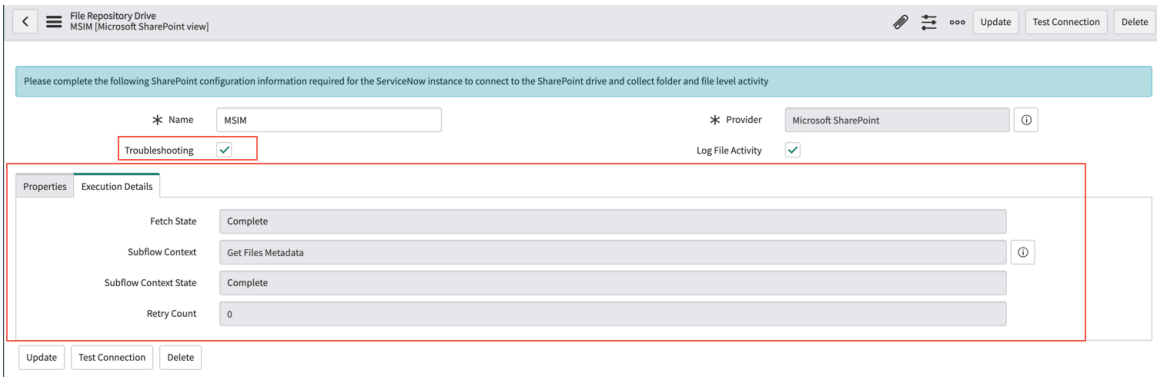
5. Cliquez sur **Activer** pour activer le référentiel de fichiers.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cochez la case **Dépannage** pour vérifier les **détails d'exécution** du référentiel de fichiers et vérifier le **État d'extraction** est terminé et assurez-vous que l'abonnement au lecteur est créé et que l'état Microsoft SharePoint est terminé.



Remarque : À l'aide du bouton **Test de la connexion** , MSI Administrator ou MSI Manager peut uniquement valider la configuration du référentiel de fichiers.

Configurer les paramètres d'action de fichier et de dossier

Déterminez les actions de dossier et de fichier que vous souhaitez activer à partir du composant Explorateur de fichiers sur l'espace de travail Major Security Incident Management, à l'aide de la page de configuration des paramètres d'action de fichier et de dossier. En tant qu'administrateur MSI, vous pouvez contrôler les actions individuelles de dossier et de fichier affichées sur le composant de l'explorateur de fichiers.

Avant de commencer

Voici les options d'opérations de fichier implémentées dans le composant de l'explorateur de fichiers à l'aide du concepteur de ServiceNow® flux :

Options d'opérations de fichiers

Opération fichier	Description
Ouvrir dans Microsoft SharePoint	Ouvre un nouvel onglet de navigateur pour afficher Microsoft SharePoint la vue de fichier de la bibliothèque de documents
Créer un dossier	Capacité de créer des dossiers ad hoc supplémentaires après la création de l'incident de sécurité majeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Options d'opérations de fichiers (suite)

Opération fichier	Description
Renommer un dossier	Possibilité de renommer les dossiers créés.
Déplacer le fichier	Permet de déplacer des fichiers entre des dossiers dans le composant Explorateur de fichiers de l'espace de travail, ce qui entraîne le déplacement des fichiers dans Microsoft SharePoint
Localiser le fichier	Affiche l'emplacement du dossier lors de l'utilisation de **Récents** de l'Explorateur de fichiers.
Supprimer le fichier	Supprimez le fichier.
Supprimer un dossier	Supprimez le dossier.
Télécharger le fichier	Télécharge le fichier dans l'onglet de navigateur de l'espace de travail MSIM existant pour une visualisation rapide.
Renommer le fichier	Renomme le fichier.

Remarque :

1. Toutes les actions répertoriées sont actuellement activées par défaut. Vous devrez modifier le **Paramètres de l'action de fichier** si vous ne souhaitez pas que certaines actions apparaissent. Tous les paramètres sont actuellement globaux pour tous les utilisateurs, ce qui signifie qu'il est impossible d'activer des actions pour un sous-ensemble d'utilisateurs disposant d'un rôle spécifique.
2. **Révoquer l'accès de l'utilisateur** et **Ajoutez des autorisations** Les actions sont des actions liées au système. Il est recommandé de ne pas modifier ces actions de fichier.

L'exemple de procédure suivant décrit l'une des capacités d'opérations de fichiers permettant de désactiver toute action spécifique sur un dossier et un fichier lors de la configuration du référentiel de l'explorateur de fichiers. Cette procédure s'applique à toutes les autres actions qui peuvent avoir besoin d'être modifiées :

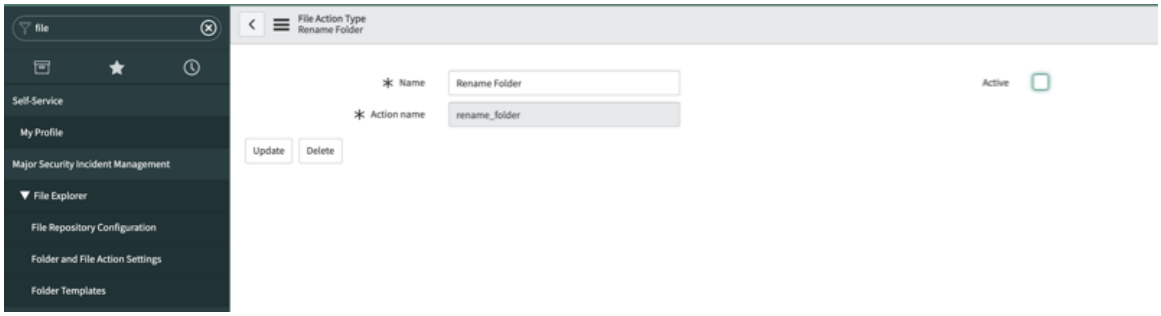
Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Explorateur de fichiers** > **Options pour l'action de fichier et de dossier**.
2. Sélectionnez l'enregistrement souhaité pour activer ou désactiver respectivement l'action de dossier ou de fichier.
3. Désélectionner l'icône **Actif** Case à cocher pour désactiver l'action de dossier et de fichier.

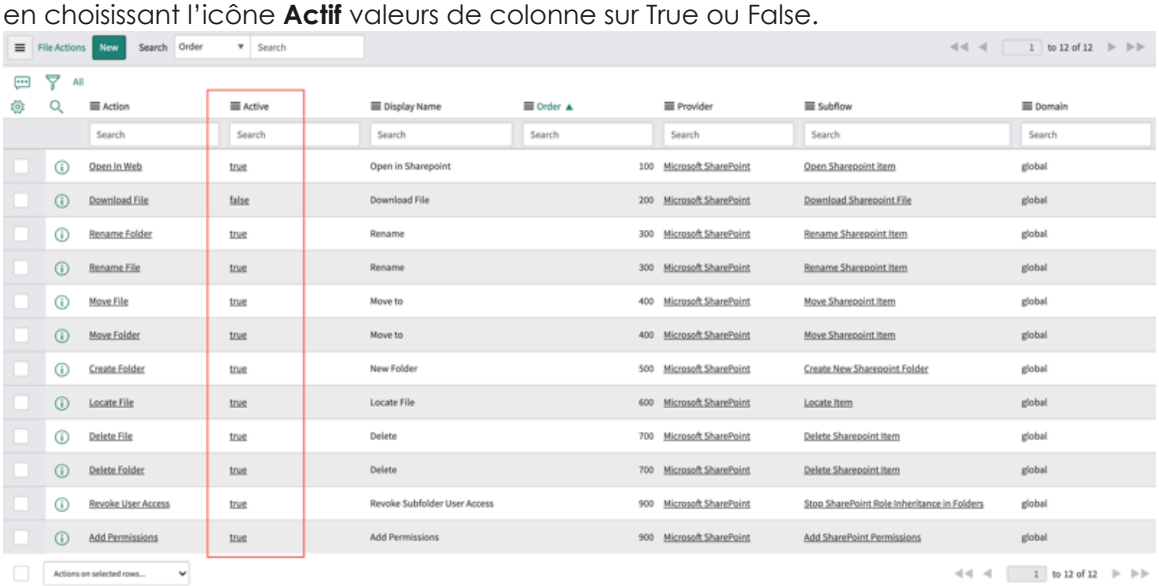
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

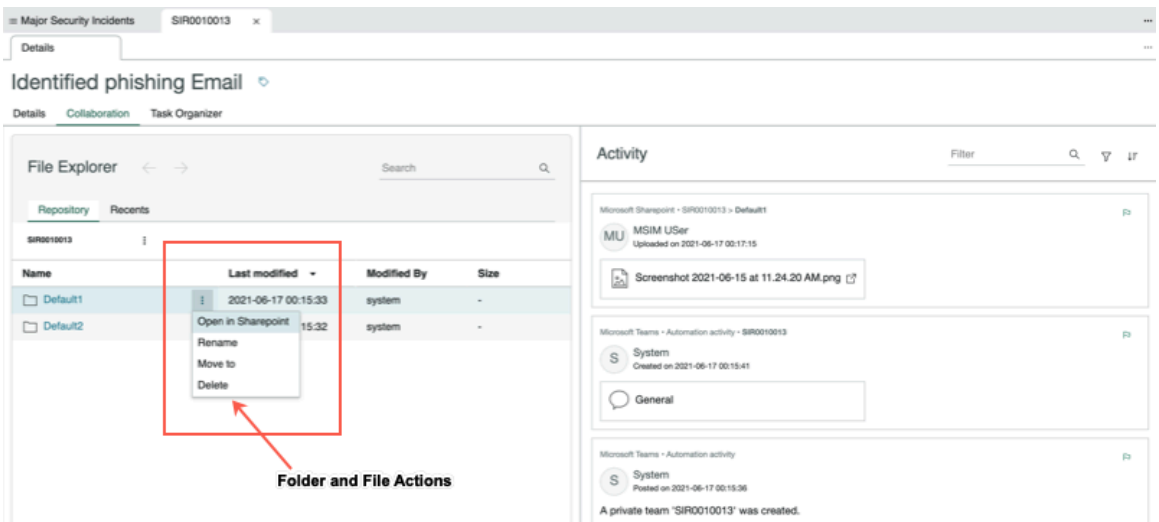


4. **Mettez à jour** l'enregistrement du lecteur.

Remarque : Vous pouvez également effectuer l'action fichier directement à partir de la liste des opérations sur les fichiers affichés en choisissant l'icône **Actif** valeurs de colonne sur True ou False.



Si l'action de fichier effectuée est désactivée, l'action ne sera pas affichée sur le **Collaborations** de l'onglet **Gestion des incidents de sécurité majeurs** Espace.



Créer des modèles de dossier

Utilisez des modèles de dossiers pour créer automatiquement des dossiers uniques pour différents types d'incidents de sécurité majeurs. Les modèles de dossiers du composant

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de l'explorateur de fichiers sont utilisés pour créer une structure de dossiers de base pour l'incident de sécurité dans le Microsoft SharePoint.

Avant de commencer
En tant qu'administrateur MSI, vous définissez la structure de dossiers initiale nécessaire pour permettre la collaboration entre différents groupes d'intervenants en cas d'incident et attribuez les privilèges d'accès appropriés au niveau d'un sous-dossier. Plusieurs configurations peuvent être créées pour différents Incident de sécurité majeur types à l'aide d'un créateur de conditions pour des valeurs de champ spécifiques Incident de sécurité majeur , ce qui inclut l'autorisation de l'accès à différents utilisateurs et groupes d'utilisateurs à chaque niveau de sous-dossier.

Remarque : Ces modèles de dossiers sont utilisés par tous les incidents de sécurité majeurs qui remplissent les conditions spécifiées dans le générateur de conditions. Il est recommandé d'envisager d'utiliser des variables de champ d'incident, telles que le numéro ou la catégorie d'incident, pour créer des noms de dossiers racine uniques qui distinguent un ensemble de sous-dossiers avec des noms de dossiers communs pour un incident de sécurité majeur des dossiers similaires avec ces noms qui font partie d'un autre incident de sécurité majeur.

La configuration des modèles de dossiers définie n'est appliquée à l'incident de sécurité majeur que lorsque la condition est remplie.

Remarque : Une configuration système de base (sans sous-dossier) est appliquée à tous les incidents de sécurité. Vous pouvez modifier cette configuration par défaut pour inclure des sous-dossiers spécifiques ou en créer une nouvelle basée sur un ensemble spécifié de valeurs de champ d'incident de sécurité majeur. Par exemple, catégorie = activité du code malveillant.

Rôle requis : sn_msi.workspace_admin

Procédure

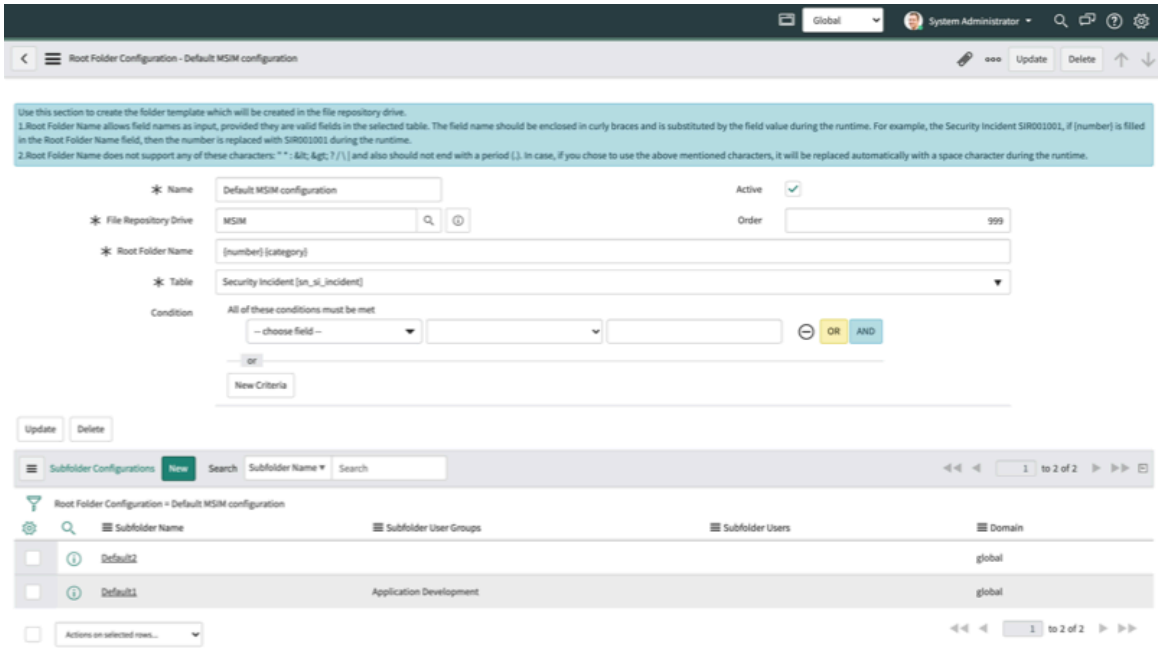
1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Explorateur de fichiers** > **Modèles de dossier**.
2. Cliquer sur **Nouveau** pour la configuration du dossier racine.
3. Renseignez les champs du formulaire.

Nom de champ	Description
Nom	Nom du modèle de dossier.
Lecteur de référentiel de fichiers	
Nom du dossier racine	Nom du dossier racine qui apparaîtra dans Microsoft SharePoint l'explorateur de fichiers et qui devrait probablement inclure des variables de champ d'incident telles que le numéro et la catégorie de l'incident de sécurité majeur afin qu'un incident de sécurité majeur puisse être distingué d'un autre.
Table	

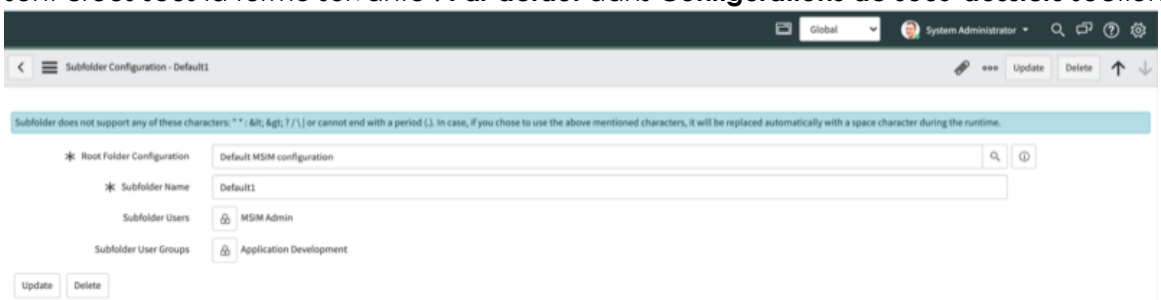
4. Définir l'incident de sécurité **Condition** Valeurs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. **Mettre à jour** le compte rendu.
   Les sous-dossiers sont créés avec les valeurs définies.
6. Cliquez sur le **sous-dossier** souhaité.
   Si vous ne créez pas de sous-dossier avec un nom approprié, les noms des sous-dossiers sont créés sous la forme suivante : **Par défaut** dans **Configurations de sous-dossiers** section.



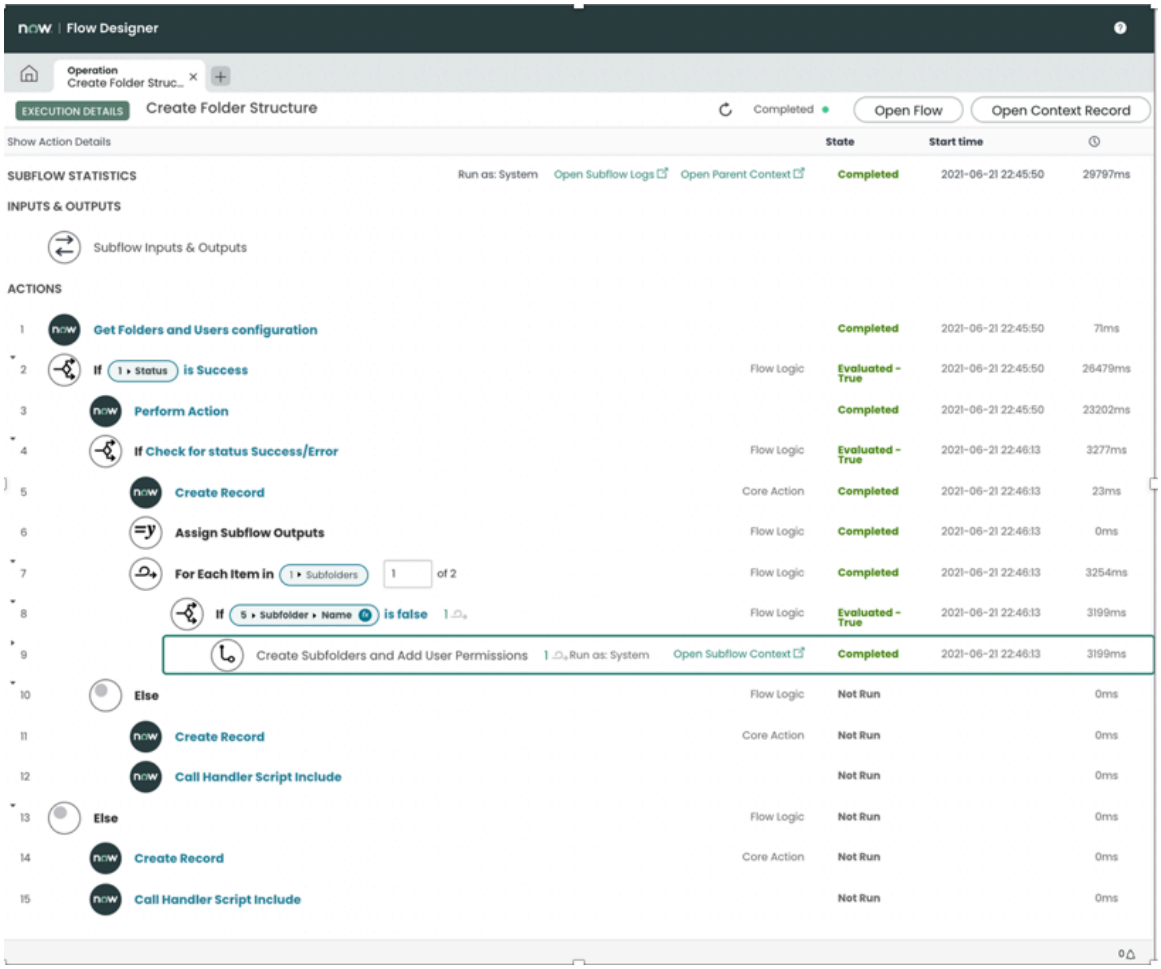
La même structure de dossiers sera créée automatiquement dans le Microsoft SharePoint à l'aide des mêmes privilèges d'accès que ceux configurés sur le **Modèles de dossier** la page.

Remarque :

- **Nom du dossier racine** autorise les noms de variables de champ en tant qu'entrée, à condition qu'il s'agisse de champs valides dans la table sélectionnée. Le nom de champ doit être entouré d'accolades et est remplacé par la valeur du champ pendant l'exécution du flux. Par exemple, dans le SIR001001 d'incident de sécurité, si la variable {number} est configurée dans le champ **Nom du dossier racine** , le numéro est remplacé par SIR001001 pendant l'exécution.
- **Nom du dossier racine** ne prend en charge aucun de ces caractères : " * : < > ? / \ | et aussi, ne doit pas se terminer par un point (.). Si vous utilisez les caractères mentionnés ci-dessus, ils seront automatiquement remplacés par un espace pendant l'exécution.
- Si le nom du **dossier racine** et du **sous-dossier** dépasse la limite définie (256 caractères), le nom du dossier est tronqué.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voici l'exécution au moment de l'exécution du flux secondaire Créer une structure de dossier :



File Explorer Flux d'activité dans l'espace de travail

Utilisez la section Explorateur de fichiers de l'espace de travail pour afficher les dossiers et les fichiers, l'ordre dans lequel ils ont été créés dans Microsoft SharePoint la Gestion des incidents de sécurité majeurs bibliothèque de documents.

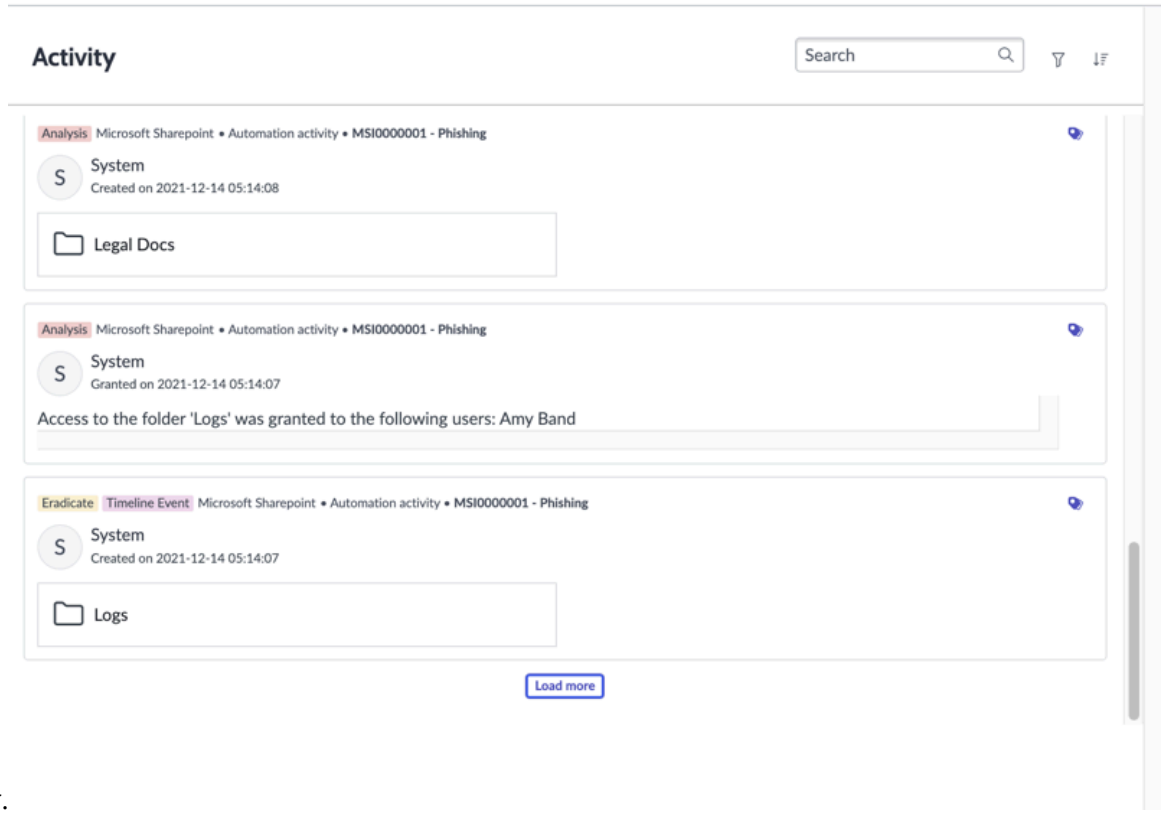
Le flux d'activité répertorie toutes les publications d'activité d'automatisation chaque fois qu'une activité de dossier ou de fichier, ou des journaux se produisent pendant la Incident de sécurité majeur résolution. La structure du flux d'activité est alignée dans le même format que celui de la Microsoft SharePoint bibliothèque, qui affiche les dossiers qui ont été créés et les utilisateurs ou groupes d'utilisateurs qui ont été affectés à ces dossiers.

Flux d'activité permet aux gestionnaires de l'espace de travail et aux autres utilisateurs ou groupes d'utilisateurs de communiquer et de collaborer efficacement, de répertorier les activités qui ont été effectuées sur Microsoft SharePoint les dossiers et les fichiers, de surveiller l'état de l'incident, de publier les notes ou d'ajouter des commentaires supplémentaires qu'ils ont sur l'enregistrement d'incident. Les gestionnaires d'espaces

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de travail peuvent récupérer et travailler en fonction de la dernière activité mise à



jour.

Dépannage de File Explorer

La section de dépannage peut vous aider à résoudre certains des problèmes techniques que vous pouvez rencontrer lors de la configuration File Explorer du composant.

Consultez en détail la section suivante sur les travaux planifiés, les propriétés système et File Explorer les flux secondaires de Flow Designer.

Travaux planifiés pour File Explorer

Les travaux planifiés sont des travaux automatisés exécutés pour traiter les notifications provenant de , ingérer les métadonnées des Microsoft SharePointfichiers dans ServiceNow l'instance et renouveler les abonnements au référentiel de fichiers selon un calendrier récurrent.

Les travaux planifiés sont des travaux automatisés qui sont exécutés en arrière-plan pour :

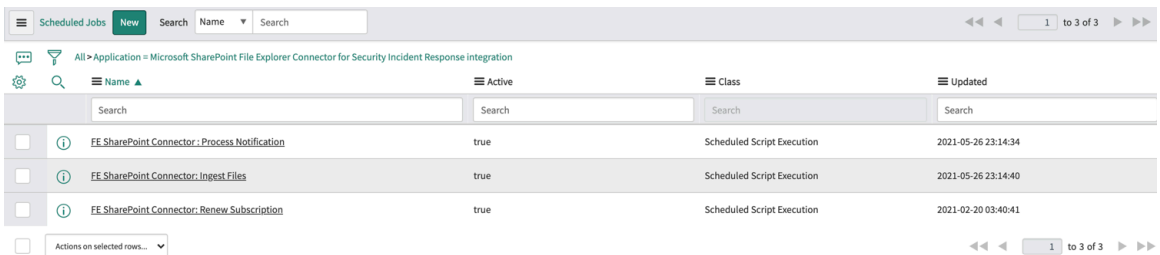
- traiter les notifications provenant de Microsoft Microsoft SharePoint.
- Ingérer les métadonnées des fichiers dans l'instance Now Platform .
- Renouvelez l'abonnement à Microsoft SharePoint la bibliothèque de documents pour recevoir des notifications.

Tâche	Description
Microsoft SharePoint File Explorer Connecteur : traiter la notification	S'exécute toutes les 30 secondes et est responsable de la lecture des notifications qui indiquent tout changement survenu dans la bibliothèque de documents abonnée et marquent l'état des lecteurs (sn_fe_file_repo_drive) comme en attente.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
Microsoft SharePoint File Explorer Connecteur : ingérer des fichiers	S'exécute toutes les 30 secondes et est principalement responsable du traitement des lecteurs (sn_fe_file_repo_drive) qui sont à l'état en attente et extrait les changements de fichier delta de la bibliothèque de documents configurée Microsoft SharePoint depuis la dernière extraction.
Microsoft SharePoint File Explorer: renouveler l'abonnement	S'exécute toutes les 10 minutes et est responsable du renouvellement de l'abonnement à la Microsoft SharePoint bibliothèque de documents un jour avant sa date d'expiration. Habituellement, ces abonnements expirent dans 30 jours.



Propriétés système de l'explorateur de fichiers disponibles

Les propriétés système du connecteur de l'explorateur de fichiers disponibles Microsoft SharePoint sont les suivantes.

Propriétés système

Nom de la propriété	Description
sn_fe_sharepoint.max_retry_count	Contrôle la fréquence des tentatives Microsoft SharePoint par l'application du connecteur d'extraire le lecteur défaillant ou de renouveler l'abonnement ayant échoué. La valeur de fréquence par défaut est définie sur 50.
sn_fe_sharepoint.retry_after_seconds	Intervalle de temps entre chaque tentative d'extraction du lecteur défaillant ou de renouvellement de l'abonnement. La valeur par défaut est définie sur 900 s ou 15 minutes.
sn_fe_sharepoint.max_subscription_expiration_period	Période maximale d'expiration de l'abonnement en nombre de jours pour Microsoft SharePoint. La période d'expiration par défaut est fixée à 30 jours.

File Explorer Flux secondaires Flow Designer

Voici les flux secondaires de Flow Designer installés avec Microsoft SharePoint File Explorer le connecteur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux secondaires

Nom	Description
Ajoutez Microsoft SharePoint des autorisations	Accorde une autorisation de modification pour un dossier spécifique à des utilisateurs spécifiques.
Créer un abonnement au lecteur	S'abonne à une bibliothèque de documents configurée Microsoft SharePoint pour recevoir des notifications sur les mises à jour qui se produisent dans la bibliothèque de documents.
Créer un Microsoft SharePoint dossier	Crée un nouveau Microsoft SharePoint dossier sous un dossier parent donné.
Supprimer l'élément Microsoft SharePoint	Supprime des Microsoft SharePoint fichiers et des dossiers.
Télécharger le Microsoft SharePoint fichier	Renvoie l'URL de téléchargement des Microsoft SharePoint fichiers
Obtenir les métadonnées des fichiers	Souscrit et extrait les modifications de la bibliothèque de Microsoft SharePoint documents.
Déplacer Microsoft SharePoint l'élément	Déplace les Microsoft SharePoint fichiers/ dossiers vers le dossier de destination
Ouvrir Microsoft SharePoint l'élément	Renvoie l'URL Web du fichier/dossier Microsoft SharePoint à ouvrir dans un navigateur.
Renouveler l'abonnement Drive	Renouvelle l'abonnement avec Microsoft SharePoint la bibliothèque de documents.
Créer une structure de dossier	Suit les configurations du modèle de dossier et crée la structure du dossier dans Microsoft SharePoint la bibliothèque de documents.

Configurer Microsoft Teams

Intégrez et collaborez facilement Microsoft Teams pour résoudre Incident de sécurité majeur l'affichage et le filtrage des activités de Collaboration Chat.

La configuration et l'abonnement à un Microsoft Teams environnement de messagerie instantanée, la récupération des conversations de messagerie instantanée à partir des canaux spécifiés et l'archivage de l'équipe et des canaux associés sont inclus dans le processus de fermeture de l'incident. Un environnement désigné Microsoft Teams et une configuration d'API connexe Microsoft Teams Graph sont nécessaires pour créer des canaux individuels spécifiques à un Incident de sécurité majeur.

Pour configurer Microsoft Teams, activez Teams en tant que fournisseur de messagerie instantanée. Vous pouvez ensuite créer des canaux de messagerie instantanée pour les différentes parties prenantes et les différents groupes qui communiquent sur les activités et suivre les conversations de messagerie instantanée pour résoudre le Incident de sécurité majeur. La configuration de Microsoft Teams et de l'API Microsoft Graph comprend les éléments suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Établir une connexion MS Teams Graph sur Now Platform
- Activer MS Teams en tant que fournisseur de messagerie instantanée
- Créer un modèle de canal de messagerie instantanée
- Afficher l'activité des messages de messagerie instantanée

Introduction à Microsoft Teams

Passez en revue les informations suivantes avant de commencer à travailler en Microsoft Teams tant qu'application de connecteur.

Assurez-vous que les modules d'extension suivants sont installés avant de commencer à établir, activer et valider les Microsoft Teams connexions de configuration.

Modules d'extension requis

Nom	Description
Intégration de la messagerie instantanée à Gestion des incidents de sécurité	Utilisez **sn_chat_collab_core** ID de module d'extension pour rechercher et installer Microsoft Teams la messagerie instantanée. L'installation de ce module d'extension vous permet de suivre l'activité de messagerie instantanée pour des applications tierces telles que Microsoft Teams (ou Slack et d'autres applications de messagerie instantanée tierces).
Connecteur de messagerie instantanée Microsoft Teams pour la gestion des incidents de sécurité	Utilisez **sn_ms_teams_connector** ID de module d'extension pour rechercher et installer le connecteur de messagerie instantanée Microsoft Teams pour la gestion des incidents de sécurité majeurs. L'installation de ce module d'extension vous permet de suivre les activités de messagerie instantanée à l'aide du composant de collaboration spécifique à Microsoft Teams.
Microsoft Teams Spoke graphique	L'installation de ce module d'extension établit une connexion de spoke Graph avec Microsoft Teams. Pour plus d'informations, consultez Spoke Microsoft Teams Graph

Activer MS Teams en tant que fournisseur de messagerie instantanée

Activer Microsoft Teams en validant la Microsoft Teams connexion.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Une fois la connexion activée et validée, un message d'information s'affiche indiquant que la connexion du fournisseur est validée avec succès. Vous pouvez modifier la configuration des canaux en ajoutant et en supprimant des utilisateurs, et éventuellement en ajoutant d'autres canaux ou en renommant les canaux existants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Configuration du fournisseur de messagerie instantanée**.
2. Sélectionnez **l'enregistrement Microsoft Teams**.
3. Cliquez sur **Valider la connexion**.
   Un message de confirmation s'affiche indiquant que la connexion du fournisseur est validée avec succès.
4. Cochez la case **Actif** pour activer l'enregistrement du fournisseur.
   Un message de confirmation s'affiche indiquant que la connexion du fournisseur est validée avec succès.
5. **Enregistrez** le formulaire après avoir activé la configuration du fournisseur de messagerie instantanée.
   Avec cela, la connexion entre Microsoft Teams et Now Platform l'instance est établie avec succès.

Créer un modèle de canal de messagerie instantanée

Configurez les équipes de messagerie instantanée et les modèles de canaux pour créer des équipes de messagerie instantanée et des canaux pour collaborer, suivre les conversations de messagerie instantanée et ajouter des utilisateurs et des groupes d'utilisateurs à ces canaux de messagerie instantanée. Ces modèles de canal sont créés dans Microsoft Teams lorsqu'un incident de sécurité majeur est promu.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Canal de messagerie instantanée** > **Modèles de canaux**.
2. Dans le formulaire Configuration du canal de messagerie instantanée, cliquez sur **Nouveau** dans l'en-tête du formulaire.
3. Renseignez les champs du formulaire.

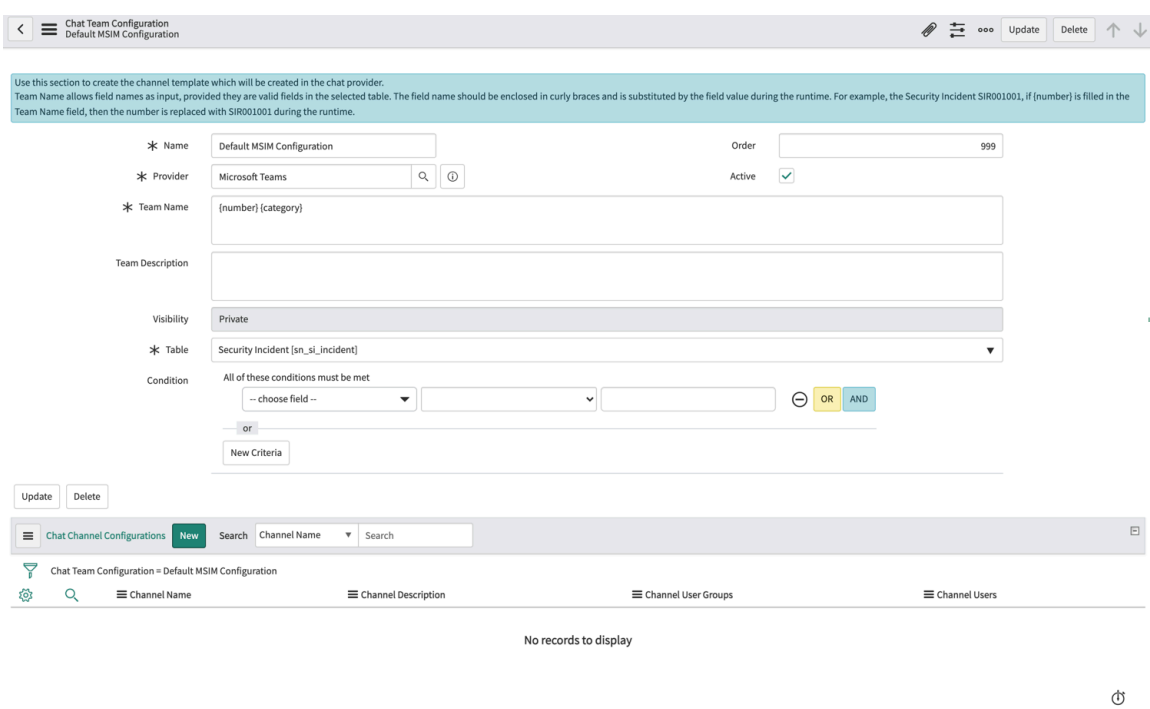
Formulaire Configuration d'équipe de messagerie instantanée

Champ	Description
Nom	Nom du dossier.
Fournisseur	Microsoft Teams.
Nom de l'équipe	Nom de l'équipe, par exemple au format {number}-{category}.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Le nom d'équipe fourni ici sera utilisé dans tous les enregistrements d'incidents de sécurité majeurs. Pour vous assurer que le nom réel de l'équipe Microsoft est affiché dans l'application MS Teams et qu'il a une valeur de nom unique pour différents incidents de sécurité majeurs, il est recommandé d'utiliser une valeur de champ d'incident unique, telle que le numéro d'incident : {number}. Comme le montre l'exemple de capture d'écran, le {number} suivi d'un séparateur « - » et de la variable de champ {category} fournirait un numéro et une description uniques de l'incident de sécurité majeur pour lequel Microsoft Teams est créé, par exemple {number} - {category}.
Description de l'équipe	Description facultative de l'équipe.
Table	Incident de sécurité majeur (sn_msi_incident).



4. Cliquez sur **Envoyer**.
5. Accédez à la section Configuration du canal de messagerie instantanée.
6. Cliquer sur **Nouveau** pour créer une configuration de canal de messagerie instantanée.

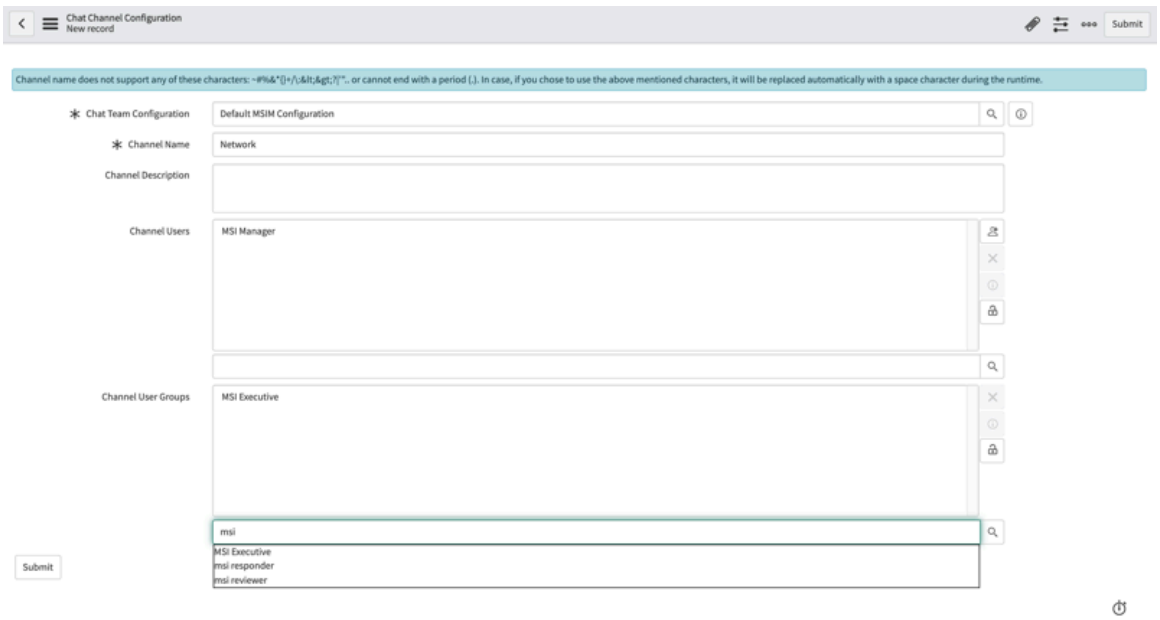
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Entrez le **Configuration d'équipe de messagerie instantanée** et **Nom du canal**.

   Remarque : Le nouveau canal que vous avez créé ici sera également le nom de votre canal dans Microsoft Teams. Vous pouvez rechercher le même canal et ajouter vos conversations.

8. Ajouter le **Utilisateur de canal** et **Groupes d'utilisateurs de canaux** dans la liste de recherche.
9. **Soumettre** Enregistrement de configuration du nouveau canal de messagerie instantanée.



Traduction automatique

Résultats

Le canal de messagerie instantanée est maintenant créé et les utilisateurs sont affectés à ces groupes de canaux de messagerie instantanée. Vous pouvez afficher les activités de Collaboration Chat à la fois dans Microsoft Teams et dans le flux d'activité de collaboration de l'espace de travail MSIM avec la structure hiérarchique des canaux de messagerie instantanée organisée telle que configurée dans la configuration du fournisseur de canal de messagerie instantanée.

Afficher l'activité des messages de messagerie instantanée

L'activité des messages de messagerie instantanée est enregistrée et affichée dans l'onglet Collaboration de l'espace de travail Major Security Incident Management.

L'activité de message de messagerie instantanée inclut toutes les conversations de messagerie instantanée qui ont eu lieu entre les participants, différents groupes d'utilisateurs.

Dépannage du connecteur de messagerie instantanée MS Teams pour MSIM

Reportez-vous à la section de dépannage du connecteur de messagerie instantanée Microsoft Teams sur les travaux planifiés, les propriétés système et les flux secondaires du concepteur de flux Microsoft Teams.

Vérifiez que le connecteur de messagerie instantanée traite les travaux planifiés dans tous les cas si vous ne voyez pas que les messages de Collaboration Chat sont publiés sur Microsoft Team et sur le flux d'activité de collaboration externe de l'espace de travail MSIM.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Travaux planifiés pour Microsoft Teams

Les travaux planifiés sont des travaux automatisés qui sont exécutés pour traiter les notifications du connecteur de Microsoft Teams messagerie instantanée et renouveler les abonnements Microsoft Teams selon un calendrier récurrent.

Rôle requis : admin.

- **Connecteur de messagerie instantanée MS Teams : traiter la notification**

  Pour chaque événement de message de messagerie instantanée, une notification sera reçue qui aura l'ID de ressource et la notification qui sont stockés dans une table. Une tâche planifiée est exécutée toutes les 30 secondes pour sélectionner les notifications non traitées et interroger l'API Microsoft Teams pour obtenir le contenu réel des messages, qui est ensuite stocké dans une autre table.

- **Connecteur de messagerie instantanée MS Teams : renouveler les abonnements**

  Pour chaque canal au sein de l'équipe, des abonnements sont créés pour être averti des événements créés, mis à jour et supprimés. Cet abonnement est actif pendant 60 minutes seulement. Les abonnements sont renouvelés toutes les 25 minutes via la tâche planifiée Connecteur Microsoft Teams : renouveler la notification.

Microsoft Teams Flux fonctionnel du connecteur de messagerie instantanée

Consultez cette section pour comprendre les flux secondaires du Microsoft Teams concepteur de flux connexes utilisés pour gérer la création du ou des canaux de messagerie instantanée et l'accès des utilisateurs à partir d'un incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

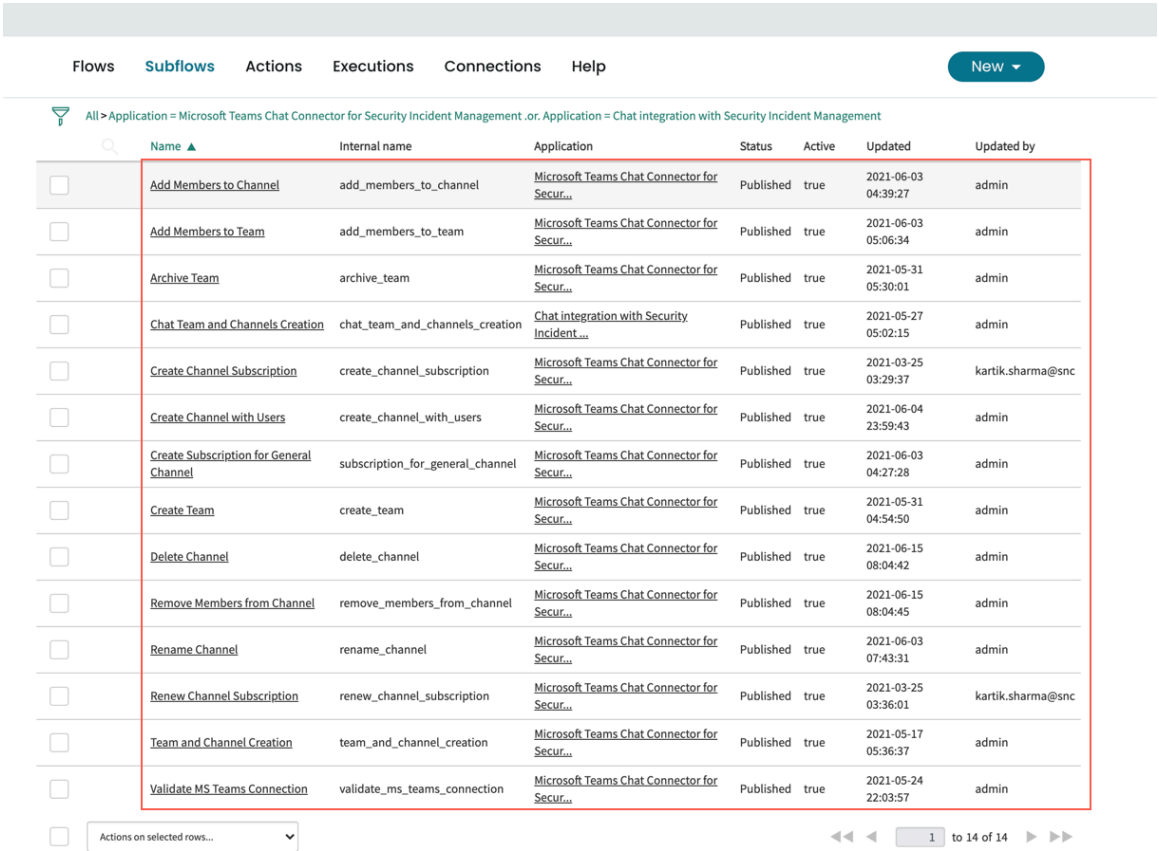
Procédure

1. Accédez à la **Tout** > **Concepteur de flux**.
2. Ajouter des membres au canal
3. Ajouter des membres à l'équipe
4. Équipe d'archivage
5. Création d'une équipe de messagerie instantanée et de canaux
6. Créer un abonnement à un canal
7. Créer un canal avec des utilisateurs
8. Créer un abonnement pour le canal général
9. Créer l'équipe
10. Supprimer un canal
11. Supprimer des membres du canal
12. Renommer un canal
13. Renouveler l'abonnement à un canal
14. Création d'une équipe et d'un canal

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

15. Valider la connexion MS Teams



Configurer le connecteur de messagerie instantanée Slack pour les incidents de sécurité majeurs

Intégrez et collaborez avec Slack pour résoudre l'incident de sécurité majeur afin d'afficher et de filtrer les activités de Collaboration Chat.

La configuration et l'abonnement à un Slack environnement de messagerie instantanée, la récupération de conversations de messagerie instantanée à partir de canaux spécifiés et l'archivage de Slack et des canaux associés sont inclus dans le processus de fermeture de l'incident. Un environnement désigné Slack et une configuration d'API connexe Slack sont nécessaires pour créer des canaux individuels spécifiques à un Incident de sécurité majeur.

Pour configurer Slack, activez Slack en tant que fournisseur de messagerie instantanée. Vous pouvez ensuite créer des canaux de messagerie instantanée pour les différentes parties prenantes et les différents groupes qui communiquent sur les activités et suivre les conversations de messagerie instantanée pour résoudre le Incident de sécurité majeur. La configuration de l'API Slack AND Slack comprend :

- Premiers pas avec la configuration du connecteur de messagerie instantanée Slack
- Activer Slack en tant que fournisseur de canaux
- Créer un modèle de canal de messagerie instantanée pour Slack
- Afficher les activités de message de messagerie instantanée dans Slack

Premiers pas avec la configuration du connecteur de messagerie instantanée Slack

Passez en revue les informations suivantes avant de commencer à travailler en Slack tant qu'application de connecteur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Assurez-vous que les modules d'extension suivants sont installés avant de commencer à établir, activer et valider les Slack connexions de configuration.

Modules d'extension requis

Nom	Description
Slack Connecteur de messagerie instantanée pour Gestion des incidents de sécurité	Utilisez **sn_slack_connector** ID de module d'extension pour rechercher et installer Slack le connecteur pour Major Security Incident Management. L'installation de ce module d'extension vous permet de suivre les activités de messagerie instantanée à l'aide du composant de collaboration spécifique à Slack.
Spoke Slack	L'installation de ce module d'extension établit une connexion de spoke avec Slack. Pour plus d'informations, voir Slack Rayon

Créer un modèle de canal de messagerie instantanée pour Slack

Configurez les équipes de messagerie instantanée et les modèles de canaux pour créer des équipes de messagerie instantanée et des canaux pour collaborer, suivre les conversations de messagerie instantanée et ajouter des utilisateurs et des groupes d'utilisateurs à ces canaux de messagerie instantanée. Ces modèles de canal sont créés lors Slack de la promotion d'un incident de sécurité majeur.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Pourquoi et quand exécuter cette tâche
Le nouveau canal que vous créez sera également le nom de Slack votre canal. Vous pouvez rechercher le même canal et ajouter vos conversations.

Procédure
1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Canal de messagerie instantanée** > **Modèles de canaux**.
2. Sélectionnez **Configuration du canal Slack** pour afficher les détails de la configuration de Slack.
3. Cochez la case **Actif** pour activer la configuration du canal de messagerie instantanée Slack.
4. Dans le champ Nom de l'équipe, indiquez le numéro MSI et le nom de code.

   Par défaut, tous les canaux Slack portent le numéro d'incident en préfixe. Par exemple, `MSI000000 - {nom du canal}`. Vous pouvez modifier le préfixe de n'importe quel champ de votre choix au format suivant : `{field_name}`.

   Remarque : Le nom d'équipe fourni ici sera utilisé dans tous les enregistrements d'incidents de sécurité majeurs. Pour vérifier que la valeur réelle Slack est affichée dans Slack l'application et qu'elle a une valeur de nom unique pour différents incidents de sécurité majeurs, il est recommandé d'utiliser une valeur de champ d'incident, qui est unique, telle que la `MSI000000 : {nom du canal}`.

Traduction automatique

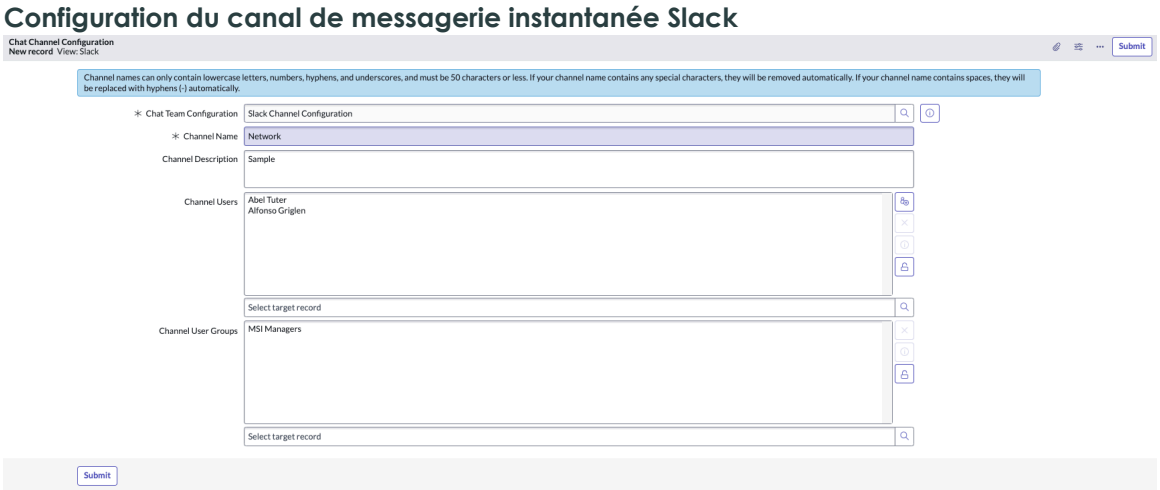
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez avec le bouton droit sur la configuration, puis sélectionnez **Enregistrer**.
6. Accédez à la section Configuration du canal de messagerie instantanée.
7. Sélectionner **Nouveau** pour créer une configuration de canal de messagerie instantanée.
8. Renseignez les champs du formulaire.

Champ	Description
Configuration d'équipe de messagerie instantanée	Nom de la configuration de l'équipe de messagerie instantanée. Par exemple, configuration du canal Slack.
Nom du canal	Nom du canal. Par exemple, juridique. **Remarque :** ◦ Les noms de canaux ne peuvent contenir que des lettres minuscules, des chiffres, des tirets et des traits de soulignement et doivent comporter 50 caractères maximum. Si le nom de votre chaîne contient des caractères spéciaux, ils sont automatiquement supprimés. Si le nom de votre chaîne contient des espaces, ils sont automatiquement remplacés par des traits d'union (-). ◦ Le nouveau canal que vous créez ici sera également le nom Slack de votre canal. Vous pouvez rechercher le même canal et ajouter vos conversations.
Description du canal	Description unique pour le canal.
Utilisateur de canal	Sélectionnez l'icône **Déverrouiller les utilisateurs du canal** et ajoutez les utilisateurs qui peuvent accéder à ce canal à partir de la liste de recherche. Sélectionnez l'icône **Verrouiller les utilisateurs du canal** pour verrouiller la liste sélectionnée des utilisateurs du canal.
Groupes d'utilisateurs de canaux	Sélectionnez l'icône **Déverrouiller les groupes d'utilisateurs du canal** et ajoutez les groupes d'utilisateurs qui peuvent accéder à ce canal à partir de la liste de recherche. Vous pouvez également utiliser l'icône **Ajouter ma personne** pour vous ajouter. Sélectionnez l'icône **Verrouiller les groupes d'utilisateurs de canaux** pour verrouiller la liste sélectionnée de groupes d'utilisateurs de canaux.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Sélectionnez **Soumettre**.

Résultats

Le canal de messagerie instantanée est maintenant créé et les utilisateurs sont affectés à ces groupes de canaux de messagerie instantanée. Vous pouvez afficher les activités de Collaboration Chat à la fois dans Slack et dans le flux d'activité de collaboration de l'espace de travail MSIM avec la structure hiérarchique des canaux de messagerie instantanée organisée telle que configurée dans la configuration du fournisseur de canal de messagerie instantanée.

Activer Slack en tant que fournisseur de canaux

Activer Slack en validant la Slack connexion.

Avant de commencer

Rôle requis :

- sn_msi.workspace_admin : écriture
- sn_msi.chat_collab_provider : lire

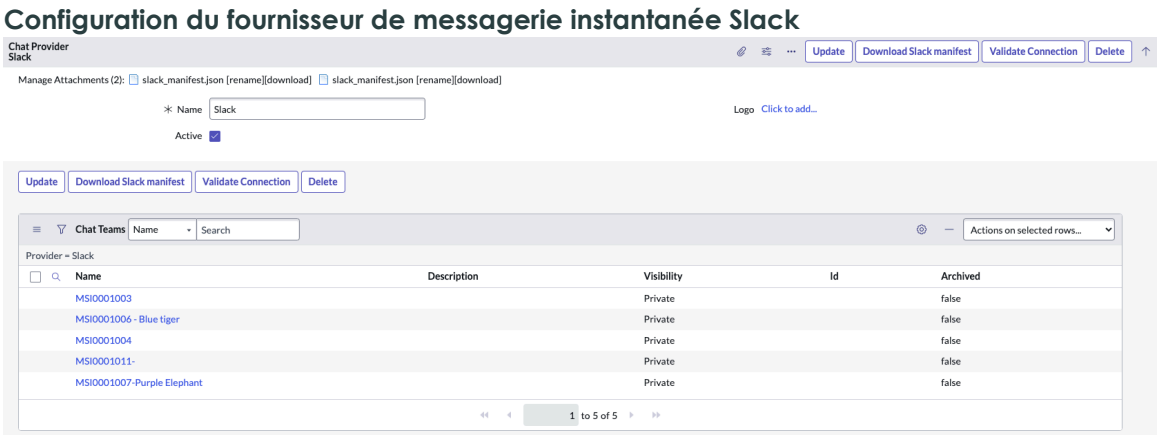
Une fois la connexion activée et validée, un message d'information s'affiche indiquant que la connexion du fournisseur est validée avec succès. Vous pouvez modifier la configuration des canaux en ajoutant et en supprimant des utilisateurs, et éventuellement en ajoutant d'autres canaux ou en renommant les canaux existants.

Procédure

1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Canal de messagerie instantanée** > **Configuration du fournisseur de messagerie instantanée**.
2. Sélectionnez **Slack** pour ouvrir la configuration du fournisseur de messagerie instantanée Slack.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Sélectionnez **Télécharger le manifeste Slack** pour télécharger le fichier `slack_manifest.json` .
   Ce fichier `slack_manifest.json` contient la configuration complète de la configuration de Slack et vous permet de configurer Slack automatiquement. Vous devez charger ce fichier JSON dans la configuration Marge.
4. Ouvrez le fichier `slack_manifest.json` et procédez comme suit :

   a. Accédez à l'URL `api.slack.com/apps` de votre navigateur Web.

   b. Sélectionnez **Créer une action d'application** .

   c. Dans la fenêtre contextuelle Créer une application, choisissez l'option **À partir d'un manifeste d'application** .

   d. Dans la fenêtre contextuelle Choisir un espace de travail pour développer votre application, choisissez un espace de travail dans la liste et sélectionnez **Suivant**.
   Par exemple, Espace de travail MSIM Slack.

   e. Dans la fenêtre contextuelle Entrer le manifeste de l'application ci-dessous, sélectionnez l'onglet **JSON** et copiez le code du fichier `slack_manifest.json` .

   f. Sélectionnez **Suivant**.

   g. Dans la fenêtre contextuelle Récapitulatif de l'examen et création de votre application, sélectionnez **Créer**.
   Votre application a maintenant été créée.

   h. Dans la page Informations de base, sélectionnez **Installer dans Workspace**.
   Le bot d'intégration de Slack vous demande l'autorisation d'accéder à l'espace de travail MSIM Slack.

   i. Sélectionner **Autoriser**.

   j. Dans la section Informations d'identification de l'application, renseignez les détails en revenant à l'instance ServiceNow.

   k. Sélectionner **Tout** > **Configurations de Slack**.
   Vous avez besoin du rôle sn_msi.workspace_admin pour cette action.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l. Sélectionnez une propriété **Secret de signature** .

m. Copiez le secret de signature et collez-le dans la section Informations d'identification de l'application de Slack.

n. Dans l'instance ServiceNow, accédez à **Tout** > **Concepteur de flux**.

o. Accédez à la **Connexions** > **Slack** > **Afficher les détails** > **Configurer**.

p. Renseignez les champs du formulaire.

Champ	Description
Nom de la connexion	Nom de cette connexion. Par exemple, Slack.
URL de connexion	URL de cette connexion. Par exemple, https://slack.com
Nom des informations d'identification	Nom des informations d'identification. Par exemple, les informations d'identification Slack.
Nom OAuth	Nom de l'OAuth. Par exemple, Slack OAuth.
ID client OAuth	L'ID client généré pour le compte que vous avez créé dans Slack.
Secret client OAuth	Le secret client pour le compte que vous avez créé dans Slack.
URL de redirection OAuth	Nom de l'instance de redirection OAuth. Par exemple, msimslack.service-now.com/oauth_redirect.do

q. Sélectionnez **Configurer et obtenir un jeton OAuth**.
Le bot d'intégration de Slack vous demande l'autorisation d'accéder à l'espace de travail MSIM Slack.

r. Sélectionner **Autoriser**.
Le jeton d'accès OAuth est disponible et expirera le <AAAA-MM-JJ> <HH :MM :SS>.

5. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Canal de messagerie instantanée** > **Configuration du fournisseur de messagerie instantanée**.
6. Cochez la case **Actif** pour activer l'enregistrement du fournisseur de messagerie instantanée.
7. Sélectionnez **Valider la connexion** pour tester la connexion.
Un message de confirmation s'affiche pour indiquer que la connexion du fournisseur est validée avec succès.
8. Cliquez avec le bouton droit sur l'enregistrement et sélectionnez **Enregistrer**.
Ensuite, la connexion entre Slack et Now Platform l'instance est établie avec succès.
9. Accédez à la **api.slack.com/apps** > **Fonctionnalités** > **OAuth et autorisations**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Vérifiez si tous les champs d'application sont corrects.

b. Accédez à la **Fonctionnalités** > **Abonnements d'événement**.

c. Dans le champ URL de la demande, sélectionnez **Réessayer**.
Vous pouvez voir un message vérifié.

d. Sélectionnez **Enregistrer**.

Afficher les activités de message de messagerie instantanée dans Slack

L'activité des messages de messagerie instantanée est enregistrée et affichée dans l'onglet Collaboration de l'espace de travail Major Security Incident Management.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Pourquoi et quand exécuter cette tâche
L'activité de message de messagerie instantanée inclut toutes les conversations de messagerie instantanée qui ont eu lieu entre les participants, différents groupes d'utilisateurs. Pour plus d'informations, consultez Gérer les communications des canaux de messagerie instantanée à l'aide de Slack.

Administration Gestion des incidents de sécurité majeurs

Planifiez et configurez votre implémentation Gestion des incidents de sécurité majeurs.

Vous pouvez configurer les aspects suivants de l'administration Gestion des incidents de sécurité majeurs :

Activer la proposition, la promotion et la liaison des incidents de sécurité majeurs

Permettez aux utilisateurs de décider de proposer ou de promouvoir des incidents en tant qu'incidents de sécurité majeurs. Suivez facilement tous les incidents liés à un incident de sécurité majeur en permettant de lier les incidents de sécurité à l'incident parent ou enfant.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configurations**.
2. Permettez aux utilisateurs de proposer un incident de sécurité pour un incident de sécurité majeur en cochant la case **Proposer un incident de sécurité majeur** dans la section Actions de l'espace de travail SIR/VR.
3. Autorisez les utilisateurs à promouvoir un incident de sécurité en incident de sécurité majeur en cochant la case **Promouvoir en incident de sécurité majeur** .
4. Activez la liaison d'un incident de sécurité à un incident de sécurité majeur afin qu'ils puissent être suivis ensemble en cochant la case **Lier à l'incident de sécurité majeur** .
5. Sélectionnez **Mettre à jour**.

Marquer les incidents de sécurité comme incidents de sécurité majeurs

Balisez ou étiquetez les incidents de sécurité ou les enregistrements vulnérables en incident de sécurité majeur lorsque l'incident est proposé ou promu. Si un incident de sécurité est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

proposé, l'enregistrement d'incident est désigné comme candidat à un incident de sécurité majeur. Lorsqu'une sécurité est promue, l'enregistrement d'incident est appelé Incident de sécurité majeur avec l'état Accepté.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configurations**.
2. Cochez la case Activer les **étiquettes d'affichage** pour étiqueter le candidat d'incident proposé comme incident de sécurité majeur en sélectionnant le champ **de recherche Nom de l'étiquette : proposer en tant que candidat** et sélectionnez Candidat d'incident de sécurité majeur dans la section **Étiquettes de l'espace de travail SIR/VR** .
3. Cochez la case Activer les **étiquettes d'affichage** pour étiqueter le candidat à l'incident promu comme incident de sécurité majeur en sélectionnant le champ **de recherche Nom de l'étiquette - Promotion en incident de sécurité majeur** et en sélectionnant Incident de sécurité majeur dans la section **Étiquettes de l'espace de travail SIR/VR** .
4. Sélectionnez **Mettre à jour**.

Configurer des étiquettes pour les incidents de sécurité majeurs

Configurez les étiquettes dans Major Security Incident Management pour créer des étiquettes personnalisées et filtrer les activités et tâches de collaboration externes dans le flux d'activité. Les différents types d'étiquettes implémentées sont les étiquettes d'état et les étiquettes de chronologie.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configurations**.
2. Cochez la case Activer **les étiquettes d'affichage** pour activer l'étiquetage des différents états d'incident tels que Analyse, Contenir, Éradiquer, Récupérer, Réviser, Événement de chronologie dans la section **Étiquettes de l'espace de travail MSIM (Afficher dans les activités et les tâches de collaboration).**
3. Sélectionnez **Mettre à jour**.

Configurer des étiquettes pour les incidents de sécurité majeurs

Configurez différents types d'étiquettes pour mieux filtrer et indiquer les états des incidents. Les étiquettes d'incidents de sécurité majeurs offrent la flexibilité d'étiqueter les activités et les tâches de collaboration des enregistrements d'incidents.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Vous pouvez sélectionner ou désélectionner les étiquettes à l'aide de l'icône des étiquettes disponible dans la section Flux d'activité de la section Organisateur de collaboration et de tâches de l'espace de travail MSIM.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Étiquettes MSI**.
2. Cliquez sur **Nouveau** pour créer une étiquette.
3. Remplissez le formulaire avec le **nom de l'étiquette** et la **couleur de l'étiquette**.
4. Cliquez sur **Créer une étiquette**.
5. Dans le cadre du système de base, les étiquettes suivantes sont configurées pour chaque état d'incident et vous ne pouvez pas modifier le nom ou la couleur de l'étiquette :
   - Analyse
   - Contenir
   - Éradiquer
   - Revue
   - Récupérer
   - Événement de chronologie

Remarque : Vous pouvez modifier les étiquettes personnalisées et leurs propriétés.

Configurer des catégories de chronologie pour les incidents de sécurité majeurs

Configurez et affectez des catégories de chronologie telles que Menace, Réponse ou Personnalisé à vos incidents de sécurité majeurs à l'aide de la section Chronologie de l'onglet Vue d'ensemble.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Catégories de chronologie**.
   Les catégories de chronologie suivantes sont fournies dans le cadre du système de base :
   - **Sur mesure**.
   - **Réponse**.
   - **Menace**.
2. Pour modifier une catégorie d'événement de chronologie existante, procédez comme suit :
   a. Sélectionnez une catégorie d'événement de chronologie dans la liste.
   b. Vous pouvez modifier le nom de la catégorie d'événement de chronologie.
   c. Vous pouvez modifier la couleur de l'événement et sélectionner une autre couleur pour votre catégorie d'événement de chronologie.
   d. Sélectionnez **Mettre à jour**.
3. Pour créer une catégorie d'événement de chronologie, procédez comme suit :
   a. Sélectionnez **Nouveau**.
   b. Dans le champ Nom, saisissez un nom pour la catégorie d'événement de chronologie.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Dans le champ Couleur de l'événement, choisissez une couleur pour la catégorie de chronologie de l'événement à l'aide de la liste déroulante.

d. Sélectionnez **Soumettre**.

Définir les préférences de notification pour MSIM

Automatisez le processus de notification par e-mail et notifiez les utilisateurs lorsqu'un incident de sécurité est proposé ou promu au rang de candidat à un incident de sécurité majeur.

Rôle requis : sn_msi.workspace_admin.

Les notifications ne sont déclenchées que lorsqu'un incident de sécurité est proposé et envoyées à tous les utilisateurs et groupes configurés dans la liste de notifications. Par défaut, la notification par e-mail est reçue par l'utilisateur qui a proposé l'incident de sécurité en tant que candidat à l'incident de sécurité majeur.

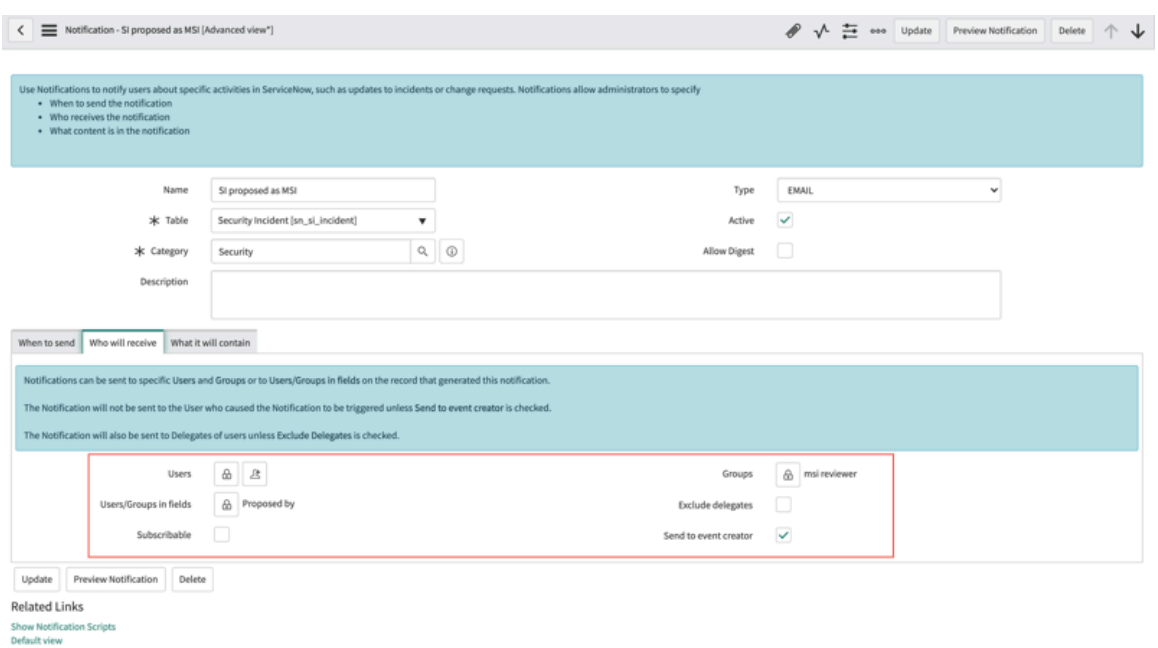
Notification : incident de sécurité proposé (SI) en tant qu'incident de sécurité majeur (MSI)

Qui recevra :

- Par défaut **Réviseurs MSI** Le nom de groupe est créé et tout utilisateur ajouté à ce groupe a le privilège d'être **Gestionnaire MSIM** et les utilisateurs qui appartiennent à ce groupe recevront les e-mails de notification.
- Tout utilisateur spécifique ajouté à **Utilisateurs** list recevra également les e-mails de notification.

Ce qu'il contiendra :

Si vous souhaitez modifier le contenu de l'e-mail, tel que le corps de l'e-mail, qui inclut l'objet ou le message HTML, vous devez disposer du rôle d'administrateur système auquel vous avez accès ou être affecté en tant qu'administrateur système et non en tant qu'administrateur MSI.



Notification : incident de sécurité promu (SI) en tant qu'incident de sécurité majeur (MSI)

Cette notification est déclenchée lorsqu'un incident de sécurité est promu et lorsque l'explorateur de fichiers et Microsoft Teams la structure de base sont créés. Par défaut,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

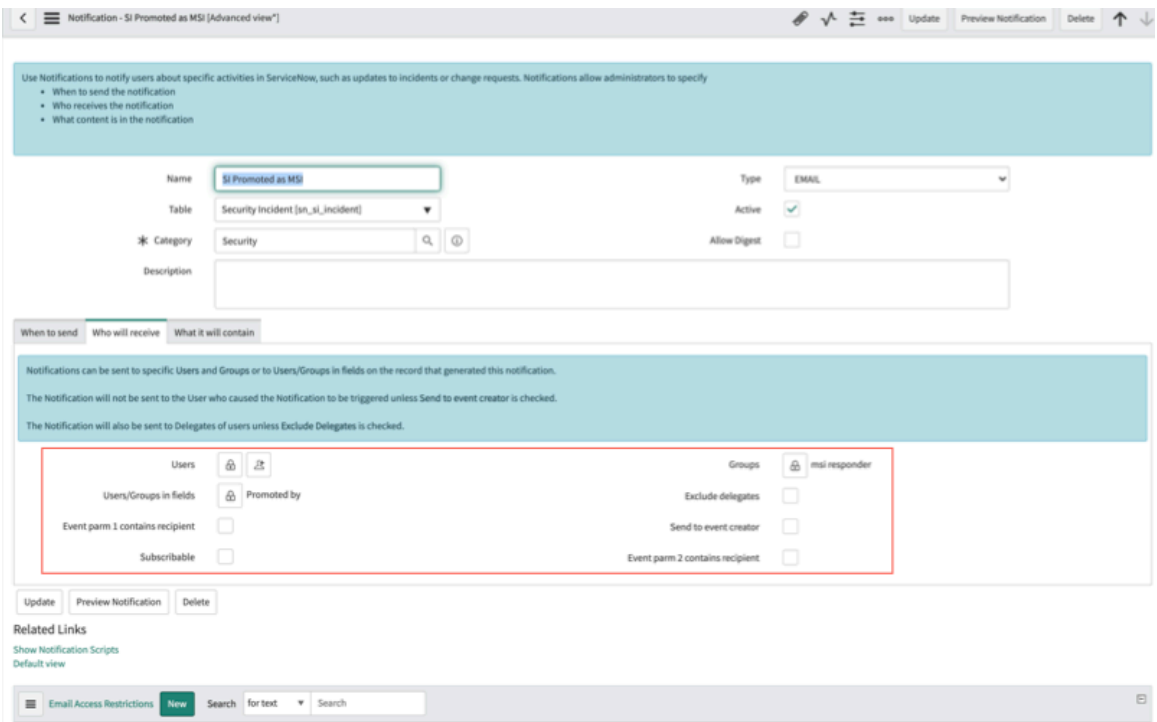
cette notification est reçue par l'utilisateur qui a promu l'incident de sécurité en incident de sécurité majeur.

Qui recevra

- Par défaut, un **Groupe** par nom **Répondeur MSI** est créé et tout utilisateur ajouté à ce groupe aura le privilège d'avoir **Répondeur MSIM** et tous les utilisateurs qui se trouvent dans ce groupe recevront l'e-mail de notification.
- Tout utilisateur spécifique ajouté à **Utilisateurs** list recevra également les e-mails de notification.

Ce que cela contiendra

Si vous souhaitez modifier le contenu de l'e-mail, tel que le corps de l'e-mail, qui inclut l'objet ou le message HTML, vous devez disposer du rôle d'administrateur système d'un accès ou être affecté en tant qu'administrateur système et non en tant qu'administrateur MSI.



Configurer les activités de fermeture MSI

Définissez des actions qui se produiront automatiquement lors de la fermeture d'un incident de sécurité majeur. Renforcez la sécurité en archivant et en supprimant automatiquement l'accès aux dossiers contenant des informations de résolution.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configurations**.
2. Archiver les communications de messagerie instantanée liées à la résolution de l'incident en sélectionnant la case à cocher **Archiver les canaux de collaboration** dans la section Actions de fermeture automatisées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Supprimez les dossiers contenant des documents liés à la résolution de l'incident en sélectionnant la case à cocher **Supprimer les dossiers de collaboration** .
4. Sélectionnez **Mettre à jour**.

Gestion des incidents de sécurité majeurs Workspace

Gestion des incidents de sécurité majeurs fournit un espace de travail dédié à la gestion des incidents de sécurité majeurs, spécialement conçu pour le Incident de sécurité majeur gestionnaire.

Collaborez facilement sur des activités qui aident à résoudre les incidents de sécurité majeurs en partageant et en visualisant des fichiers et des dossiers, en visualisant et en mettant à jour les tâches d'incident et en communiquant avec les personnes travaillant sur l'incident via des canaux de messagerie instantanée dédiés.

Gestion des incidents de sécurité majeurs (MSIM) fournit un mécanisme de suivi et de résolution des incidents de sécurité majeurs. MSIM fonctionne conjointement avec les capacités existantes du produit de réponse aux incidents de sécurité et aux vulnérabilités et améliore le processus de remédiation des incidents de sécurité majeurs avec les fonctionnalités suivantes :

- Espace de travail dédié à la gestion des incidents de sécurité majeurs, spécialement conçu pour le rôle d'utilisateur responsable des incidents de sécurité majeurs.
- Organisez les tâches majeures de réponse aux incidents de sécurité, y compris les tâches suivies sur les incidents de sécurité liés et les groupes de vulnérabilité.
- Automatisez la création de dossiers de collaboration et de canaux de communication par messagerie instantanée lorsqu'un incident de sécurité majeur est créé, ainsi que l'archivage dans le cadre de la clôture de l'incident.
- Composant d'explorateur de fichiers permettant d'organiser et de suivre la collecte d'artefacts (fichiers) liés à l'incident de sécurité majeur via une Microsoft SharePoint intégration.
- Gestionnaire de canal de messagerie instantanée et composants de flux d'activité pour gérer les communications entre plusieurs groupes de sécurité, informatiques et fonctionnels via une Microsoft Teams intégration.
- Rapports récapitulatifs de l'impact et des mesures de progression des incidents de sécurité majeurs, y compris le déploiement des actifs, des utilisateurs, des emplacements et des ressources d'équipe affectés, ainsi que la chronologie des étapes importantes de l'incident.

Utilisez l'espace de travail MSIM pour suivre et résoudre les incidents de sécurité majeurs :

1. Consultez les graphiques de tendance et la progression de l'incident de sécurité majeur.
2. Suivez et organisez l'activité des fichiers Microsoft SharePoint via l'espace de travail MSIM.
3. Suivez et organisez l'activité de messagerie instantanée Microsoft Teams via l'espace de travail MSIM.
4. Affichez et mettez à jour les détails de l'incident via l'espace de travail MSIM.
5. Filtrer les activités de collaboration dans le flux d'activité de l'espace de travail MSIM.

Utiliser Gestion des incidents de sécurité majeurs

Les gestionnaires peuvent utiliser Gestion des incidents de sécurité majeurs l'espace de travail pour afficher les enregistrements d'incidents proposés, promus, liés et rejetés et suivre leurs activités connexes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Proposer, promouvoir et lier des enregistrements d'incidents

Proposez ou promouvez des incidents de sécurité en tant qu'incidents de sécurité majeurs lorsque les incidents sont identifiés comme une menace critique pour l'organisation.

Une fois la gestion des incidents de sécurité majeurs installée sur votre ServiceNow instance, vous pouvez gérer la transition des incidents de sécurité vers les incidents majeurs comme suit :

- Proposez un incident de sécurité au candidat à un incident de sécurité majeur afin de lancer un processus d'examen.
- Promouvoir directement un incident de sécurité en un incident de sécurité majeur sans processus de révision.
- Rejeter un incident de sécurité proposé comme incident de sécurité majeur.

Vous pouvez également lier un incident de sécurité en tant qu'incident enfant à l'incident de sécurité majeur afin que tous les incidents de sécurité associés puissent être suivis ensemble.

Proposer en tant que Incident de sécurité majeur

Proposez un incident de sécurité en incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Listes**.
2. Sélectionnez l'incident de sécurité dans la catégorie connexe que vous souhaitez proposer comme incident de sécurité majeur.
3. Sélectionnez l'icône **Actions supplémentaires** , puis sélectionnez **Proposer comme incident de sécurité majeur**.
4. Renseignez les champs de la boîte de dialogue Proposer comme incident de sécurité majeur.
   a. **Date de détection** : date à laquelle l'incident de sécurité majeur a été créé ou proposé pour la première fois.
   b. **Justification** : fournissez la justification de la proposition de l'incident.
   c. **Impact potentiel** : indiquez l'impact de l'incident.
5. Sélectionnez **Proposer**.

Résultats

L'incident est proposé et les actions suivantes se produisent :

- Dans l'enregistrement d'incident de sécurité, un message de bannière de vérification s'affiche et la balise d'incident de sécurité majeur définie apparaît.
- L'enregistrement apparaît dans la liste connexe des incidents de sécurité majeurs dans l'enregistrement d'incident, avec l'état Proposé, et dans la liste des candidats de l'espace de travail MSIM.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La section Activité de l'espace de travail MSIM indique que l'incident de sécurité a été proposé pour être promu en incident de sécurité majeur.

- Un message contenant un lien vers l'enregistrement d'incident et l'onglet Détails de l'incident est envoyé aux personnes figurant dans la liste de notification définie.

Promouvoir à Incident de sécurité majeur

Promouvoir un incident de sécurité en un incident de sécurité majeur ou rejeter les propositions promues via l'espace Gestion des incidents de sécurité majeurs de travail (MSIM).

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Listes**.
2. Sélectionnez l'incident de sécurité dans la catégorie connexe que vous souhaitez promouvoir comme incident de sécurité majeur.
   Passez en revue les détails de l'incident de sécurité dans la section Détails ou affichez les détails étendus dans l'enregistrement d'incident dans un onglet distinct en cliquant sur **Afficher plus de détails**.
3. Sélectionnez l'icône **Actions supplémentaires** , puis sélectionnez **Promouvoir en incident de sécurité majeur**.
4. Renseignez les champs de la boîte de dialogue Promouvoir un incident de sécurité majeur.

   a. **Date de détection** : date à laquelle l'incident de sécurité majeur a été créé ou proposé pour la première fois.

   b. **Date de résolution estimée** : date de résolution estimée à laquelle l'incident de sécurité majeur est censé être résolu.

   c. **Nom** de code : sélectionnez le nom de code de l'incident de sécurité majeur.
   Par exemple, Blue Tiger.

   d. **Catégorie** : sélectionnez la catégorie pour l'incident de sécurité majeur.
   Par exemple, Mauvaise configuration.

   e. **Justification** : fournissez la justification de la proposition de l'incident.

   f. **Impact potentiel** : indiquez l'impact de l'incident.

5. Sélectionnez **Proposer**.
6. Faites la promotion de l'incident de sécurité ou rejetez la proposition de promotion.
   - Pour promouvoir l'incident, cliquez sur **Promouvoir en incident de sécurité majeur**.
   - Pour rejeter la proposition de promotion, cliquez sur **Rejeter en tant qu'incident de sécurité majeur**.
7. Sélectionnez **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

- Si vous avez rejeté la proposition de promotion, l'incident n'est pas promu et l'entrée de l'incident est déplacée vers l'onglet Rejeté.
- Si vous avez promu l'incident, l'entrée de l'incident passe dans l'onglet Ouvrir et l'enregistrement de sécurité affiche une balise indiquant qu'il s'agit d'un incident de sécurité majeur.
- La décision est répertoriée dans la section Activité de l'espace de travail MSIM.

Une fois qu'un incident est promu, la configuration par défaut est appliquée.

- Une structure de dossiers est créée en fonction de la configuration du modèle de dossier.
- Les canaux de messagerie instantanée sont créés en fonction de la configuration des canaux.
- Un message électronique est envoyé aux utilisateurs désignés. La notification par défaut contient un lien vers l'incident de sécurité majeur et les détails de l'incident. Les utilisateurs désignés ont également accès aux ressources de collaboration, de sorte que la notification inclut également le nom de l'équipe Microsoft et un lien vers les dossiers Microsoft SharePoint associés à l'incident.

Lier à Incident de sécurité majeur

Lier les incidents de sécurité à un incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité dans la catégorie connexe que vous souhaitez lier à l'incident de sécurité majeur.
3. Sélectionnez l'icône **Actions supplémentaires** , puis **Lier à l'incident de sécurité majeur**.
4. Sélectionnez l'incident de sécurité majeur que vous souhaitez associer.
   a. Dans la boîte de dialogue, sélectionnez l'icône Rechercher à l'aide de la liste.
   b. Sélectionnez l'incident de sécurité majeur auquel vous souhaitez créer un lien.
   c. Sélectionnez **OK**.
5. Sélectionnez **Proposer**.

Résultats

La proposition est soumise et les mesures suivantes sont prises :

- Dans l'enregistrement d'incident de sécurité, un message de bannière de vérification s'affiche et la balise d'incident de sécurité majeur définie apparaît à côté du champ **Sélectionner une balise de sécurité** .
- Dans l'onglet **Détails** de l'incident de sécurité majeur en Gestion des incidents de sécurité majeurs, la liste déroulante Numéro d'enregistrement inclut les deux incidents.
- L'enregistrement apparaît dans la liste connexe Incident de sécurité majeur de l'enregistrement d'incident, avec l'état répertorié comme Proposé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Un message contenant un lien vers l'enregistrement d'incident et l'onglet Détails de l'incident est envoyé aux personnes figurant dans la liste de notification définie.

- La section **Activité** de l'espace de travail MSIM indique que l'incident de sécurité a été ajouté en tant qu'incident de sécurité enfant à l'incident de sécurité majeur avec un lien.

Utilisation de la vue de liste MSI dans l'espace de travail MSIM

La vue de liste de l'espace de travail MSIM vous permet d'afficher les incidents de sécurité majeurs proposés, promus et rejetés.

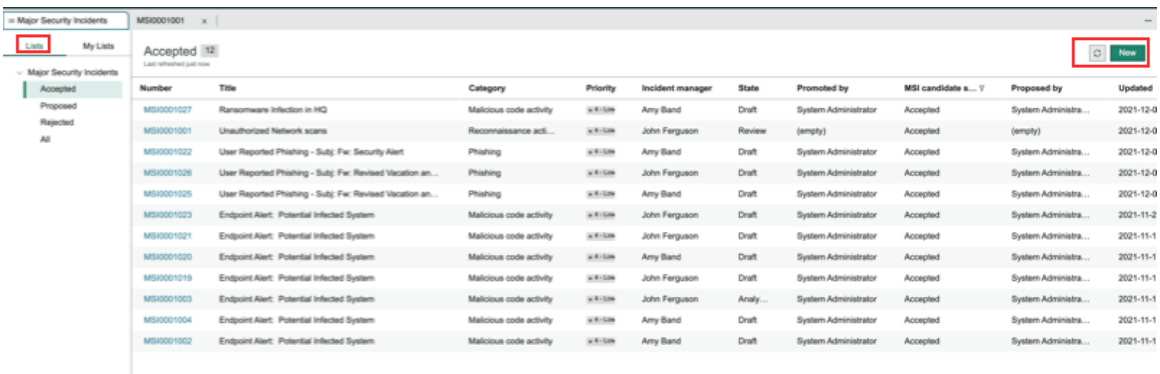
Avant de commencer

Rôle requis : sn_msi.workspace_manager

Vous pouvez également créer de nouveaux incidents à l'aide du bouton **Nouveau** disponible dans le coin supérieur droit de l'espace de travail.

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Espace de travail MSIM**.
2. Sélectionnez l'onglet Listes pour afficher la vue Listes.



3. Sélectionnez **Mes listes** pour créer votre propre liste des incidents de sécurité majeurs.
4. Reportez-vous à la table suivante pour savoir ce que vous pouvez faire à partir de la vue de liste :

Tâche	Description
Mes listes	Créez de nouvelles listes d'enregistrements MSI et affichez les listes que vous avez créées.
Définir des filtres pour une colonne d'une liste	Sélectionnez une colonne et développez le menu à points verticaux pour afficher les options qui filtrent davantage les données de la colonne.
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	◦ Afficher les éléments correspondants : affiche uniquement les éléments qui correspondent à l'élément sélectionné dans la colonne. ◦ Filtrer : filtre les éléments de la colonne qui correspondent à l'élément sélectionné dans la colonne respective.
Actualiser la liste	Actualisez les listes et affichez les listes complètes qui ont été mises à jour.
Nouveau	Créez un nouvel enregistrement MSI.

Afficher Incident de sécurité majeur les mesures d'impact

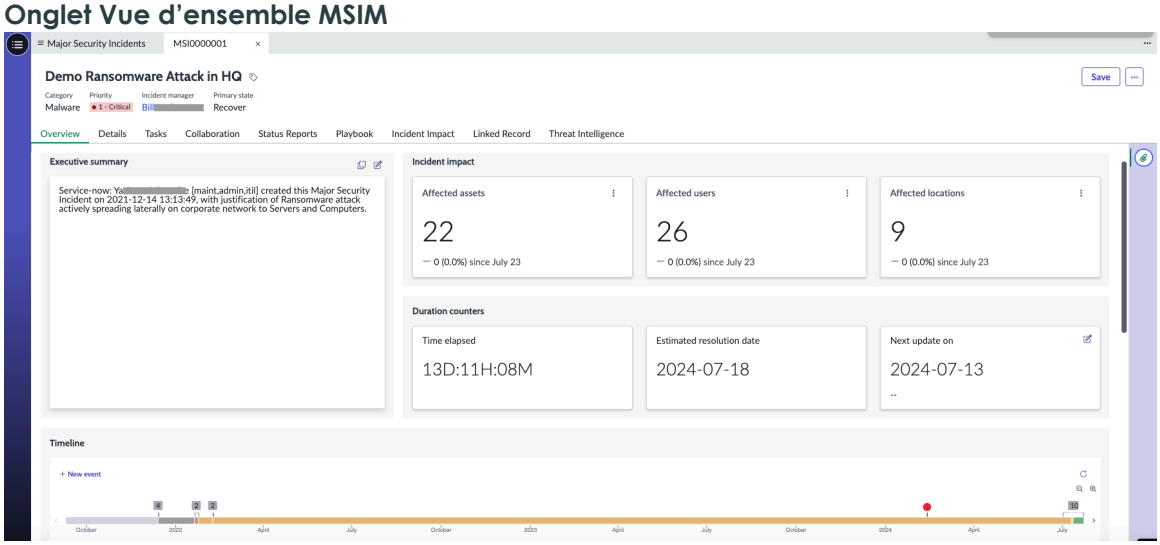
Fournit un rapport récapitulatif à jour de l'impact et de la progression des incidents de sécurité majeurs, ce qui est un aspect important de la gestion d'un incident de sécurité majeur à l'aide du nouvel espace de travail.

L'onglet **Vue d'ensemble** fournit les mesures pertinentes pour gérer à la fois le champ d'application et la progression de l'incident, y compris un déploiement des actifs, des utilisateurs, des emplacements et des ressources d'équipe affectés, ainsi que la chronologie des jalons importants de l'incident.

La chronologie fournit une vue horizontale des événements et jalons clés qui se sont produits dans le cadre de la résolution d'un incident de sécurité majeur spécifique. Le composant de chronologie s'affiche au-dessus de tous les onglets de l'espace de travail Major Security Incident Management. Il est possible de le réduire et de le développer pour l'afficher selon les besoins. Les données d'événements représentées seront mises à jour et actualisées chaque fois que des événements jalons ou des jalons désignés sont ajoutés ou mis à jour.

Chaque événement ou jalon est indiqué par une option de type d'événement de chronologie différente pour identifier le nombre et le type d'événements ou de jalons. Par exemple, mises à jour d'enregistrements NOW, activités de collaboration. En outre, la période des différents états d'incident de sécurité majeur est suivie automatiquement et affichée à l'aide de plages à code couleur affichées avec la durée de chaque état d'incident.

Onglet Vue d'ensemble MSIM



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résumé analytique et impact de l'incident

Tâche	Description
Résumé analytique	Bref résumé de l'incident de sécurité majeur avec le nom d'utilisateur, le rôle de l'utilisateur et les détails de l'horodatage. • Vous pouvez modifier le résumé en sélectionnant l'icône **Modifier** . Une fois que vous avez apporté les modifications requises, sélectionnez l'option **Mettre à jour** . • Pour copier le résumé et le coller dans un incident de sécurité majeur, sélectionnez l'icône **Copier** et collez le résumé dans l'incident de sécurité majeur requis.
Impact de l'incident	Ces composants affichent les ressources impactées en fonction d'un déploiement de toutes les tâches actives et des incidents liés avec les actifs, les utilisateurs, les emplacements et les membres de l'équipe affectés identifiés. Les ressources impactées sont les suivantes : • **Actifs affectés** • **Utilisateurs affectés** • **Emplacements affectés** La sélection des valeurs numériques vous permet d'explorer et d'accéder aux actifs, aux utilisateurs et aux détails d'emplacement impactés, et affiche les tâches connexes dans l'onglet **Impact de l'incident** de l'espace de travail. En fonction du lien du type d'impact de l'incident que vous avez sélectionné, les détails de l'incident connexe, tels que le type de tâche et sa description, le groupe d'affectation et l'état de l'incident, s'affichent dans le **Impact de l'incident** de l'espace de travail MSIM.
Compteurs de durée	Ces composants affichent la durée de l'incident de sécurité majeur. Les ressources impactées sont les suivantes : • **Temps écoulé** : affiche le temps écoulé depuis le moment où l'incident de sécurité majeur est détecté. • **Date de résolution estimée** : affiche la date de résolution estimée à laquelle la résolution de l'incident de sécurité majeur est estimée.

Traduction automatique

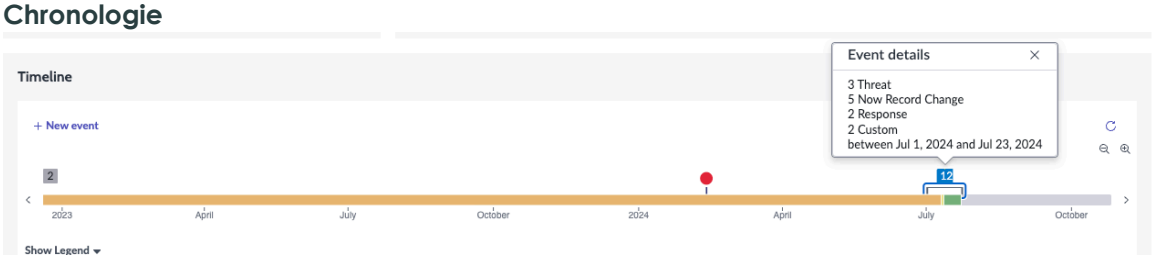
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résumé analytique et impact de l'incident (suite)

Tâche	Description
	• **Prochaine mise à jour le** : date et heure de la prochaine mise à jour pour la résolution de l'incident de sécurité majeur. Par exemple, 17h00 HNE le 25 mars 2024. Vous pouvez modifier la **prochaine mise à jour en** sélectionnant l'icône **Modifier** . Sélectionnez la nouvelle date et la nouvelle heure, puis sélectionnez **Mettre à jour**.

Vous pouvez activer ou désactiver l'affichage de certains types d'événements pour les indicateurs de chronologie et les plages de chronologie en conséquence à l'aide des boutons de bascule de filtre.

Chronologie



Consultez le tableau suivant pour connaître les options supplémentaires disponibles avec le composant de chronologie.

Options supplémentaires du composant de chronologie

Tâche	Description
Nouvel événement	Crée de nouveaux événements personnalisés et associe ces événements à l'enregistrement MSI. Cela permet de créer des événements pour des dates passées et futures qui pourraient ne pas être capturées autrement via une tâche étiquetée, un changement d'état d'enregistrement ou une activité de collaboration étiquetée, qui sont affichés par défaut sur la chronologie.
Actualiser	Actualise les événements de chronologie pour afficher les dernières mises à jour.
Indicateurs de chronologie	Répertorie les différents types d'événements tels que les changements de champ Now Record, les activités de collaboration étiquetées et Autre (personnalisé), ainsi que les icônes et le nombre total d'événements qui se sont produits en ce qui concerne chaque indicateur de type d'événement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Options supplémentaires du composant de chronologie (suite)

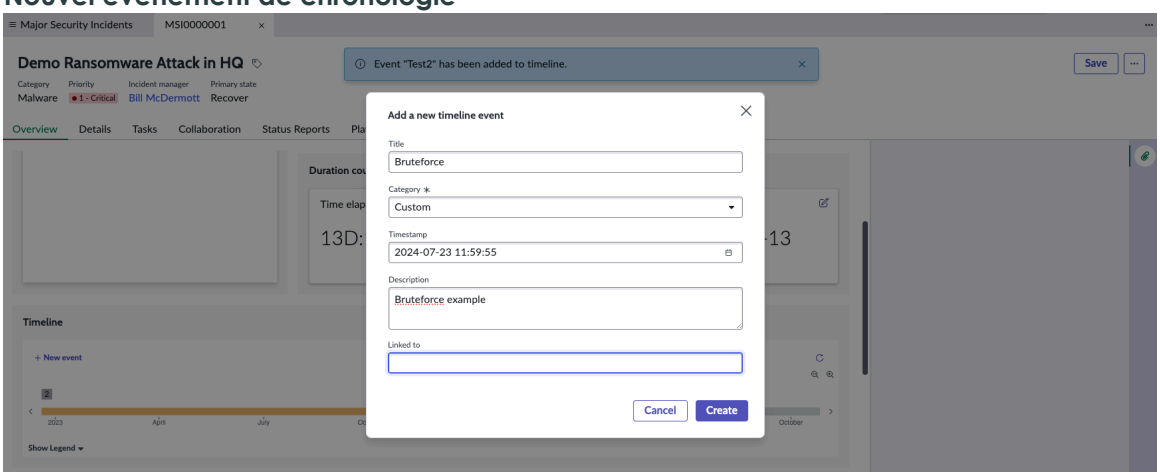
Tâche	Description
	Le curseur vous permet d'activer ou de désactiver tous les événements pour un type d'événement spécifique.
Afficher la légende	Sélectionnez cette option pour afficher la légende de la liste déroulante avec différents types d'indicateurs de chronologie.
Barre de progression de la chronologie	Affiche la progression globale de l'incident via des événements de chronologie désignés ou des jalons qui se sont produits dans les différentes plages de chronologie affichées. Vous pouvez également lier un type d'événement à une catégorie d'événement. Une fois que vous l'avez lié, les détails de l'événement sont mis à jour aux deux emplacements de la chronologie.
Plages de chronologie	Affiche les différents types d'état et durée des incidents à mesure que l'incident progresse tout au long du cycle de vie complet de l'incident de sécurité majeur. Activer ou désactiver un événement spécifique en fonction de l'état de l'incident.

Créer un événement de chronologie

Pour créer un nouvel événement de chronologie, procédez comme suit :

1. Dans l'onglet Vue d'ensemble, accédez à la section **Chronologie** .
2. Sélectionner **+ Nouvel événement**.
3. Renseignez les champs de la fenêtre contextuelle Ajouter un nouvel événement de chronologie.

Nouvel événement de chronologie



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
Titre	Saisissez le titre de l'événement de chronologie.
Catégorie	Sélectionnez une catégorie pour l'événement de chronologie. Les catégories suivantes sont fournies dans le cadre du système de base, et vous pouvez en choisir une en fonction de vos besoins. ◦ **Sur mesure**. ◦ **Réponse**. ◦ **Menace**. Pour ajouter ou configurer une catégorie d'événement de chronologie, reportez-vous à la section Configurer des catégories de chronologie pour les incidents de sécurité majeurs.
Horodatage	Sélectionnez la date et l'heure de l'événement de chronologie à l'aide du calendrier Horodatage. Vous pouvez ajouter des événements à la chronologie avant et après la date de début.
Description	Fournissez une brève description de l'événement de chronologie.
Lié à	Option permettant de lier l'événement de chronologie à un enregistrement d'incident de sécurité majeur.

4. Sélectionner **Créer**.
5. Vous pouvez utiliser les icônes **de zoom avant** et **arrière** pour effectuer un zoom avant ou arrière sur la barre de progression de la chronologie, ce qui inclut l'affichage d'événements individuels lorsque des nombres sont affichés pour représenter plusieurs événements à proximité rapprochée.

   Vous pouvez également ajouter le niveau de zoom par défaut pour afficher tous les événements.
6. Sélectionnez l'icône **Actualiser** pour afficher les derniers événements de chronologie.

Afficher Incident de sécurité majeur les graphiques de tendance

Affichez les mesures de progression de l'impact d'un incident de sécurité majeur sous forme de graphiques à barres et de diagrammes.

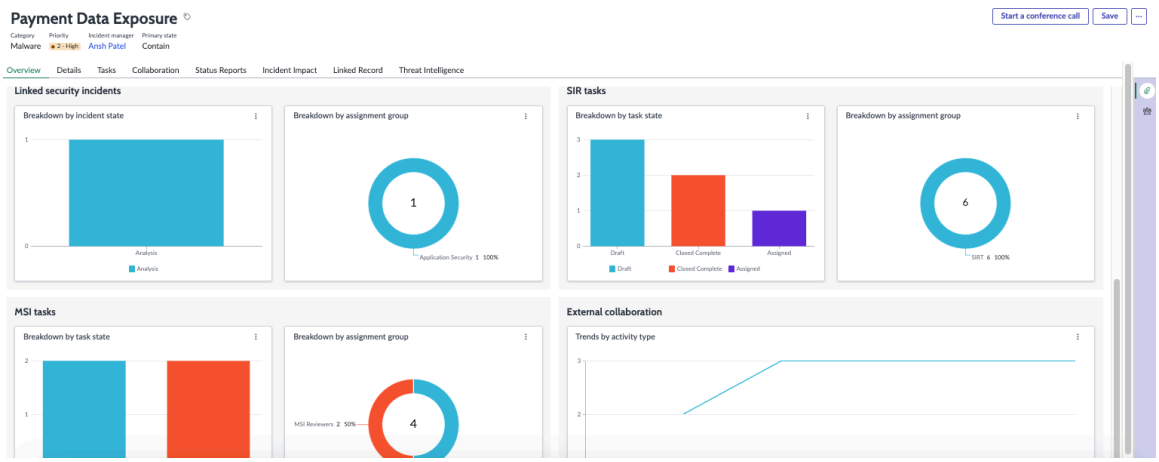
En plus de la chronologie des incidents et des graphiques de tendance de progression, le **Vue d'ensemble** L'onglet fournit des mesures d'impact pertinentes pour gérer l'évolution du champ d'application de l'incident, y compris le déploiement des actifs, des utilisateurs, des emplacements et des ressources d'équipe affectés.

Les nombres affichés dans les composants de visualisation sont basés sur les tâches actives sur les incidents liés Réponse aux incidents de sécurité (SIR). Au fur et à mesure que les tâches sont ouvertes et fermées, ces nombres changent en termes de nature et de volume d'activité restante planifiée pour l'incident de sécurité majeur afin de représenter les tendances affichées dans les composants de visualisation du graphique de tendances.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures de l'impact de l'onglet Vue d'ensemble MSIM



Consultez le tableau suivant pour connaître les actions d'interface utilisateur que vous pouvez effectuer à partir du **Vue d'ensemble** section:

Vue d'ensemble des sections de l'interface utilisateur

Titre	Description
Heure	Affiche la période, en nombre total, de jours à partir du moment où l'incident de sécurité majeur est actif. Le temps est calculé en fonction de la **Date de détection** saisi dans le champ **Détails** de l'espace de travail. La date de détection est souvent capturée initialement lorsque l'incident de sécurité majeur a été créé ou proposé pour la première fois. Chaque fois que cette date est modifiée, l'heure est automatiquement calculée, rafraîchie et affichée au format jours : heures : minutes, par exemple 20J : 13H : 58M. **Date de résolution estimée**: date à laquelle la date estimée de résolution de l'incident est résolue. Cette date est souvent capturée initialement lors de la création ou de la promotion de l'incident de sécurité majeur. La date est mise à jour et actualisée en fonction de la date estimée fournie dans le champ **Détails** de l'espace de travail. Si la date estimée n'est pas fournie dans la section Détails, cette section affiche un « trait d'union » sans valeur de date.
Équipe active	Affiche les différentes équipes d'intervention et les membres de chaque équipe qui travaillent activement sur l'incident de sécurité majeur et ses tâches connexes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble des sections de l'interface utilisateur (suite)

Titre	Description
	Équipe active tendance : affiche le graphique de tendance de chaque équipe et des membres de son équipe qui travaillent activement sur l'incident de sécurité majeur et les tâches connexes à intervalles réguliers. **Remarque :** Afficher les groupes actifs affectés à partir de **Détails** de l'espace de travail.
Incidents SIR liés	**Par état de l'incident**: affichez la distribution des incidents de sécurité liés en fonction d'un état d'incident tel que Analyse, Maîtriser, Éradiquer, Récupérer ou Réviser. **Tendances par l'état d'incident**: indique en outre la vue de tendance de la progression du nombre d'incidents liés en fonction de l'état de l'incident. La sélection de chaque lien d'état d'incident vous permet de naviguer et d'afficher les détails de l'incident de sécurité lié directement sur le **SI/VI lié** de l'espace de travail. Cette section est mise à jour et actualisée automatiquement chaque fois que des changements sont apportés aux incidents sous-jacents.
Tâches SIR	Affiche les totaux de tâches actives qui sont liés à l'enregistrement MSI via les incidents SIR. • **Par état de la tâche**: affichez les tâches de réponse aux incidents en fonction de l'état de l'incident, par exemple Brouillon, Affecté, Travail en cours, Fermé terminé. Ce graphique de distribution permet une répartition supplémentaire de la distribution par groupes d'affectation. La sélection de chaque état de tâche vous permet d'afficher une liste filtrée par état de tâche d'incident sur le **Tâches** de l'espace de travail. La vue filtrée vous permet d'afficher et de mettre à jour les détails d'une tâche individuelle. • **Tâches en cours par étiquette d'état d'incident**: affiche les tâches et les groupes actifs en fonction de l'étiquette d'état de l'incident qui doit être

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble des sections de l'interface utilisateur (suite)

Titre	Description
	appliquée dans les composants de l'organisateur de tâche. Ces étiquettes par défaut ont des valeurs telles que Analyse, Contenir, Éradiquer, Récupérer ou Examiner pour indiquer la nature de la tâche impliquée. • **En retard**: affiche les tâches de réponse aux incidents de sécurité qui sont actives et ont dépassé la date d'échéance. Vous pouvez afficher les détails de toutes les tâches en retard en sélectionnant le nombre total de tâches en retard et en le faisant naviguer automatiquement vers l'onglet Tâches. • **Tendances par état de tâche**: affichez la tendance de progression des tâches de réponse en cours et fermées sur la durée de l'incident. **Remarque :** Le graphique de tendance récupère les dernières données en fonction de la tâche planifiée. Vous pouvez configurer ou modifier l'intervalle de temps de récupération des données selon vos besoins.
Tâches MSI	Affiche les tâches actives au total, qui ont été créées directement sur l'enregistrement MSI (et ce ne sont pas des tâches de réponse liées) : **Par état de la tâche :** Affichez les tâches créées pour l'incident de sécurité majeur, les tâches affectées et les informations connexes. La sélection de chaque état de tâche vous permet d'afficher une liste filtrée par état de tâche d'incident sur le **Tâches** de l'espace de travail. La vue filtrée permet d'afficher et de mettre à jour les détails de chaque tâche.
Collaboration externe	Affiche les activités de collaboration au total pour toutes les activités de collaboration étiquetées du flux d'activité de collaboration :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble des sections de l'interface utilisateur (suite)

Titre	Description
	• **Par étiquette d'état d'incident :**Affichez les données des activités de collaboration d'incident qui sont coordonnées avec Microsoft Teams les Microsoft SharePoint fichiers et dossiers et qui sont étiquetées à l'aide d'étiquettes d'état d'incident telles que Analyse, Contenir, Éradiquer ou Récupérer dans l'onglet **Collaboration** de l'espace de travail. • **Tendances par type d'activité**: affichez le graphique de tendance du nombre d'activités de fichiers et de dossiers sur la durée de Microsoft TeamsMicrosoft SharePoint l'incident.

Mettre à jour Incident de sécurité majeur les détails

Affichez et mettez à jour des détails spécifiques liés à l'incident de sécurité majeur, tels que les détails de l'enregistrement de l'incident, les participants actifs de l'équipe et le journal d'activité correspondant.

Tous les détails connexes de l'incident de sécurité majeur sont affichés avec différentes sections de formulaire dans l'onglet **Détails** de l'espace de travail. Affiche les détails tels que les détails de l'enregistrement d'incident, les participants de l'équipe actifs et le journal d'activité correspondant. Vous pouvez également afficher les incidents SIR liés, les détails de l'enregistrement du groupe de vulnérabilité et la possibilité de diffuser une publication d'activité à tous les enregistrements d'incident liés.

L'onglet Détails contient principalement :

1. Champs de formulaire d'incident de sécurité majeur et sections de l'interface utilisateur liées aux incidents.
2. Flux d'activité

La table suivante fournit les détails des champs du formulaire d'incident de sécurité majeur :

Sections du formulaire Incident de sécurité majeur

Champ	Description
Incident	
Numéro	Numéro d'incident de sécurité majeur.
État primaire	État primaire de l'incident de sécurité majeur.
Date de détection	Date à laquelle l'incident de sécurité majeur a été créé ou proposé pour la première fois. Chaque fois que vous modifiez la date de détection dans l'onglet Détails, la date et l'heure du MSI sont automatiquement

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sections du formulaire Incident de sécurité majeur (suite)

Champ	Description
	calculées, actualisées et affichées sur le **Heure** > **Délai depuis le début de l'incident** dans la section **Vue d'ensemble** de l'espace de travail.
Titre	Titre de l'incident de sécurité majeur.
Nom de code	Nom de code de l'incident de sécurité majeur. Par exemple, Blue Tiger.
Prochaine mise à jour le	Date et heure de la prochaine mise à jour pour la résolution de l'incident de sécurité majeur. Par exemple, 17h00 HNE le 25 mars 2024.
Catégorie	Catégorie de l'incident de sécurité majeur.
Sous-catégorie	Type de sous-catégorie de l'incident de sécurité majeur.
Date de résolution estimée	Date à laquelle la date estimée de résolution de l'incident est résolue. La date estimée est la date à laquelle l'incident de sécurité majeur a été créé ou promu pour la première fois.
Priorité	Priorité de l'incident de sécurité majeur.
Capteur d'alerte	Capteur d'alerte de l'incident de sécurité majeur. Par exemple, Hameçonnage signalé par un utilisateur.
Source	Source de l'incident de sécurité majeur.
Équipe active	
Gestionnaire d'incidents	Nom du gestionnaire d'incidents.
Groupes d'affectation	Indique les différentes équipes de réponse et les membres de chaque équipe qui travaillent activement sur l'incident de sécurité majeur.
Candidat	
État du candidat MSI	Indique l'état du candidat à l'incident de sécurité majeur, tel que Proposé ou Promu. Si l'incident est promu, l'état s'affiche comme Accepté.
Promus par	Utilisateur ayant promu l'incident de sécurité majeur.
Promu(e)	Date à laquelle l'incident de sécurité majeur a été promu.
Justification	Justification de l'incident de sécurité majeur. La justification doit inclure le numéro MSI et le nom de code.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sections du formulaire Incident de sécurité majeur (suite)

Champ	Description
Impact potentiel	Impact et gravité potentiels de l'incident de sécurité majeur. L'impact potentiel doit inclure le numéro MSI et le nom de code.
Restriction	
Appliquer la restriction	Sélectionnez cette option pour appliquer des restrictions à certaines restrictions d'incident de sécurité majeur. Vous pouvez appliquer des restrictions pour limiter la vue ou modifier l'accès à certains utilisateurs ou groupes. Pour plus d'informations, voir Restreindre l'accès à certains incidents de sécurité majeurs
Membres autorisés	Liste des utilisateurs qui peuvent accéder à l'incident de sécurité majeur.
Groupes autorisés	Liste des groupes qui peuvent accéder à l'incident de sécurité majeur.
Autres actions	
Pièce jointe	Toutes les pièces jointes associées à l'incident de sécurité majeur. Sélectionnez l'option **Sélectionner** pour ajouter des pièces jointes à l'incident.
Téléconférence	Utilisez les téléconférences avec les fournisseurs de services tiers comme canal de communication pour rencontrer les personnes concernées afin de résoudre les incidents de sécurité majeurs. Pour plus d'informations, voir Gestion des incidents de sécurité majeurs Intégration de la téléconférence

Activité :

Utilisez la section Activité pour ajouter vos notes de travail et vos commentaires, publier votre activité en privé et ajouter des commentaires supplémentaires si nécessaire à l'aide de la section Composer. Enregistrez l'activité après avoir publié vos notes de travail et commentaires pour afficher l'activité ou les notes de travail ajoutées dans la section Activité.

Remarque : Cliquez sur le lien **Afficher plus** de détails pour afficher les détails d'un enregistrement d'incident de sécurité spécifique, qui sont associés à cet incident de sécurité majeur.

Vous définissez vos préférences pour afficher les activités connexes telles que :

1. **Filtres** : sélectionnez l'icône **Jeux de filtres** pour définir des filtres.

   Définissez des filtres pour afficher les conversations d'activité telles que les activités ajoutées aux notes de travail, à l'e-mail, à la chronologie et à tous les commentaires supplémentaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. **Marqué** : cliquez sur l'icône **Marqué** pour marquer les activités.

   Marquez toutes les conversations d'activité importantes pour que vous puissiez les revoir rapidement si nécessaire.

Restreindre l'accès à certains incidents de sécurité majeurs

Gérez qui peut afficher ou modifier les incidents de sécurité majeurs qui contiennent des informations sensibles. Vous pouvez appliquer des restrictions d'incidents de sécurité majeurs pour déterminer qui a accès à l'affichage ou à la modification de certains enregistrements d'incidents de sécurité majeurs et listes connexes, et limiter l'accès en lecture ou en écriture uniquement à certains utilisateurs ou groupes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche

Les restrictions d'incidents de sécurité majeurs vous permettent de masquer les incidents de sécurité majeurs critiques afin qu'ils ne soient pas accessibles ou modifiés par tous les utilisateurs ou groupes d'une organisation donnée. Ces restrictions vous permettent de fournir un moyen plus granulaire de contrôler les incidents de sécurité majeurs qu'un utilisateur ou un groupe peut afficher ou modifier. Vous pouvez appliquer une restriction d'incident de sécurité majeur en cochant la case **Appliquer la restriction** , puis en sélectionnant les utilisateurs ou les groupes autorisés à afficher ou à modifier l'incident de sécurité majeur particulier.

Une fois que vous avez appliqué la restriction sur les incidents de sécurité majeurs ou les listes connexes à certains utilisateurs ou groupes, tous les autres utilisateurs ou groupes de votre organisation ne sont plus en mesure d'afficher ou de modifier ces incidents de sécurité majeurs ou ces listes connexes.

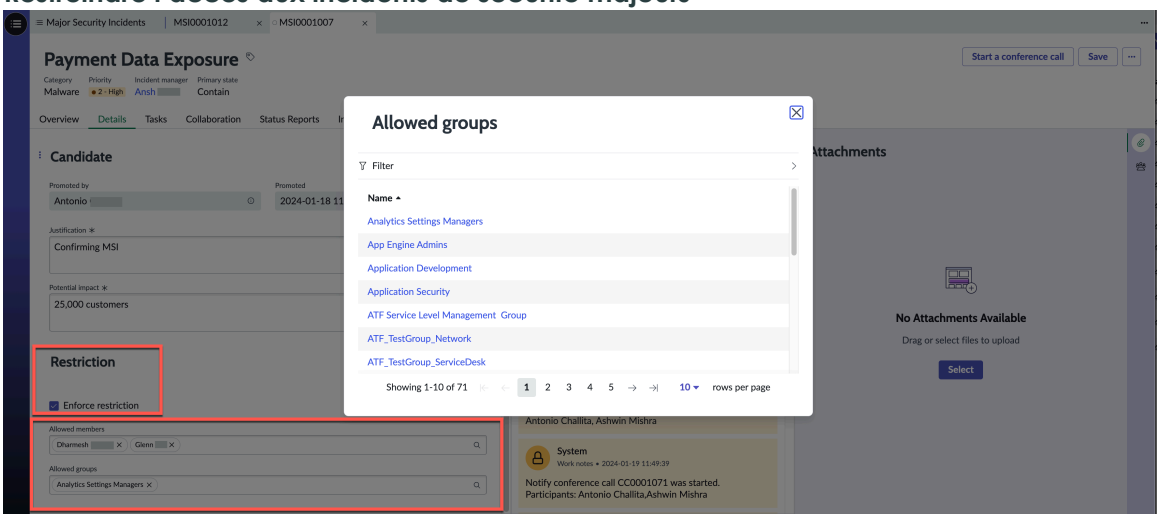
Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Détails**.
5. Faites défiler vers le bas et sélectionnez la section **Restriction** .
6. Cochez la case **Appliquer la restriction** pour activer la restriction de l'incident de sécurité majeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Restreindre l'accès aux incidents de sécurité majeurs



7. Dans le champ Membres autorisés, sélectionnez les utilisateurs qui peuvent afficher ou modifier l'incident de sécurité majeur à l'aide de l'option Rechercher.
8. Dans le champ Groupes autorisés, sélectionnez les groupes qui peuvent afficher ou modifier l'incident de sécurité majeur à l'aide de l'option Rechercher.

> **Remarque :** Une fois la case à cocher **Appliquer la restriction** activée pour l'incident de sécurité majeur, seuls le sn_msi.workspace_manager et les membres ou groupes autorisés ont accès à l'affichage ou à la modification de l'incident de sécurité majeur.

9. Sélectionnez **Enregistrer**.

Lier des enregistrements supplémentaires à Incident de sécurité majeur

Dans l'espace de travail, utilisez la fonctionnalité de liaison d'enregistrements pour lier les enregistrements d'incidents de sécurité connexes et ses incidents de sécurité enfants, les tâches de remédiation de Vulnerability Response et les tickets de sécurité de Threat Intelligence à un Incident de sécurité majeur enregistrement (MSI).

Avant de commencer

Rôle requis : sn_msi.workspace_manager et sn_msi.workspace_responder

Procédure

1. Accédez à la **Réponse aux incidents de sécurité majeurs** > **Espace de travail MSIM**.
2. Accédez à la vue **Listes** , qui s'affiche dans le volet gauche de l'espace de travail.
3. Cliquez sur **Accepté** pour sélectionner les enregistrements d'incidents de sécurité majeurs promus.
4. Sélectionnez l'enregistrement d'incident qui doit être lié et qui n'est pas à l'état Fermé dans la liste des enregistrements promus.
5. Cliquez sur **l'onglet Enregistrements liés** .
   Une liste déroulante est fournie pour sélectionner d'autres tables d'enregistrements liés. La section Enregistrements liés affiche les enregistrements liés et ses enregistrements connexes, qui ont été liés à l'incident de sécurité majeur.
6. Sélectionnez la vue de table souhaitée telle que Incidents de sécurité, Tâches de rattrapage (éléments vulnérables) ou Ticket de sécurité dans la liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En fonction de la vue de la table Enregistrements de type Sélection, les enregistrements liés aux enregistrements d'incidents de sécurité majeurs s'affichent.

7. Liez un enregistrement qui n'est lié à aucun enregistrement MSI et qui est à l'état **Ouvert** en sélectionnant l'enregistrement puis en cliquant sur **Lier l'enregistrement** en haut à droite de la page.

   Remarque : Vous ne pouvez pas lier un enregistrement d'incident à un enregistrement MSI s'il est à l'état **Fermé** .

8. Sélectionnez l'enregistrement à lier et cliquez sur **Lier**.
   Un message de confirmation s'affiche pour indiquer que l'enregistrement est lié avec succès et que le déploiement des enregistrements connexes sera traité en arrière-plan.

   Remarque : Une fois qu'un enregistrement est lié, la vue de liste est actualisée automatiquement et répertorie la liste mise à jour des enregistrements d'incidents.

Information associée

Dissocier les enregistrements de Incident de sécurité majeur

Dissocier les enregistrements de Incident de sécurité majeur

À l'aide de l'espace de travail Major Security Incident Management, dissociez les enregistrements d'incidents de sécurité majeurs de la section Enregistrements liés.

Avant de commencer

Rôle requis : sn_msi.workspace_manager et sn_msi.workspace_responder

Remarque : Vous ne pouvez supprimer le lien que d'un seul enregistrement à la fois. Une fois que vous avez dissocié un enregistrement, les informations cumulées connexes sont supprimées des sections Impact de l'incident et Threat Intelligence dans l'espace de travail et l'action ne peut pas être annulée.

Pour plus d'informations sur les enregistrements de déploiement, reportez-vous à Cadre de travail de déploiement pour MSIM.

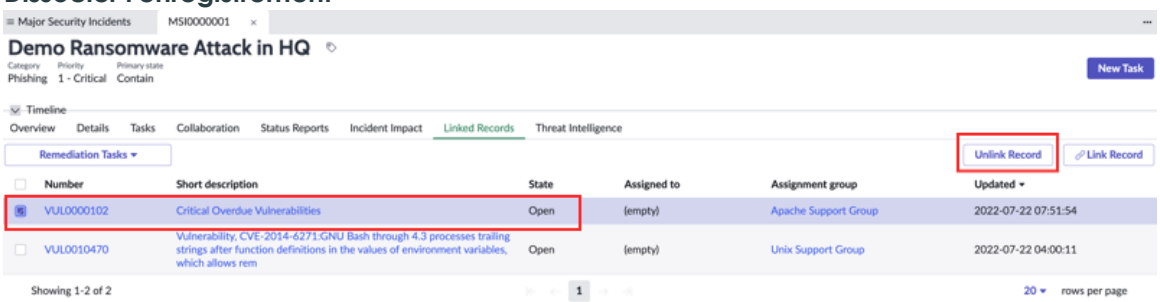
Procédure

1. Accédez à la **Réponse aux incidents de sécurité majeurs** > **Espace de travail MSIM**.
2. Accédez à la vue **Listes** , qui s'affiche dans le volet gauche de l'espace de travail.
3. Cliquez sur **Accepté** pour sélectionner les enregistrements d'incidents de sécurité majeurs promus.
4. Cliquez sur l'onglet **Enregistrements liés** .
   Cette section affiche les enregistrements liés et ses enregistrements connexes, qui sont liés à l'incident de sécurité majeur.
5. Sélectionnez la vue de table souhaitée, comme Incidents de sécurité, Tâches de remédiation (éléments vulnérables) ou Ticket de sécurité.
6. Sélectionnez l'enregistrement à dissocier de la vue de liste des enregistrements.
7. Cliquez sur **Dissocier l'enregistrement**.

Traduction automatique

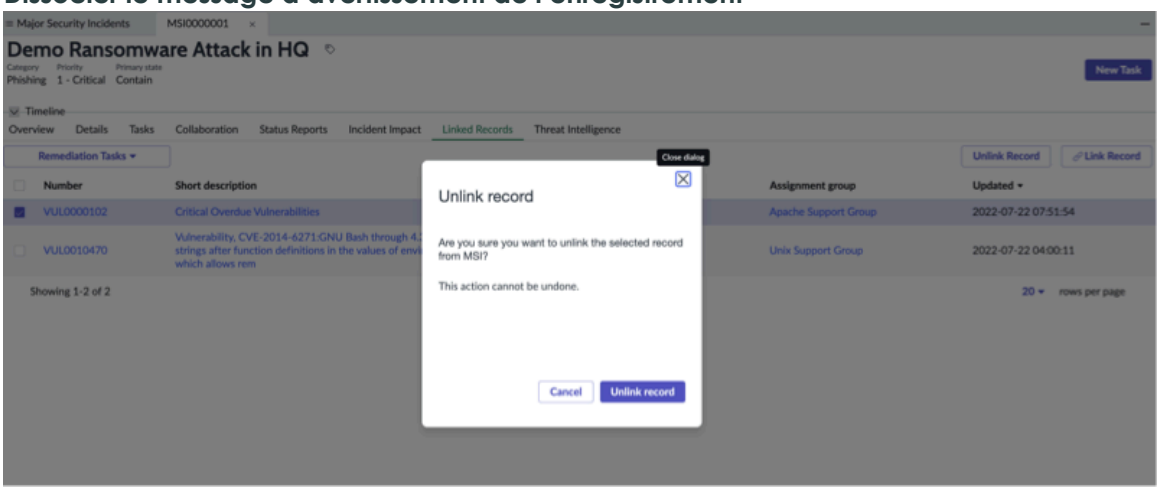
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dissocier l'enregistrement



8. Un message d'avertissement s'affiche pour vous demander si vous souhaitez dissocier l'enregistrement sélectionné de MSI.

Dissocier le message d'avertissement de l'enregistrement



9. Cliquez sur **Dissocier l'enregistrement**.
L'enregistrement est dissocié et une fois dissocié, les changements ne peuvent pas être annulés. La vue de liste des enregistrements liés sera actualisée après la suppression du lien.

Information associée

Configurer les enregistrements liés dans Gestion des incidents de sécurité majeurs

Configurer les enregistrements de déploiement dans Gestion des incidents de sécurité majeurs

Gérer les tâches dans un Incident de sécurité majeur

L'onglet Tâche vous permet de suivre et de gérer toutes les tâches associées à un incident de sécurité majeur à partir de l'espace de travail MSIM. Vous pouvez afficher les différentes tâches à l'aide du tableau visuel des tâches par défaut (vue Kanban) ou de la vue Liste.

Le sn_msi.workspace_manager peut effectuer les actions suivantes dans l'onglet Tâches :

- Créer une tâche
- Modifier les tâches
- Afficher et affecter des tâches à soi-même ou à d'autres personnes
- Supprimer des tâches

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

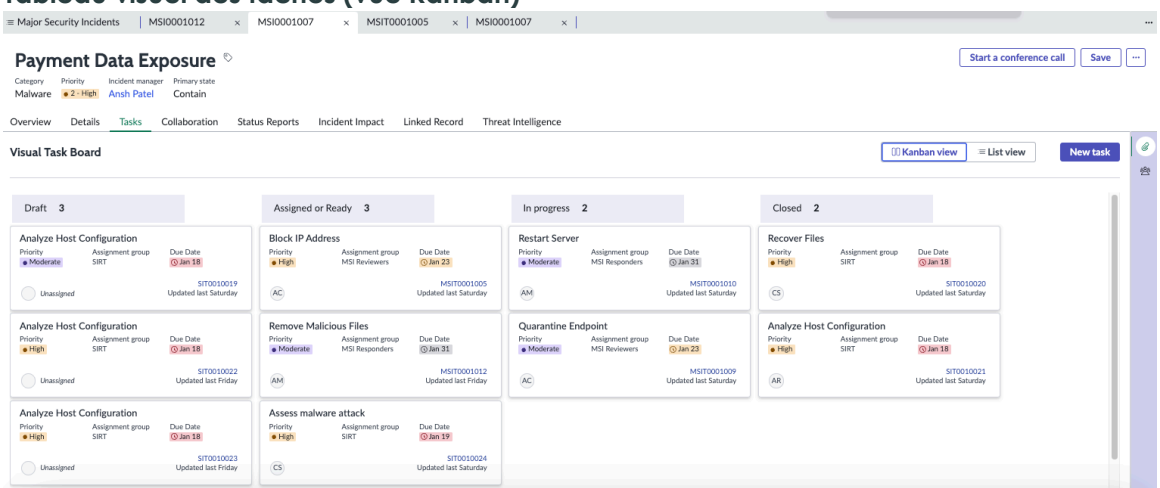
Remarque : Assurez-vous d'avoir installé l'application **Carte de tâches MSIM VTB : 1.0.1v** séparément après l'installation de l'application MSIM.

L'onglet Tâches affiche les détails de toutes les tâches associées à un incident de sécurité majeur. L'onglet Tâche prend en charge deux vues :

- **Tableau visuel des tâches (vue Kanban)** :

  Affichez et mettez à jour plusieurs enregistrements de tâches, qui apparaissent sous forme de cartes sur le tableau visuel des tâches qui peuvent être déplacées entre les voies en fonction de l'état des tâches dans l'incident de sécurité majeur.

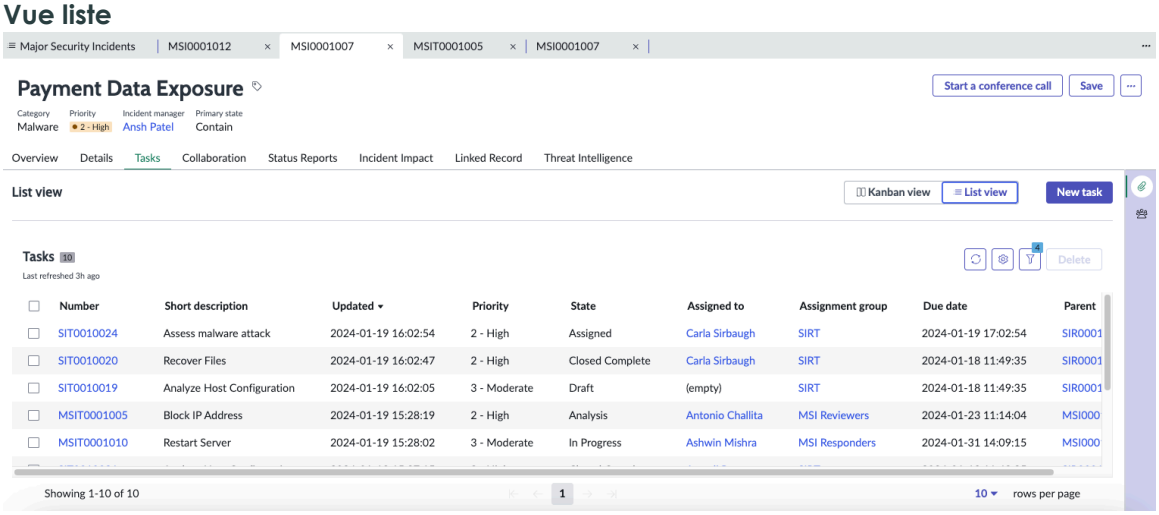
Tableau visuel des tâches (vue Kanban)



- **Vue liste** :

  Affichez et mettez à jour plusieurs enregistrements de tâches sous la forme de listes. À l'aide de ces catégories de liste et de ces filtres, vous pouvez rapidement trouver et suivre les tâches sur lesquelles vous devez travailler en cas d'incident de sécurité majeur.

Vue liste



Les activités étiquetées sont résumées et affichées dans la section Vue d'ensemble de l'incident de sécurité majeur. Un graphique de tendance est disponible dans la section Vue d'ensemble pour afficher l'état des activités de la tâche consolidée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer les tâches à l'aide du tableau visuel des tâches

Suivez et gérez toutes les tâches associées à un incident de sécurité majeur à l'aide du tableau visuel des tâches (vue Kanban).

Vous pouvez utiliser le Tableau visuel des tâches pour déplacer les cartes étape par étape entre les voies telles que Brouillon, Affecté ou Prêt, En cours et Fermé en fonction de l'état des tâches. Un flux d'activité sur le tableau affiche l'activité récente pour suivre facilement les changements de tâches. Vous pouvez ajouter des cartes de tâches à partir de n'importe quelle table qui étend la tâche pour suivre rapidement les mises à jour et modifier les incidents de sécurité majeurs directement à partir du tableau.

Créer une tâche à l'aide du Tableau visuel des tâches

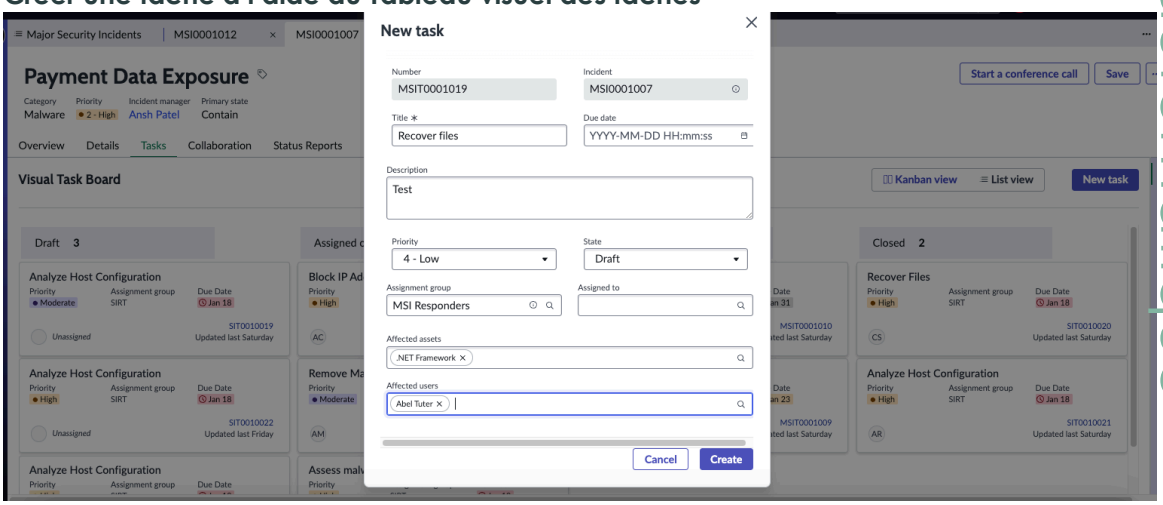
Rôle requis : sn_msi.workspace_manager.

Remarque : Assurez-vous d'avoir installé l'application **Carte de tâches MSIM VTB : 1.0.1v** séparément après l'installation de l'application MSIM.

Les gestionnaires MSI peuvent créer une tâche dans le tableau visuel des tâches en procédant comme suit :

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** .

Créer une tâche à l'aide du Tableau visuel des tâches



5. Sélectionnez **la vue Kanban**, puis choisissez **Nouvelle tâche**.
6. Renseignez les champs du formulaire.

Champ	Description
Numéro	Un numéro unique qui est généré automatiquement pour la tâche sélectionnée. Ce champ n'est pas modifiable.
Incident	Numéro d'incident de sécurité majeur. Ce champ n'est pas modifiable.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Titre	Attribuez un nom à la tâche.
Date d'échéance	Sélectionnez une date et une heure d'échéance pour l'achèvement de la tâche. Sélectionnez une date à l'aide de l'option **Calendrier** et spécifiez l'heure dans la section **Sélectionner une heure** .
Description	Fournissez une description unique pour la tâche.
Priorité	Sélectionnez la priorité de la tâche pour déterminer le moment où la tâche est exécutée. La priorité peut être l'une des valeurs suivantes : ◦ **Aucun** ◦ **1 - Critique** ◦ **2 – Élevé** ◦ **3 – Modéré** ◦ **4 : Faible** ◦ **5- Planification**
État	Sélectionnez l'état actuel de la tâche. L'état peut être l'un des suivants : ◦ **Brouillon** ◦ **Analyse** ◦ **En cours** ◦ **Fermé** L'état par défaut est **Brouillon**.
Groupe d'affectation	Sélectionnez un groupe d'affectation de l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Affecté à	Sélectionnez l'utilisateur pour affecter la tâche à l'aide de l'option de recherche.
Actifs affectés	Sélectionnez les actifs affectés par la tâche à l'aide de l'option de recherche.
Utilisateurs affectés	Sélectionnez les utilisateurs affectés par la tâche à l'aide de l'option de recherche.

Traduction automatique

7. Sélectionnez **Créer** pour créer la tâche.

Afficher et modifier une tâche à l'aide du Tableau visuel des tâches

Rôle requis : sn_msi.workspace_manager.

Remarque : Assurez-vous d'avoir installé l'application **Carte de tâches MSIM VTB : 1.0.1v** séparément après l'installation de l'application MSIM.

Les gestionnaires MSI peuvent afficher les détails d'une tâche et des informations sur l'activité à partir des intervenants MSI, et modifier une tâche dans le tableau visuel des tâches en procédant comme suit :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** , puis choisissez la **vue Kanban**.
5. Choisissez la carte de tâche souhaitée dans l'une des voies pour afficher les détails de la tâche.

   La carte de tâche peut se trouver dans l'une des voies suivantes : Brouillon, Affectée ou Prête, En cours ou Fermée.

6. Dans la section Informations sur la tâche, vous pouvez modifier les détails suivants :

Champ	Description
Numéro	Un numéro unique qui est généré automatiquement pour la tâche sélectionnée. Ce champ n'est pas modifiable.
Incident	Numéro d'incident de sécurité majeur. Ce champ n'est pas modifiable.
Titre	Attribuez un nom à la tâche.
Date d'échéance	Sélectionnez une date et une heure d'échéance pour l'achèvement de la tâche. Sélectionnez une date à l'aide de l'option **Calendrier** et spécifiez l'heure dans la section **Sélectionner une heure** .
Description	Fournissez une description unique pour la tâche.
Priorité	Sélectionnez la priorité de la tâche pour déterminer le moment où la tâche est exécutée. La priorité peut être l'une des valeurs suivantes : ◦ **Aucun** ◦ **1 - Critique** ◦ **2 – Élevé** ◦ **3 – Modéré** ◦ **4 : Faible** ◦ **5- Planification**
État	Sélectionnez l'état actuel de la tâche. L'état peut être l'un des suivants : ◦ **Brouillon** ◦ **Analyse** ◦ **En cours** ◦ **Fermé** L'état par défaut est **Brouillon**.

Traduction automatique

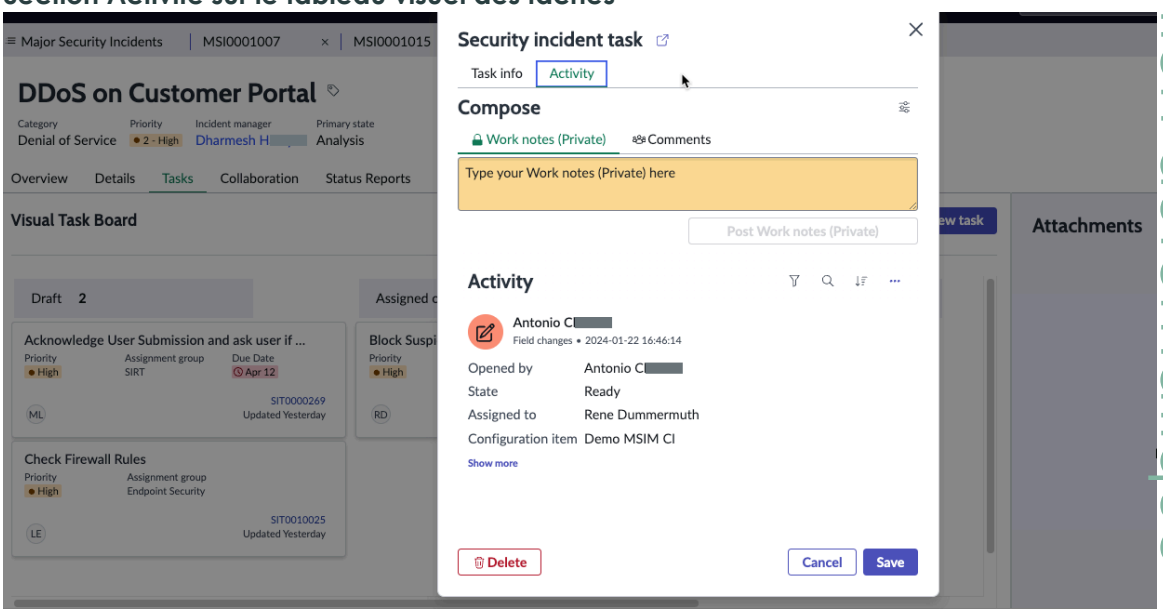
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Groupe d'affectation	Sélectionnez un groupe d'affectation de l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Affecté à	Sélectionnez l'utilisateur pour affecter la tâche à l'aide de l'option de recherche.
Actifs affectés	Sélectionnez les actifs affectés par la tâche à l'aide de l'option de recherche.
Utilisateurs affectés	Sélectionnez les utilisateurs affectés par la tâche à l'aide de l'option de recherche.

7. Sélectionnez la section **Activité** pour afficher les détails de l'activité à partir des répondeurs MSI.

   Utilisez la section Activité pour ajouter vos notes de travail et vos commentaires, publier votre activité en privé et ajouter des commentaires supplémentaires si nécessaire à l'aide de la section Composer. Enregistrez l'activité après avoir publié vos notes de travail et commentaires pour afficher l'activité ou les notes de travail ajoutées dans la section Activité.

Section Activité sur le tableau visuel des tâches



Remarque : Sélectionnez le lien **Afficher plus** de détails pour afficher les détails d'un enregistrement d'incident de sécurité spécifique, qui est associé à cet incident de sécurité majeur.

8. Sélectionnez **Enregistrer** pour mettre à jour les informations de la tâche.

   Les informations sur la tâche sont mises à jour instantanément.

Supprimer une tâche à l'aide du tableau visuel des tâches

Rôle requis : sn_msi.workspace_manager.

Remarque : Assurez-vous d'avoir installé l'application **Carte de tâches MSIM VTB : 1.0.1v** séparément après l'installation de l'application MSIM.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MSI Manager peut supprimer une tâche dans le tableau visuel des tâches en procédant comme suit :

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** , puis choisissez la **vue Kanban**
5. Choisissez la carte de tâche que vous souhaitez supprimer.
6. Dans la fenêtre contextuelle Tâche d'incident de sécurité majeur, sélectionnez l'option **Supprimer** .

   La fenêtre contextuelle Supprimer la tâche s'affiche et vous demande de confirmer la suppression de la tâche.
7. Sélectionnez **Supprimer**.

Gérer les tâches à l'aide de la vue de liste

Suivez et gérez toutes les tâches associées à un incident de sécurité majeur à l'aide de la vue Liste.

La vue de liste affiche les détails de toutes les tâches associées à l'incident de sécurité majeur, telles que le numéro de tâche, la priorité, l'état actuel, l'affectation, le groupe affecté. À l'aide de ces catégories de liste et de ces filtres, vous pouvez rapidement trouver et suivre les tâches requises sur lesquelles vous devez travailler lors d'un incident de sécurité majeur.

Créer une tâche à l'aide de la vue de liste

Rôle requis : sn_msi.workspace_manager.

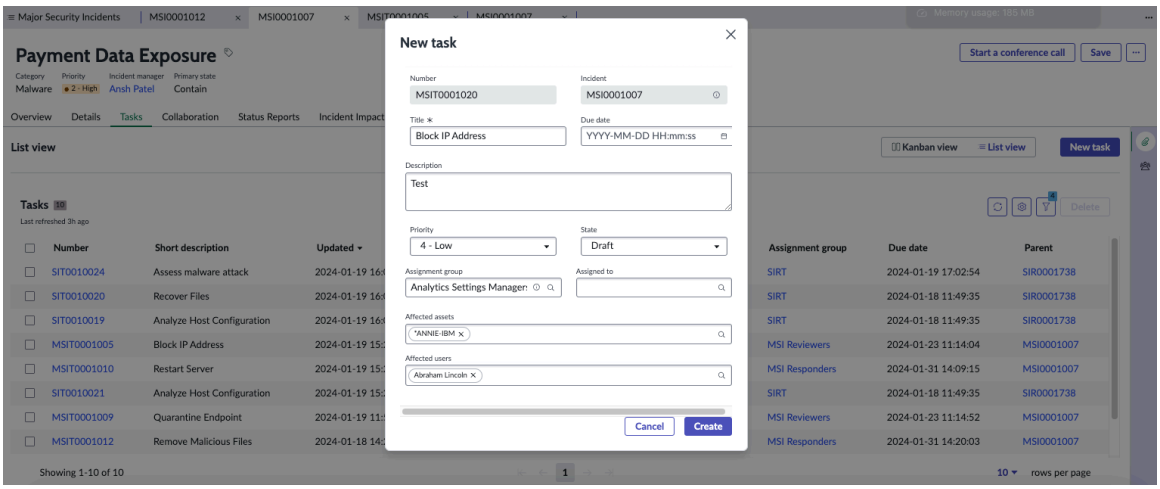
Les gestionnaires MSI peuvent créer une tâche dans la vue de liste en procédant comme suit :

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une tâche à l'aide de la vue de liste



5. Sélectionnez **Vue de liste**, puis choisissez **Nouvelle tâche**.

6. Renseignez les champs du formulaire.

Champ	Description
Numéro	Un numéro unique qui est généré automatiquement pour la tâche sélectionnée. Ce champ n'est pas modifiable.
Incident	Numéro d'incident de sécurité majeur. Ce champ n'est pas modifiable.
Titre	Attribuez un nom à la tâche.
Date d'échéance	Sélectionnez une date et une heure d'échéance pour l'achèvement de la tâche. Sélectionnez une date à l'aide de l'option **Calendrier** et spécifiez l'heure dans la section **Sélectionner une heure** .
Description	Fournissez une description unique pour la tâche.
Priorité	Sélectionnez la priorité de la tâche pour déterminer le moment où la tâche est exécutée. La priorité peut être l'une des valeurs suivantes : ◦ **Aucun** ◦ **1 - Critique** ◦ **2 : élevé** ◦ **3 – Modéré** ◦ **4 : Faible** ◦ **5- Planification**
État	Sélectionnez l'état actuel de la tâche. L'état peut être l'un des suivants : ◦ **Brouillon** ◦ **Analyse**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ **En cours** ◦ **Fermé** L'état par défaut est **Brouillon**.
Groupe d'affectation	Sélectionnez un groupe d'affectation de l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Affecté à	Sélectionnez l'utilisateur pour affecter la tâche à l'aide de l'option de recherche.
Actifs affectés	Sélectionnez les actifs affectés par la tâche à l'aide de l'option de recherche.
Utilisateurs affectés	Sélectionnez les utilisateurs affectés par la tâche à l'aide de l'option de recherche.

7. Sélectionnez **Créer** pour créer la tâche.

Afficher et modifier une tâche à l'aide de la vue de liste

Rôle requis : sn_msi.workspace_manager.

Les gestionnaires MSI peuvent afficher les détails d'une tâche et des informations sur l'activité à partir des intervenants MSI, et modifier une tâche dans la vue de liste en procédant comme suit

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** , puis choisissez **la vue Liste**.
5. Choisissez la tâche souhaitée dans la vue de liste pour afficher les détails de la tâche.
6. Dans la section Informations sur la tâche, vous pouvez modifier les détails suivants :

Champ	Description
Numéro	Un numéro unique qui est généré automatiquement pour la tâche sélectionnée. Ce champ n'est pas modifiable.
Incident	Numéro d'incident de sécurité majeur. Ce champ n'est pas modifiable.
Titre	Attribuez un nom à la tâche.
Date d'échéance	Sélectionnez une date et une heure d'échéance pour l'achèvement de la tâche. Sélectionnez une date à l'aide de l'option **Calendrier** et spécifiez l'heure dans la section **Sélectionner une heure** .
Description	Fournissez une description unique pour la tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Priorité	Sélectionnez la priorité de la tâche pour déterminer le moment où la tâche est exécutée. La priorité peut être l'une des valeurs suivantes : ◦ **Aucun** ◦ **1 - Critique** ◦ **2 : élevé** ◦ **3 – Modéré** ◦ **4 : Faible** ◦ **5- Planification**
État	Sélectionnez l'état actuel de la tâche. L'état peut être l'un des suivants : ◦ **Brouillon** ◦ **Analyse** ◦ **En cours** ◦ **Fermé** L'état par défaut est **Brouillon**.
Groupe d'affectation	Sélectionnez un groupe d'affectation de l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Affecté à	Sélectionnez l'utilisateur pour affecter la tâche à l'aide de l'option de recherche.
Actifs affectés	Sélectionnez les actifs affectés par la tâche à l'aide de l'option de recherche.
Utilisateurs affectés	Sélectionnez les utilisateurs affectés par la tâche à l'aide de l'option de recherche.

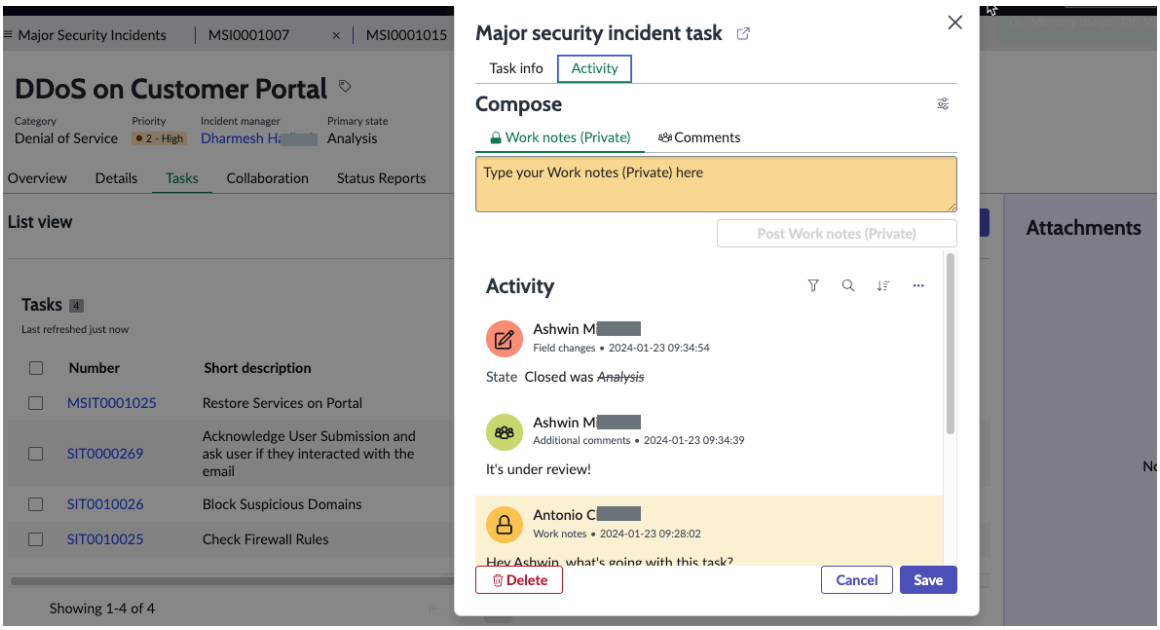
7. Sélectionnez la section **Activité** pour afficher les détails de l'activité à partir des répondeurs MSI.

   Utilisez la section Activité pour ajouter vos notes de travail et vos commentaires, publier votre activité en privé et ajouter des commentaires supplémentaires si nécessaire à l'aide de la section Composer. Enregistrez l'activité après avoir publié vos notes de travail et commentaires pour afficher l'activité ou les notes de travail ajoutées dans la section Activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Section Activité de la vue de liste



Remarque : Sélectionnez le lien **Afficher plus** de détails pour afficher les détails d'un enregistrement d'incident de sécurité spécifique, qui est associé à cet incident de sécurité majeur.

8. Sélectionnez **Enregistrer** pour mettre à jour les informations de la tâche.

   Les informations sur la tâche sont mises à jour instantanément.

9. Vous pouvez également effectuer les actions suivantes dans la vue de liste :
   a. Sélectionnez l'icône **Actualiser** pour actualiser la liste de tâches dans la vue de liste.
   b. Sélectionnez l'icône **Paramètres** , puis utilisez l'option **Modifier les colonnes** pour modifier la liste des colonnes qui apparaissent dans la vue de liste. Utilisez l'option **Réinitialiser les largeurs** pour réinitialiser les largeurs des colonnes.

Supprimer une tâche à l'aide de la vue de liste

Rôle requis : sn_msi.workspace_manager.

MSI Manager peut supprimer une tâche dans la vue de liste en procédant comme suit :

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** .
5. Sélectionnez **la vue Liste**.
6. Choisissez une tâche que vous souhaitez supprimer de la liste.
7. Dans la fenêtre contextuelle Tâche d'incident de sécurité majeur, sélectionnez l'option **Supprimer** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La fenêtre contextuelle Supprimer la tâche s'affiche et vous demande de confirmer la suppression de la tâche.

8. Sélectionnez **Supprimer**.

Suivre l'activité de collaboration via l'espace MSIM de travail

Suivez les activités de messagerie instantanée et de fichier liées à la résolution d'incidents de sécurité majeurs via l'espace de travail MSIM.

Les activités sont coordonnées à l'aide Microsoft Teams de la messagerie instantanée Microsoft SharePoint , de fichiers et de dossiers, puis renvoyées via les Incident de sécurité majeur intégrations.

Une fois Microsoft Teams Microsoft SharePoint intégré à Gestion des incidents de sécurité majeurs, vous pouvez utiliser l'espace de travail pour suivre la collaboration entre les MSIM utilisateurs de la réponse aux incidents et d'autres groupes qui contribuent à la résolution d'un incident de sécurité majeur. Toutes les mises à jour des dossiers et des fichiers de collaboration sont Microsoft SharePoint synchronisées avec l'espace de MSIM travail File Explorer et reflétées dans les composants du flux d'activité.

Lorsqu'un incident de sécurité est promu en incident de sécurité majeur :

1. Une structure de dossiers sera créée en Microsoft SharePoint fonction de la configuration du modèle de dossier. La même structure de dossiers sera reflétée sur le composant de l'espace File Explorer de travail.
2. Une équipe avec plusieurs canaux est créée sous Microsoft Teams l'application et la même chose sera reflétée dans le composant Gestion de la messagerie instantanée de l'espace de travail.

Rôle requis : sn_msi.workspace_manager.

Interagir avec les fichiers et les dossiers

L'Explorateur de fichiers affiche le système de fichiers afin que vous puissiez afficher et interagir avec les fichiers et dossiers liés à la résolution de l'incident.

Affiche le fichier et les dossiers qui sont capturés sur Microsoft SharePoint pour un incident de sécurité spécifique. Ces dossiers seront automatiquement créés sur Microsoft SharePoint pour cet incident de sécurité majeur. Vous pouvez utiliser ces dossiers créés par défaut pour charger des fichiers de support, si nécessaire. Vous pouvez renommer, déplacer ou supprimer ces fichiers et dossiers selon vos besoins.

De plus, chaque fois que vous chargez un fichier dans l'un des dossiers, l'activité correspondant à ces dossiers sera automatiquement associée aux dossiers de l'Explorateur de fichiers dans l'onglet Collaboration et l'activité sera enregistrée et affichée dans la section Activité de l'espace de travail Major Security Incident Management.

Remarque : Dans l'onglet **Collaboration** , l'enregistrement d'incident est ajouté au fichier parent sur SharePoint avec un numéro d'incident et une catégorie d'incident uniques.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. **Vue du référentiel** : répertorie les fichiers et dossiers répertoriés dans Microsoft SharePoint pour cet incident de sécurité spécifique. Pour chaque fichier ou dossier, la vue du référentiel affiche le nom, la modification, la dernière modification et la taille.

Vue du référentiel

Champ	Description
Ouvrir dans SharePoint	Sélectionnez cette option disponible en regard de votre incident de sécurité majeur. Cliquez sur le lien pour sélectionner et afficher la structure de dossiers dans Microsoft SharePoint.
Nouveau dossier	Sélectionnez cette option pour créer un nouveau dossier selon vos besoins. Une fois que vous avez créé un dossier, le même dossier est créé et associé dans votre Microsoft SharePoint, par défaut.

2. **Récents** : affiche tous les journaux d'activité récents. Ces journaux incluent à la fois vos activités SharePoint et Explorateur de fichiers. Les activités récentes sont généralement vos fichiers de support, qui incluent le dossier parent.

   Voici la procédure pour **localiser le fichier journal :**

   a. Sélectionnez le fichier respectif pour afficher les détails.

   b. Cliquez sur **Localiser le fichier**.

   Remarque : La navigation et les détails du fichier parent et des dossiers parents sont affichés sous la section Vue de liste **Récents** . Vous pouvez ouvrir le même fichier dans votre SharePoint. Chaque fois que vous chargez les fichiers journaux connexes ou des activités, tous ces fichiers et activités s'affichent à la fois dans SharePoint et dans l'Explorateur de fichiers.

Gérer les communications des canaux de messagerie instantanée à l'aide de Microsoft Teams

Le gestionnaire de canaux de messagerie instantanée affiche Microsoft Teams avec plusieurs canaux créés dans l'application Microsoft Teams en fonction d'une configuration de modèle de configuration.

Ces canaux configurés sont reflétés dans le composant Gestion de la messagerie instantanée avec les utilisateurs et les groupes d'utilisateurs qui leur sont affectés. Le gestionnaire de canaux de messagerie instantanée vous permet d'effectuer les actions suivantes :

- **Gérer les canaux de messagerie instantanée**
- **Renommer l'équipe**
- **Gérer les membres de votre équipe**

L'équipe et les canaux sont créés en fonction de la configuration du canal de messagerie instantanée dans Microsoft Teams.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer les canaux de messagerie instantanée

Le gestionnaire de canaux de messagerie instantanée vous permet de créer, modifier ou supprimer des canaux de messagerie instantanée. Pour gérer un canal de messagerie instantanée dans Microsoft Teams, procédez comme suit :

1. Sélectionnez l'onglet **Collaboration** .
2. Accédez à la **Gestionnaire de canal de messagerie instantanée** > **Créer un canal**.
3. Ajoutez un nouveau **nom** et une nouvelle **description** pour le canal, et sélectionnez les **membres** du canal.
4. Sélectionnez **Créer**.

> **Remarque :** Un nouvel enregistrement de canal est créé dans la section Canaux Microsoft Teams de l'application Microsoft Teams et le même enregistrement sera reflété dans MSIM.

5. Pour modifier un canal de messagerie instantanée, sélectionnez-en un dans la liste Gestionnaire de canaux de messagerie instantanée.
6. Vous pouvez modifier le nom du canal, la liste des membres, la liste des membres du groupe en fonction de vos besoins.
7. Sélectionnez **Enregistrer**.
8. Pour supprimer un canal de messagerie instantanée, sélectionnez-en un dans la liste Gestionnaire de canaux de messagerie instantanée.
9. Sélectionnez **Supprimer un canal**.

Renommer l'équipe

Pour renommer une équipe dans Microsoft Teams, procédez comme suit :

1. Sélectionnez l'onglet **Collaboration** .
2. Accédez à la **Gestionnaire de canal de messagerie instantanée** > **Renommer l'équipe**.
3. Dans le champ Nom de l'équipe, renommez l'équipe en fonction de vos besoins.
4. Sélectionnez **Enregistrer**.

> **Remarque :** Renommer le nom de l'équipe renomme également le nom de l'équipe dans Microsoft Teams.

Gérer les membres de votre équipe

Le gestionnaire de canaux de messagerie instantanée vous permet d'ajouter ou de supprimer des membres de l'équipe dans Microsoft Teams. Vous pouvez également ajouter des membres via des groupes. Pour gérer les membres de l'équipe dans Microsoft Teams, procédez comme suit :

1. Sélectionnez l'onglet **Collaboration** .
2. Accédez à la **Gestionnaire de canal de messagerie instantanée** > **Gérer les membres de votre équipe**.
3. Dans le champ Membres, ajoutez ou supprimez des membres de l'équipe en fonction de vos besoins.
4. Dans le champ Ajouter des membres via des groupes, sélectionnez les groupes que vous souhaitez ajouter dans Microsoft Teams.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si les membres du groupe font déjà partie de l'équipe, ces membres ne sont pas ajoutés.

5. Sélectionnez **Enregistrer**.

   Le gestionnaire de canaux de messagerie instantanée affiche les détails du nombre total de membres de l'équipe et le nombre de nouveaux membres qui seront ajoutés.

Gérer les communications des canaux de messagerie instantanée à l'aide de Slack

Le gestionnaire de canaux de messagerie instantanée affiche Slack avec plusieurs canaux créés dans l'application Slack en fonction d'une configuration de modèle de configuration.

Ces canaux configurés sont reflétés dans le composant Gestion de la messagerie instantanée avec les utilisateurs et les groupes d'utilisateurs qui leur sont affectés. Le gestionnaire de canaux de messagerie instantanée vous permet de **gérer les canaux de messagerie instantanée**. L'équipe et les canaux sont créés en fonction de la configuration du canal de messagerie instantanée dans Slack.

Gérer les canaux de messagerie instantanée

Le gestionnaire de canaux de messagerie instantanée vous permet de créer, modifier ou supprimer des canaux de messagerie instantanée dans Slack. Pour gérer un canal de messagerie instantanée, procédez comme suit :

1. Sélectionnez l'onglet **Collaboration** .
2. Accédez à la **Gestionnaire de canal de messagerie instantanée** > **Créer un canal**.
3. Ajoutez un nouveau **nom** et une nouvelle **description** pour le canal, et sélectionnez les **membres** du canal.
4. Sélectionnez **Créer**.

   Remarque : Un nouvel enregistrement de canal est créé dans la section Canaux Slack de l'application Slack et le même enregistrement est reflété dans MSIM.

5. Pour modifier un canal de messagerie instantanée, sélectionnez-en un dans la liste Gestionnaire de canaux de messagerie instantanée.
6. Vous pouvez modifier le nom du canal, la liste des membres, la liste des membres du groupe en fonction de vos besoins.
7. Sélectionnez **Enregistrer**.
8. Pour supprimer un canal de messagerie instantanée, sélectionnez-en un dans la liste Gestionnaire de canaux de messagerie instantanée.
9. Sélectionnez **Supprimer un canal**.

Gérer les conversations de flux d'activité

Affiche l'ensemble des activités, des journaux, de l'état qui ont été exécutés sur , l'explorateur Microsoft SharePointde fichiers et Microsoft Teams.

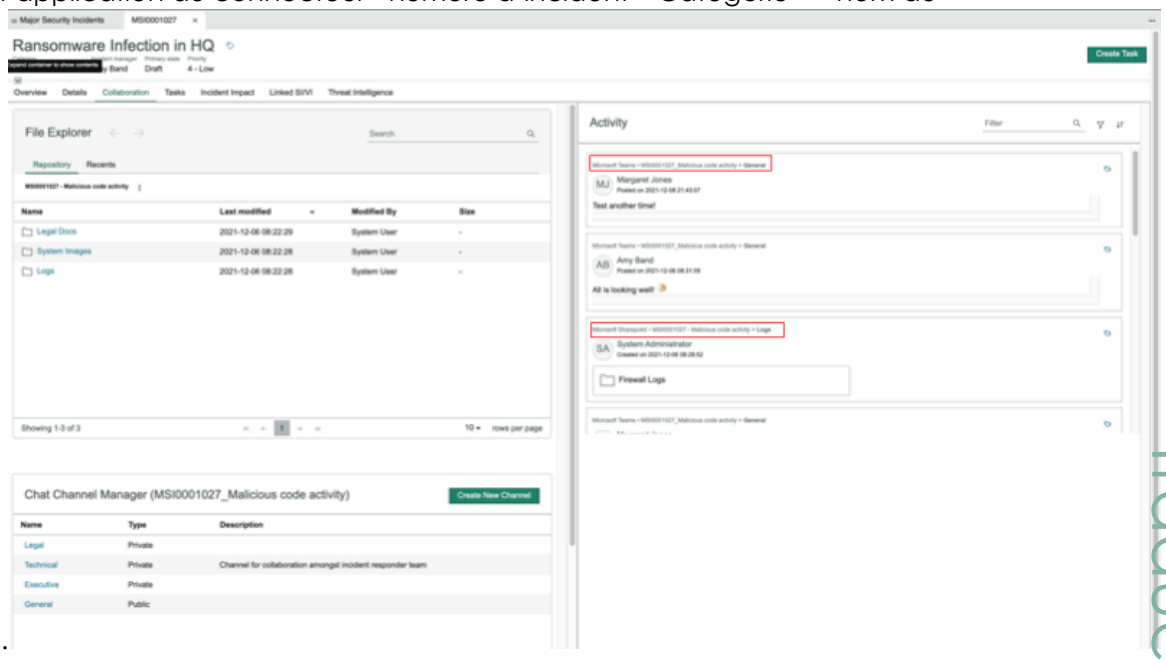
Si vous souhaitez afficher une activité spécifique ou rechercher les détails de l'activité de collaboration qui ont été interagies entre différents fichiers et dossiers, ainsi que sur Microsoft Teams, vous pouvez utiliser la fonction de filtre qui s'affiche en haut à droite de la section Flux d'activité et localiser les détails de l'activité souhaitée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

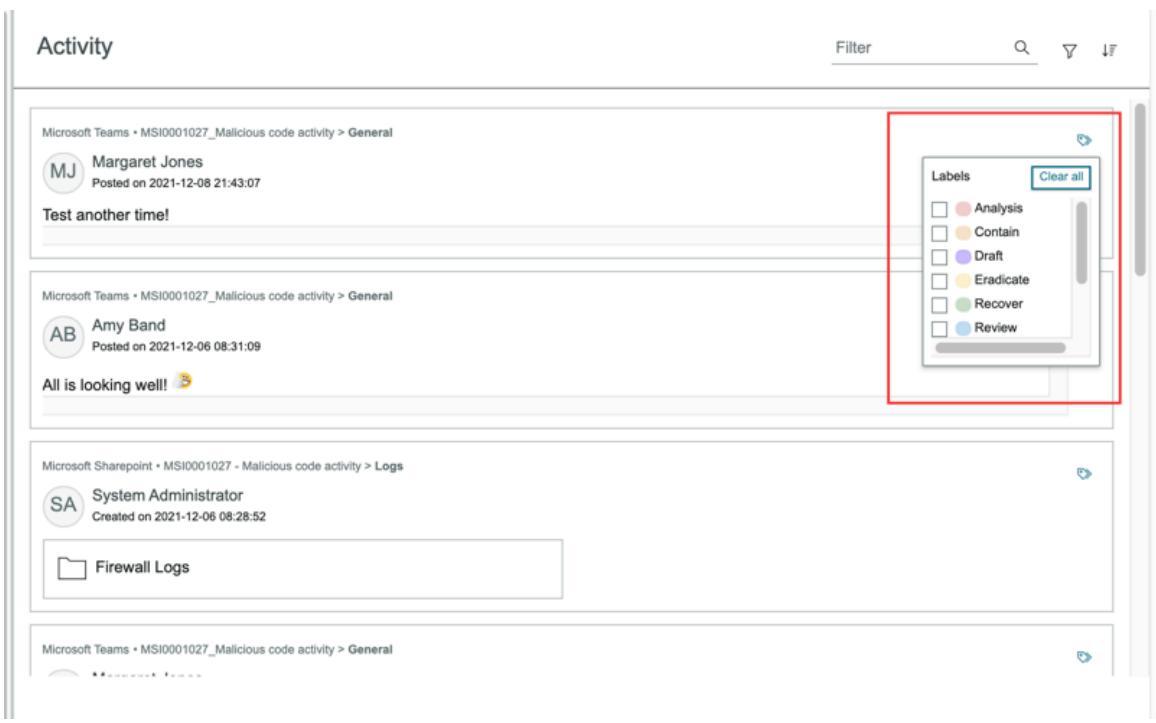
Les dossiers et les conversations de messagerie instantanée partagés avec la Gestion des incidents de sécurité majeurs sont considérés comme des fils d'Ariane avec la structure :

Nom de l'application du connecteur <numéro d'incident – Catégorie > <nom du dossier>).



Étiquetez les activités :

1. Cliquez sur l'icône **Étiquette** .
2. Cochez la case correspondant à l'étiquette d'activité de l'incident, comme indiqué dans la capture d'écran ci-dessous.



3. Les activités étiquetées sont codées par couleur et représentées sous forme de graphique de tendance de progression dans la section **Collaboration externe** de l'espace de travail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer et distribuer MSIM des rapports d'état

Incident de sécurité majeur En tant que gestionnaire, vous pouvez créer et distribuer les différents rapports d'état à différentes personnes concernées à différents intervalles en fonction du modèle de rapport configuré ou d'un rapport d'état précédent tout au long de la résolution de l'incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Vous pouvez prévisualiser les éléments de données du rapport de résumé précédemment configurés, ajouter du texte ou un résumé supplémentaire, supprimer des composants de rapport individuels si nécessaire et vérifier l'exactitude et l'exhaustivité du rapport avant de le distribuer à différentes personnes concernées.

Créez les rapports d'état en sélectionnant le modèle de rapport souhaité initialement configuré sur la page Configuration des modèles de rapport MSI.

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Sélectionnez l'enregistrement MSI promu respectif.
4. Sélectionnez l'onglet **Rapports d'état** .
   L'onglet Rapports d'état contient trois types différents de sous-sections, comme ci-dessous.

Champ	Description
Nom du rapport	Nom du modèle de rapport d'état. **Remarque :** La vue Rapports d'état répertorie les modèles de rapport prédéfinis existants qui sont disponibles dans le système de base pour le profil concerné. Par exemple, les rapports d'état de la haute direction par courriel (adaptés aux appareils mobiles), les rapports d'état technique et les rapports d'état de la direction au format PDF.
Mis à jour	Date à laquelle le modèle de rapport a été mis à jour pour la dernière fois.
Type de rapport	Type de rapport d'état. Le rapport d'état peut être de l'un des types suivants : ◦ PDF ◦ E-mail
État	État des rapports d'état. Les rapports d'état peuvent se trouver dans l'un des états suivants :

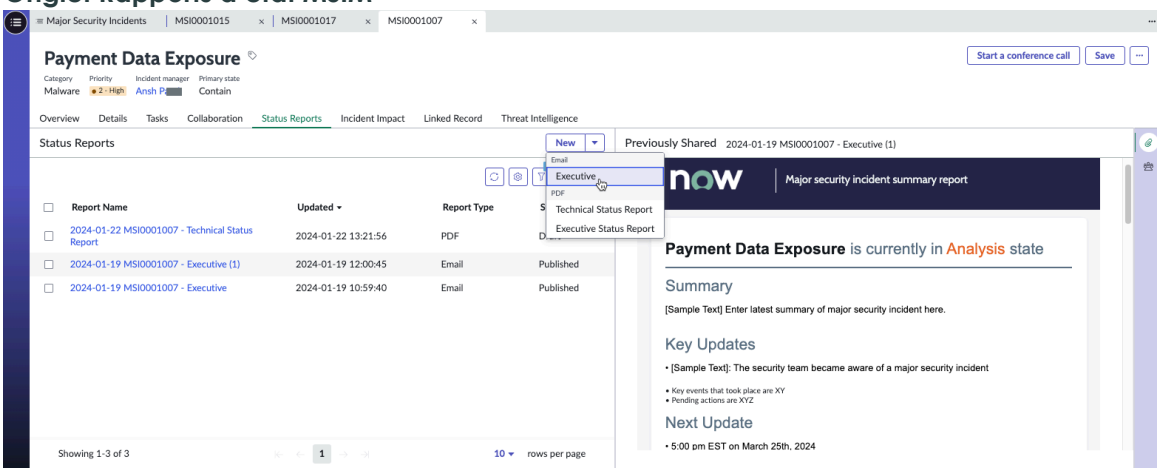
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Brouillon ◦ Mis en file d'attente ◦ Publié

5. Sélectionnez le type de rapport d'état que vous souhaitez afficher ou sélectionnez **Nouveau** pour créer un rapport d'état.

Onglet Rapports d'état MSIM



6. Choisissez l'un des types de rapports d'état suivants dans la liste.
   - **Exécutif** Rapports d'état des e-mails adaptés aux mobiles.
   - **Rapport d'état technique** PDF
   - **Rapport d'état de la direction** PDF

   Remarque : Lorsque vous sélectionnez un modèle de rapport souhaité, l'aperçu du rapport sélectionné est immédiatement généré dans le volet droit. Vous pouvez afficher le rapport d'état sélectionné du MSI.

7. Dans le modèle Rapport d'état d'e-mail de la direction, renseignez les sections avec les détails du rapport d'état.

Section de rapport	Description
Mises à jour	Fournissez un résumé de la mise à jour de statut. Cette section contient les éléments suivants : ◦ **Résumé MSI** : fournissez un bref résumé de l'incident de sécurité majeur. ◦ **Ajouter le texte du dernier rapport partagé** : sélectionnez cette option pour ajouter le texte du dernier rapport partagé.
Explication	Ajoutez une explication sur ce qui a changé depuis la dernière mise à jour de statut. Cette section contient les éléments suivants : ◦ **Mises à jour clés** : fournissez des mises à jour clés telles que ce que l'équipe de sécurité doit savoir sur l'incident de sécurité majeur, nommez

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

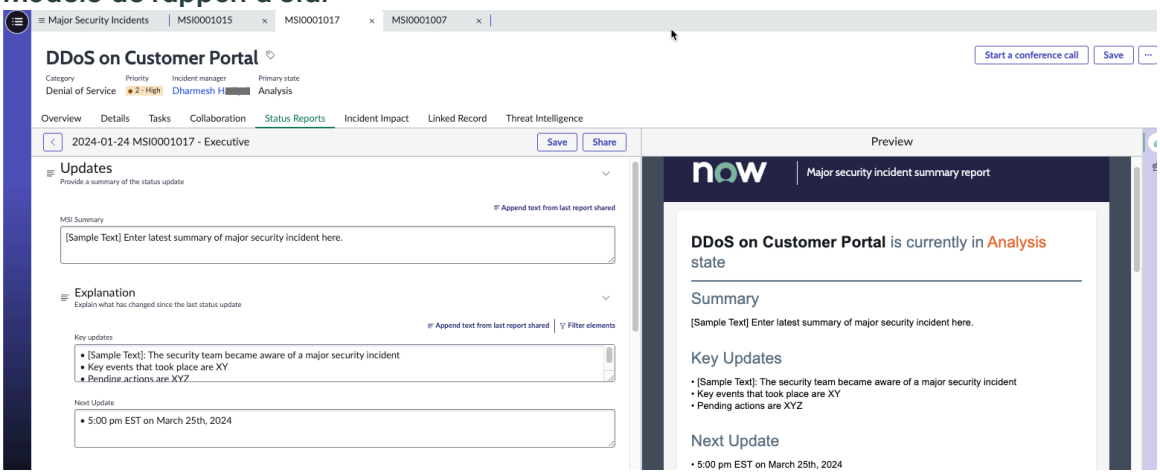
Section de rapport	Description
	les événements clés qui ont eu lieu et répertoriez toutes les actions en attente. ◦ **Prochaine mise à jour** : indiquez la date et l'heure de la prochaine mise à jour pour résoudre l'incident de sécurité majeur. Par exemple, 17h00 HNE le 25 mars 2024. ◦ **Ajouter le texte du dernier rapport partagé** : sélectionnez cette option pour ajouter le texte du dernier rapport partagé. ◦ **Éléments de filtre** : sélectionnez les éléments de rapport à inclure dans le rapport. Par exemple, Mises à jour clés ou Prochaines mises à jour.
Informations supplémentaires	Fournissez des détails spécifiques pertinents pour la mise à jour de l'état.
Visualisations	Sélectionnez les visualisations qui aident le mieux à communiquer la mise à jour de statut. ◦ **Impact de l'incident** : sélectionnez les mesures de l'impact de l'incident telles que Actifs affectés, Emplacement affecté, Utilisateurs affectés qui sont associées à la mise à jour de l'état. ◦ **Éléments de filtre** : sélectionnez les éléments de rapport à inclure dans le rapport. Par exemple, Impact d'un incident.
Listes	Sélectionnez des listes d'enregistrements qui fournissent un contexte à la mise à jour de statut. ◦ **Enregistrements liés** : sélectionnez les enregistrements qui sont liés à la mise à jour de l'état de l'incident de sécurité majeur. Par exemple, Incident de sécurité lié. ◦ **Éléments de filtre** : sélectionnez les éléments de rapport à inclure dans le rapport. Par exemple, Enregistrements liés.

Remarque : Les options que vous avez sélectionnées dans la section Rapports d'état sont les mêmes que celles affichées dans le rapport d'aperçu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modèle de rapport d'état



8. Sélectionnez **Enregistrer** pour enregistrer les mises à jour que vous avez apportées au rapport d'état.
9. Sélectionnez **Partager** pour partager le rapport d'état avec les personnes concernées internes et externes.
   La boîte de dialogue Partager s'affiche.

   a. Dans le champ Objet, saisissez l'objet du rapport d'e-mail.

   b. Dans le champ Ajouter des destinataires internes, tapez et sélectionnez les destinataires du rapport d'e-mail.

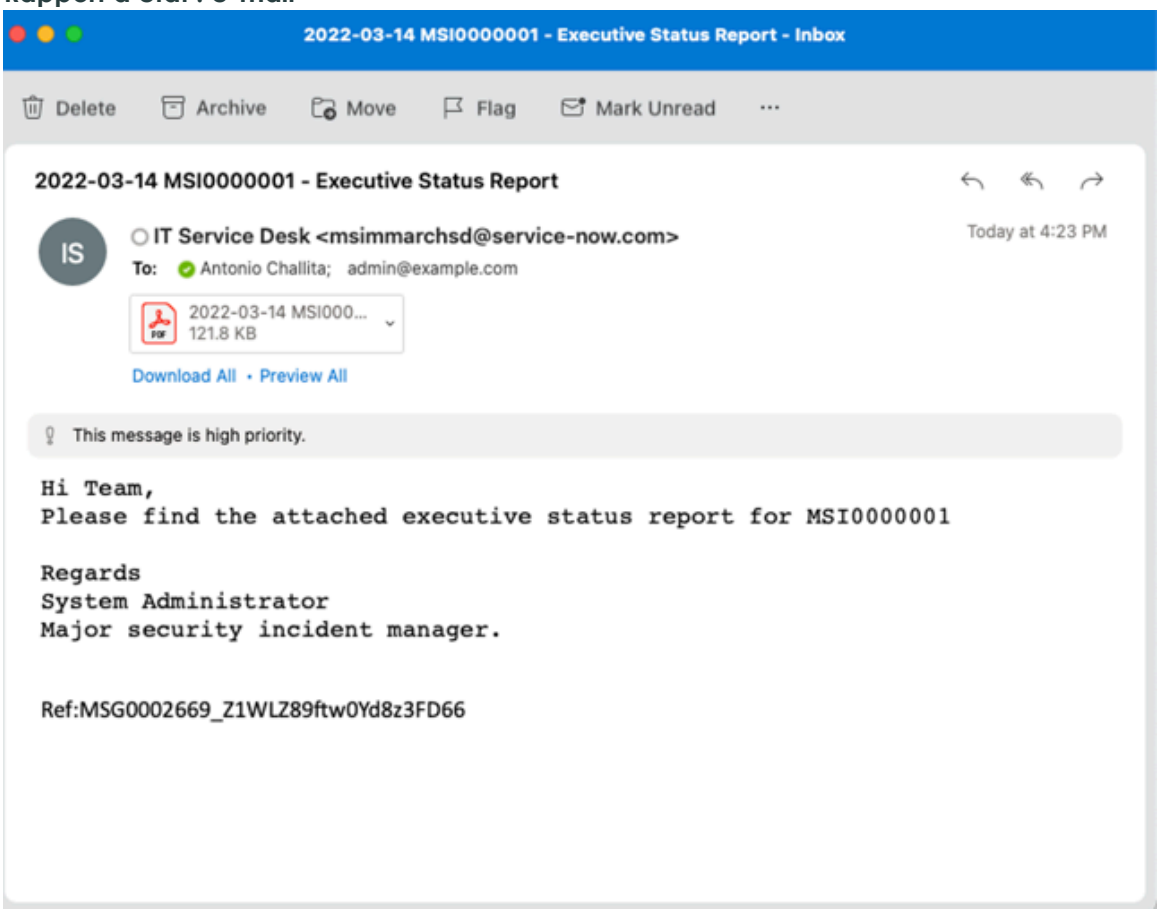
   c. Dans le champ Ajouter des destinataires externes, saisissez l'e-mail des destinataires ou le DL pour le rapport d'e-mail.
   Vous pouvez ajouter plusieurs ID d'e-mail à l'aide d'une virgule ou d'un point-virgule.

10. Sélectionnez **Envoyer le rapport par e-mail**.
    Un e-mail avec le rapport d'état PDF en pièce jointe est envoyé avec succès au destinataire concerné pour qu'il le vérifie.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapport d'état : e-mail



11. Vous pouvez également effectuer les actions suivantes dans l'onglet Rapports d'état :
    a. Utilisez l'action **Actualiser** de la vue Rapports d'état pour actualiser la liste des rapports d'état.
    b. Utilisez l'action **Actions de** liste de la vue Rapports d'état pour modifier des colonnes ou réinitialiser les largeurs de la liste des rapports d'état.
    c. Utilisez l'action **Filtrer** de la vue Rapports d'état pour filtrer les rapports d'état en fonction de certaines conditions.

Information associée

Configurer les Incident de sécurité majeur rapports d'état

Gestion des rapports d'état MSIM

Les rapports d'état fournissent des graphiques de tendance préconfigurés avec des visualisations de données exploitables pour améliorer les processus des opérations de sécurité, mesurer et analyser la chronologie de résolution, le nombre de retards et l'état de chaque tâche affectée.

Configurer les Incident de sécurité majeur rapports d'état

Configurez les rapports d'incidents de sécurité majeurs pour configurer et télécharger les rapports en fonction des besoins de votre entreprise tout au long du cycle de vie du processus de rattrapage des enregistrements d'incidents de sécurité majeurs.

Vous pouvez créer des modèles de rapport avec un format et une mise en page spécifiques et personnaliser ces rapports en fonction de vos besoins spécifiques à l'aide de la

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

fonctionnalité Rapports d'état de l'espace Gestion des incidents de sécurité majeurs de travail.

Un utilisateur disposant du rôle sn_msi.workspace_manager peut créer et configurer des modèles de rapport qui décrivent le type d'informations sur le rapport qui peut être utilisé pour générer tous les rapports d'état, qui peuvent être partagés avec des utilisateurs spécifiques tels que les personnes concernées par la direction, les services juridiques, et mapper ces modèles sur les enregistrements d'incidents de sécurité majeurs.

Pour personnaliser vos rapports d'état MSI, vous devez d'abord configurer les modèles de rapport à l'aide **de modèles de rapport.** À l'aide des modèles de rapport, vous pouvez créer les types de modèles de rapport, définir les composants de rapport pour ces modèles de rapport, ajouter des informations supplémentaires, créer des données visualisées pour suivre les mesures de portée et de progression, ajouter des données de liste connexe et générer des rapports d'état.

Ce qui suit décrit les champs par défaut fournis dans tous les types de modèles de rapport. Vous pouvez configurer et formater le modèle de rapport en fonction de vos besoins à l'aide de sections, de sous-sections et de ses éléments :

Composants de rapports d'état

Type de composant	Description
Titre de rapport	Titre du type de rapport. Par exemple, le format par défaut du type de rapport est le suivant : {MSI Number} - {Executive Stakeholder Report} représenté comme MSI0001001 : Executive Stakeholder Report.
Nom	Affiche le nom de l'utilisateur qui a généré le rapport à l'aide de la section Rapports d'état de l'espace de travail Major Security Incident Management.
Résumé	Affiche un bref résumé du rapport.
Date	Affiche la date à laquelle le rapport est partagé avec le destinataire concerné.
Progression	Affiche les mesures du champ d'application et de l'avancement telles que les incidents SIR liés, les tâches de réponse, les tâches supplémentaires, la collaboration externe, les composants de chronologie et les événements de chronologie récents.
Défis	Cette section affiche une brève description des défis à relever tout au long du processus de rattrapage d'un incident de sécurité majeur.
Étapes suivantes	Cette section affiche une brève description des étapes suivantes impliquées dans la résolution de l'incident de sécurité majeur. Par exemple, la sous-section Équipe active du rapport des parties prenantes de la direction vous fournit des informations lors de l'étape suivante de l'affectation de l'équipe qui est impliquée dans une analyse plus

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composants de rapports d'état (suite)

Type de composant	Description
	approfondie de l'enregistrement d'incident de sécurité majeur.
Autres personnalisations	Le modèle de rapport vous offre également la possibilité de charger le logo et de personnaliser les en-têtes et les pieds de page du rapport.

Voici les types de catégories de rapport qui peuvent être configurés et visualisés :

- **Exécutif** Messagerie électronique
- **Rapport d'état technique** PDF
- **Rapport d'état de la direction** PDF

Les rapports ci-dessus sont configurés et disponibles pour que l'utilisateur les sélectionne, les affiche et les génère à partir de l'espace de travail Major Security Incident Management.

Rapports d'état de la direction adaptés aux appareils mobiles - E-mail

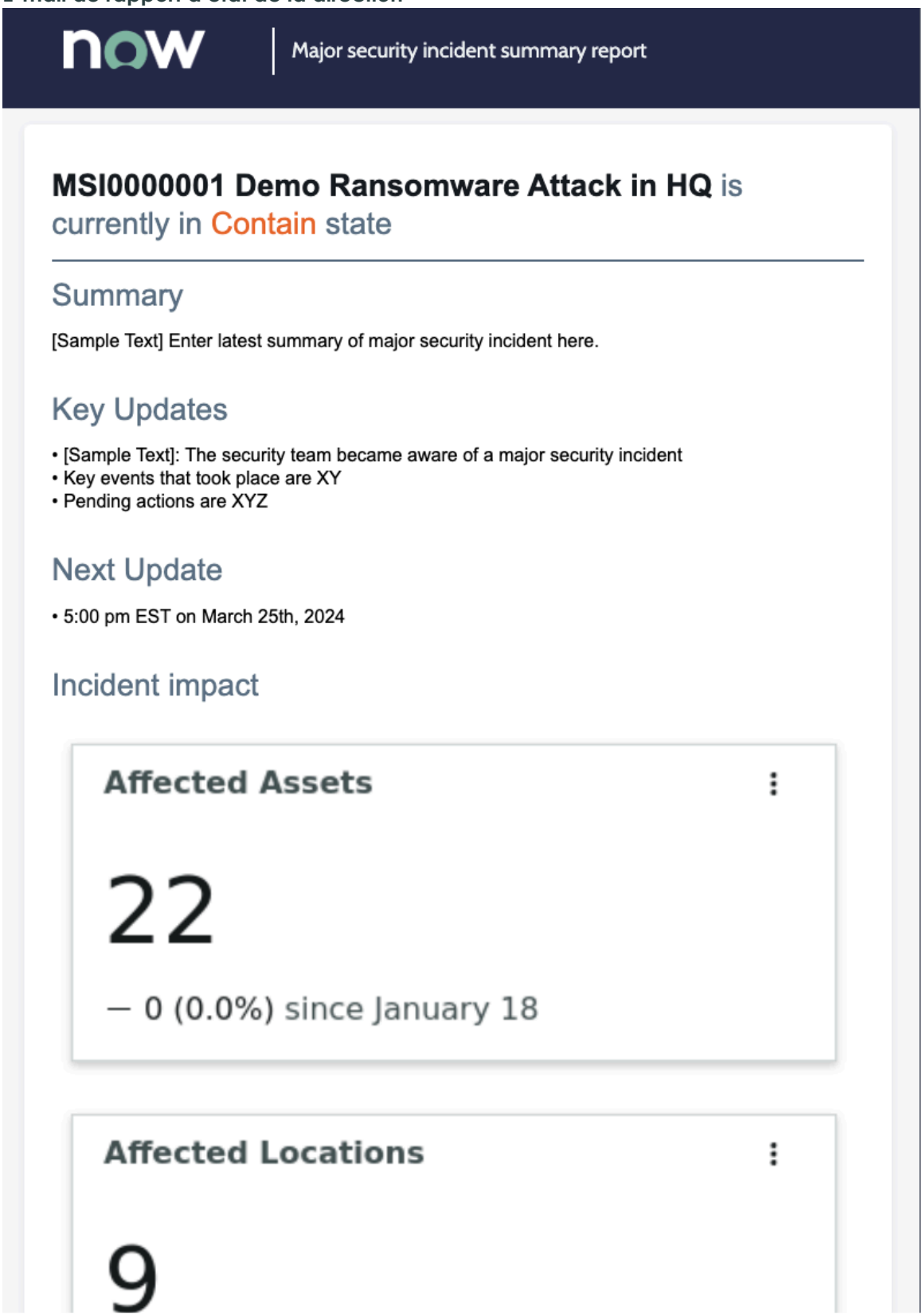
Les rapports d'état de la direction - E-mail sont des rapports d'état adaptés aux appareils mobiles qui sont générés sous forme d'e-mail. La section Rapport comprend un résumé du rapport, la colonne Durée MSI, le périmètre/l'impact de l'incident, les mesures de l'équipe active, les mesures de progression et des composants de chronologie tels que les événements de chronologie récents pour cet enregistrement spécifique d'incident de sécurité majeur.

Personnalisez et configurez les fonctionnalités de modèle de rapport suivantes pour ajouter des informations supplémentaires au rapport. Un exemple de rapport d'état des e-mails de la direction est présenté ci-dessous à titre de référence.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

E-mail de rapport d'état de la direction



Traduction automatique

Rapports d'état de la haute direction - PDF

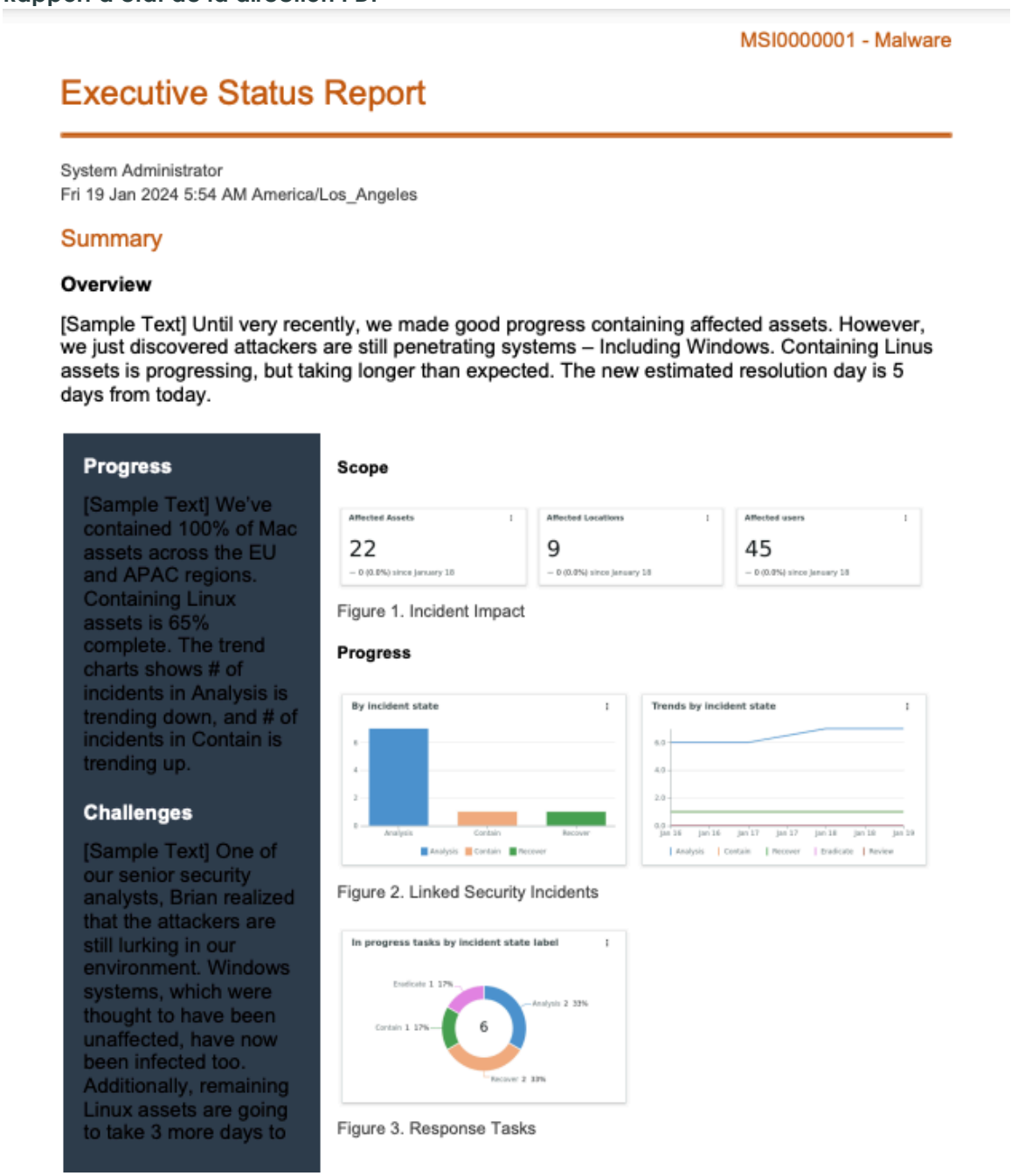
Les rapports d'état de la direction - PDF sont des rapports d'état qui sont générés au format PDF. La section Rapport comprend un résumé du rapport, la colonne Durée MSI, le périmètre/l'impact de l'incident, les mesures de l'équipe active, les mesures de progression

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

et des composants de chronologie tels que les événements de chronologie récents pour cet enregistrement spécifique d'incident de sécurité majeur.

Personnalisez et configurez les fonctionnalités de modèle de rapport suivantes pour ajouter des informations supplémentaires au rapport. Un exemple de rapport exécutif est présenté ci-dessous à titre de référence.

Rapport d'état de la direction PDF



MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets: 22
Affected Locations: 9
Affected users: 45

Figure 1. Incident Impact

Progress

By incident state

Trends by incident state

Figure 2. Linked Security Incidents

In progress tasks by incident state label

Figure 3. Response Tasks

Rapports d'état technique - PDF

Les rapports d'état technique - PDF sont des rapports d'état qui sont générés au format PDF. La section du rapport comprend un résumé du rapport, la colonne de durée MSI, le périmètre/l'impact de l'incident, les mesures de l'équipe active, les mesures de progression et des composants de chronologie tels que les événements de chronologie récents pour cet enregistrement d'incident de sécurité majeur spécifique, les mises à jour des tâches étiquetées et les activités étiquetées, en fonction du groupe d'affectation et de l'étiquette

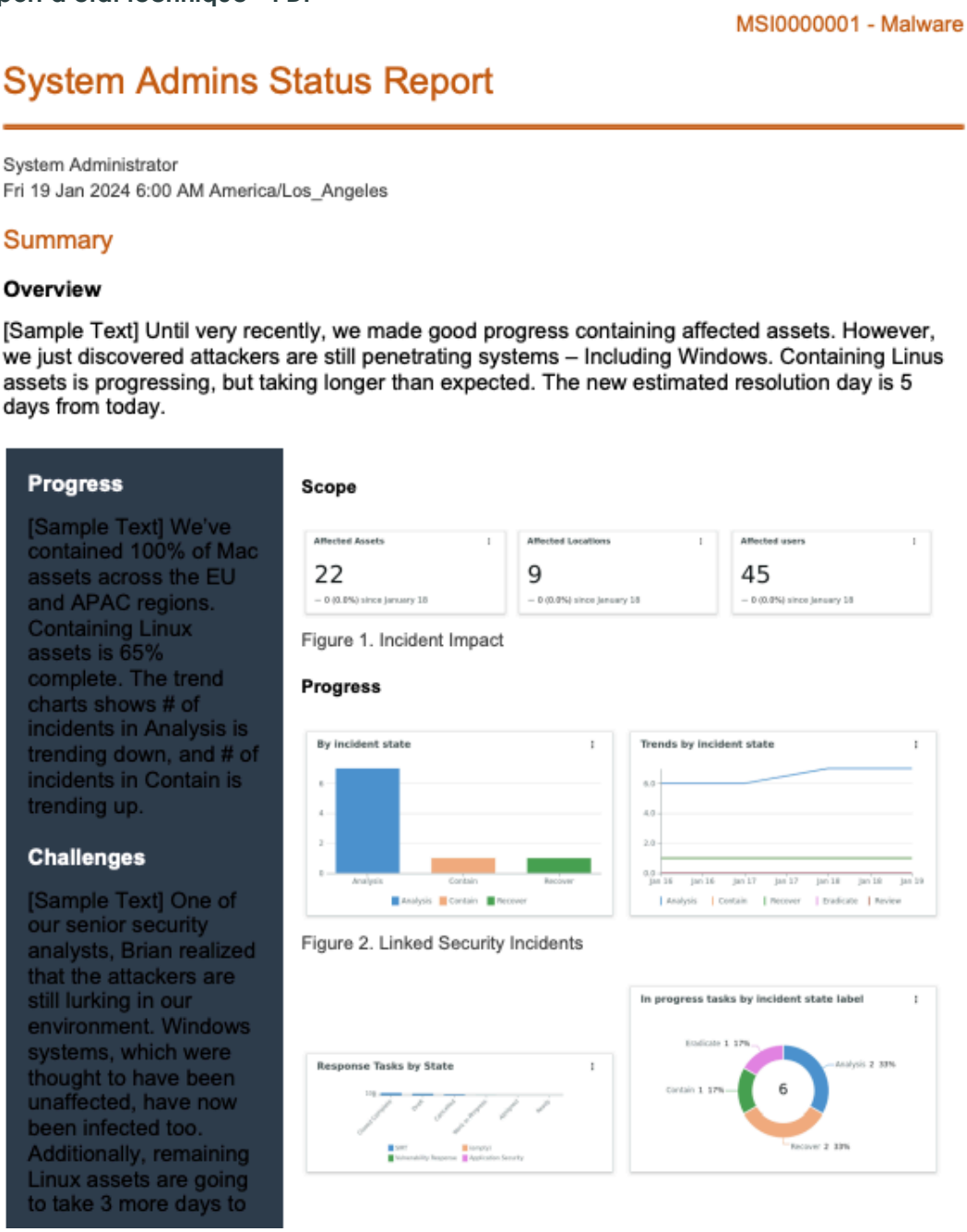
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de la balise sélectionnée depuis laquelle le dernier rapport d'état est généré. et des informations supplémentaires telles que l'impact de l'incident et les incidents liés.

Personnalisez et configurez le modèle de rapport pour ajouter des informations supplémentaires au rapport. Un exemple de rapport technique présentant des informations supplémentaires, telles que l'impact de l'incident, est illustré ci-dessous à titre de référence, et la partie restante des informations du rapport est similaire aux rapports exécutifs.

Rapport d'état technique - PDF


MSI0000001 - Malware

System Admins Status Report

System Administrator
Fri 19 Jan 2024 6:00 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

Response Tasks by State
In progress tasks by incident state label

Les sections du modèle de rapport contiennent diverses sous-sections, qui décrivent comment vous pouvez construire les sous-sections de rapport et ses éléments, telles que :

1. Marque: Ajouter une personnalisation à vos modèles de rapport
2. Scripts de modèle : Utiliser des scripts de modèle dans vos modèles de rapport
3. Utiliser des visualisations dans des modèles de rapports
4. Utiliser des listes de rapports dans des modèles de rapports

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un modèle de rapport

Créez différents modèles de rapport qui peuvent être appliqués aux incidents de sécurité majeurs et générez un rapport d'état. Vous pouvez ajouter au modèle de rapport des champs de formulaire standard et personnalisés de réponse aux incidents de sécurité majeurs qui peuvent être remontés pas à pas. En outre, vous pouvez formater et configurer le rapport en fonction de vos besoins à l'aide de sections, de sous-sections et de ses éléments.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche

Vous pouvez définir des composants de rapport pour vos modèles de rapport et fournir des informations supplémentaires. Créez des données visualisées pour suivre le champ d'application et les mesures de progression, ajouter des données de liste connexe, prévisualiser et générer ou partager les rapports d'état.

Procédure

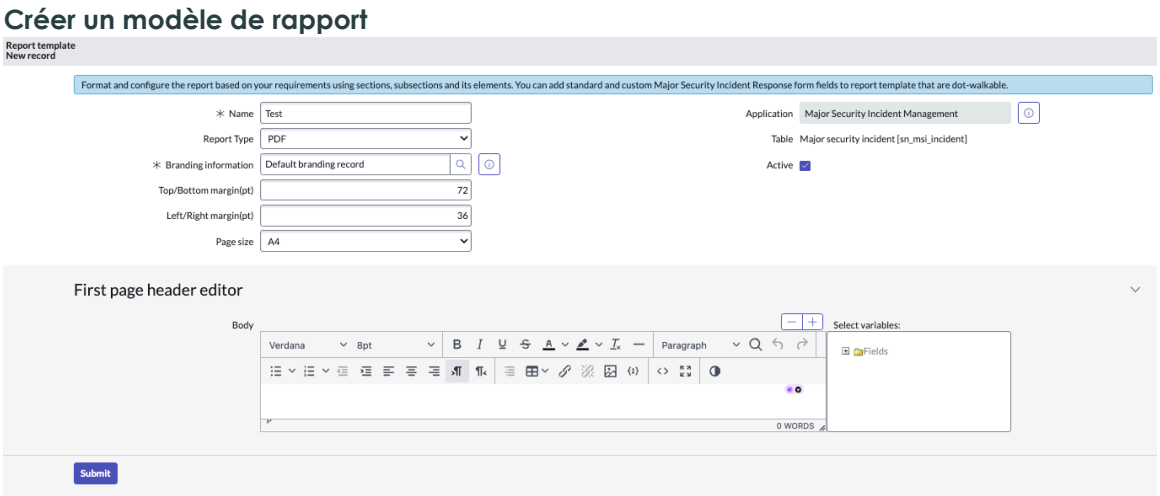
1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Sélectionnez **Nouveau** pour créer un modèle de rapport.
4. Renseignez les champs du formulaire Modèle de rapport.

Champ	Description
Nom	Nom du modèle de rapport.
Information sur la marque	Sélectionnez les informations de personnalisation de votre modèle de rapport, telles que le logo, l'en-tête et le texte de pied de page. Par exemple, Enregistrement de la marque par défaut.
Type de rapport	Type de rapport d'état. Le rapport d'état peut être de l'un des types suivants : ◦ PDF ◦ E-mail
Table	Nom de la table du modèle de rapport.
Marge supérieure/inférieure	Définissez les indentations de marge supérieure et inférieure requises lors de la génération du rapport.
Marge gauche/droite	Définissez les indentations des marges gauche et droite requises lors de la génération du rapport.
Taille de page	Taille de page de votre modèle de rapport. Par exemple, le format par défaut est A4.
Actif	Cochez la case pour que le gestionnaire MSI génère un rapport à partir du modèle créé à partir de la section **Modèle de rapports** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si la case est décochée, le gestionnaire MSI ne peut pas créer de rapport pour ce type de modèle de rapport spécifique dans l'espace de travail MSIM.
Éditeur d'en-tête de la première page	Permet de définir le corps du modèle. Sélectionnez les variables requises à ajouter à la section de l'éditeur de modèle.



5. **Soumettez** le nouvel enregistrement de modèle de rapport.
   Un nouveau modèle de rapport est créé sous la page Modèles de rapports.

Information associée

Créer et distribuer MSIM des rapports d'état

Ajouter une personnalisation à vos modèles de rapport

Ajoutez des marques à vos rapports. Vous pouvez ajouter une image d'en-tête et de pied de page, ainsi que du texte d'en-tête et de pied de page. Vous pouvez inclure ces informations de marques dans n'importe quel type de modèle de rapport que vous souhaitez créer, à l'exception des deux rapports prédéfinis.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche

Les principaux éléments à prendre en compte lors de l'ajout d'une personnalisation à vos modèles de rapport sont les suivants :

- Téléchargez l'image d'en-tête et de pied de page et alignez la position de l'image.
- La limite de taille maximale pour les images d'en-tête et de pied de page est de 5 Mo. Si la taille dépasse la limite spécifiée, un message d'erreur « Le format d'image ne peut pas être reconnu » s'affiche dans l'incident de sécurité majeur.
- Ajustez la hauteur de l'image d'en-tête et de pied de page.
- La longueur du texte du pied de page est limitée à 100 caractères.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
2. Explorer jusqu'à **Modèle de rapport** > **Marques**.
3. Sélectionnez **Configurer**.
4. Sélectionnez **Nouveau** pour ajouter une marque à votre modèle de rapport.
5. Renseignez les champs du formulaire Modèle de marque.

Champ	Description
Nom	Nom du modèle de la marque.
Image d'en-tête	Ajoutez une image d'en-tête pour le modèle de marque en procédant comme suit : **a.** Sélectionnez **Cliquer pour ajouter**. **b.** Sélectionner **Choisir un fichier** **c.** Choisissez une image dans votre système et sélectionnez **OK.**
Image de pied de page	Ajoutez une image de pied de page pour le modèle de marques en procédant comme suit : **a.** Sélectionnez **Cliquer pour ajouter**. **b.** Sélectionner **Choisir un fichier** **c.** Choisissez une image dans votre système et sélectionnez **OK.**
Position de l'image d'en-tête	Sélectionnez une position de l'image d'en-tête pour le modèle de marque. Vous pouvez choisir **Gauche**, **Centre** ou **Droite**.
Position de l'image de pied de page	Sélectionnez une position de l'image d'en-tête pour le modèle de marque. Vous pouvez choisir **En haut à gauche**, **En haut au centre**, **En haut à droite**, **En bas à gauche**, **En bas au centre** ou **En bas à droite**.
Hauteur de l'image d'en-tête	Fournissez une valeur de hauteur (en pt) pour l'image d'en-tête du modèle de marque.
Hauteur de l'image de pied de page	Fournissez une valeur de hauteur (en pt) pour l'image de pied de page du modèle de marque.
Texte de pied de page	Fournissez un texte de pied de page pour le modèle de personnalisation. Vous pouvez inclure des informations de classification ou de confidentialité. Par exemple, cet e-mail est classé comme confidentiel, interne uniquement ou secret professionnel de l'avocat.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Position du texte de pied de page	Sélectionnez une position de texte de pied de page pour le modèle de marque. Vous pouvez choisir **En haut à gauche**, **En haut au centre**, **En haut à droite**, **En bas à gauche**, **En bas au centre** ou **En bas à droite**.

6. Sélectionnez **Soumettre**.
   Un nouveau modèle de marques est créé sous la page Modèles de marques.

Utiliser des visualisations dans des modèles de rapports

Utilisez les widgets de rapports pour définir et inclure des éléments du générateur d'interface utilisateur (UIB) tels que des visualisations de données dans les rapports d'état MSIM.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Tout** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Explorer jusqu'à **Modèle de rapport** > **Visualisations**.
3. Sélectionnez **Configurer**.
   Voici les visualisations UIB prédéfinies dans le cadre du système de base, que vous pouvez utiliser pour configurer et modifier vos rapports d'état.

Nom du widget	Description
Équipe active	Affiche la liste des équipes actives impliquées dans la résolution du MSI.
Actifs affectés	Affiche la liste des actifs affectés.
Emplacements affectés	Affiche la liste des emplacements affectés.
Utilisateurs affectés	Affiche la liste des utilisateurs affectés.
Graphique à secteurs pour collaboration	Inclut les activités de collaboration dans le graphique à secteurs.
Graphique de tendance de collaboration	Affiche les activités de collaboration sous la forme d'un graphique de tendance.
Date de résolution estimée	Affiche la date de résolution estimée au moment où la résolution du MSI est estimée.
Graphique à barres pour les incidents liés	Affiche le graphique à barres des incidents liés.
Graphique de tendance des incidents liés	Affiche le graphique de tendance des incidents liés.
Graphique à barres pour tâches de réponse MSI	Affiche le graphique des tâches de réponse MSI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom du widget	Description
Graphique à barres pour tâches de réponse	Affiche le graphique à barres Tâches de réponse.
Tâches de réponse en cours par étiquettes	Affiche les tâches de réponse en cours par étiquettes.
Tâches de réponse en retard	Affiche le total des tâches de réponse dont la fermeture est en retard.
Graphique de tendance des tâches de réponse	Affiche le graphique de tendance des tâches de réponse.
Temps écoulé depuis la détection de l'incident	Affiche le temps écoulé depuis la détection de l'incident.
Chronologie	Affiche la chronologie des événements clés et des jalons qui se sont produits dans le cadre de l'incident de sécurité majeur.

Information associée

Créer un élément de type de visualisation

Utiliser des listes de rapports dans des modèles de rapports

Utilisez les listes de rapports pour définir et inclure les artefacts de liste connexes afin de générer des listes au format PDF en fonction de vos enregistrements de liste MSI configurés.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Explorer jusqu'à **Modèle de rapport** > **Listes**.
3. Sélectionnez **Configurer**.
   La section Listes des rapports d'état MSI décrit la façon dont chaque liste connexe spécifique est affectée depuis la création de l'incident. Vous trouverez ci-dessous les listes de rapports MSI prédéfinies dans le système de base, que vous pouvez utiliser pour configurer et modifier vos rapports d'état.

Listes de rapports MSI	Description
Actifs affectés	La liste connexe des actifs affectés s'affiche dans le rapport d'état.
Emplacements affectés	La liste connexe des emplacements affectés s'affiche dans le rapport d'état.
Utilisateurs affectés	La liste connexe des utilisateurs affectés s'affiche dans le rapport d'état.
Indicateurs	La vue de liste connexe des indicateurs dans le rapport d'état.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes de rapports MSI	Description
Incident de sécurité lié	La liste connexe des incidents de sécurité liés s'affiche dans le rapport d'état.
Observables	La liste connexe des observables s'affiche dans le rapport d'état.

Information associée

Créer un élément de type liste

Utiliser des scripts de modèle dans vos modèles de rapport

Créez un script pour inclure les données des listes connexes, les opérations de date et toutes les autres données qui ne sont pas directement accessibles par une remontée pas à pas.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser ce script de modèle prédéfini dans vos modèles de rapport pour inclure toutes les données connexes une fois que les modèles de rapport sont configurés et personnalisés.

Construisez un script de modèle pour afficher les données de la liste connexe sur le modèle de rapport. Si vous souhaitez utiliser et remplir un script de modèle, vous devez ajouter la balise de script de modèle de balise comme suit : `${template_script :nom du script}`.

Exemple : `${template_script :msi_collab_cards}`

Remarque : Vous ne pouvez pas supprimer les scripts de modèle prédéfinis. Un message d'erreur s'affiche si un utilisateur disposant d'un rôle administrateur tente de supprimer un enregistrement de script de modèle s'il est mappé avec un modèle de rapport.

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Explorer jusqu'à **Modèle de rapport** > **Scripts de modèle**.
3. Sélectionnez **Configurer**.
   Vous trouverez ci-dessous les scripts de modèle prédéfinis dans le cadre du système de base, que vous pouvez utiliser pour configurer et modifier vos rapports d'état.

Nom du script de modèle	Description
formatted_current_date	Renvoie la date et l'heure locales actuelles au format JJMMAAA 00h00 ou après-midi. Par exemple, 21 janv. 2021 15:51 PST.
msi_active_team	Générer du code HTML pour les cartes d'équipe actives.
msi_collab_cards	Générer du code HTML pour les cartes d'activité de collaboration.
msi_task_activities	Générer du code HTML pour les cartes de tâches.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom du script de modèle	Description
msi_timeline_events	Générez du code HTML pour les cartes d'événements de chronologie.
si_affected_users	Renvoie les utilisateurs affectés de la liste connexe sous forme de tableau.
si_assessments	Renvoie les résultats de l'évaluation post-incident sous forme de tableau.
si_associated_phish_emails	Renvoie les e-mails d'hameçonnage associés de la liste connexe sous forme de tableau.
si_associated_phish_headers	Renvoie les en-têtes d'hameçonnage associés de la liste connexe sous forme de tableau.
si_business_criticality	Renvoie une valeur de criticité opérationnelle codée par couleur.
si_malicious_observables	Renvoie les observables malveillants de la liste connexe sous forme de tableau.
si_observables	Renvoie les observables de la liste connexe sous forme de tableau.
si_priority	Renvoie une valeur de priorité codée par couleur.
si_response_tasks	Renvoie les tâches de réponse de la liste connexe sous forme de tableau.
si_time_to_identify	Renvoie la durée passée à l'état Brouillon et analyse.
si_time_to_resolve	Renvoie l'heure de résolution de l'incident.

Remarque : Vous pouvez également créer votre propre script de modèle pour inclure les données des listes connexes, les opérations de date et toutes les autres données qui ne sont pas directement accessibles par une remontée pas à pas, en plus des scripts de modèle répertoriés.

Traduction automatique

Prévisualiser le modèle de rapport

Utilisez la fonctionnalité Aperçu pour prévisualiser votre modèle de rapport au moment de la conception afin de générer et de partager le rapport avec d'autres personnes concernées pendant l'exécution à partir de l'espace Gestion des incidents de sécurité majeurs de travail.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Sélectionnez le modèle de rapport souhaité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez le type de rapport **E-mail** ou **PDF** en fonction de vos besoins.
5. Sélectionnez l'action **Enregistrer et prévisualiser le rapport** .

   La boîte de dialogue Aperçu du rapport s'affiche.
6. Sélectionnez un incident de sécurité majeur à l'aide de l'option Rechercher pour prévisualiser un rapport avec le modèle sélectionné.
7. Sélectionnez **Aperçu du rapport**.
   Le rapport génère un aperçu en fonction de la configuration de modèle sélectionnée. Si vous avez sélectionné le type de rapport **E-mail**, l'aperçu est alors au format de modèle d'e-mail. Les rapports d'état au format e-mail sont adaptés aux mobiles.

Créer un modèle de section de rapport

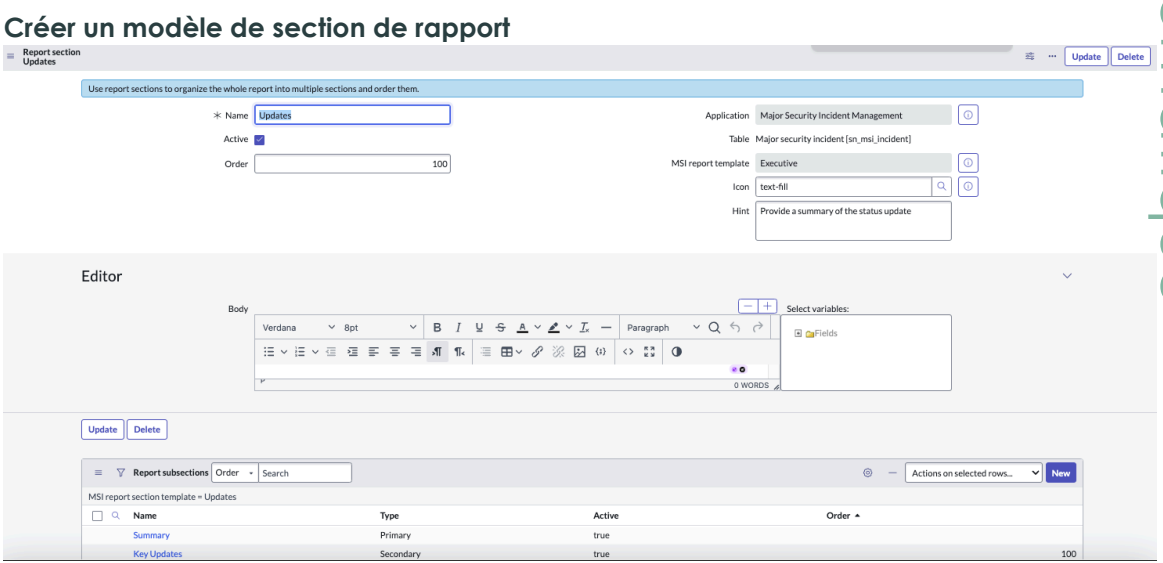
Un rapport peut en outre être divisé en plusieurs sections. Utilisez la section Rapport pour décomposer le rapport en plusieurs sections et les réorganiser dans l'ordre.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant.
4. Accédez à la **Sections de rapport** > **Nouveau**.
   La nouvelle page de section de rapport s'affiche.



5. Renseignez les champs du formulaire Modèle de section de rapport.

Champ	Description
Nom	Nom de la section du modèle de rapport. Par exemple, Résumé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Table	Nom de la table du modèle de rapport.
Actif	Cochez la case pour créer une section de rapport pour le modèle sélectionné dans l'espace de travail MSIM. **Remarque :** Si la case n'est pas cochée, le gestionnaire MSI ne peut pas créer de section de rapport pour ce modèle dans l'espace de travail MSIM.
Modèle de rapport MSI	Nom du modèle de rapport MSI pour lequel le rapport est divisé en sections.
Ordre	Ordre dans lequel les sections de rapport seront rendues.
Icône	Utilisez l'icône pour afficher les icônes système dans le rapport.
Conseil	Utilisez le texte de conseil pour guider la création du rapport. Dans le rapport, le texte de conseil s'affiche sous le titre de la section.
Éditeur : corps	Définissez le corps de la section du modèle. Vous pouvez définir le corps de la section en sélectionnant les jetons ou les variables personnalisés dans l'éditeur.

6. **Enregistrez et soumettez** la section Nouveau modèle de rapport.

Créer un modèle de sous-section de rapport

Utilisez la sous-section de rapport pour organiser davantage la section en plusieurs sous-sections et configurer leur alignement et leur position à l'aide des types disponibles, tels que Texte, panneau latéral, Primaire et Secondaire.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

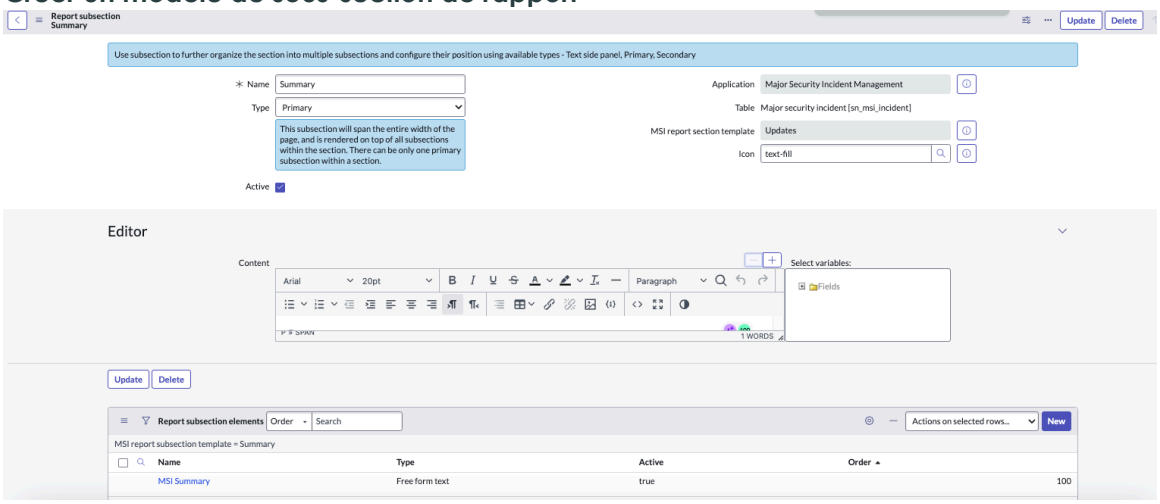
Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport correspondante.
4. Dans la liste Sections de rapport, ouvrez un modèle de section de rapport existant.
5. Accédez à la **Sous-sections de rapport** > **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un modèle de sous-section de rapport



6. Renseignez les champs du formulaire Sous-section de rapport.

Champ	Description
Nom	Nom de la sous-section du modèle de rapport. Par exemple, Périmètre. **Remarque :** Les sous-sections existantes pour les rapports prédéfinis sont : Vue d'ensemble, Périmètre, Progression, Explication. ◦ **Vue d'ensemble** : affiche la vue d'ensemble sous forme de sous-section dans le rapport. ◦ **Champ d'application** : affiche les éléments de visualisation dans le rapport, tels que les compteurs de durée, l'impact de l'incident, les équipes actives et la tendance des équipes actives. ◦ **Progression** : affiche les éléments de visualisation dans le rapport, tels que les graphiques des incidents de sécurité liés, le graphique des tâches de réponse et les graphiques de collaboration.
Type	Type de sous-section de rapport. Les types disponibles sont les suivants : ◦ **Primaire** : cette sous-section s'étend sur toute la largeur de la page et s'affiche au-dessus de toutes les sous-sections de la section. Il ne peut y avoir qu'une seule sous-section primaire dans une section.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ **Secondaire** : cette sous-section couvre toute la largeur de la page, sauf si elle est utilisée avec le panneau latéral de texte. ◦ **Panneau latéral de texte** : cette sous-section accompagne le panneau secondaire et ne prend en charge que le texte.
Table	Nom de la table du modèle de rapport.
Modèle de section de rapport MSI	Nom du modèle de rapport MSI pour lequel vous divisez le rapport en sections.
Ordre	Ordre dans lequel les sous-sections de rapport seront rendues.
Icône	Utilisez l'icône pour indiquer ou mettre en surbrillance le conteneur de section sur le formulaire de configuration d'exécution de rapport.
Actif	Cochez la case pour créer une sous-section de rapport pour le modèle sélectionné dans l'espace de travail MSIM. **Remarque :** Si la case n'est pas cochée, le gestionnaire MSI ne peut pas créer de sous-section de rapport pour ce modèle dans l'espace de travail MSIM.
Éditeur de contenu	Définissez le contenu de la sous-section du modèle.

7. **Enregistrez et soumettez** la section Nouveau modèle de rapport.

Créer un modèle d'élément de sous-section de rapport

Utilisez les éléments de sous-section pour organiser davantage une sous-section en plusieurs éléments. Les éléments de sous-section permettent de définir des visualisations, des listes et du texte de forme libre de manière plus déclarative avec des options de filtre telles que les groupes d'affectation et les étiquettes.

Avant de commencer

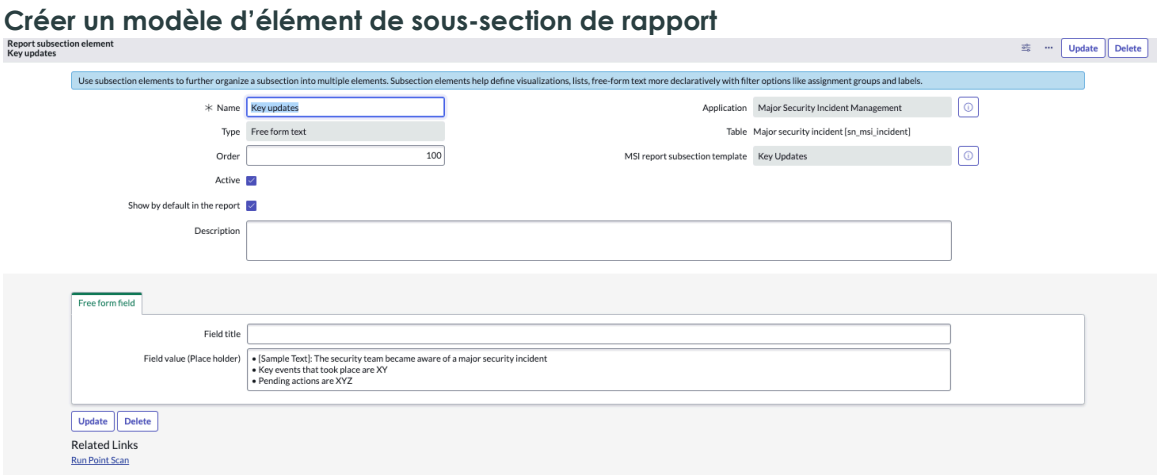
Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport correspondante.
4. Dans la liste Sections de rapport, ouvrez un modèle de section de rapport existant.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.



7. Renseignez les champs du formulaire Éléments de sous-section de rapport.

Champ	Description
Nom	Nom de l'élément de sous-section du modèle de rapport. Par exemple, Périmètre. **Remarque :** Les sous-sections existantes pour les rapports prédéfinis sont : Compteurs de durée, Impact de l'incident, Équipe active, Tendance de l'équipe active. ◦ **Compteurs de durée** : affiche le compteur de durée sous la forme d'un élément de sous-section tel que le temps estimé pour résoudre l'incident dans le rapport d'état. ◦ **Impact de l'incident** : affiche les éléments de visualisation dans le rapport, tels que les actifs impactés, les emplacements impactés et les utilisateurs concernés. ◦ **Équipe active** : affiche les éléments de visualisation dans le rapport, tels que le nombre d'équipes actives impliquées dans la fermeture de l'incident de sécurité majeur. ◦ **Tendance de l'équipe active :** Représente la tendance des équipes actives dans une représentation graphique.
Type	Type d'élément de sous-section de rapport. Les types disponibles sont les suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Texte de formulaire libre ◦ Visualisation ◦ Personnalisé ◦ Liste
Table	Nom de la table du modèle de rapport.
Actif	Cochez la case pour créer une section de rapport pour le modèle sélectionné dans l'espace de travail MSIM. **Remarque :** Si la case n'est pas cochée, le gestionnaire MSI ne peut pas créer de section de rapport pour ce modèle dans l'espace de travail MSIM.
Afficher par défaut dans le rapport	Cochez cette case si vous souhaitez inclure la section dans le rapport afin d'afficher rapidement les éléments.
Modèle de rapport MSI	Nom du modèle de rapport MSI pour lequel vous divisez le rapport en sections.
Ordre	Ordre dans lequel les sections de rapport seront rendues.
Description	Fournissez une description au type d'élément de sous-section.

8. **Enregistrez et mettez à jour** la section Nouveau modèle de rapport.

Créer un élément de type de formulaire libre

Créez un type d'élément de formulaire libre pour définir le texte de formulaire libre de manière plus déclarative avec des options de filtre telles que les groupes d'affectation et les étiquettes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport correspondante.
4. Dans la liste Sections de rapport, ouvrez un modèle de section de rapport existant.
5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Renseignez le formulaire Éléments de sous-section de rapport avec les détails requis, comme expliqué à la section Créer un modèle d'élément de sous-section de rapport.
8. Accédez au champ Type d'élément de sous-section de rapport et sélectionnez l'option de **champ Formulaire libre** .
   La section **de champ de formulaire libre** s'affiche.
9. Renseignez les champs de l'onglet Formulaire libre.

Champ	Description
Titre de champ	Nom du titre de champ. Par exemple, Vue d'ensemble.
Valeur du champ (espace réservé)	Saisissez la description de la valeur de champ. Par exemple, voici un exemple de texte de vue d'ensemble. `Nous avons bien progressé dans la maîtrise des actifs touchés. Cependant, nous venons de découvrir que les attaquants pénètrent toujours dans les systèmes, y compris Windows. Le confinement des actifs Linus progresse, mais prend plus de temps que prévu. Le nouveau jour de résolution estimé est de 5 jours à partir d'aujourd'hui.`

Créer un élément de type de visualisation

Créez un type d'élément de visualisation pour définir les éléments de visualisation de manière plus déclarative avec des options de filtre telles que les groupes d'affectation et les étiquettes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page Configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport correspondante.
4. Dans la liste Sections de rapport, ouvrez un modèle de section de rapport existant.
5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.
7. Renseignez le formulaire Éléments de sous-section de rapport avec les détails requis, comme expliqué à la section Créer un modèle d'élément de sous-section de rapport.
8. Accédez au champ Type d'élément de sous-section de rapport et sélectionnez l'option **Visualisation** .
   La section **Visualisation** s'affiche.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

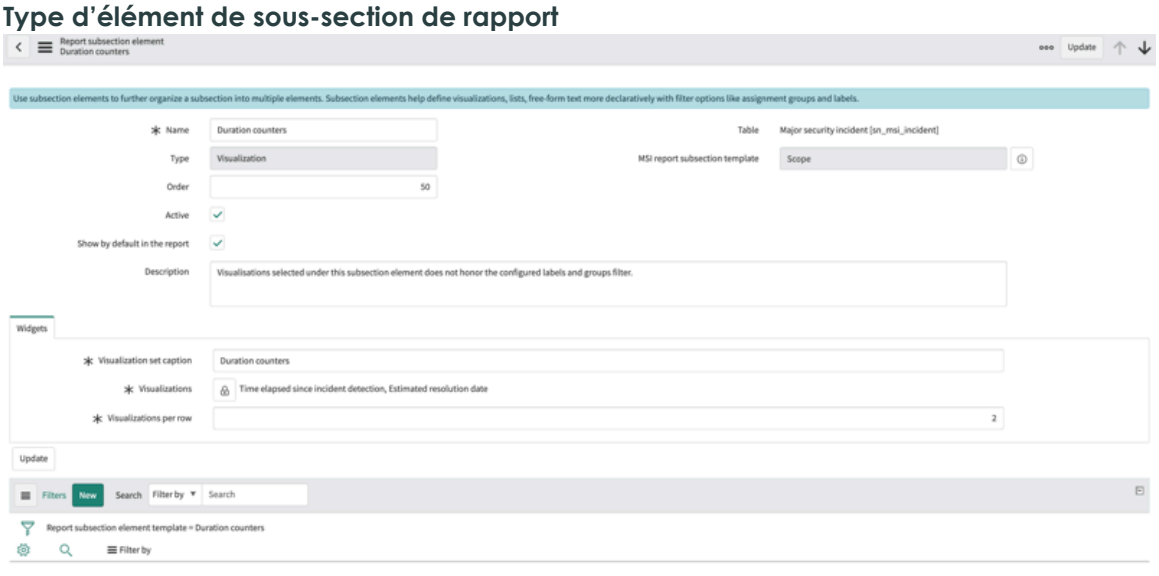
9. Renseignez les champs du formulaire Visualisation.

Champ	Description
Légende définie pour les visualisations	Saisissez le nom de la légende de l'ensemble de visualisations. Par exemple, Compteurs de durée.
Visualisations	Sélectionnez le type de visualisations. Par exemple, sélectionnez Temps écoulé depuis la détection de l'incident, Date de résolution estimée pour le type de sous-section : Compteurs de durée.
Visualisations par ligne	Sélectionnez le nombre de visualisations affichées en fonction de chaque ligne.

10. Sélectionnez **Soumettre**.

Example: Type d'élément de sous-section de modèle de rapport pour un rapport d'état technique

Type d'élément de sous-section de rapport



Créer un élément de type liste

Créez un élément de type liste, qui définit les éléments de liste connexes de manière plus déclarative avec des options de filtre telles que les groupes d'affectation et les étiquettes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport correspondante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans la liste Sections de rapport, ouvrez un modèle de section de rapport existant.
5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.
7. Renseignez le formulaire Éléments de sous-section de rapport avec les détails requis, comme expliqué à la section Créer un modèle d'élément de sous-section de rapport.
8. Accédez au champ Type d'élément de sous-section de rapport et sélectionnez l'option **Liste** .
   La section **Listes** s'affiche.
9. Renseignez les champs du formulaire Liste.

Champ	Description
Listes	Nom des listes connexes associées au MSI. Par exemple, Observables, Indicateurs. Sélectionnez une liste à l'aide de l'option de recherche.

Créer un élément de type personnalisé

Créez un élément de type liste, qui définit les éléments de liste connexes de manière plus déclarative avec des options de filtre telles que les groupes d'affectation et les étiquettes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport correspondante.
4. Dans la liste Sections de rapport, ouvrez un modèle de section de rapport existant.
5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.
7. Renseignez le formulaire Éléments de sous-section de rapport avec les détails requis, comme expliqué à la section Créer un modèle d'élément de sous-section de rapport.
8. Accédez au champ Type d'élément de sous-section de rapport et sélectionnez l'option **Personnalisé** .
   La section **Contenu personnalisé** s'affiche.
9. Renseignez les champs du formulaire Contenu personnalisé.

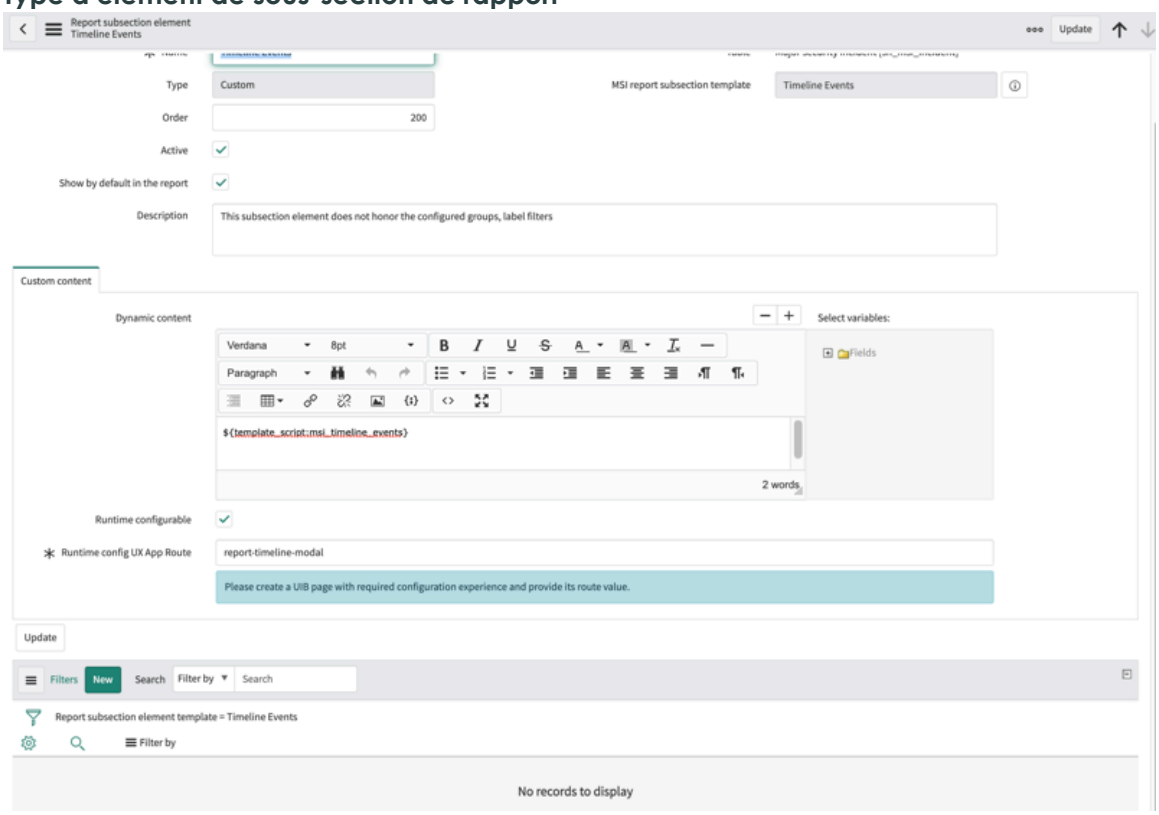
Champ	Description
Contenu dynamique	Saisissez le contenu dynamique tel que les scripts de modèle.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Temps d'exécution configurable	Cochez cette case si le type d'élément personnalisé est configurable au moment de l'exécution.
Configuration de l'exécution pour chemin de l'application UX	Saisissez la valeur Acheminement de l'application UX de configuration d'exécution lorsqu'une page UIB est créée avec l'expérience de configuration requise. **Remarque :** Ce champ s'affiche uniquement lorsque l'option **de configuration Temps d'exécution** est sélectionnée.

Example: Voici un exemple de type d'élément de sous-section de modèle de rapport pour un rapport d'état technique

Type d'élément de sous-section de rapport



Ajouter des propriétés système

Ajoutez des propriétés système pour contrôler le comportement de l'application MSIM. Voici les propriétés système par défaut introduites dans le cadre des rapports d'état Gestion des incidents de sécurité majeurs .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés système

Nom de la propriété	Description
sn_msi.export_img	Utilisez cette propriété pour contrôler l'exportation d'images. La valeur par défaut est définie sur ACTIVÉ.
sn_msi.export_img_log	Utilisez cette propriété pour activer la connexion à la console du navigateur. La valeur par défaut est définie sur OFF.
sn_msi.export_img_parallel_threshold	Utilisez cette propriété pour contrôler le nombre maximal de demandes parallèles afin de générer les images à partir des configurations de widget de rapport. La valeur par défaut est définie sur 14.
sn_msi.img_export_log	Utilisez cette propriété pour activer les journaux de la console dans le navigateur.
sn_msi.img_export_poll_interval	Utilisez cette propriété pour contrôler l'écart de temps entre les interrogations qui vérifient si l'image est générée ou non. L'intervalle d'interrogation par défaut est défini sur 3 000 millisecondes.
sn_msi.export_poll_request_timeout	Utilisez cette propriété pour contrôler la durée maximale d'interrogation que le système peut interroger pour l'image exportée. La valeur par défaut est de 120 000 millisecondes.
sn_msi.msi_report_uib_element_js_path	Utilisez cette propriété pour contrôler le chemin d'accès générique afin de capturer l'image hors de la portion de page UIB.
sn_msi.report_default_style_objects	Utilisez cette propriété pour modifier le CSS des fichiers PDF générés, tels que la taille de police, la couleur de police ou la valeur de champ. Par exemple, si sn_msi.workspace_manager préfère changer la couleur de police du panneau de gauche du rapport d'état PDF généré, le gestionnaire de l'espace de travail peut modifier la couleur de police des propriétés système et afficher le PDF dans la vue souhaitée.

Playbooks sur la gestion des incidents de sécurité majeurs

Vous pouvez invoquer le flux du playbook Gestion des incidents de sécurité majeurs automatiquement ou manuellement.

Un Playbook n'est visible que si au moins un Playbook est associé à un incident de sécurité. Le composant Playbook n'est pris en charge que pour le designer d'automatisation de processus (PAD) créé. La gestion des incidents de sécurité majeurs fournit le playbook des demandes juridiques avec le système de base.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook pour la demande juridique

Le playbook de demande juridique fournit des conseils étape par étape sur la façon d'informer le service juridique du dernier résumé d'un MSI afin qu'il puisse en informer la SEC dans le délai de 4 jours requis pour les violations importantes.

Vue d'ensemble

En tant que gestionnaire d'incidents, vous pouvez utiliser le playbook de demande juridique pour informer l'équipe juridique du dernier résumé d'un MSI afin qu'elle puisse notifier la SEC en cas de violations importantes. Vous pouvez utiliser les modèles Concepteur d'automatisation de processus (PAD) pour effectuer les étapes du playbook de demande juridique et en informer l'équipe juridique.

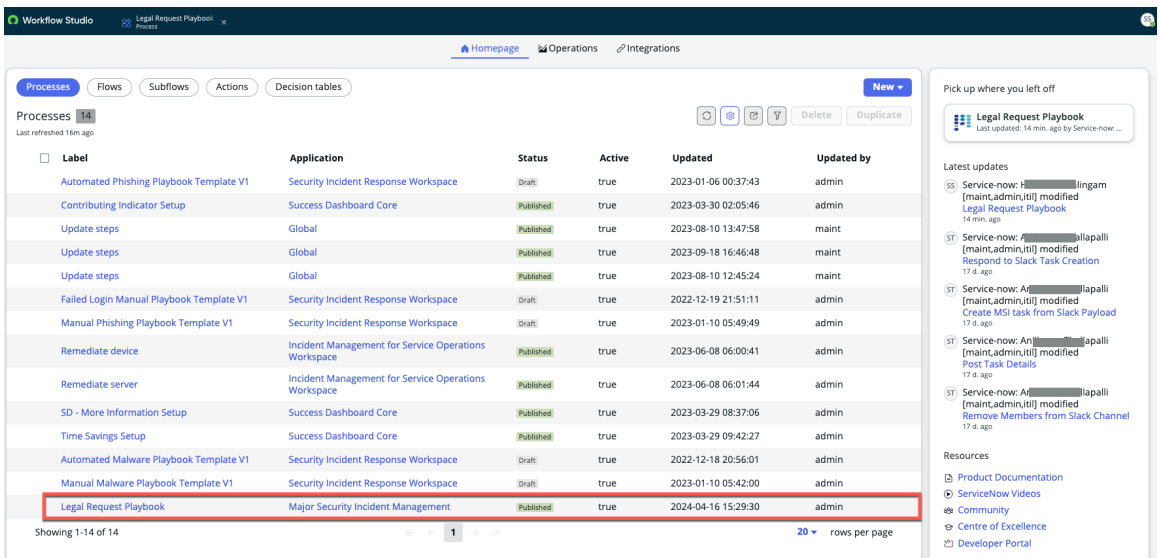
Ce playbook peut être utilisé si un incident de sécurité majeur est créé ou mis à jour. Vous devez activer le playbook de demande juridique sur PAD, puis effectuer toutes les tâches, telles que l'analyse, le contenu, l'élimination et la révision.

Les voies suivantes sont les voies de la définition du processus et correspondent à l'état de l'incident de sécurité majeur :

- Analyse
- Contenir
- Éradiquer
- Revue

Chaque voie contient certaines activités.

Playbook pour la demande juridique



Une fois que vous marquez une tâche comme terminée dans une voie, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une voie, vous pouvez passer à la voie suivante. L'état est reflété dans le panneau de gauche lorsque vous continuez à accomplir des tâches et à utiliser des voies. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les informations que vous avez saisies dans toutes les voies. Vous pouvez choisir de modifier n'importe quel champ ou de sélectionner **Terminer** pour terminer le processus de création de l'autorisation.

Créer des processus pour le playbook des demandes juridiques

Suivez ces étapes pour créer des processus pour le playbook de demandes juridiques dans Concepteur d'automatisation de processus (PAD).

Avant de commencer

Rôle requis : sn_msi.workspace_manager.

Procédure

1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

   Par exemple, Playbook pour les demandes juridiques.

2. Entrez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour l'exécution de votre processus** et sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions à définir à quel moment votre processus doit s'exécuter en sélectionnant une table et en renseignant les conditions.
7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle voie**.
   Le volet Propriétés de la voie s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans la fenêtre Lane properties (Propriétés de la voie), saisissez les détails suivants : **Name**, **Description**, Run condition (Condition **d'exécution) et Indicate when (Indiquer quand démarrer**).
   Les champs **Condition d'exécution** et **Indiquer quand démarrer** impliquent le moment où la voie s'exécutera.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre voie, cliquez sur **Ajouter une autre voie**.
    De même, vous pouvez créer autant de voies que vous le souhaitez. Dans cet exemple, vous pouvez créer une voie pour Analyse, Maîtriser, Éradiquer et Réviser respectivement. Dans l'exemple suivant, la voie **d'analyse** démarre immédiatement et n'a pas de condition d'exécution. **Contenir** le début de la voie une fois la voie précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité dans la voie précédente.
    Après avoir ajouté les voies, vous devez ajouter des activités de processus pour chaque voie.
12. Cliquez sur **Ajouter une autre activité de processus** sous une voie particulière (par exemple, voie d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les voies. De même, vous pouvez créer d'autres activités de processus sous chaque voie.
14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité du processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité à partir de la définition d'activité.

À l'aide du playbook des demandes juridiques

Suivez ces étapes pour apprendre à utiliser le playbook des demandes juridiques dans l'espace de travail MSIM et ses options.

Avant de commencer

Rôle requis : sn_msi.workspace_manager.

Procédure

1. Dans l'espace de travail MSIM, ouvrez un incident de sécurité majeur.
2. Sélectionnez l'onglet **Playbook**.

   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité majeur.

   Remarque : Si vous ne voyez pas les playbooks répertoriés, vous devez accéder à PAD et leur permettre de le voir dans l'onglet **Playbook** .

3. Sélectionnez le **playbook de demande juridique**.
4. Cliquez sur chaque voie pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse. Vous avez la possibilité de le modifier selon vos besoins.
6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Réviser pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action utilisateur à effectuer, elle est affichée dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase concernée et effectuez l'action pour terminer l'activité.

Cadre de travail de déploiement pour MSIM

Étend la possibilité de lier les enregistrements sources à partir de l'espace de Gestion des incidents de sécurité majeurs travail.

Vue d'ensemble

Rollup Framework rend le flux de déploiement configurable et extensible. Utilisez ce modèle de cadre de travail pour configurer les informations qui peuvent être déployées dans un incident de sécurité majeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Auparavant, sn_msi.workspace_manager était en mesure de lier les incidents de sécurité et les éléments vulnérables proposés ou promus en tant que MSI. Après avoir lié l'incident de sécurité ou l'élément vulnérable, les informations ont ensuite été déployées pour un incident de sécurité majeur. Le type d'informations à déployer était codé en dur dans les scripts.

Vous pouvez utiliser le modèle de cadre de travail pour configurer le flux de déploiement, qui prend en charge les fonctionnalités suivantes et résout également les problèmes existants dans l'application :

Le modèle de cadre de travail de déploiement offre à sn_msi.workspace_manager les avantages suivants :

- Ajoutez ou supprimez les options de liaison, de proposition ou de promotion MSI d'enregistrement sur n'importe quelle table, ce qui étend la table de tâches.
- Contrôlez le type d'informations à déployer MSI lors de l'exécution d'actions telles que lier/proposer/promouvoir sur les enregistrements d'incident.
- Prise en charge de la liaison, proposition ou promotion des incidents de sécurité, des tâches de rattrapage et des tickets de sécurité prêts à l'emploi (OOTB) à la fois à partir de l'environnement classique et Gestion des incidents de sécurité majeurs de l'espace de travail.

Le cadre de travail de déploiement présente les configurations comme expliqué dans la table suivante.

Configurations de Rollup Framework

Nom	Description
Configuration d'enregistrement lié	Stocke les informations des tables de tâches qui peuvent être utilisées pour lier/promouvoir/proposer à Incident de sécurité majeur.
Configuration d'enregistrement de déploiement	Capture les informations qui peuvent être déployées à partir de la table de tâches lors de l'exécution d'actions de lien/promotion/proposition.
Configuration de la mise en page de liste	Contrôle les étiquettes et la mise en page des listes de diverses tables, comme indiqué dans les onglets de l'espace de travail tels que Impact de l'incident Gestion des incidents de sécurité majeurs , Enregistrements liés et Renseignements sur les menaces.

Configurer les enregistrements liés dans Gestion des incidents de sécurité majeurs

Utilisez la configuration des enregistrements liés pour stocker les informations des tables de tâches qui peuvent être utilisées pour lier/promouvoir/proposer à Incident de sécurité majeur.

Rôle requis : admin et sn_msi.workspace_admin.

Remarque : L'administrateur peut créer l'enregistrement et MSIM l'administrateur de l'espace de travail peut mettre à jour l'enregistrement.

Procédure

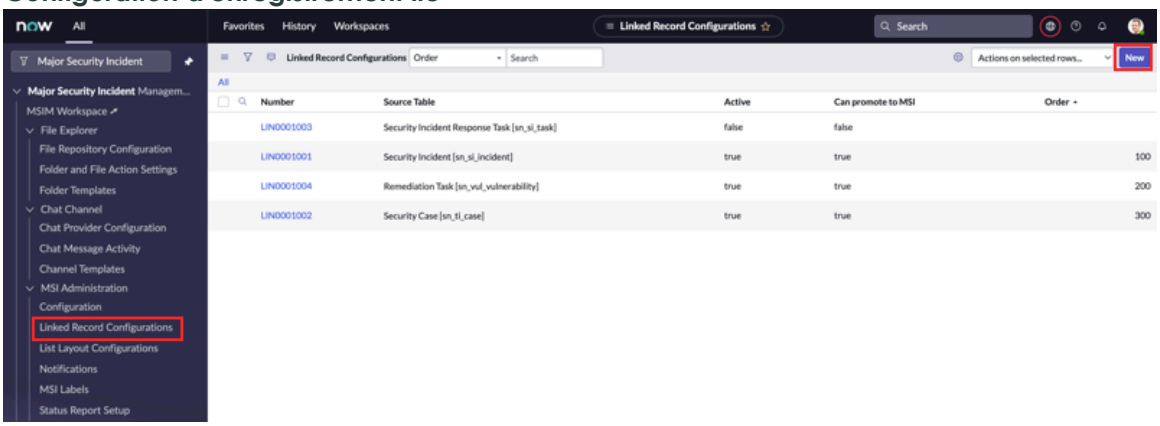
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Configurations d'enregistrements liés**.

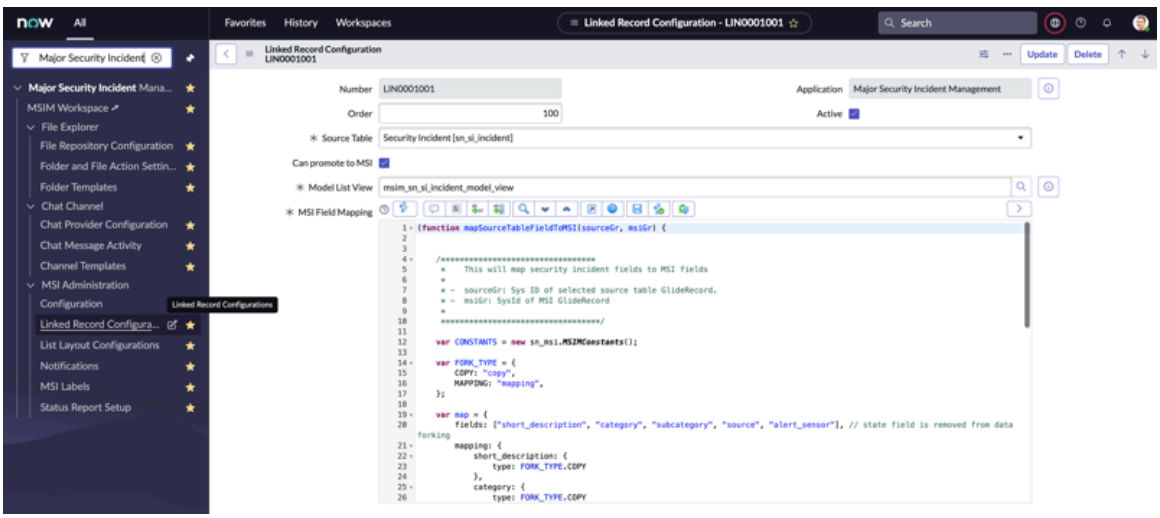
   La page Configuration de l'enregistrement lié s'affiche.

Configuration d'enregistrement lié



2. Sur la page Configuration de l'enregistrement lié, cliquez sur **Nouveau**

   Remarque : Assurez-vous que l'application se trouve dans Gestion des incidents de sécurité majeurs le périmètre.



3. Renseignez les champs du formulaire de configuration d'enregistrement.

Descriptions des champs d'enregistrements liés

Champ	Description
Table source	Indique la table de tâches qui doit être liée et déployée sur Incident de sécurité majeur.
Ordre	Permet de contrôler l'ordre de la table source actuelle dans la liste déroulante de l'espace de travail MSIM. Vous trouverez ci-dessous un exemple de la **commande**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Reportez-vous à l'image 1 ci-dessous, qui se trouve à la suite de ce tableau.
Modèle ListView	Sélectionnez une vue permettant de contrôler la mise en page de la liste affichée dans la liste modale d'enregistrement lié.
Peut promouvoir à MSI	Cochez cette case pour confirmer si l'enregistrement est un enregistrement primaire. Vous trouverez ci-dessous un exemple de sélection de **l'option Peut promouvoir à MSI** . Reportez-vous à l'image 2 suivante, qui se trouve après ce tableau. Si cette case est cochée et que la valeur est vraie, alors : ◦ Vous pouvez directement proposer et promouvoir un enregistrement source à l'aide des actions d'environnement Incident de sécurité majeur classiques avec des configurations supplémentaires. ◦ Vous pouvez lier des enregistrements sources à des incidents de sécurité majeurs à la fois à partir de l'environnement classique et MSIM de l'espace de travail. ◦ Gestion des incidents de sécurité majeurs La page d'enregistrement lié de l'espace de travail affiche les enregistrements de la table source liée. **Remarque :** Si un enregistrement peut être directement proposé/promu en tant que Incident de sécurité majeur, alors cet enregistrement est un enregistrement primaire. Par exemple, dans la configuration de la table Tâche de réponse de sécurité, la valeur de **Peut convertir en MSI** est faux, car vous ne pouvez pas promouvoir directement la tâche de réponse de sécurité en Incident de sécurité majeur. Par conséquent, il n'apparaît pas dans la liste déroulante de l'onglet d'enregistrement lié de l'espace MSIM de travail.
MSI Mappage de champs	Écrivez un script pour mapper les champs de l'enregistrement source à un incident de sécurité majeur nouvellement créé lorsque

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	l'enregistrement des tables sources est en cours de proposition ou de promotion. Ce script s'exécute uniquement lorsque la valeur **Peut promouvoir à MSI** est définie sur vrai.

Image 1 : Ordre de la vue de liste des enregistrements liés

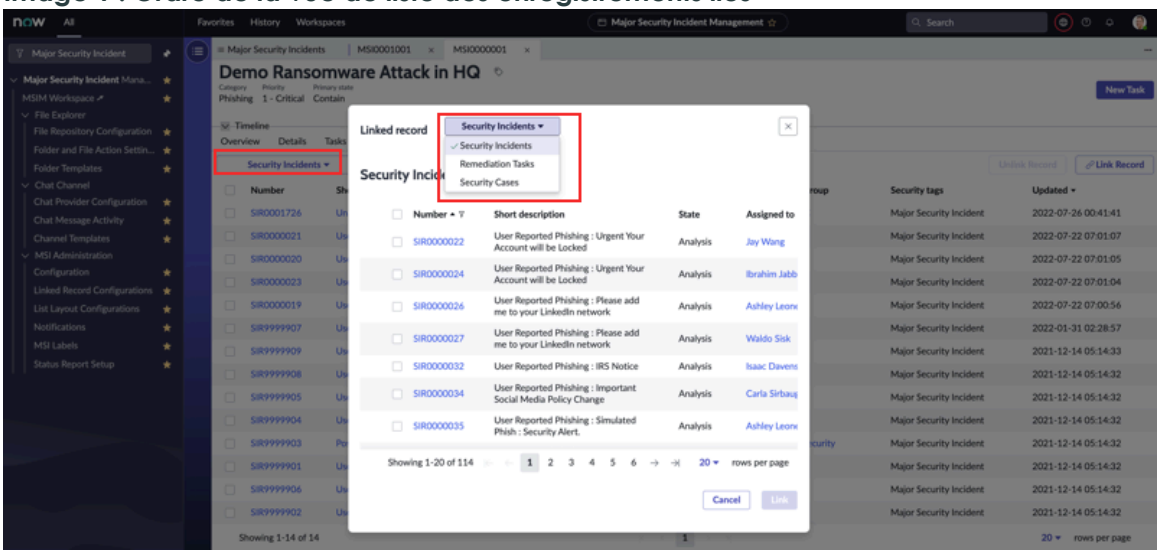
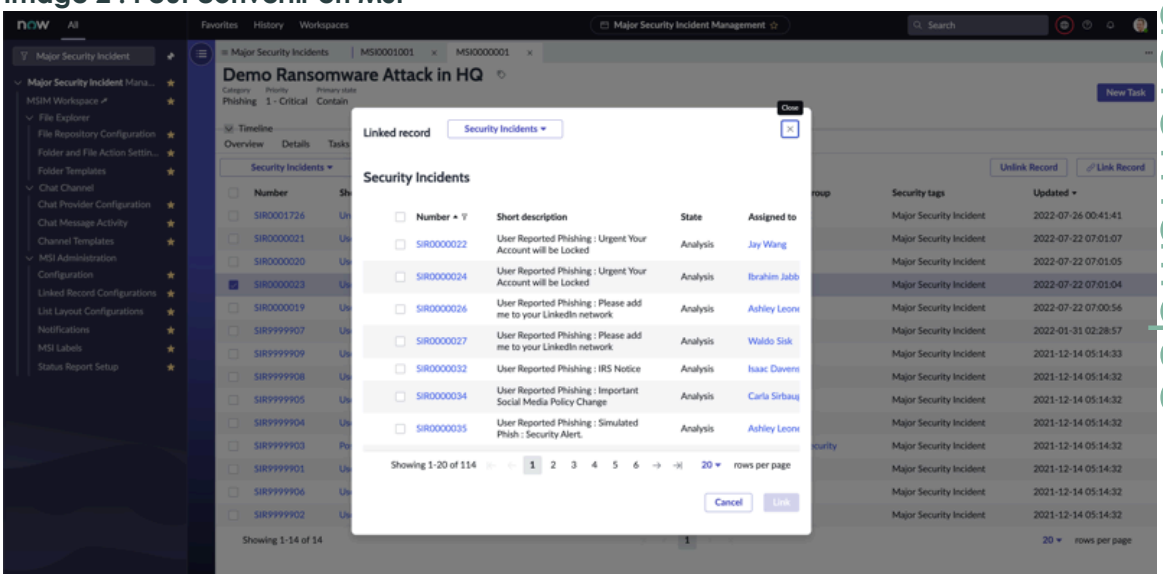


Image 2 : Peut convertir en MSI



Traduction automatique

Configurer les enregistrements de déploiement dans Gestion des incidents de sécurité majeurs

Configurez les enregistrements de déploiement pour Gestion des incidents de sécurité majeurs contrôler les informations, qui seront déployées lorsque l'enregistrement source sera lié/proposé/promu en tant qu'incidents de sécurité majeurs.

Rôle requis : admin et sn_msi.workspace_admin.

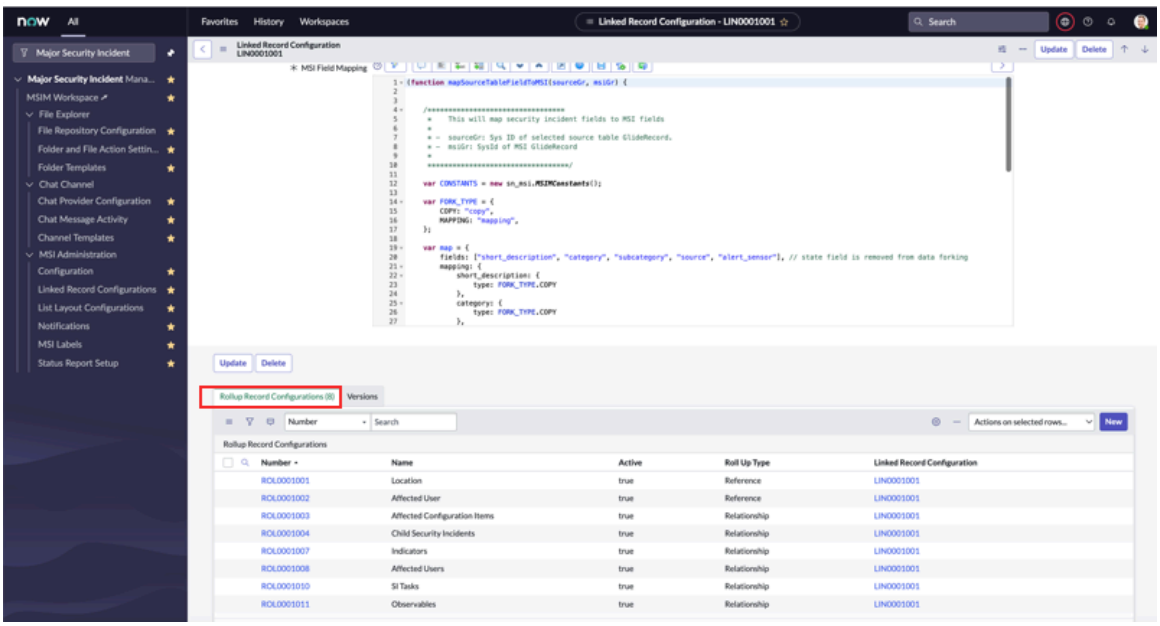
Remarque : L'administrateur système peut créer l'enregistrement et l'administrateur de l'espace de travail MSI peut le mettre à jour.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

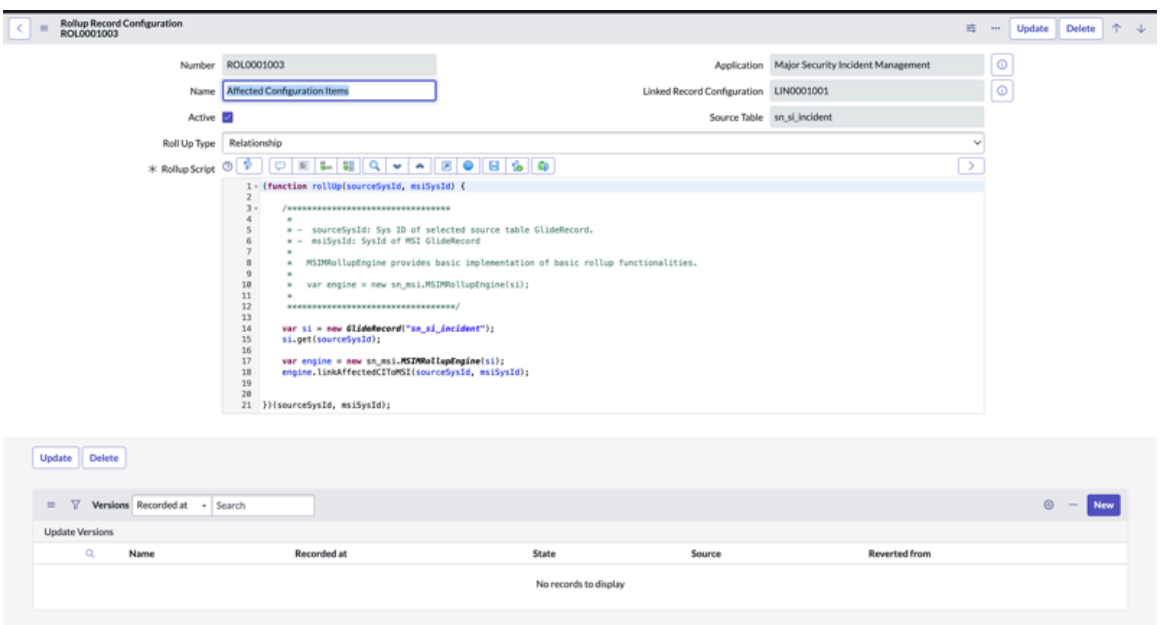
Procédure

1. Accédez à la **Réponse aux incidents de sécurité majeurs** > **Configuration des enregistrements liés**. La page Configurations d'enregistrement lié s'affiche.
2. Sélectionnez ou créez un nouvel enregistrement lié et accédez à la section **Configuration de l'enregistrement de déploiement** à partir de la même page.

Section Configuration d'enregistrement de déploiement



3. Cliquez sur **Nouveau**.



4. Renseignez les champs de la page de configuration.

Configuration d'enregistrement de déploiement

Nom de champ	Description de champ
Nom	Indique le nom de l'enregistrement de déploiement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description de champ
Actif	Cochez cette case pour implémenter la configuration actuelle lors du déploiement de l'enregistrement source.
Configuration d'enregistrement lié	Indique un numéro unique, qui fait référence à la configuration et à la lecture seule de vos enregistrements liés parents.
Table source	Nom de la table source utilisée dans la configuration de l'enregistrement lié, qui est en lecture seule.
Type de déploiement	Décrit le type d'informations qui doivent être déployées. ◦ **Relation** : sélectionnez cette option si les données doivent être présentes en tant que liste connexe. ◦ **Référence** : sélectionnez cette option si les données sont présentes en tant que champ de référence sur le formulaire de table source.
Script de déploiement	Si le type de déploiement est : **Relation**, le champ **Script de déploiement** est activé, ce qui vous permet d'écrire un script et peut être utilisé pour déployer des informations. Ici, le script recevra les entrées contenant des informations sur l'enregistrement source et l'incident de sécurité majeur. Le script doit être capable de trouver les informations à partir des tables de relations et de les déployer vers la table d'enregistrement lié (sn_msi_m2m_child).
Champ source	Si le type de déploiement est : **Référence**, le **champ Source** est disponible. Cela vous permet de sélectionner le champ de référence Table source qui contient les informations à déployer.
Champ cible	Si le type de déploiement est : **Référence**, le **champ Cible** est disponible. Cela vous permet de référencer le champ à partir de la table d'enregistrement lié (sn_msi_m2m_child) et stockera les données présentes dans le champ source sélectionné et dans l'enregistrement de table source.

Écriture d'un script pour le déploiement

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

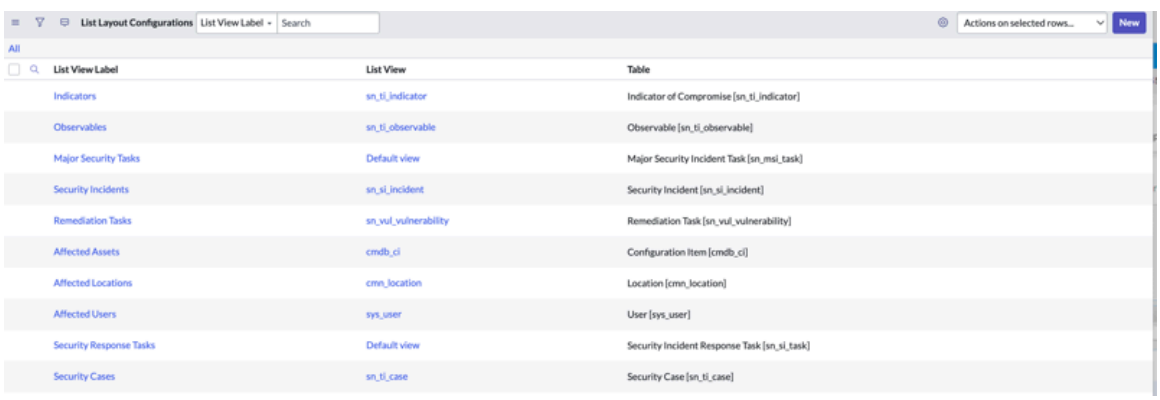
Nom	Description
Entrées	• sourceSysId : ID système de l'enregistrement de la table source qui est soit en cours de liaison/proposé/promu. • msiSysId : ID système de l'incident de sécurité majeur auquel l'enregistrement source est lié/proposé/promu.
Sortie	Aucune valeur de retour de sortie.
Responsabilité	Le script doit déployer les informations dans la table d'enregistrement lié ou sn_msi_m2m_child. • Utilisez sourceSysID pour interroger les données à partir de tables de ServiceNow relations. • Une fois les données extraites, déployez-les dans un enregistrement lié (sn_msi_m2m_child) à l'aide de l'utilitaire MSIRollupEngine pour déployer les données.

Configurer la mise en page de la liste dans Gestion des incidents de sécurité majeurs

Configurez la mise en page de la liste pour personnaliser la mise en page et les étiquettes utilisées dans l'espace de travail, notamment les Gestion des incidents de sécurité majeurs onglets Impact de l'incident, Enregistrements liés et Threat Intelligence.

Rôle requis : admin et sn_msi.workspace_admin.

Remarque : L'administrateur système peut créer l'enregistrement et l'administrateur de l'espace de travail MSI peut le mettre à jour.

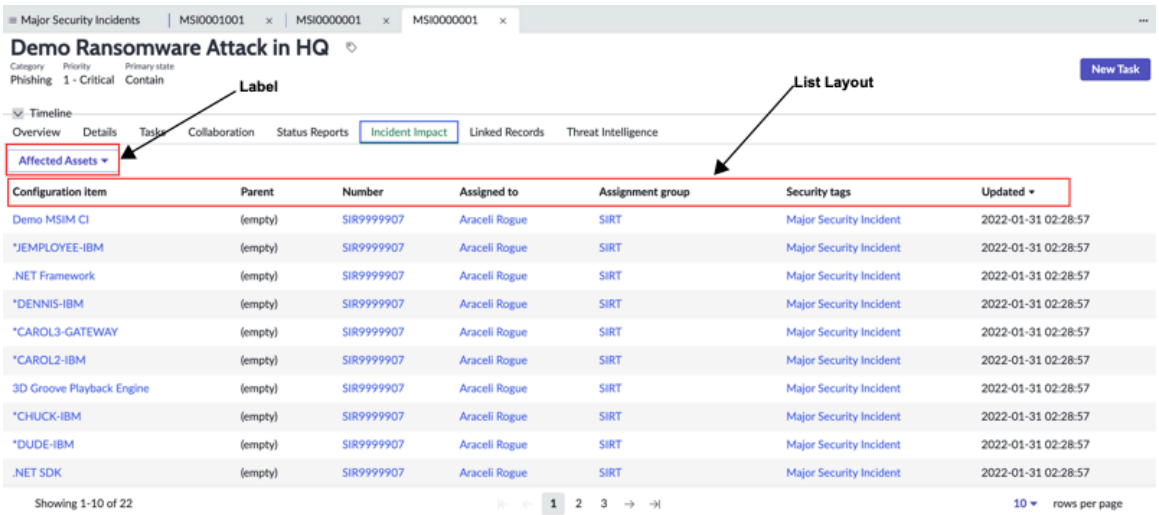


Les configurations de mise en page de liste ont déjà été expédiées pour les tables connues existantes affichées dans l'espace Gestion des incidents de sécurité majeurs de travail.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si vous souhaitez afficher la vue personnalisée pour les tables existantes, vous pouvez mettre à jour l'enregistrement de table respectif dans la configuration de mise en page de liste avec la vue de liste personnalisée.
- Pour les nouvelles tables de tâches, vous pouvez créer une nouvelle configuration de mise en page de liste afin d'afficher la vue de liste personnalisée et les étiquettes. Pour une procédure plus détaillée, voir comment Étape 4. Créer une vue pour un nouvel onglet d'enregistrement lié pour un ticket de sécurité



Exemple d'implémentation de cas d'utilisation de déploiement pour un ticket de sécurité

Les étapes suivantes expliquent un exemple de cas d'utilisation sur la façon d'ajouter la prise en charge de la liaison/de la proposition/de la promotion vers un incident de sécurité majeur pour une table de ticket de sécurité.

- Étape 1. Créer une configuration d'enregistrement lié pour un ticket de sécurité
- Étape 2. Créer une vue pour la fenêtre modale d'un ticket de sécurité
- Étape 3. Créer des actions d'interface utilisateur pour la table source d'un ticket de sécurité
- Étape 4. Créer une vue pour un nouvel onglet d'enregistrement lié pour un ticket de sécurité
- Étape 5. Ajouter des listes de contrôle d'accès (ACL) pour Gestion des incidents de sécurité majeurs les utilisateurs de l'espace de travail
- Étape 6. Créer des règles métier pour un ticket de sécurité
- Étape 7. Créer des configurations d'enregistrement de déploiement

Étape 1. Créer une configuration d'enregistrement lié pour un ticket de sécurité

Créez une configuration d'enregistrement lié pour un ticket de sécurité.

Avant de commencer
Rôle requis : admin et sn_msi.workspace_admin

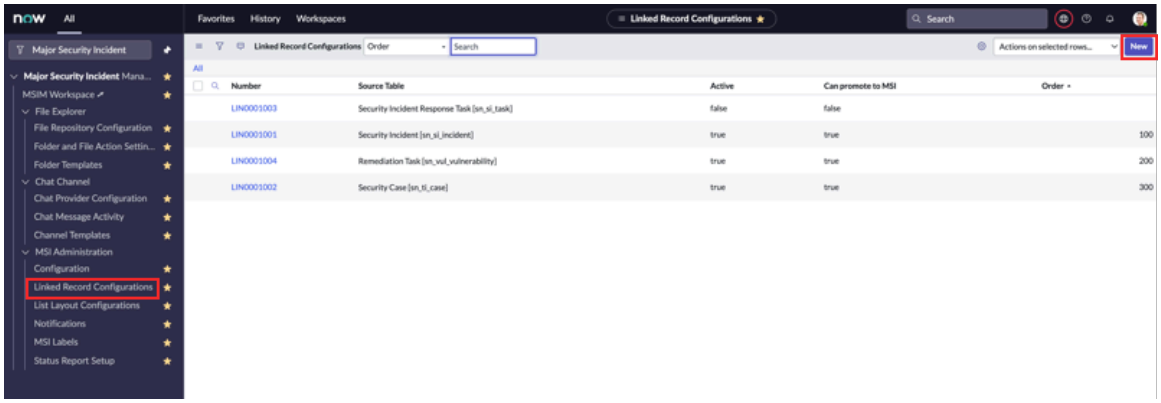
Remarque : L'administrateur système peut créer l'enregistrement et l'administrateur de l'espace de travail MSI peut le mettre à jour.

Traduction automatique

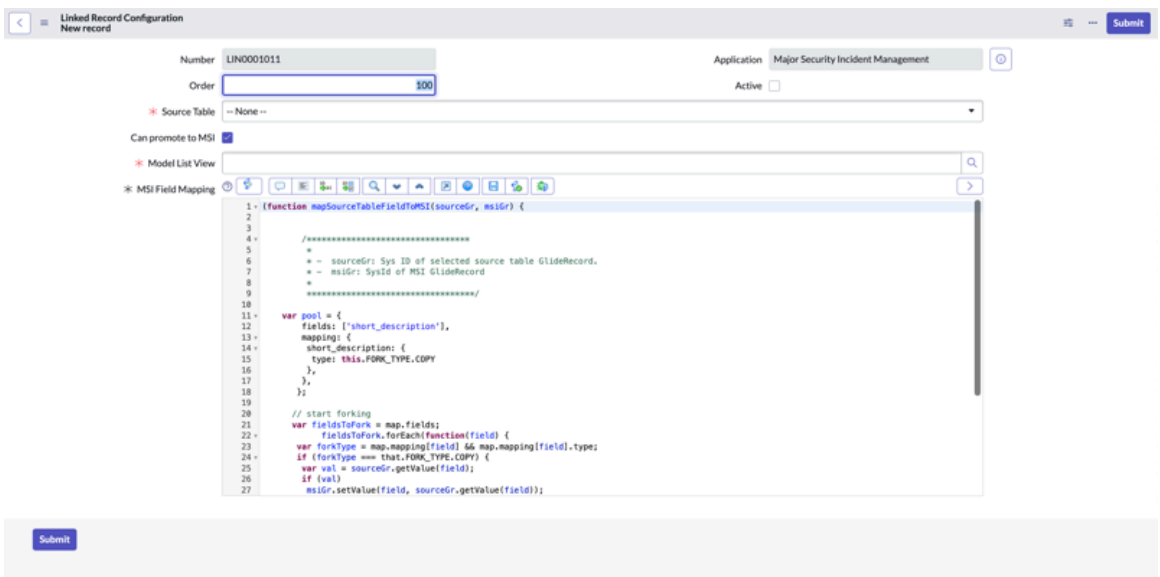
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Recherchez la configuration d'enregistrement lié dans le volet de navigation de gauche.
2. Cliquez sur **Nouveau**.



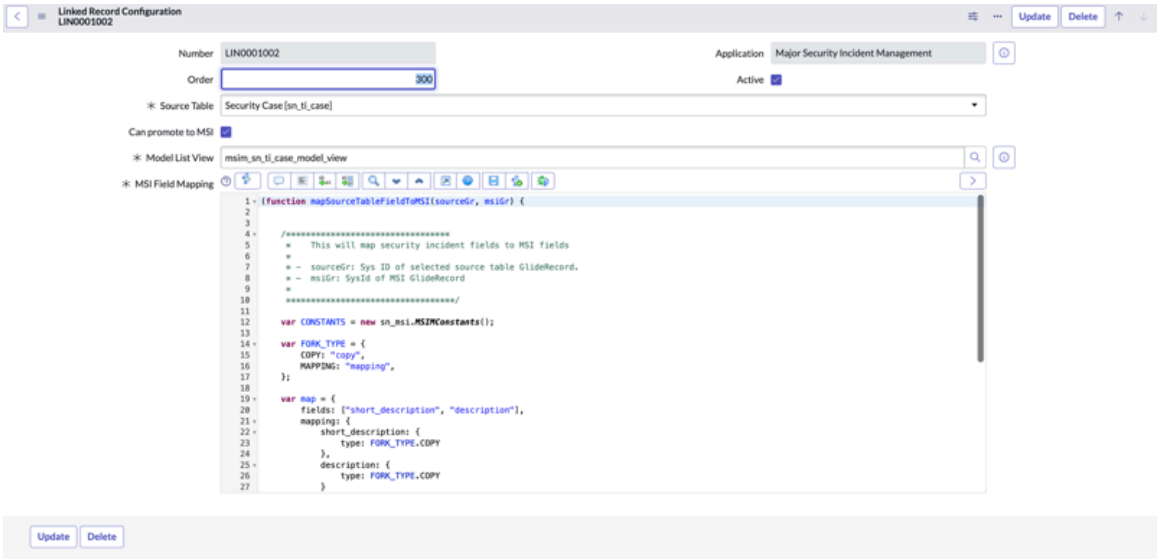
3. Remplissez le formulaire avec les colonnes requises et écrivez un script de mappage de champ.



4. Vous avez créé une configuration d'enregistrement lié pour le ticket de sécurité en ajoutant les valeurs décrites dans la table suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Nom	Description
Table source	Ticket de sécurité (sn_ti_case). Ici, dans cet exemple, liez/promouvez/proposez un ticket de sécurité en tant que MSI.
Ordre	Valeur d'entrée : 300 **Remarque :** L'ordre inférieur est prioritaire sur les ordres supérieurs. Étant donné qu'un ticket de sécurité est d'un ordre supérieur à celui de l'incident de sécurité et de la tâche de rattrapage, il apparaîtra dans la dernière séquence.
Peut convertir en MSI	Vrai, cochez cette case pour promouvoir le ticket de sécurité en MSI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
	Remarque : ◦ Lier et dissocier les enregistrements de tickets de sécurité aux incidents de sécurité majeurs à partir de l'espace de Gestion des incidents de sécurité majeurs travail. De plus, la fonctionnalité Dissocier l'enregistrement n'est visible que pour les enregistrements liés. ▪ Cela permet de lier, de promouvoir et de proposer un ticket de sécurité à un incident de sécurité majeur à l'aide d'actions d'environnement classiques, mais ces actions d'interface utilisateur ne sont pas disponibles prêtes à l'emploi. Chaque action d'interface utilisateur doit être créée manuellement. Pour plus d'informations, consultez Étape 3. Créer des actions d'interface utilisateur pour la table source d'un ticket de sécurité. ▪ Les actions d'interface utilisateur Lier/Promouvoir/Proposer sont disponibles pour l'incident de sécurité, la tâche de rattrapage et le ticket de sécurité prêtes à l'emploi. ◦ La page d'enregistrement lié de l'espace de travail MSIM affiche les enregistrements de tickets de sécurité liés. Reportez-vous à l'image 1 ci-dessous pour afficher les options disponibles après avoir coché cette case.
Vue de liste modale	msim_sn_ti_case_model_view **Remarque :** Cette vue contient des champs et l'ordre des champs affichés dans la vue de liste sur le modal d'enregistrement de lien dans l'espace de travail MSIM. Pour plus d'informations, voir Étape 2. Créer une vue pour la fenêtre modale d'un ticket de sécurité Reportez-vous à l'image 2 ci-dessous pour afficher à partir de la page **Enregistrements liés** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
Script de mappage de champs	Ce script décrit les champs de l'enregistrement des tables sources mappé à l'incident de sécurité majeur nouvellement créé lorsque l'enregistrement des tables sources est proposé ou promu. qui recevront des entrées : ◦ sourceGr : objet d'enregistrement Glide de ticket de sécurité ◦ msiGr : objet d'enregistrement Glide d'incident de sécurité majeur Le script lit la brève description du ticket de sécurité et la copie comme titre dans un incident de sécurité majeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Image 1 : Peut convertir en MSI

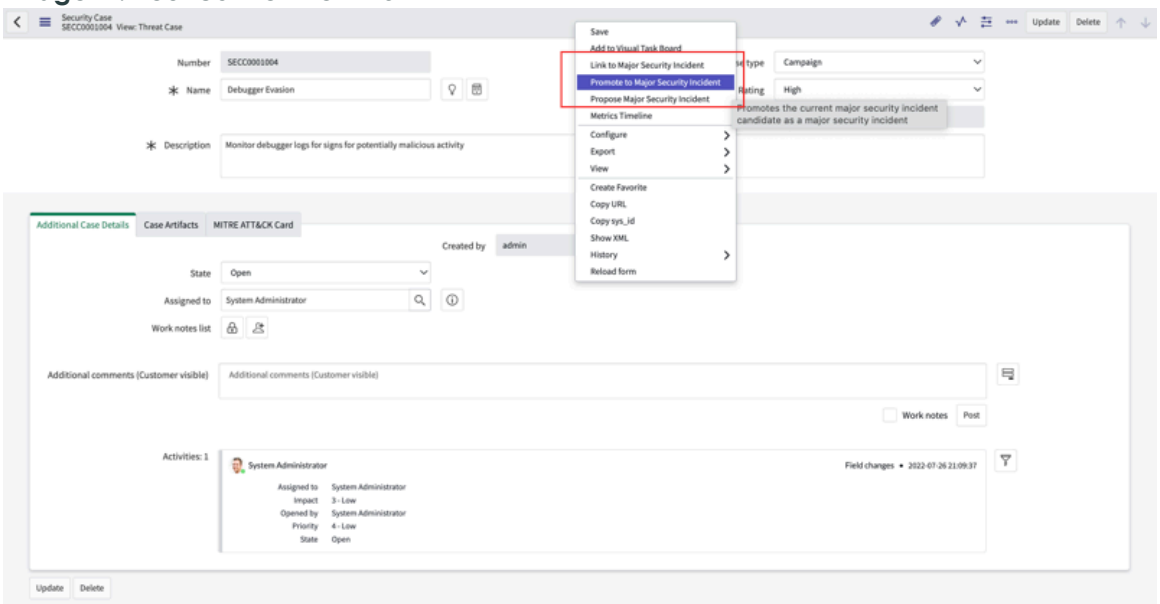
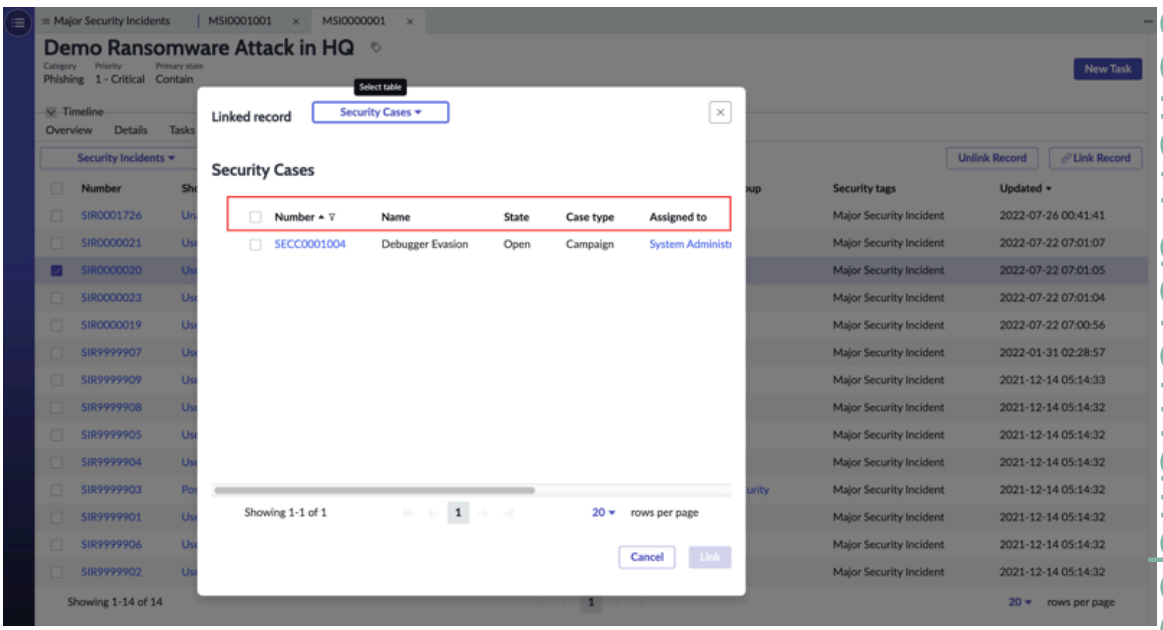


Illustration 2. Vue modale



Traduction automatique

Étape 2. Créer une vue pour la fenêtre modale d'un ticket de sécurité

Créez une vue pour la fenêtre modale d'un ticket de sécurité.

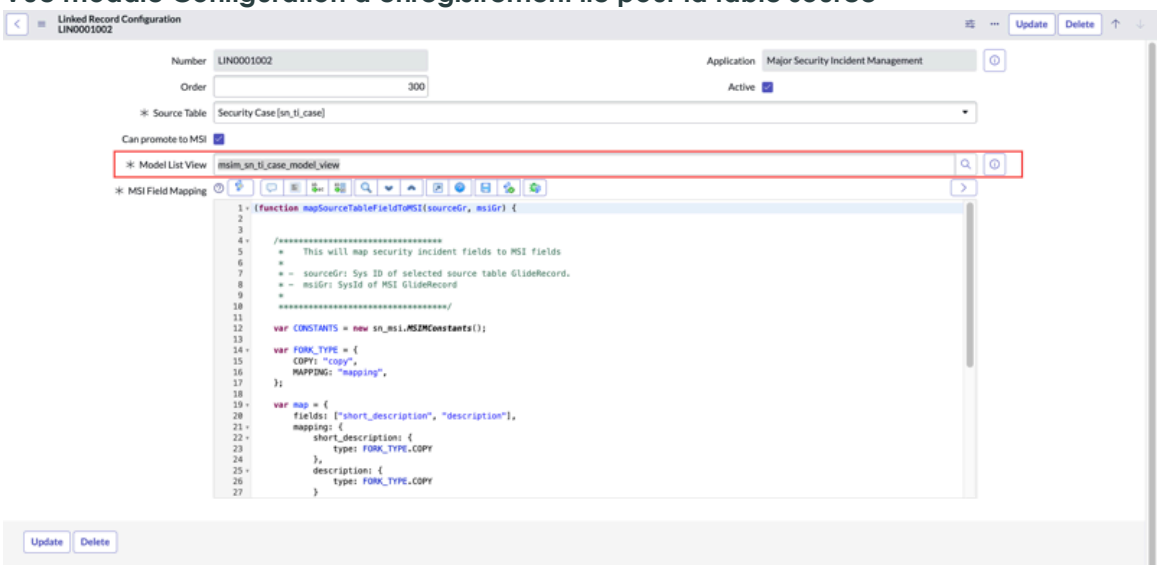
Avant de commencer

Élément clé à prendre en compte :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Par défaut, la liste modale d'enregistrement lié affiche uniquement la mise en page de liste **par défaut** . Si vous souhaitez personnaliser la mise en page de la liste, vous pouvez le faire à l'aide de **l'option Vue personnalisée** de la table source.
- Si vous souhaitez afficher la vue personnalisée, celle-ci doit également être sélectionnée dans la configuration d'enregistrement lié pour la table source.

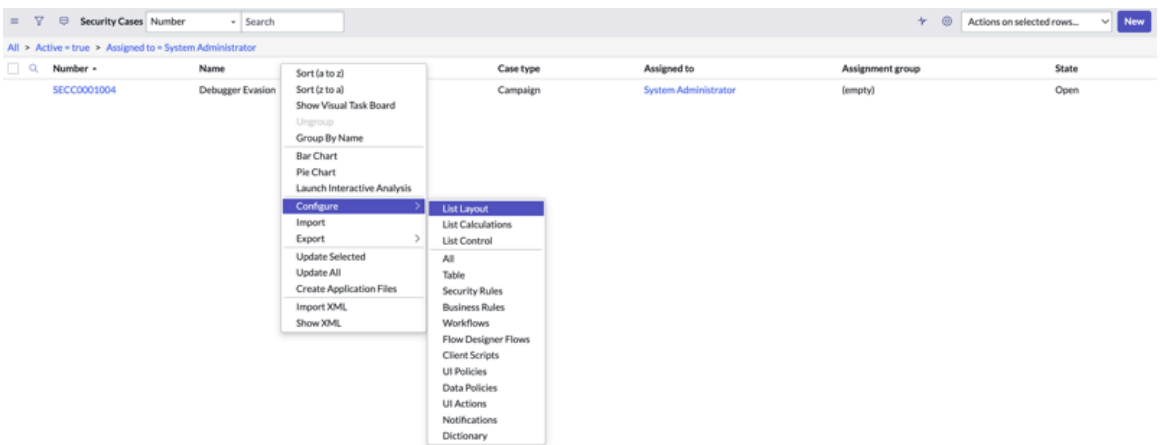
Vue modale Configuration d'enregistrement lié pour la table source



Rôle requis : administrateur

Procédure

1. Accédez à la table source et cliquez sur **Configurer** > **Mise en page de la liste**.



2. Accéder à **Vue liste** > **Nom de vue**.
3. Cliquez sur **Nouveau** dans la liste déroulante Nom de la vue et créez une vue, par exemple msim_sn_ti_case_modal_view.
4. Sélectionnez la vue nouvellement créée.
   Une fois cette option sélectionnée, vous pouvez choisir les champs requis dans la liste Disponible.
5. Cliquez sur **Enregistrer**.
6. Accédez à la **Menu** > **Vues** pour vérifier si la vue s'est correctement rendue.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étape 3. Créer des actions d'interface utilisateur pour la table source d'un ticket de sécurité

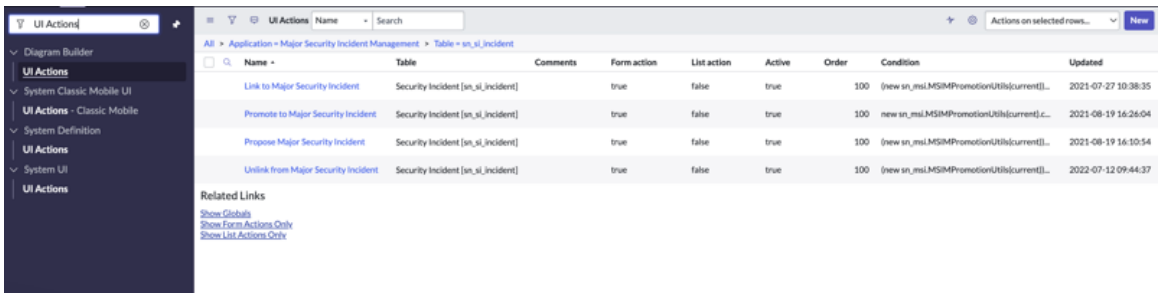
Créez des actions d'interface utilisateur pour la table source d'un ticket de sécurité.

Avant de commencer

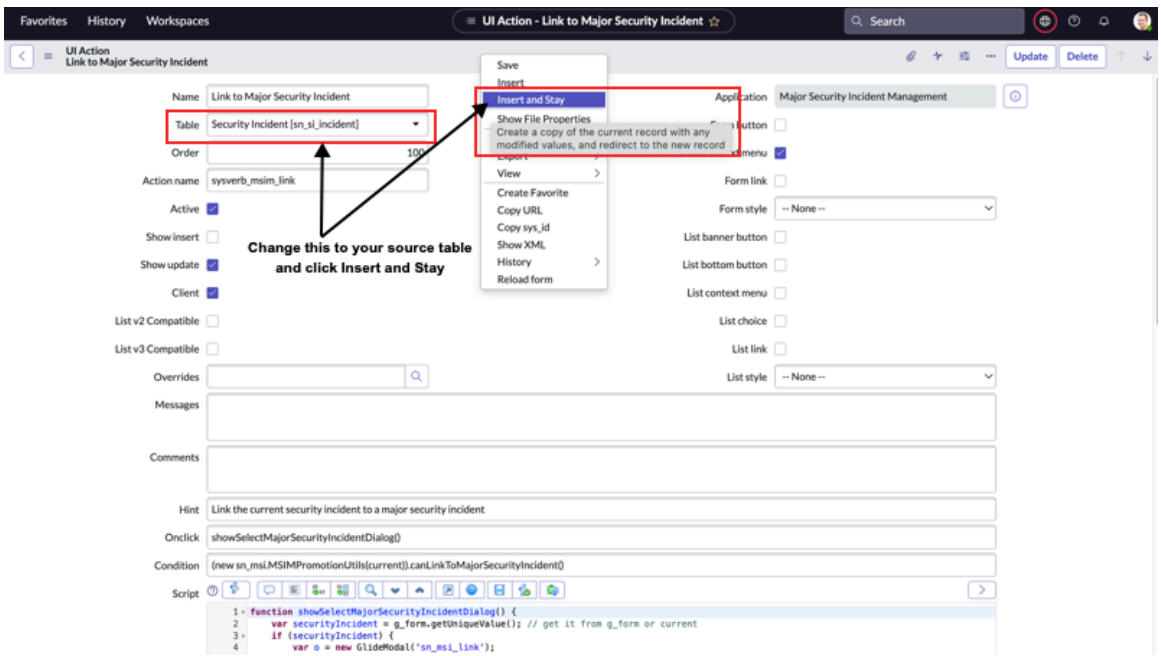
Rôle requis : administrateur

Procédure

1. Accédez à la **Définition du système** > **Actions d'interface utilisateur**.
2. Exécutez l'option Filtre pour filtrer la liste par **Application** : Gestion des incidents de sécurité majeurs et **Table** : sn_si_incident.



3. Sélectionnez chaque action d'interface utilisateur une par une et enregistrez les détails de la table source.



4. Répétez les mêmes étapes que ci-dessus pour les actions d'interface utilisateur suivantes :
   - Lier à l'incident de sécurité majeur
   - Incident de sécurité majeur proposé
   - Dissocier d'un incident de sécurité majeur
   - Promouvoir en incident de sécurité majeur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

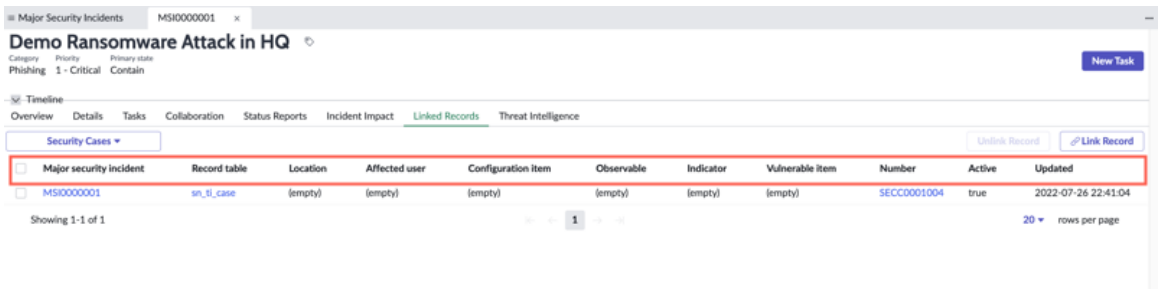
Étape 4. Créer une vue pour un nouvel onglet d'enregistrement lié pour un ticket de sécurité

Personnalisez la mise en page de la liste d'une table de tickets de sécurité lorsqu'elle s'affiche sur la page Lier les enregistrements avec l'espace Gestion des incidents de sécurité majeurs de travail.

Avant de commencer

Conditions préalables :

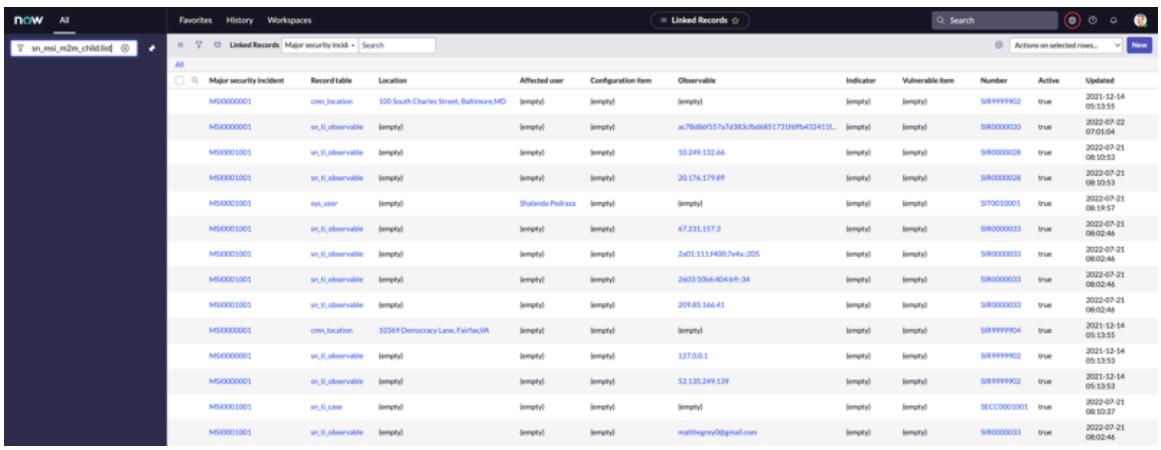
- Choisissez la colonne qui doit être visible lorsqu'une liste est restituée pour une table de ticket de sécurité.
- Choisissez l'ordre des champs à afficher dans la liste déroulante.



Rôle requis : administrateur

Procédure

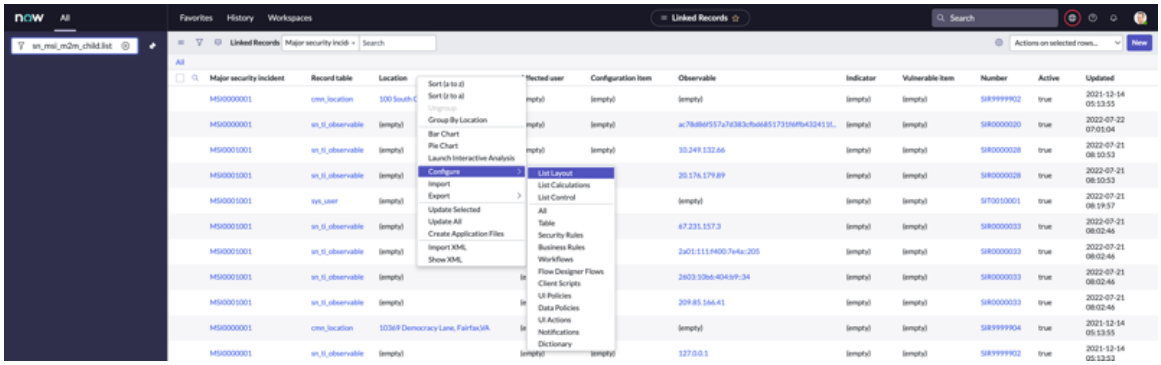
1. Recherchez **sn_msi_m2m_child.list** à l'aide du volet de navigation de gauche.
   La table Enregistrements liés s'affiche.



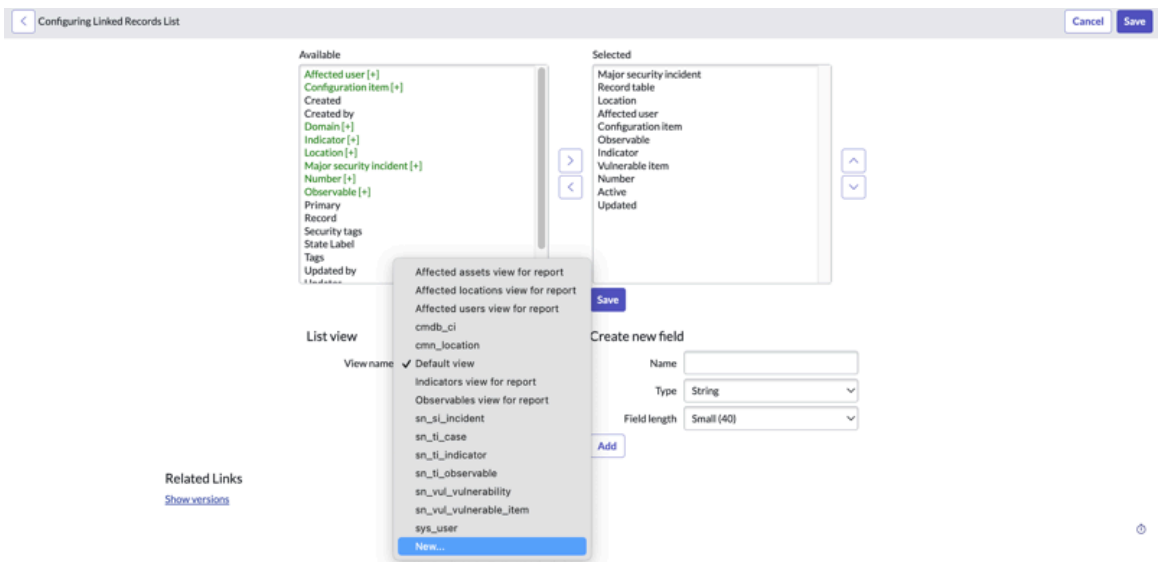
2. Cliquez avec le bouton droit sur l'en-tête et sélectionnez **Configurer** > **Mise en page de la liste**.
   La page Configuration de la liste des enregistrements liés s'affiche.

Traduction automatique

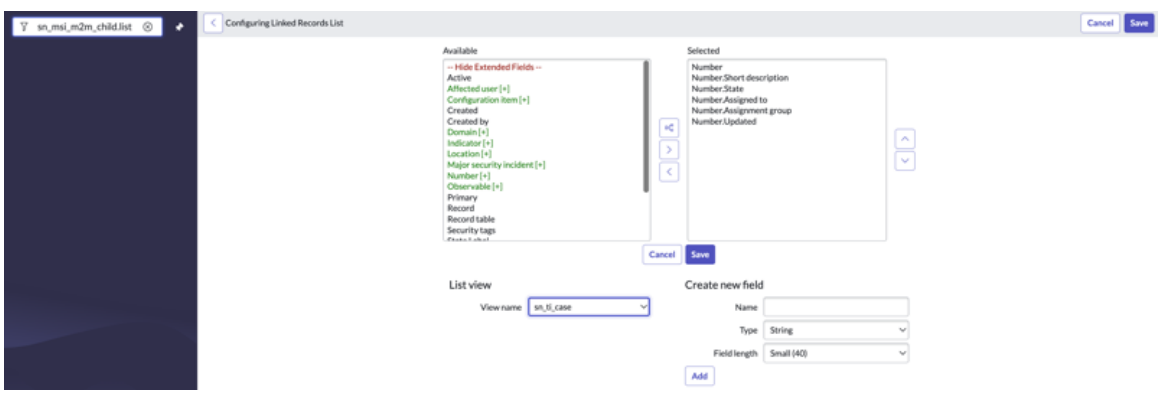
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Accéder à **Vue liste** > **Nom de vue**.
4. Sélectionnez **Nouveau** dans la liste déroulante Nom de vue.



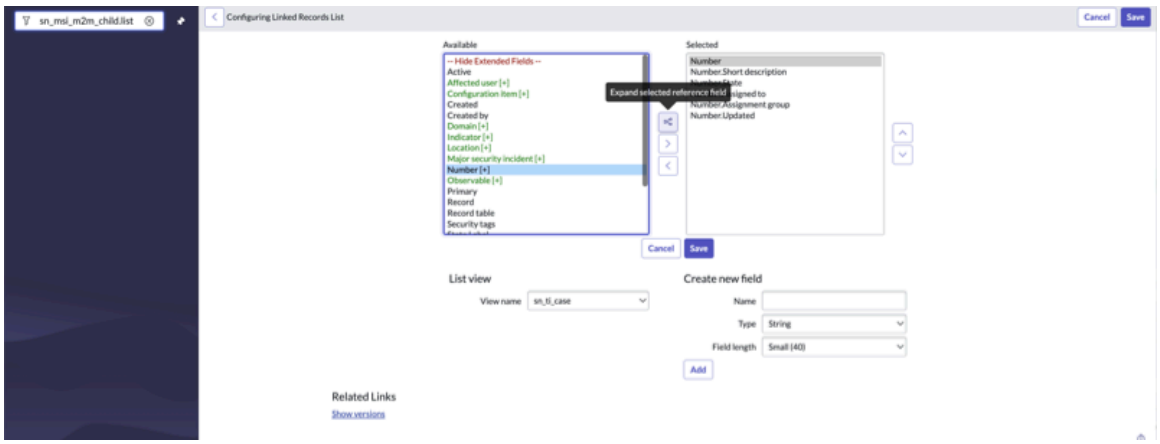
5. Sélectionnez les colonnes qui s'afficheront dans la vue de liste de l'espace de travail. L'enregistrement du ticket de sécurité est stocké dans la colonne **Numéro** . Pour afficher les informations d'un ticket de sécurité, vous devez effectuer une remontée pas à pas sur la colonne **Numéro** .



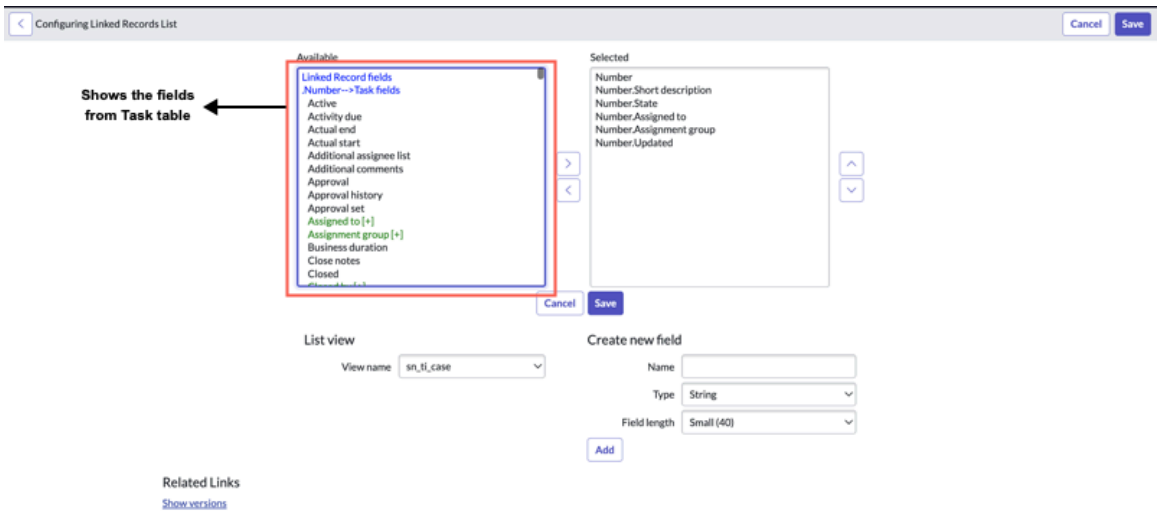
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Pour effectuer une remontée pas à pas, sélectionnez d'abord la colonne **Nombre** dans la liste Disponible, puis cliquez sur **Développer le champ de référence sélectionné**.



b. Développez les colonnes à partir de **Numéro** pour les sélectionner et déplacez-les vers la liste Sélectionné.



c. Cliquez sur **Enregistrer** pour enregistrer et créer une vue.

6. L'étape suivante consiste à afficher la vue créée dans l'espace Gestion des incidents de sécurité majeurs de travail, vous devez créer une **configuration de mise en page de liste**.

a. Recherchez la configuration de la **mise en page de la liste** à l'aide du volet de navigation de gauche.

b. Cliquer sur **Administration MSI** > **Configurations des mises en page de listes**.

c. Cliquez sur **Nouveau** pour créer une nouvelle configuration.

d. Sélectionnez la table source dans la colonne Table et sélectionnez la vue nouvellement créée dans le champ Vue de liste.

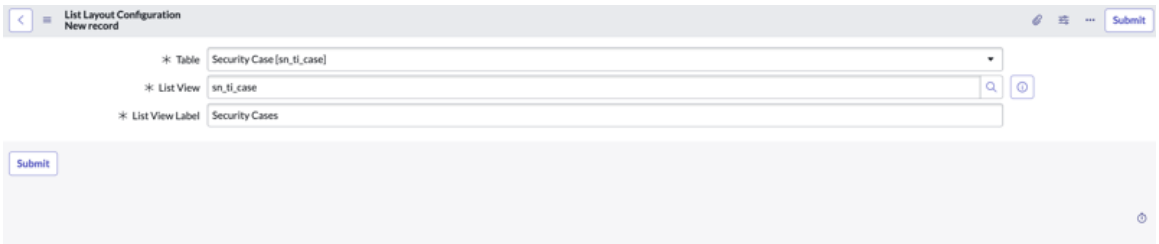
e. L'étiquette **Vue de liste** vous permet de contrôler les étiquettes lorsque la même table source est restituée dans l'espace Gestion des incidents de sécurité majeurs de travail.

f. Enregistrez l'enregistrement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Une fois l'enregistrement enregistré, accédez à l'espace Gestion des incidents de sécurité majeurs de travail pour afficher la vue de liste et l'étiquette restituées dans l'espace de travail.



Étape 5. Ajouter des listes de contrôle d'accès (ACL) pour Gestion des incidents de sécurité majeurs les utilisateurs de l'espace de travail

Ajoutez des listes de contrôle d'accès (ACL) pour Gestion des incidents de sécurité majeurs les utilisateurs de l'espace de travail.

Avant de commencer

Rôle requis : administrateur

Remarque : Les autorisations requises pour lier et dissocier des options sont contrôlées par le rôle sn_msi.linkedsivi_read .

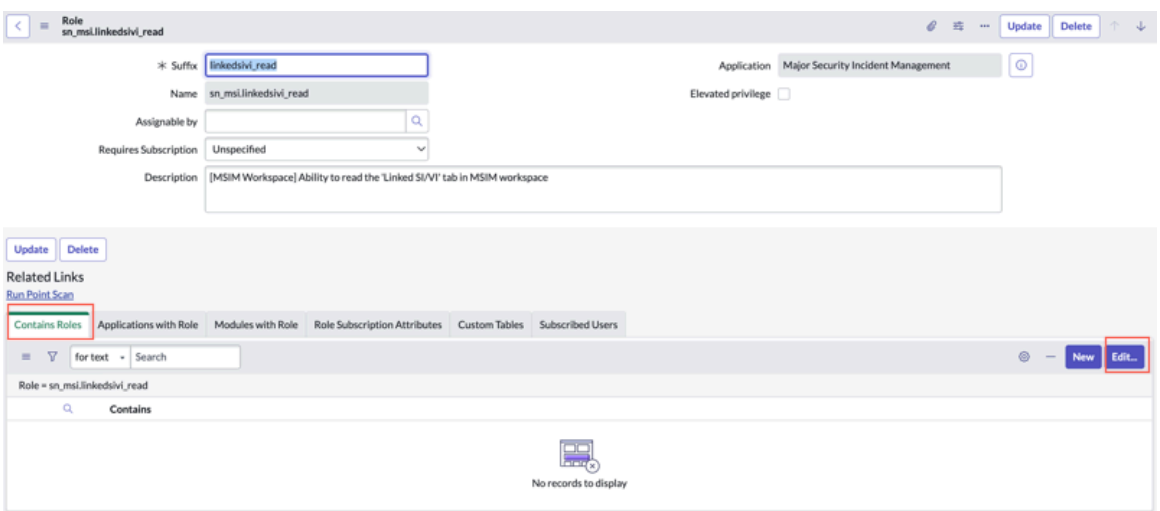
Gestion des incidents de sécurité majeurs Le profil contient le rôle sn_msi.linkedsivi_read.

1. sn_msi.workspace_admin (administrateur de l'espace de travail MSIM)
2. sn_msi.workspace_manager (Gestionnaire de l'espace de travail MSIM)
3. sn_msi.workspace_responder (répondeur de l'espace de travail MSIM)

Remarque : Pour n'importe quelle table source, vous devez vous assurer que les rôles requis sont ajoutés au rôle sn_msi.linkedsivi_read .

Procédure

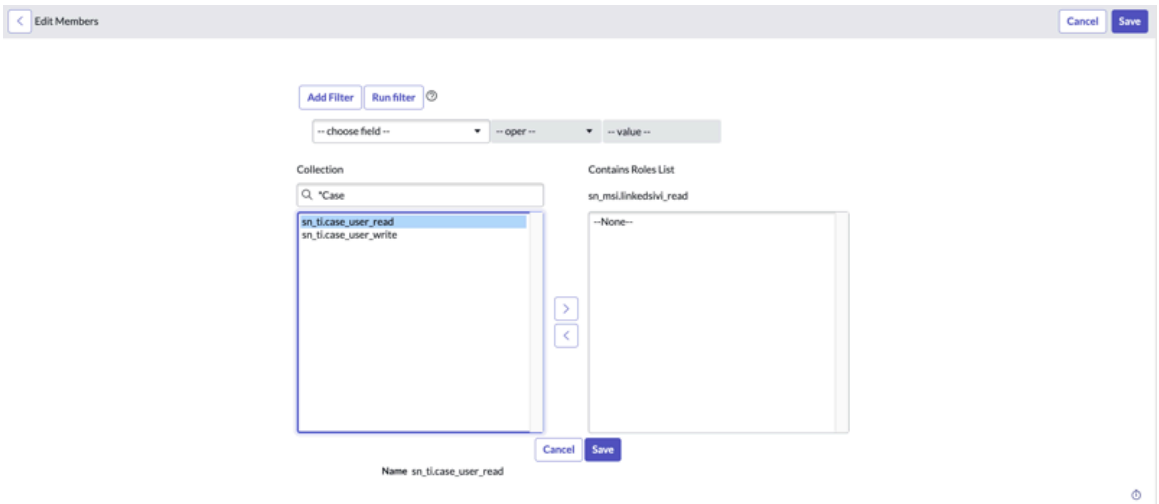
1. Accédez à la **Administration utilisateurs** > **Rôles** et recherchez **le rôle sn_msi.linkedsivi_read** .
2. Cliquez sur **Modifier** dans la section de la liste connexe Contient les rôles.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Assurez-vous que vos rôles de table source sont ajoutés dans la section Contient les rôles. La page Modifier les membres s'affiche pour configurer les rôles requis pour un ticket de sécurité.



4. Recherchez les rôles dans la table source, dans la section Collections. Sélectionnez les rôles requis qui autorisent l'accès en lecture et en écriture sur la table source pour un ticket de sécurité.

Remarque :

- Pour un ticket de sécurité, deux rôles distincts pour la lecture et l'écriture sont nécessaires.
- Accès en écriture sur les tables pour la possibilité de sélectionner l'enregistrement source à partir du modal d'enregistrement lié à l'espace de Gestion des incidents de sécurité majeurs travail.

5. Cliquez sur **Enregistrer** pour ajouter des rôles.
6. Vérifiez que les rôles sont correctement ajoutés à la section de liste connexe **Contient les rôles** .

Étape 6. Créer des règles métier pour un ticket de sécurité

Créez les règles métier requises pour un ticket de sécurité.

Avant de commencer
Rôle requis : administrateur

Créez les trois règles métier suivantes pour la nouvelle table source Ticket de sécurité (sn_ti_case). Ces règles métier sont nécessaires pour maintenir la cohérence du comportement avec la table source prête à l'emploi fournie telle que Incident de sécurité (sn_si_incident).

Règles métier pour la nouvelle table source :

1. **Désactiver le lien lorsqu'il est inactif** : une fois le ticket de sécurité fermé, les informations connexes ne s'affichent plus dans Gestion des incidents de sécurité majeurs la page de l'espace de travail.
2. **Synchroniser les informations d'équipe lors de la mise à jour : l'onglet** Détails de l'incident de sécurité majeur affiche les informations sur toutes les équipes actives et les utilisateurs travaillant sur différentes tâches. Une fois que nous avons mis à jour l'utilisateur ou le groupe d'affectation affecté est modifié dans le ticket de sécurité, nous devons mettre à

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

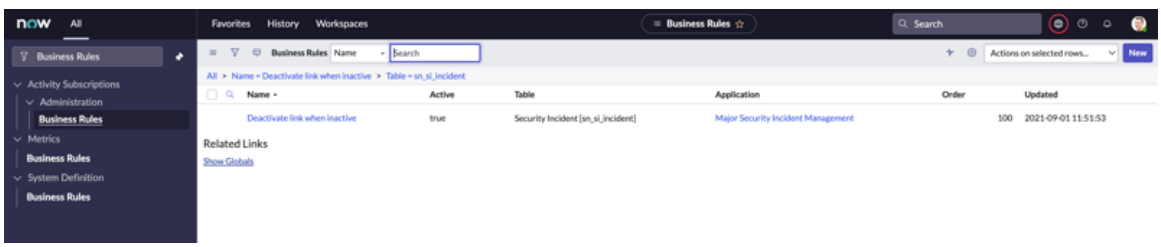
jour les informations de l'équipe de ticket de sécurité dans la section de l'équipe active de l'incident de sécurité majeur. Ces règles métier mettront à jour le nouvel utilisateur affecté et le nouveau groupe d'affectation dans la section Équipe active.

3. **Synchroniser les informations d'équipe lors de la suppression : l'onglet** Détails de l'incident de sécurité majeur affiche les informations sur toutes les équipes actives et les utilisateurs travaillant sur différentes tâches. Une fois que nous avons fermé le ticket de sécurité, nous n'avons plus besoin d'afficher les informations de l'équipe de ticket de sécurité dans la section de l'équipe active de l'incident de sécurité majeur. Ces règles métier suppriment l'utilisateur et le groupe d'affectation affectés de l'équipe active.

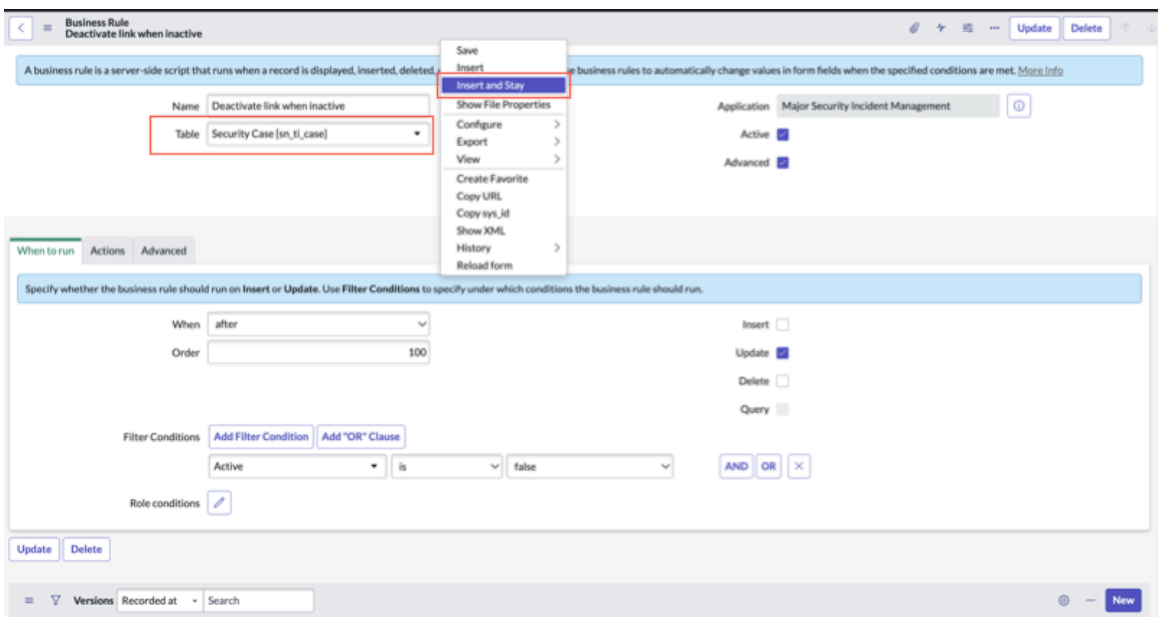
Créez des règles métier pour la nouvelle table source :

Procédure

1. Accédez à la **Définition du système** > **Règles métier**.
2. Exécutez l'option de filtre pour filtrer les critères de règles métier avec les informations ci-dessous :
   - **Nom** : désactiver le lien lorsqu'il est inactif
   - **Table** : sn_si_incident



3. Ouvrez l'enregistrement et remplacez le nom de table par une nouvelle table source : sn_ti_case.
4. Cliquez avec le bouton droit sur le menu de la page, puis cliquez sur **Insérer et rester** pour créer l'enregistrement.



5. Répétez également la procédure pour deux autres règles métier.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Synchroniser les informations de l'équipe lors de la suppression
- Synchroniser les informations d'équipe lors de la mise à jour

Étape 7. Créer des configurations d'enregistrement de déploiement

Créez une configuration d'enregistrement de déploiement pour lier et dissocier des enregistrements supplémentaires à MSI.

Avant de commencer

Rôle requis : admin et sn_msi.workspace_admin

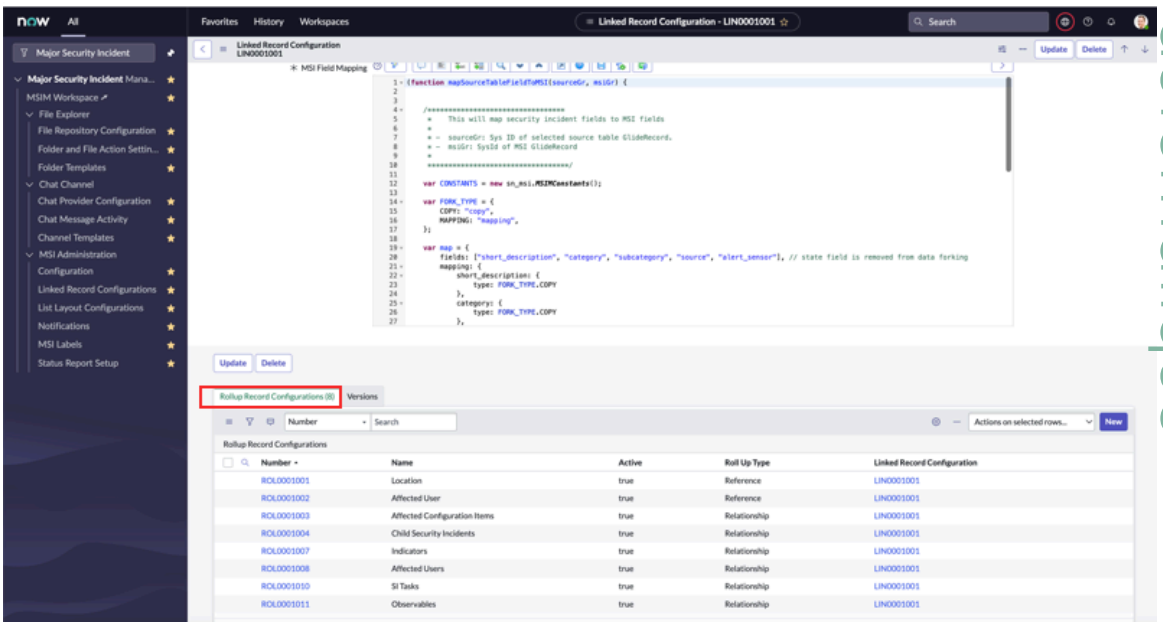
Remarque : L'administrateur système peut créer l'enregistrement et l'administrateur de l'espace de travail MSI peut le mettre à jour.

Pour déployer des informations telles que des éléments de configuration, des observables et un indicateur de compromission liées à un ticket de sécurité, créez une configuration d'enregistrement de déploiement.

Procédure

1. Accédez à la **Réponse aux incidents de sécurité majeurs** > **Configuration des enregistrements liés**.
   La page Configurations d'enregistrement lié s'affiche.
2. Sélectionnez ou créez un nouvel enregistrement lié et accédez à la section **Configuration de l'enregistrement de déploiement** à partir de la même page.

Section Configuration d'enregistrement de déploiement



Que faire ensuite

- Pour plus d'informations, voir Configurer les enregistrements de déploiement dans Gestion des incidents de sécurité majeurs
- Pour obtenir des exemples d'informations sur un ticket de sécurité, consultezÉcriture d'un script pour un ticket de sécurité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Écriture d'un script pour un ticket de sécurité

Écriture d'un script pour un ticket de sécurité afin de déployer la configuration d'enregistrement.

Avant de commencer

Rôle requis : admin et sn_msi.workspace_admin

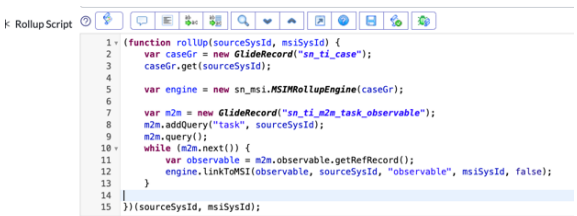
Remarque : L'administrateur système peut créer l'enregistrement et l'administrateur de l'espace de travail MSI peut le mettre à jour.

Procédure

1. Recherchez les configurations d'enregistrement lié à l'aide du volet de navigation de gauche.
2. Accédez à la **Administration MSI** > **Configuration d'enregistrement lié**.
3. Ouvrez l'enregistrement de configuration qui a été créé pour un ticket de sécurité.
4. La configuration de l'enregistrement de déploiement s'affiche dans la section Liste connexe.
5. Cliquez sur **Nouveau** pour créer une configuration d'enregistrement de déploiement.

   Voici un exemple d'enregistrement créé pour déployer les données observables liées au ticket de sécurité que nous essayons de déployer avec les valeurs de champ comme suit :

Nom	Description
Type de déploiement	Relation **Remarque :** Les informations observables sont disponibles sous la forme d'une liste connexe.

Script de déploiement	L'entrée sourceSysId contient l'ID système du ticket de sécurité et msiSysId contient l'ID système de l'incident de sécurité majeur.
	
	
	Rollup Script
	1 (function rollUp(sourceSysId, msiSysId) {
	2 var caseGr = new GlideRecord("sn_ti_case");
	3 caseGr.get(sourceSysId);
	4
	5 var engine = new sn_msi.MSIMRollupEngine(caseGr);
	6
	7 var m2m = new GlideRecord("sn_ti_m2m_task_observable");
	8 m2m.addQuery("task", sourceSysId);
	9 m2m.query();
	10 while (m2m.next()) {
	11 var observable = m2m.observable.getRefRecord();
	12 engine.linkToMSI(observable, sourceSysId, "observable", msiSysId, false);
	13 }
	14
	15 })(sourceSysId, msiSysId);
	
	◦ `Line 2: As a first step, query for Glide Record for sourceSysId from` **`Security Case(sn_ti_case)`** `table.`
	
	◦ `Line 7: Next, query` **`sn_ti_m2m_task_observable`** `table using security case sys`

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
	ID to figure out all the linked observables to a security case. ◦ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method: *MSIMRollupEngine.linkToMSI(« entityGr », « sourceSysId », « fieldNameInLinkedRecordTable », « msiSysId », « isPrimaryRecord »)*

Effectuer un déploiement atomique à la demande

Le cadre de travail de déploiement ne peut pas gérer les mises à jour des enregistrements liés existants. Dans de tels cas, un déploiement atomique à la demande doit se produire pour les enregistrements liés, ce qui peut être réalisé via des règles métier.

Pour capturer les mises à jour des enregistrements liés, des règles métier doivent être créées sur la table source.

Ces règles métier fonctionnent sur les opérations d'insertion, de mise à jour et de suppression. Lorsque vous effectuez une opération d'insertion ou de mise à jour, vous devez ajouter ou mettre à jour les informations cumulées dans MSI. Si vous effectuez une suppression, les informations cumulées seront supprimées de MSI.

Par exemple, une fois qu'un incident de sécurité est lié à MSI, les informations connexes seront déployées automatiquement MSI. Mais plus tard, si vous ajoutez un nouvel observable à un MSI, alors l'observable nouvellement ajouté sera également déployé dans MSI. Ici, la règle métier **Synchroniser l'observable déployé** capture la mise à jour et déploie l'enregistrement mis à jour dans MSI. De même, la même règle métier gère également la suppression des observables cumulés existants, s'ils sont supprimés de l'incident de sécurité.

Règles métier prédéfinies

Voici quelques règles métier prédéfinies qui vous aident à comprendre comment gérer les déploiements atomiques

Règle	Description
Indicateur de synchronisation cumulée (sn_ti_m2m_task_indicator)	Utilisez cette règle métier pour gérer le déploiement et la suppression de l'indicateur de compromission de l'incident de sécurité, du ticket de sécurité et de la tâche de rattrapage.
Synchroniser l'observable déployé (sn_ti_m2m_task_observable)	L'utilisation de cette règle métier gère le déploiement et la suppression des observables liés de l'incident de sécurité, du ticket de sécurité et de la tâche de rattrapage.
Synchroniser l'utilisateur affecté cumulé (sn_si_m2m_task_affected_user)	L'utilisation de cette règle métier gère le déploiement et la suppression des utilisateurs

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles métier prédéfinies

Voici quelques règles métier prédéfinies qui vous aident à comprendre comment gérer les déploiements atomiques

(suite)

Règle	Description
	affectés liés de l'incident de sécurité, du ticket de sécurité et de la tâche de rattrapage.
CI affectés synchronisés et reportés (task_ci)	L'utilisation de cette règle métier gère le déploiement et la suppression des éléments de configuration associés de l'incident de sécurité, du ticket de sécurité et de la tâche de rattrapage.

Intégrations de Réponse aux incidents de sécurité

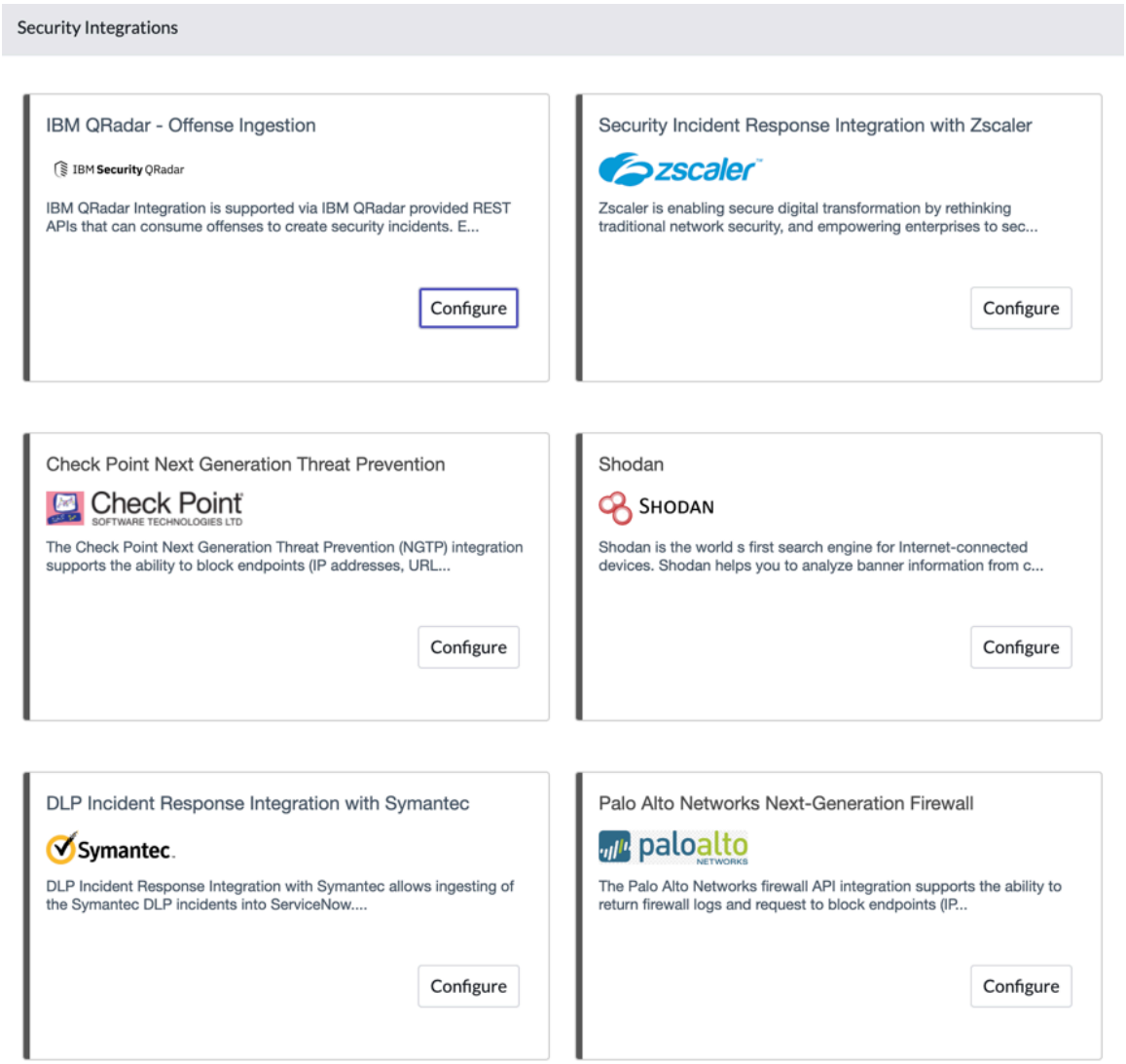
Opérations de sécurité Toutes les applications principales et les intégrations tierces non essentielles sont disponibles à partir du ServiceNow Store. Cette section fournit des instructions pour l'activation des intégrations et la configuration ServiceNow des intégrations tierces. Vous y trouverez également des directives de base pour le développement de vos propres intégrations, ainsi que des détails sur les intégrations spécifiques incluses dans le système de base.

Configurations d'intégration

Le système de base comprend une série de « cartes » pour chacune des implémentations d'intégration que vous pouvez activer et utiliser. En outre, des cartes s'affichent pour toutes les intégrations publiées sur le ServiceNow Store qui ont des dépendances sur Opérations de sécurité des modules d'extension. Vous pouvez afficher les cartes d'intégration en sélectionnant **Security Operations** > **Configurations d'intégration**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez filtrer les intégrations visibles à l'aide du menu déroulant **Catégorie** . Le menu déroulant **Afficher les configurations** vous permet de voir plusieurs instances d'implémentations qui autorisent leur création.

Boutons sur les cartes d'intégration

Les cartes d'intégration affichent différents boutons en fonction de l'état actuel de l'intégration et de la source de la carte.

Bouton	Description
Installer le module d'extension	Cliquez sur ce bouton pour installer le module d'extension applicable afin d'activer l'intégration. Une fois le module d'extension installé, le bouton bascule sur **Configurer**.
Configurer	Cliquez sur ce bouton pour entrer les informations de configuration de l'intégration. Pour certaines intégrations, vous devrez peut-être saisir des clés API ou des URL acquises à partir du site Web de l'intégration tierce.
Nouveau	Certaines intégrations, telles que Carbon Black et IBM QRadar, vous permettent de définir plusieurs implémentations d'une même intégration. Pour ces intégrations, cliquez sur **Nouveau** une fois le module d'extension

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bouton	Description
	activé. Les cartes vous permettent d'installer des modules d'extension (le cas échéant) et de configurer les implémentations à utiliser.
Ouvrir la page	Dans le système de base, votre instance envoie une requête au ServiceNow Store pour toutes les applications qui ont des dépendances à Opérations de sécurité des modules d'extension. Lorsque ces applications sont trouvées et que les modules d'extension d'application associés sont activés, leurs cartes d'intégration s'affichent avec les autres cartes d'intégration de sécurité. Cliquez sur **Ouvrir la page** pour accéder au site web de l'application tierce pour configurer l'intégration. Une fois la configuration terminée, le bouton **Ouvrir la page** bascule sur **Configurer**.

ArcSight ESM Ingestion d'événement pour Opérations de sécurité l'intégration

L'intégration ArcSight ESM de l'ingestion d'événements Réponse aux incidents de sécurité au produit permet aux analystes d'incidents de sécurité de collecter des événements corrélés et d'automatiser la création d'incidents de sécurité avec la ServiceNow plateforme. Les données sont ingérées en continu en fonction d'un calendrier d'interrogation configuré, et elles sont utilisées par les analystes pour identifier les menaces potentielles de cybersécurité et y répondre.

Avec cette intégration, les événements corrélés qui sont des candidats aux incidents de sécurité peuvent être ingérés périodiquement. Vous pouvez mapper les champs d'événements corrélés à des champs d'incident de sécurité, prévisualiser la configuration d'un événement en tant qu'incident de sécurité et configurer l'ingestion planifiée d'événements pour créer automatiquement des incidents de sécurité en continu.

Vue d'ensemble

Cette intégration fournit à un analyste du centre des opérations de sécurité (SOC) une visibilité sur les événements de corrélation dans ArcSight ESM. Ces données peuvent être intégrées dans Now Platform les incidents de sécurité Security Incident Response (SIR) pour une enquête et une correction plus approfondies. Les profils sont créés dans votre Now Platform instance pour gérer différents types d'événements de corrélation créés et mis à disposition via des visionneuses de requêtes de corrélation dans ArcSight ESM. Ces profils personnalisent la façon dont les différents ArcSight ESM champs d'événements corrélés sont affichés sur les incidents de sécurité SIR.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

- Créez plusieurs profils d'ingestion d'événements pour créer des SIR incidents de sécurité pour des types de menaces spécifiques tels que les programmes malveillants et les tentatives d'accès non autorisé.
- Glisser-déplacer le mappage des valeurs de champ d'événement de ArcSight ESM corrélation aux champs d'incident de sécurité associés SIR .
- Aperçu de la mise en page de l'incident de sécurité basée sur des SIR exemples d'événements de corrélation pour valider les détails du mappage d'événements.
- Ingérer des événements de corrélation historiques, ainsi que de nouveaux événements notables à intervalles configurables.
- Filtrer les événements de corrélation qui ne répondent pas aux SIR critères de génération d'incidents, par exemple les événements de faible priorité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Regroupez les événements en incidents de sécurité existants SIR en fonction des valeurs de champ correspondantes pour éviter les incidents de sécurité en double.
- Mettre à jour les événements de corrélation en fonction SIR des conditions de création et/ou de fermeture d'incident via une interface bidirectionnelle.

Versions prises en charge Now Platform

Cette intégration prend en charge les versions New York Patch 6 et Orlando Now Platform.

Les applications Security Operations suivantes doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour garantir une installation fluide :

1. Cadre de travail de Security Integration
2. Security Support Common
3. Réponse aux incidents de sécurité
4. Ingestion d'événements et d'alertes pour Security Operations
5. Modules d'extension du concentrateur d'intégration
   a. Exécution du concentrateur d'intégration ServiceNow
   b. Étape d'action du concentrateur d'intégration ServiceNow : REST

Pour plus d'informations sur l'installation des Opérations de sécurité applications principales, consultez et .

ArcSight ESM Versions prises en charge

Cette intégration a été testée avec la ArcSight ESM version 7.0.0.2436 du gestionnaire. L'intégration prend en charge à la fois les environnements de services sur site et dans le ArcSight ESM cloud/hébergés.

Serveur MID

Cette intégration nécessite l'installation et la configuration d'un serveur MID Server dans votre Now Platform® instance pour se connecter au ArcSight ESM service lorsque le ArcSight ESM serveur est déployé au sein de votre réseau d'entreprise. Si vous utilisez le service cloud, un serveur MID n'est ArcSight ESM pas nécessaire. Consultez le site web de la documentation produit ServiceNow pour plus d'informations sur les MID Servers.

Références

Référence	Identificateur de document	Titre de document
1	ArcSight ESM Documentation du produit	Documentation produit ArcSight .
2	ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer votre Now Platform® instance pour l'intégration de l'ingestion d'événements ArcSight ESM

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform® instance avant d'installer l'application à partir du ServiceNow Store.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application pour garantir une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform® et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre Now Platform® instance. • Un utilisateur disposant du rôle administrateur Now Platform® (admin) installe l'application à partir de et ServiceNow Store affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Un utilisateur disposant du rôle sn_si.admin supervise les tâches suivantes dans :Now Platform® ◦ Nomme, crée et modifie les profils d'événements. ◦ Sélectionne et mappe les valeurs des événements de corrélation aux incidents de ArcSight ESM sécurité. ◦ Prévisualise l'exactitude des détails de l'incident de sécurité avant de finaliser la configuration. ◦ Planifie l'ingestion d'événements corrélés en cours. ◦ Active les mises à jour d'événements corrélés lorsqu'un incident SIR est créé et fermé. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Les utilisateurs avec l'sn_si.analyst travaillent avec des incidents de sécurité. Pour plus d'informations sur les rôles et l'affectation de rôles aux utilisateurs, consultez Rôles sur le site web de la documentation produit ServiceNow .
Vérifiez que vous utilisez la version 7.0.0.2436 ou une version ultérieure du ArcSight ESM gestionnaire. Les versions antérieures ne sont pas prises en charge.	Si vous avez accès à la ArcSight ESM visionneuse de requêtes, vous avez accès à l'API requise pour cette intégration. Aucune autre configuration spéciale n'est requise pour l'API.
Configurez la visionneuse de requêtes dans ArcSight ESM.	Avant de pouvoir ingérer des événements de corrélation, vous devez configurer la visionneuse de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	requêtes dans la ArcSight ESM console. Consultez Configurer la visionneuse de ArcSight ESM requêtes pour en savoir plus.
Facultatif Créez des étapes personnalisées pour les mises à jour d'événements ArcSight ESM de corrélation.	Un événement de corrélation passe par de nombreuses étapes dans son cycle de vie avant d'être fermé. ArcSight ESM fournit des étapes par défaut telles que Initiale, Surveillance, Mis en file d'attente et Fermé. Certaines de ces étapes nécessitent des entrées de l'utilisateur, mais d'autres étapes sont automatiquement appliquées à l'événement sans aucune intervention de l'utilisateur (le champ **Requis par l'utilisateur** n'est pas coché dans la ArcSight ESM console. Vous pouvez créer des étapes personnalisées qui ne nécessitent aucune intervention de l'utilisateur et les utiliser dans votre Now Platform® instance. Consultez Options supplémentaires : automatisez les mises à jour et la fermeture des événements corrélés en fonction de l'état de SIR l'incident pour en savoir plus.
Vérifiez que vous avez installé et configuré une application de Serveur MID.	Application de Serveur MID configurée Un serveur MID dans votre Now Platform® instance est requis pour se connecter au ArcSight ESM service si le ArcSight ESM serveur est déployé au sein de votre réseau d'entreprise. Consultez Installez et configurez l'application ServiceNow pour l'intégration d'ingestion d'événements ArcSight ESM pour obtenir des instructions sur la configuration d'une application de Serveur MID. Reportez-vous au serveur MID pour en savoir plus sur les serveurs MID. Si vous utilisez un service hébergé ou infonuagique, c'est-à-dire accessible sur Internet, un serveur MID n'est pas nécessaire.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Ingestion d'événements et d'alertes pour Security Operations : Cette application nécessite :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	◦ com.glide.hub.integration.runtime => l'exécution du Centre d'intégration ServiceNow ◦ com.glide.hub.action_step.rest => Étape d'action du Centre d'intégration ServiceNow : REST **5.** Cœur de la menace Pour plus d'informations sur l'installation des Opérations de sécurité applications principales, consultez et .

Que faire ensuite

Vous avez correctement configuré votre Now Platform® instance pour l'intégration. L'étape suivante consiste à installer l'application ArcSight ESM Security Event Ingestion pour Security Operations à partir de ServiceNow Store pour l'intégration.

Configurer la visionneuse de ArcSight ESM requêtes

Créez une visionneuse de requêtes et définissez des filtres qui incluront les événements de corrélation récemment créés qui seront ingérés ServiceNow.

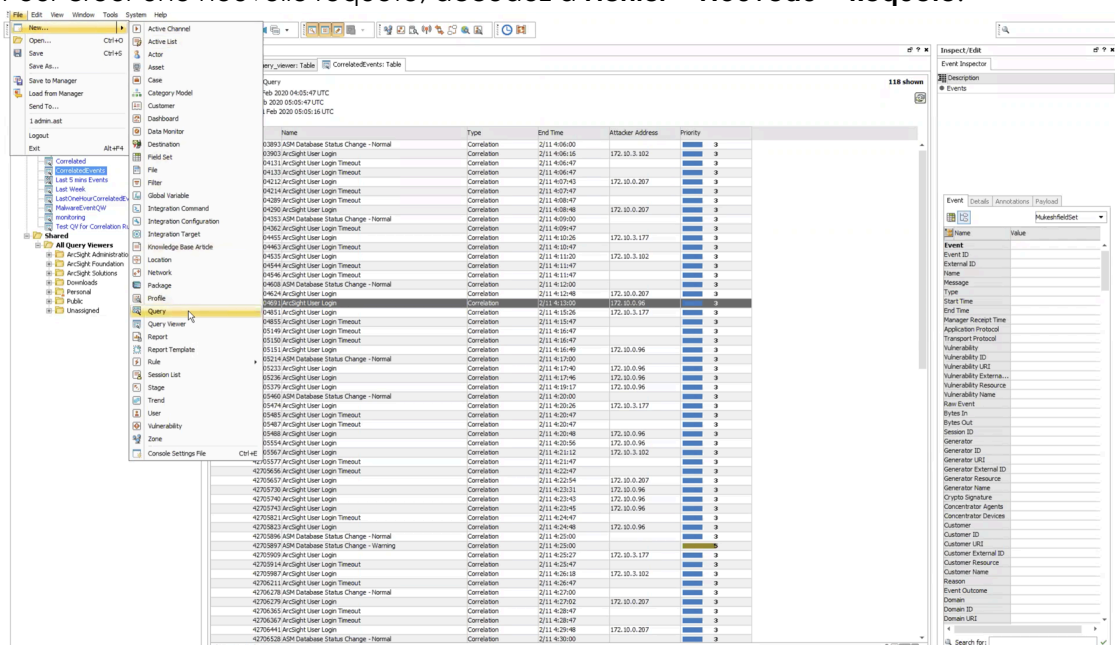
Avant de commencer

Rôle requis : Administrateur ArcSight

Procédure

1. Connectez-vous à la ArcSight ESM console pour créer une visionneuse de requêtes.

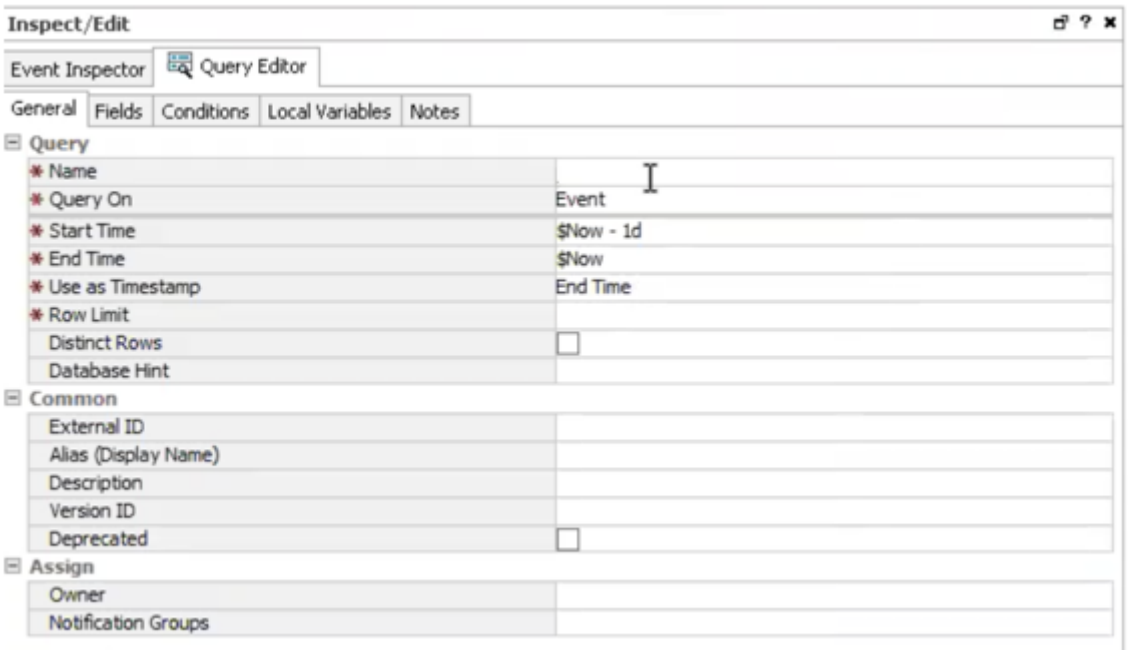
2. Pour créer une nouvelle requête, accédez à **Fichier** > **Nouveau** > **Requête**.



3. Définissez les conditions de la visionneuse de requêtes dans le panneau **Inspecter/ Modifier** .

Traduction automatique

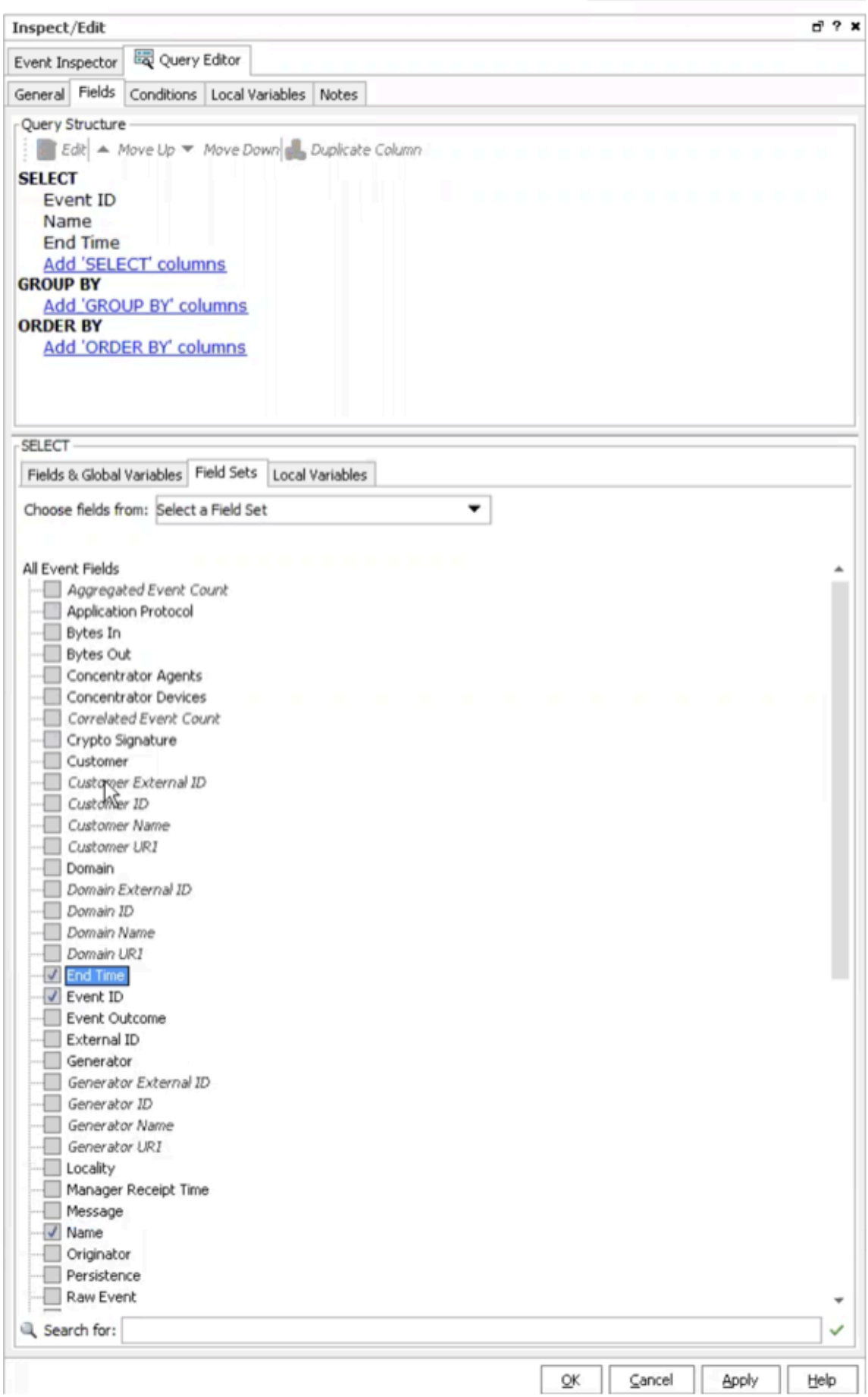
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Nom de champ	Description
Nom	Saisissez un nom pour la requête.
Requête sur	Sélectionnez **Événement** dans la liste déroulante.
Heure de début	Pour ingérer les données les plus récentes, sélectionnez la date des événements à ingérer. Spécifiez une date antérieure d'un jour ou de quelques jours à la date actuelle. **Remarque :** Vous ne pouvez pas spécifier une date postérieure de plus de 7 jours à la date actuelle. Si vous ingérez un grand nombre d'événements, vous devez spécifier une date antérieure de 1 ou 2 jours à la date actuelle.
Heure de fin	Il s'agit de la date du jour.
Limite de ligne	Le nombre maximal d'événements qui peuvent être ingérés à la fois. Spécifiez ici une valeur inférieure à 5 000.

4. Cliquez sur l'onglet **Champs** .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

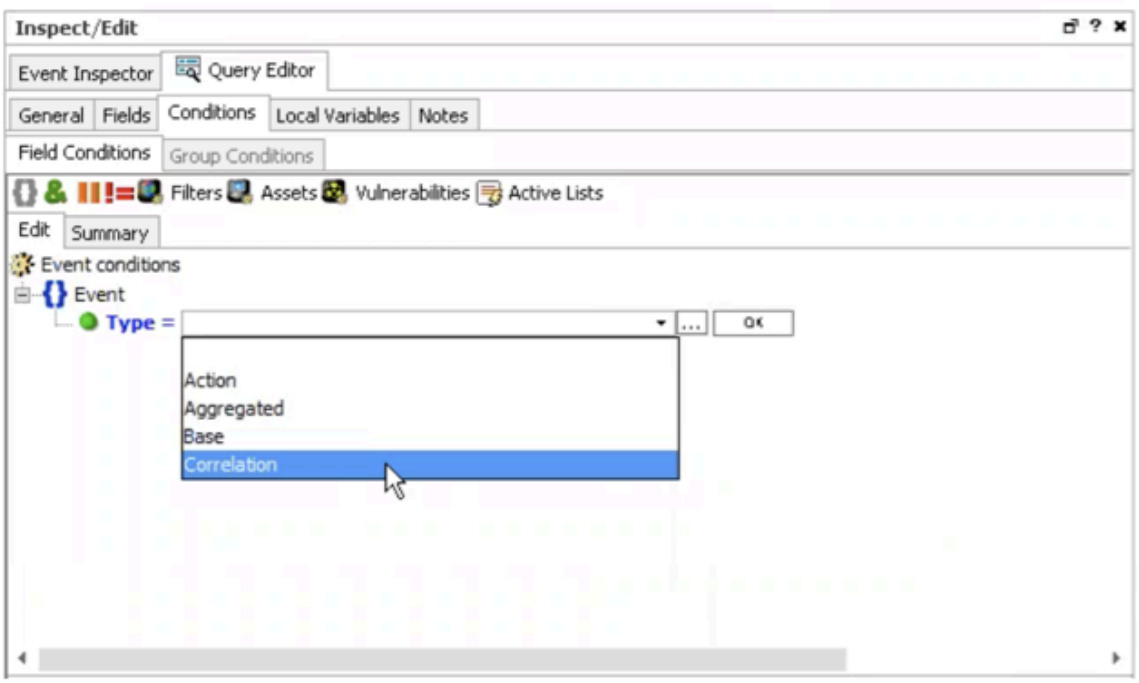


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez les champs qui doivent être inclus lors de l'ingestion.
   Vous devez sélectionner les champs *ID d'événement*, *Nom* et *Heure de fin* pour que l'ingestion réussisse.
6. Cliquez sur le lien **Ajouter des colonnes « TRIER PAR »** et sélectionnez le champ **ID d'événement** et spécifiez l'ordre de tri par **ordre décroissant** pour vous assurer que les derniers événements sont ingérés.
7. Cliquez sur l'onglet **Conditions** .
8. Cliquez avec le bouton droit sur **Événement** sous **Conditions de l'événement** dans la section **Résumé** .
9. Cliquer sur **Nouvelle condition** > **Racine** > **Type** et sélectionnez le type d'événement **Corrélation**.

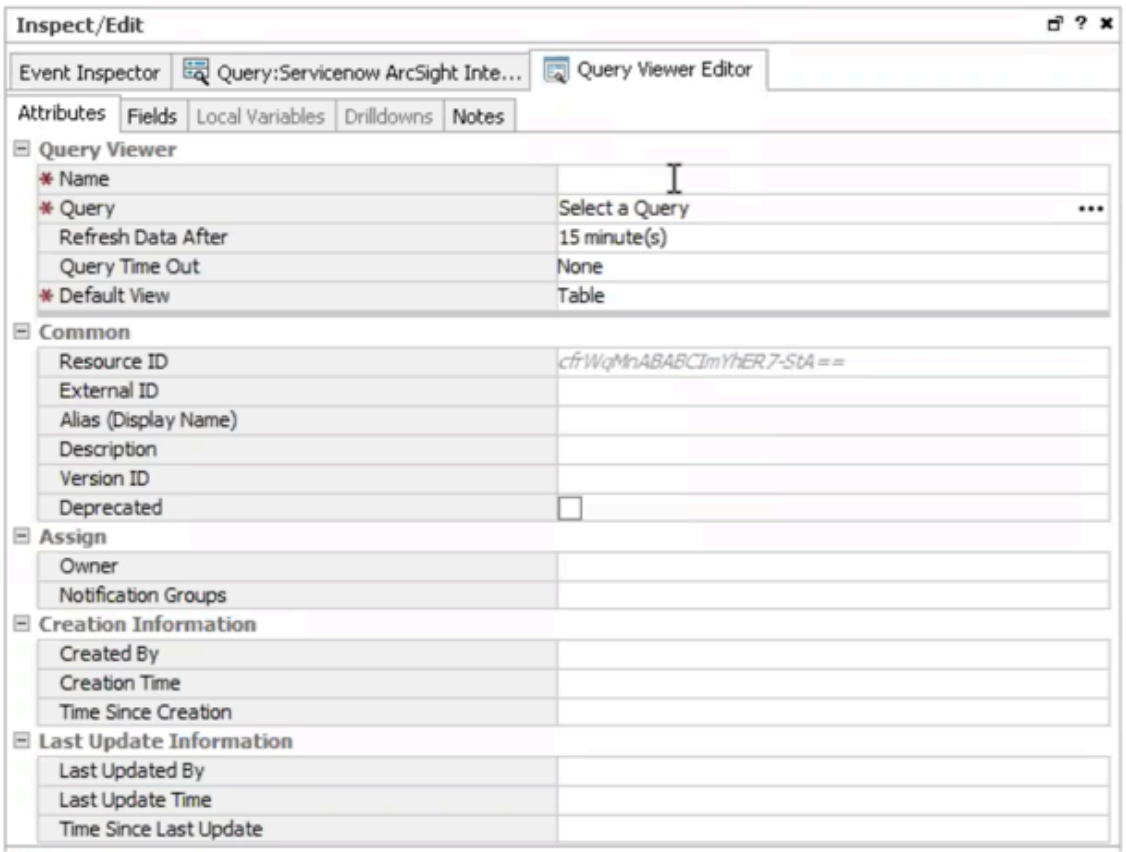
> **Important :** Seuls les événements de corrélation seront récupérés ; Les événements de base pour les corrélations ne seront pas récupérés.



10. Cliquez sur **OK** pour enregistrer la requête.
    L'étape suivante consiste à créer une visionneuse de requêtes pour cette requête.
11. Accédez à la **Fichier** > **Nouveau** > **Visionneuse de requêtes**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



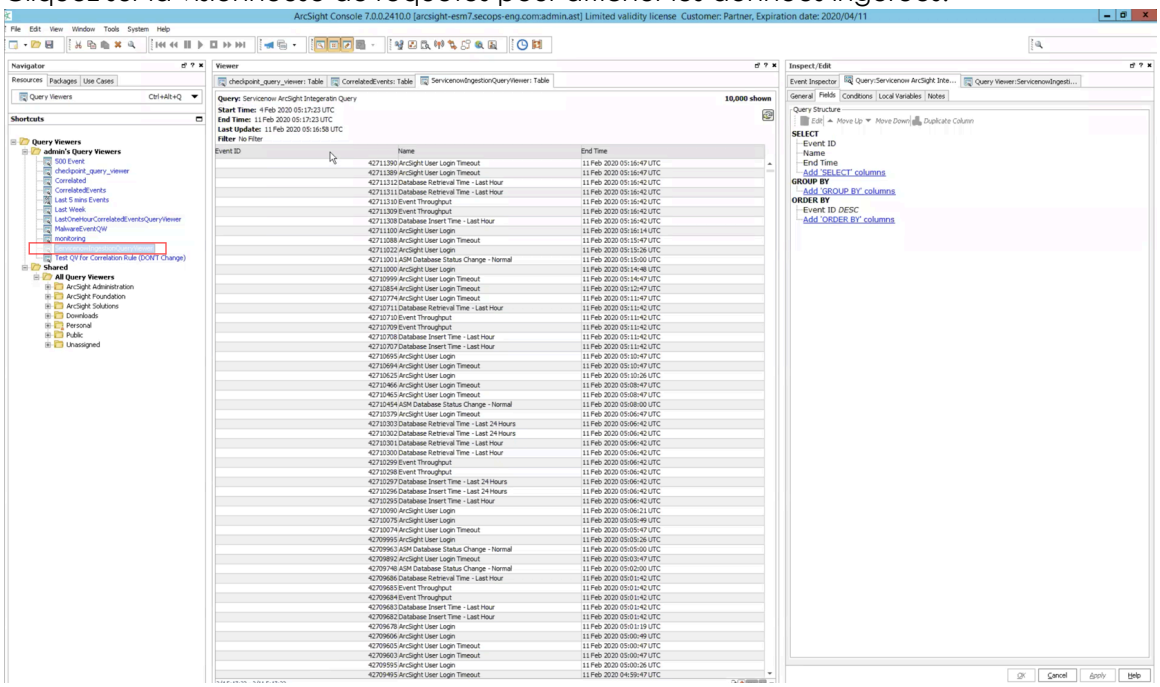
Nom de champ	Description
Nom	Entrez un nom pour la visionneuse de requêtes.
Requête	Sélectionnez la requête que vous venez de créer.
Actualiser les données après	Spécifiez la fréquence à laquelle les données doivent être actualisées.

12. Cliquez sur l'onglet **Champs** et assurez-vous que les champs obligatoires (*ID d'événement, Nom, Heure de fin*) que vous avez spécifiés dans votre requête sont sélectionnés.
13. Cliquez sur **Appliquer** pour enregistrer la visionneuse de requêtes.
    La nouvelle visionneuse de requêtes que vous avez créée est répertoriée dans la section Visionneuses de requêtes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

14. Cliquez sur la visionneuse de requêtes pour afficher les données ingérées.



Installez et configurez l'application ServiceNow pour l'intégration d'ingestion d'événements ArcSight ESM

Avant d'exécuter l'intégration sur votre Now Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre Réponse aux incidents de sécurité correctement aux produits et Opérations de sécurité sur votre Now Platform instance.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si vous n'avez pas installé l'application ArcSight ESM à partir de ServiceNow Store pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la ArcSight ESM tuile.
3. Pour configurer l'application, cliquez sur **Nouveau**.
4. Si un bouton **Configurer** s'affiche sur une mosaïque, cliquez dessus pour modifier une configuration existante.
5. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom unique du ArcSight ESM gestionnaire qui sera utilisé dans la configuration du profil d'intégration pour distinguer plusieurs ArcSight ESM sources de gestionnaire si nécessaire. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL du point de terminaison d'API ArcSight	URL de votre ArcSight ESM serveur Manager. Notez que l'URL doit inclure le port API, par exemple : `https://arcsight-esm.com:8443`
Nom d'utilisateur du compte API	Nom d'utilisateur que vous avez créé pour votre compte d'utilisateur API dans la console du ArcSight ESM gestionnaire.
Mot de passe API	Mot de passe que vous avez créé pour votre compte utilisateur API dans la console du ArcSight ESM gestionnaire.
Déploiement sur site	Cette option n'est pas cochée par défaut. Si vous utilisez la version infonuagique qui dispose d'un ArcSight ESM accès direct à Internet, vérifiez que la case n'est pas cochée. Pour un déploiement sur site, cochez cette case et spécifiez l'application de Serveur MID.
Application de Serveur MID	Spécifiez ici un nom d'application de Serveur MID. Cette application de Serveur MID peut pointer vers n'importe quel serveur MID qui a été configuré et n'importe quel Serveur MID disponible sera utilisé. Si aucune application de Serveur MID n'est configurée, vous devez créer une nouvelle Application de Serveur MID pour cette intégration. **Remarque :** L'application Serveur MID ne peut être configurée que par les utilisateurs disposant du rôle d'administrateur système.

Traduction automatique

Pour créer une application de Serveur MID, procédez comme suit :

a. Accédez à la **MID Server** > **Applications** et cliquez sur **Nouveau**.

b. Entrez un nom pour l'application de Serveur MID et sélectionnez un serveur MID à utiliser par défaut.

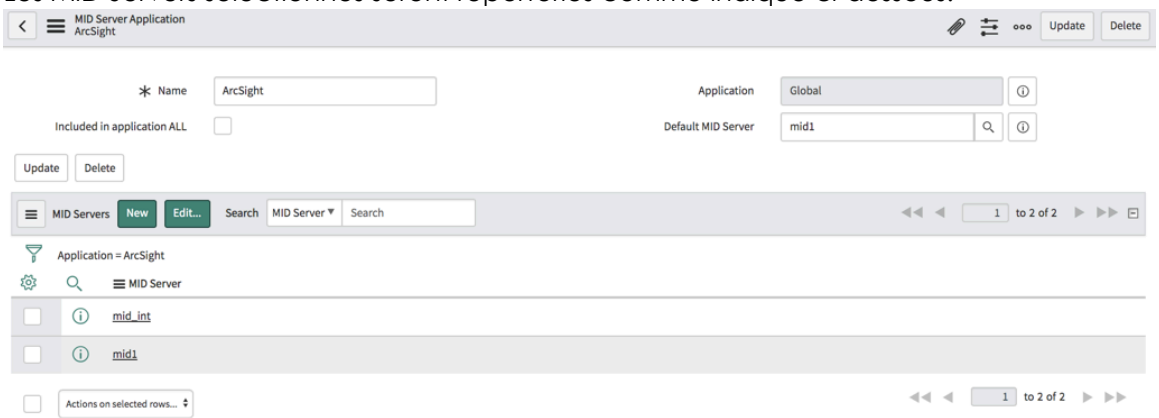
c. Décochez la case Inclus dans l'application TOUT et cliquez sur **Enregistrer**.



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

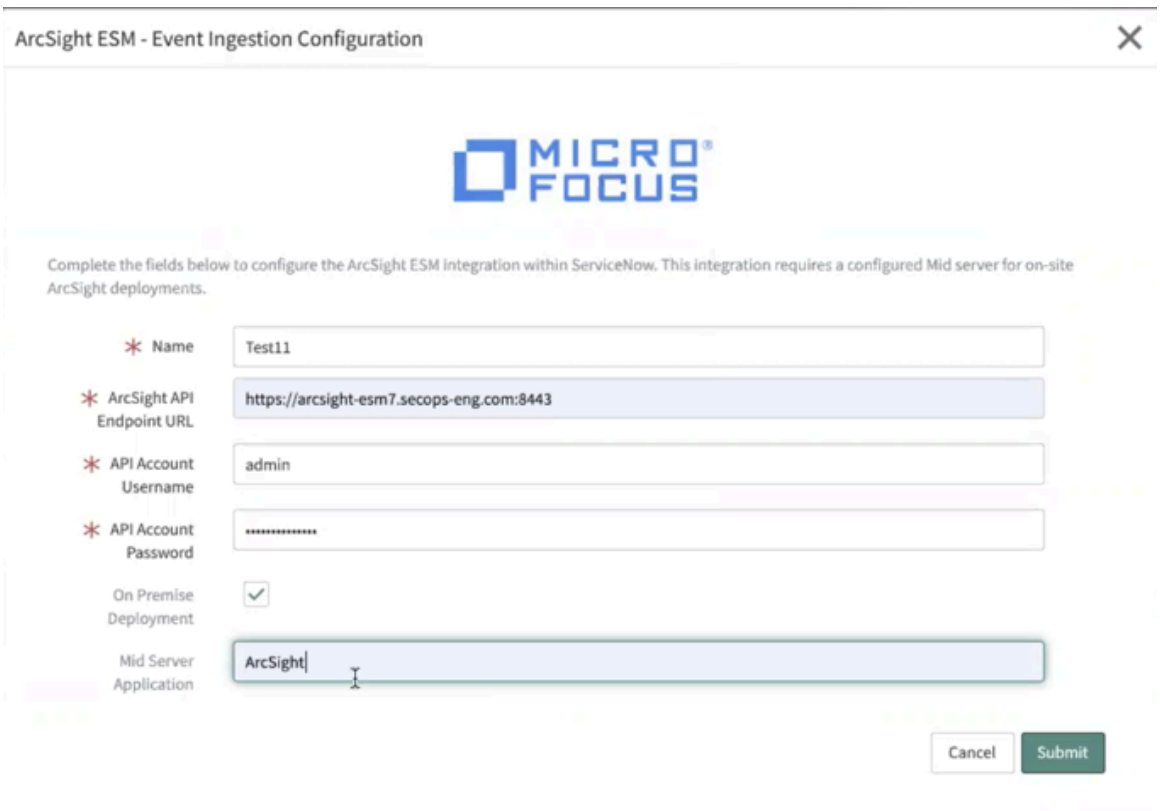
d. Cliquez sur **Modifier**. Sur la page **Modifier les membres** , sélectionnez tous les serveurs MID disponibles, déplacez-les vers la liste des serveurs MID et cliquez sur **Enregistrer**.

e. Les MID Servers sélectionnés seront répertoriés comme indiqué ci-dessous.



En fonction de la disponibilité, l'un des MID Servers configurés avec l'application MID Server sera utilisé.

6. Entrez les détails de la configuration et spécifiez l'application de Serveur MID que vous avez créée.



Chaque événement de corrélation que vous ingérez à partir de votre ArcSight ESM console Gestionnaire nécessite un profil d'événement unique dans votre instance. Toutefois, la ArcSight ESM source que vous configurez sur le formulaire de configuration de l'ingestion d'événements peut être réutilisée pour plusieurs profils, à condition que chaque profil ingère des types d'événements de corrélation uniques.

7. Cliquez sur **Envoyer**.
Une fois validée et soumise, chaque ArcSight ESM configuration de serveur est enregistrée sous forme de vignette sur la page Intégrations de sécurité. Si vos vignettes de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

configuration enregistrées ne s'affichent pas sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste de choix Afficher les configurations, cliquez sur **Oui**.

Que faire ensuite
Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer un profil d'événement.

Créer un profil pour ArcSight ESM l'intégration de l'ingestion d'événements de corrélation

En tant qu'utilisateur disposant du rôle sn_si.admin, vous créez un profil dans votre Now Platform instance et déterminez quels événements de corrélation créent des incidents de sécurité. Avant Now Platform Réponse aux incidents de sécurité que les incidents de sécurité (SIR) ne soient créés à partir d'événements de corrélation, les valeurs de champ des événements sont affichées sur la mise en page d'un Now Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera créé.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Les événements de corrélation sont automatiquement ingérés dans l'environnement Opérations de sécurité de votre Now Platform instance en fonction du type de profil défini. Un profil est l'encapsulation d'un type d'événement de corrélation, comme les tentatives d'accès non autorisé ou les programmes malveillants.

Une fois qu'un événement de corrélation a été ingéré, vous pouvez mapper les champs d'événement de corrélation individuels aux champs correspondants dans l'incident de sécurité. Vous pouvez filtrer les événements de corrélation pour spécifier quels événements créent des incidents de sécurité. Par exemple, vous pouvez préférer les filtres qui créent des incidents de sécurité uniquement pour les événements de corrélation identifiés comme à haut risque. Vous pouvez également définir des critères d'agrégation d'événements supplémentaires afin que les événements de corrélation entrants en double soient agrégés en un incident de sécurité ouvert. Enfin, vous pouvez définir un calendrier d'ingestion et activer le profil.

Les noms des profils d'événements dans votre Now Platform instance doivent être uniques et ne peuvent être mappés qu'à un profil d'événement actif à la fois.

Créer et nommer le profil pour ArcSight ESM l'intégration de l'ingestion d'événements

Vous pouvez configurer un profil pour ingérer des événements de corrélation.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Pour créer un profil d'événement pour un événement de corrélation dans votre Now Platform instance, accédez à **Intégration d'ArcSight ESM** > **Profil d'événement ArcSight ESM**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs.

   Le tableau ci-dessous un exemple de formulaire rempli.

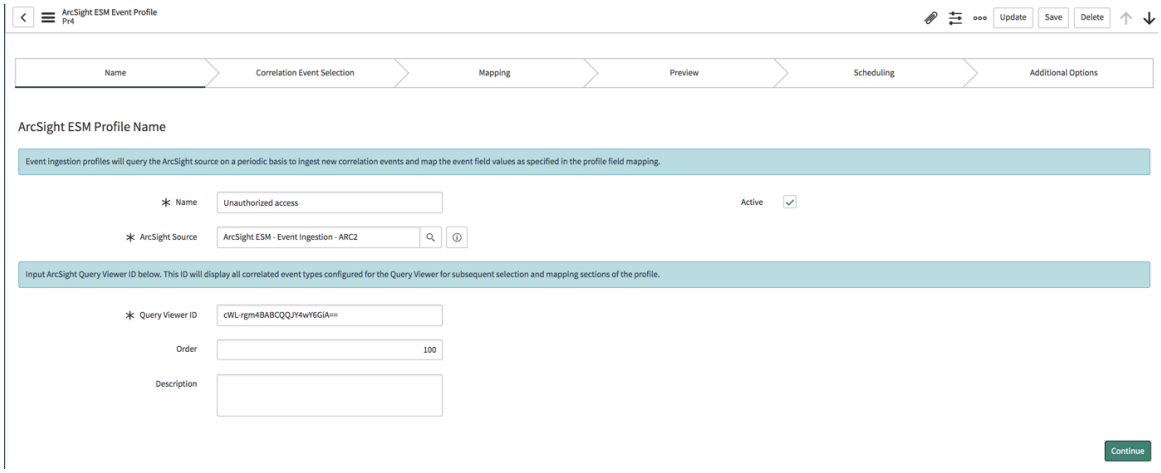
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre Now Platform instance doivent être uniques.
Actif	La case heck est désactivée par défaut. Si cette option est désactivée, le profil n'est pas actif et l'ingestion n'a pas lieu. **Remarque :** Vous devez remplir toutes les sections du profil avant de l'activer.
ArcSight Source	Serveur ArcSight ESM configuré lors de l'étape d'authentification initiale. Si vous avez configuré plusieurs ArcSight ESM serveurs, sélectionnez le serveur approprié pour les types d'événements de corrélation qui seront ingérés pour le profil. Vous devez sélectionner une valeur.
ID du visualiseur de requête	Entrez l'ID de ressource de la visionneuse de requêtes configurée dans la ArcSight ESM console. L'ID de ressource est un identificateur unique pour toute visionneuse de requêtes configurée sur le serveur ArcSight ESM. Une fois l'ID de ressource soumis, le nom de la vue de requête est renvoyé pour s'assurer que la visionneuse de requêtes appropriée a été sélectionnée. Consultez la section ci-dessous pour obtenir une capture d'écran de la façon de déterminer l'ID de ressource pour la visionneuse de requêtes sélectionnée dans ArcSight ESM.
Ordre	La valeur par défaut est 100. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Le workflow du profil dont le numéro est le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

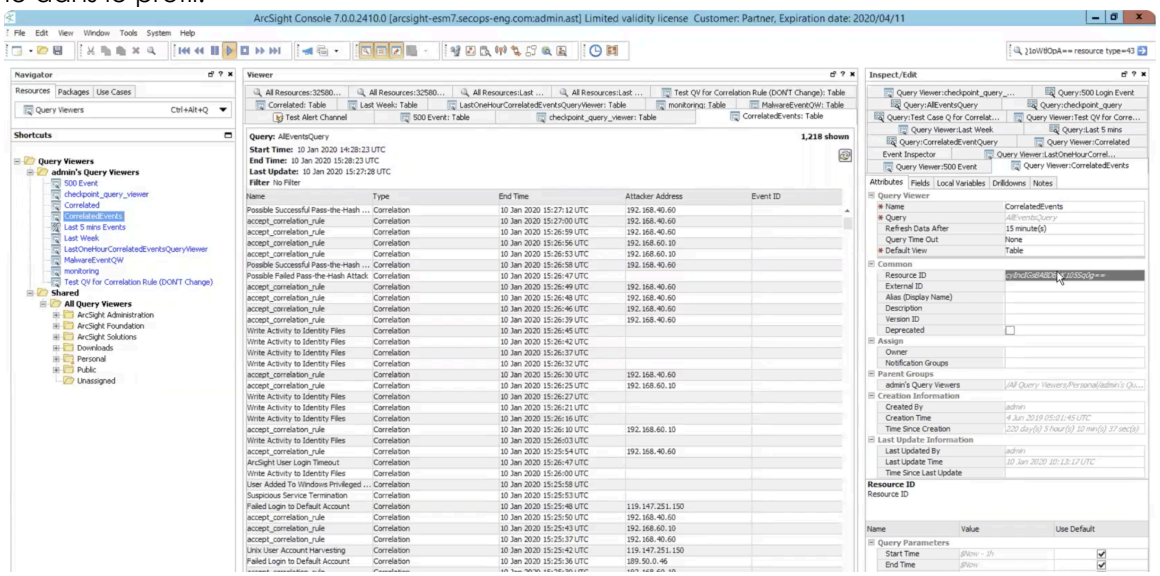
La figure suivante est un exemple de formulaire rempli.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois que vous avez saisi les détails du profil, cliquez sur **Continuer**. L'ID du visionneur de requêtes est validé et si un ID de ressource correspondant est présent dans la ArcSight ESM visionneuse de requêtes, le nom de la visionneuse de requêtes est renvoyé comme indiqué ci-dessous. Si la validation échoue, vérifiez si l'ID de ressource existe dans la ArcSight ESM console. Si l'ID de ressource est introuvable, recherchez l'ID de ressource correct et entrez-le dans le profil.



Que faire ensuite

L'étape suivante consiste à sélectionner les types d'événements de corrélation à ingérer dans la visionneuse de requêtes qui a été sélectionnée à l'étape précédente.

Sélectionner les événements de corrélation pour l'intégration ArcSight ESM de l'ingestion d'événements

En fonction de la ArcSight ESM source et de la visionneuse de requêtes configurées, sélectionnez une règle d'événement de corrélation pour le profil.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Affichez les événements de corrélation disponibles répertoriés dans la sélection d'événements de corrélation dans votre instance Now Platform afin de déterminer les événements de corrélation que vous souhaitez ingérer et créer des incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous ne pouvez sélectionner qu'un seul type de règle de corrélation dans la liste pour chaque profil.
L'ID du visionneur de requêtes et le nom du visualiseur de requêtes, tels que spécifiés dans le formulaire Visionneuse de requêtes, s'affichent. Sélectionnez un événement de corrélation dans la liste que vous pouvez utiliser pour créer un mappage de configuration pour l'événement corrélé ingéré.

Cliquez sur la liste déroulante dans le champ Liste des événements de corrélation. La liste des événements de corrélation présents dans la console de la ArcSight ESM visionneuse de requêtes s'affiche.

Cliquez sur **Continuer** pour passer à l'étape suivante dans l'assistant.

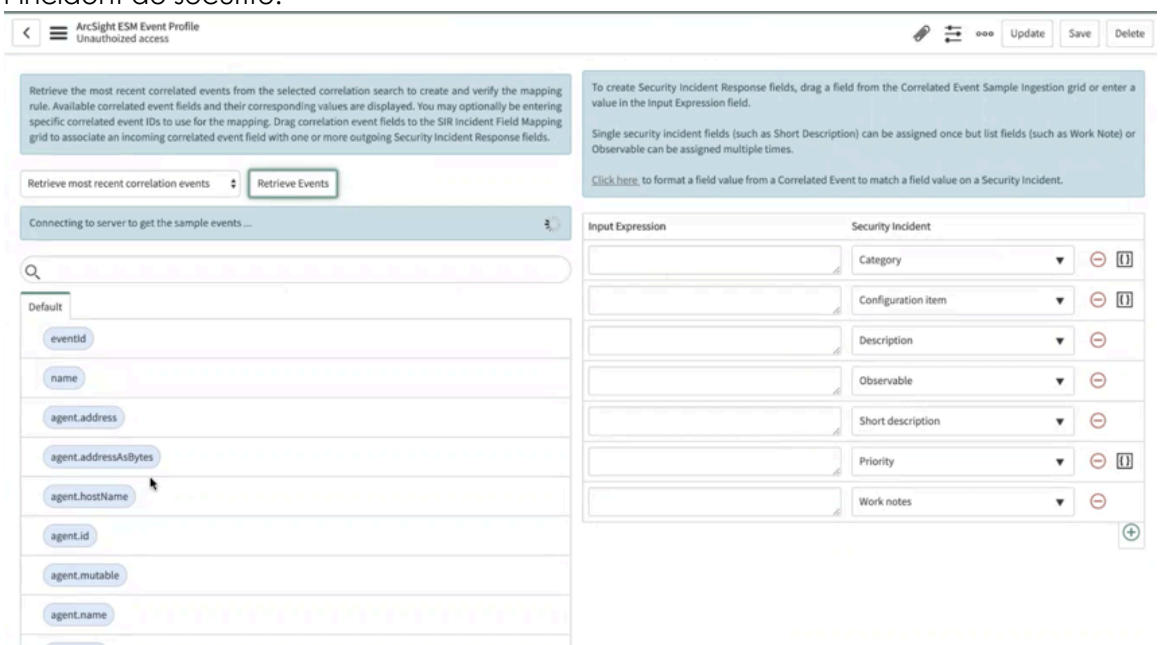
Mappage des champs d'événements de corrélation pour l'intégration de l'ingestion d'événements ArcSight ESM

Une fois que vous avez identifié la règle d'événement de corrélation spécifique dans la liste, l'étape suivante consiste à mapper les champs d'événements de corrélation aux champs du formulaire d'incident de sécurité.

Vue d'ensemble

Pour l'étape de mappage, vous pouvez ingérer des exemples d'événements de corrélation pour la règle de corrélation sélectionnée. Au cours de cette phase de mappage, vous pouvez vous assurer que toutes les données de champ d'événement de corrélation pertinentes sont mappées à l'emplacement approprié sur le formulaire d'incident SIR , puis visualiser l'incident SIR dans la section d'aperçu.

La figure suivante montre la configuration de mappage par défaut fournie pour créer le profil d'événement de corrélation. Vous pouvez personnaliser les champs qui renseignent l'incident de sécurité.



Lorsque vous cliquez sur **Récupérer des événements**, les noms des champs d'événements de corrélation et les valeurs correspondantes sont renseignés sur le côté gauche du formulaire. Il s'agit des champs d'événements ArcSight ESM de corrélation qui peuvent être mappés aux champs d'incident de sécurité.

Vous préférez peut-être examiner quelques exemples d'événements de corrélation sur votre console à ingérer pour l'étape de configuration du mappage de champs. Cette

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

étape s'intitule Mappage dans la barre de progression. Si cette page n'est pas affichée, cliquez sur **Mappage** dans la barre de progression. Vous pouvez ingérer jusqu'à cinq échantillons d'événements ArcSight ESM de corrélation à partir du gestionnaire pour la règle de corrélation sélectionnée afin d'aider au processus de mappage de champs. Il existe des options permettant soit d'ingérer les cinq événements de corrélation les plus récents pour l'événement de corrélation sélectionné, soit d'ingérer jusqu'à cinq événements de corrélation spécifiques en fonction des ID d'événement.

Vous trouverez ci-dessous un résumé des étapes requises pour mapper les événements de corrélation :

- Mappage de champs : modifiez la configuration du mappage en faisant glisser les champs d'événements de corrélation du côté gauche et en les déposant dans la section de mappage des SIR incidents située à droite. Le mappage sur la droite associe le champ d'événement de corrélation entrant à un champ d'incident de sécurité sortant.
- Expérience de mappage : personnalisez la grille de mappage en ajoutant ou en supprimant des champs à l'aide de l'icône + en bas de la section de mappage de champs d'incidents SIR. Suivez les champs négligés ou précédemment mappés avec le code couleur fourni (les champs mappés sont grisés, les champs bleus ne sont pas mappés).
- Conditions de génération d'incidents : une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de filtrer les événements de corrélation qui doivent créer des incidents de sécurité par rapport aux événements de corrélation qui doivent être filtrés (par exemple, les événements de corrélation de faible priorité). Pour ce faire, consultez la section Conditions de génération d'incidents située sous la section Ingestion d'échantillons d'événements de corrélation.
- Critères d'agrégation d'événements : définissez des critères d'agrégation d'événements supplémentaires qui regroupent un événement de corrélation entrant en un incident de sécurité existant SIR au lieu de créer des incidents similaires et potentiellement dupliqués. En utilisant des critères de valeur de correspondance de champ pour chaque profil, cette option d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données relatives aux événements notables de sécurité connexes sur un seul incident de sécurité.
- Formater la traduction du champ : dans certains cas, les valeurs de champ d'événement dans l'événement ArcSight ESM de corrélation peuvent ne pas se traduire directement dans les champs de l'incident SIR de sécurité. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez mettre en forme des valeurs similaires, mais pas identiques.

  Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident SIR de sécurité à l'aide de la fonctionnalité Formater la traduction de champ.

L'étape suivante consiste à ingérer des échantillons d'événements de corrélation et à mapper les valeurs aux champs d'incident SIR de sécurité.

Créer des mappages pour ArcSight ESM l'intégration de l'ingestion d'événements

Au cours de cette étape, vous ingérez des échantillons d'événements de corrélation et mappez les valeurs aux champs d'incident de sécurité SIR.

Avant de commencer

Rôle requis : admin, sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

En tant qu'utilisateur disposant du rôle sn_si.admin, vous pouvez examiner jusqu'à cinq exemples d'événements de corrélation à partir de la colonne Ingestion d'échantillons d'événements de corrélation à gauche du formulaire pour aider au mappage et à la traduction des valeurs de champ d'événement avec les champs d'incident de sécurité dans la colonne Mappage de champ d'incident SIR à droite.
Créez des mappages personnalisés en ajoutant ou en supprimant les champs de la grille de mappage sur le côté droit du formulaire. Les champs affichés par défaut sont généralement des champs importants à renseigner sur le formulaire de réponse aux incidents de sécurité. Toutefois, ces champs peuvent être supprimés et tous les champs supplémentaires peuvent être affichés à l'aide des boutons + et -. Créez des cartes personnalisées en ajoutant ou en supprimant les champs de la grille de mappage sur le côté droit du formulaire. La personnalisation des champs vous permet de mapper ArcSight ESM des champs qui ne sont pas affichés sur la grille de mappage par défaut sur l'incident de sécurité.

Procédure

1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Vous pouvez soit extraire les échantillons d'événements de corrélation les plus récents pour la règle de corrélation sélectionnée, soit fournir les ID d'événements de corrélation uniques pour les événements de corrélation spécifiques que vous souhaitez utiliser pour votre expérience de mappage d'événements de corrélation.
3. Dans la liste déroulante, sélectionnez l'une des options suivantes :
   - Récupérer les événements de corrélation les plus récents
   - Sélectionner les événements de corrélation basés sur l'ID d'événement

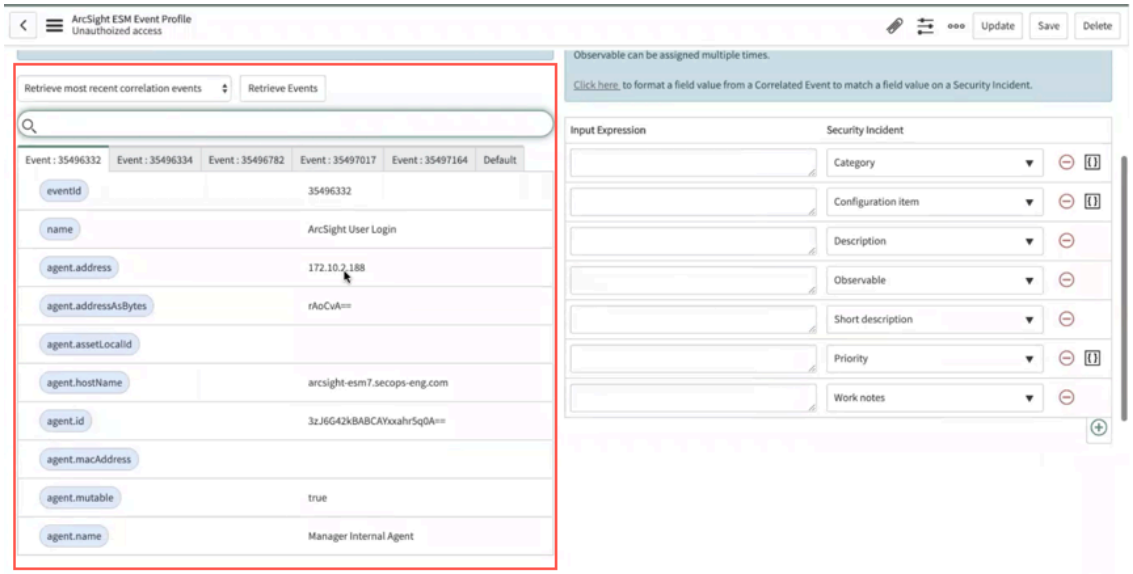
   Cliquez sur **Récupérer les événements** pour extraire les derniers exemples d'événements de corrélation de la ArcSight ESM console pour la règle de recherche de corrélation sélectionnée.

   Les champs d'événements de corrélation et les résultats des valeurs sont affichés sous forme d'onglets individuels.

   L'extraction d'événements de corrélation d'échantillons peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran.

   Dans la figure suivante, les paires de valeurs de nom de champ pour l'événement de corrélation ingéré, ou les échantillons d'événements importés, sont affichées sur le côté gauche de ce formulaire une fois l'extraction d'ingestion terminée. Ces valeurs sont les valeurs que vous mappez aux champs d'incident de sécurité du côté Mappage de champs d'incident SIR du formulaire.

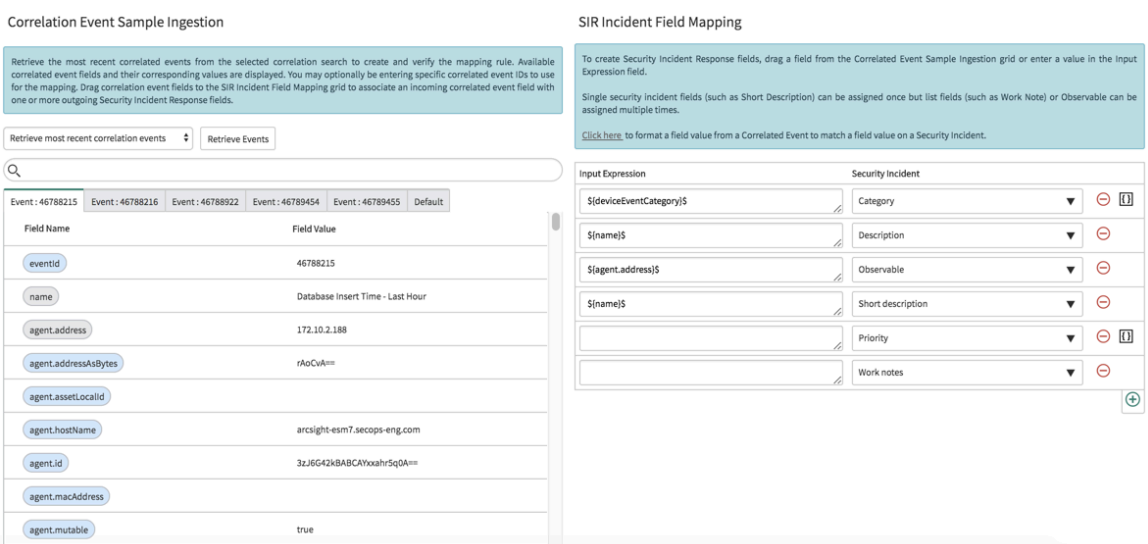
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Pour mapper une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez longuement sur un nom de champ bleu sur le côté gauche du formulaire.
5. Faites glisser le nom du champ, par exemple `agent.hostname`, et déposez-le sur un champ de la colonne Expression d'entrée en regard d'un nom de champ dans la colonne Incident de sécurité.

   Pour vous assurer qu'aucun champ d'événement n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par couleur. Les champs bleu clair sur la gauche indiquent qu'un champ d'événement de corrélation n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ de corrélation entrant à plusieurs champs sur un incident de sécurité.

   Un champ gris indique qu'un champ a été sélectionné et mappé à un champ sur l'incident de sécurité. Ce code couleur vous aide à suivre les champs d'événement qui ont déjà été utilisés pour les futurs mappages de champs d'incidents de sécurité.



6. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit.

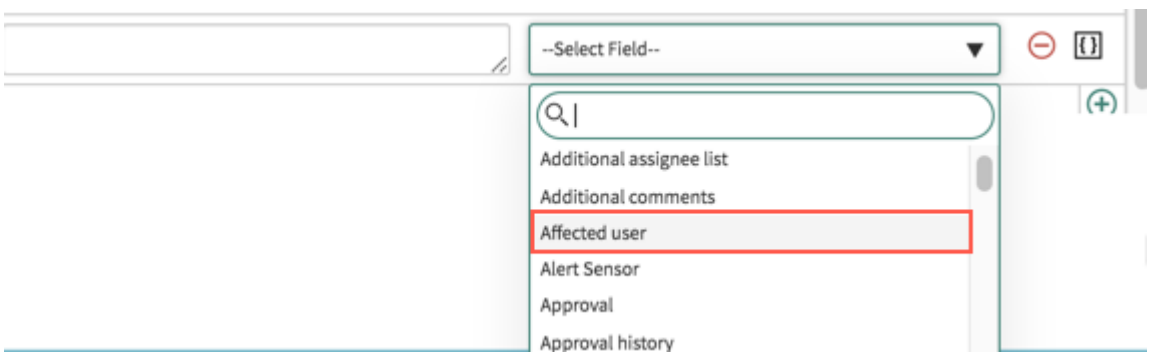
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. À droite du formulaire, dans la section Mappage des champs d'incidents SIR, en bas de la grille, cliquez sur l'icône plus.
Un nouveau champ s'affiche.

b. Dans la colonne Incident de sécurité, développez la liste de choix qui s'affiche, puis sélectionnez un champ.

Dans la liste de choix développée pour le nouveau champ, certains champs sont grisés. Dans la figure suivante, `l'utilisateur affecté` a un arrière-plan gris, car il a été mappé dans l'incident de sécurité. À l'instar du code couleur pour les champs d'événements de corrélation sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident SIR déjà mappés.



Remarque : Afin que plusieurs observables puissent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité dispose d'une liste de choix dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affiché dans la liste de choix, le champ n'est pas renseigné sur l'incident de sécurité.

c. Vous pouvez également saisir une valeur dans le champ Rechercher pour la nouvelle ligne.

d. Sur le côté gauche du formulaire, cliquez avec le bouton gauche de la souris pour sélectionner **l'ID d'événement** souhaité dans le champ **expression d'entrée** .
Grâce à la fonction glisser-déposer, mappez-le à côté de votre nouveau champ.

7. Facultatif : Ouvrez l'éditeur de script et poursuivez la modification.

(Optional) Pour plus d'informations sur l'éditeur de script, reportez-vous à la section Utiliser l'éditeur de script pour formater les valeurs d'événements de corrélation pour ArcSight ESM l'intégration.**Conditions de filtrage de génération d'incidents**

8. Facultatif : Une fois que vous avez terminé les étapes de mappage de champs précédentes, vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incidents pour définir les critères supplémentaires qu'un événement de corrélation entrant doit satisfaire pour créer un SIR incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Faites défiler l'écran jusqu'à la section Conditions de génération d'incidents du formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

(Optional) Le Créateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

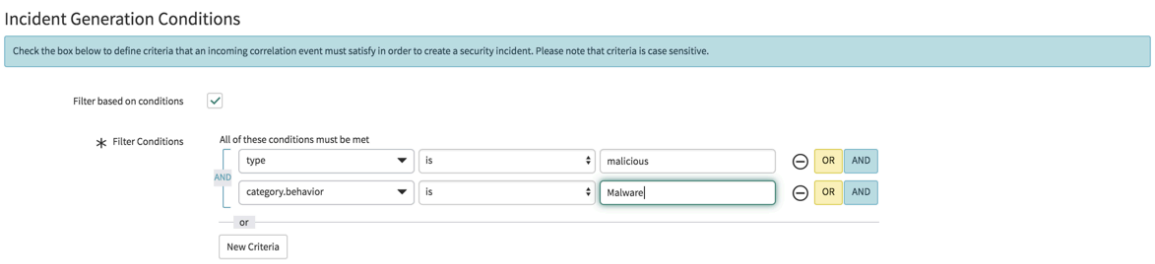
Les options des listes de choix pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Ingestion d'échantillons d'événements de corrélation pour les événements que vous avez ingérés. Ces champs sont dynamiques et changent en fonction des événements de corrélation que vous ingérez. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'événement ArcSight ESM de corrélation.

À l'aide des listes de choix et des champs du générateur de conditions, définissez des filtres pour la première ligne.

b. Pour ajouter d'autres conditions, à droite des champs, cliquez sur **ET** ou **OU**. Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

c. Facultatif : Dans la deuxième ligne, définissez une deuxième condition de filtre.

(Optional) L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création des incidents de sécurité.



(Optional) Vous avez défini les conditions de génération d'incident de sorte que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

Ce type de filtrage des conditions de génération d'incident vous permet d'affiner les événements de sécurité et de limiter le nombre d'incidents de sécurité inutiles que vous créez sans modifier la recherche de corrélation sous-jacente ni filtrer les événements dans ArcSight ESM. Si des critères de filtrage supplémentaires sont définis, seuls les

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

événements de corrélation qui correspondent à tous les critères sont mappés aux incidents.

Remarque : Si l'un des noms de champs d'événements comporte des caractères spéciaux tels que des guillemets («), des traits d'union ('), des traits de soulignement (-) ou des esperluettes (@), il peut être nécessaire de remplacer ces caractères à des fins de traduction de mappage et éventuellement de créer un nom d'événement en double. Le mappage peut être effectué correctement, mais un suffixe numérique est ajouté pour différencier les champs avec des noms d'événements en double. Par exemple, si le premier champ d'événement est `events.event` et que le second champ d'événement est `events.event`, ces champs ne peuvent pas être identifiés de manière unique car les caractères de texte standard restants sont les mêmes. Dans ce cas, un suffixe est ajouté au deuxième champ d'événement et le champ est renommé `en events@event(1).`

Critères d'agrégation d'événements pour traiter des événements de corrélation similaires et empêcher les incidents en double

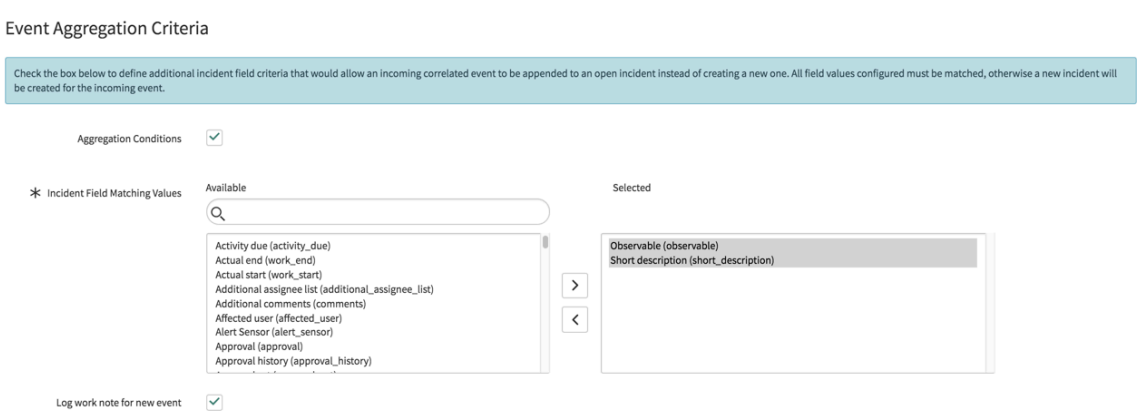
9. Facultatif : Pour éviter de créer des incidents de sécurité en double, définissez des critères d'agrégation d'événements supplémentaires afin que les événements de corrélation entrants soient agrégés en un incident de sécurité ouvert.
Pour définir les critères, procédez comme suit :

   a. Faites défiler la page jusqu'à la section **Critères d'agrégation d'événements** du formulaire et cochez la case Conditions d'agrégation pour activer cette option.

   (Optional) Les colonnes Incident Field Matching Values (Valeurs correspondantes du champ d'incident) s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés dans l'incident SIR de sécurité.

   b. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre Now Platform et déplacez-les vers la liste Sélectionné.

   (Optional) Toutes les valeurs de champ que vous sélectionnez doivent être mises en correspondance pour ajouter cet événement de corrélation entrant à un incident de sécurité existant. Cela inclut les champs, tels que les observables et les éléments de configuration, auxquels plusieurs valeurs de champ d'événement de corrélation peuvent être mappées. Toutes les valeurs doivent correspondre. Si seul un sous-ensemble de valeurs est mis en correspondance, les conditions d'agrégation d'événements ne sont pas remplies et un nouvel incident de sécurité est créé. Voir la capture d'écran ci-dessous pour le mappage de champs à valeurs multiples.

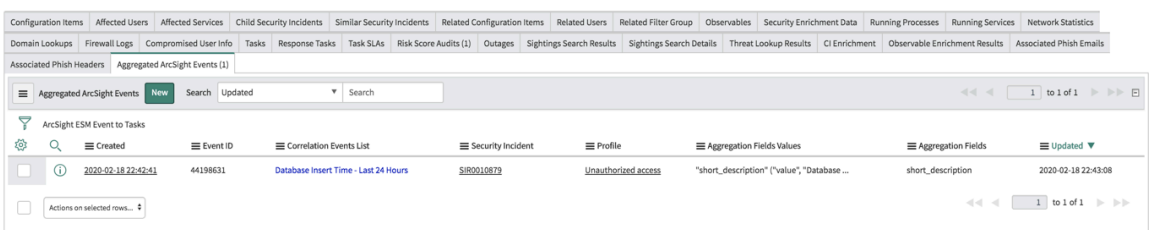


© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si un nouvel événement de corrélation correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation de l'étape de mappage, le nouvel événement de corrélation est automatiquement ajouté au dernier incident de sécurité ouvert avec les mêmes valeurs de champ. En tant qu'analyste SOC travaillant sur des incidents de sécurité, vous pouvez afficher tous les événements de corrélation agrégés ajoutés dans une liste connexe d'un incident de sécurité. Tous les événements de corrélation agrégés sur un incident de sécurité sont affichés dans la liste **connexe Agrégatd ArcSight Events** . Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi ces événements de corrélation sont regroupés aux incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de l'enregistrement sous **Liens connexes** et cliquez sur le lien **Afficher toutes les listes connexes** .

Remarque : Si cette liste connexe n'est pas visible, procédez comme suit :

- Cliquez avec le bouton droit sur l'en-tête du formulaire Incident de sécurité, puis cliquez sur **Configurer** > **Listes connexes**.
- Sélectionnez **Aggregated ArcSight Events (Événements ArcSight agrégés**) dans la liste Available (Disponible), déplacez-le vers Selected list (Sélectionné), puis cliquez sur **Save (Enregistrer**).
- Cliquez sur **Afficher les listes connexes**. Vous verrez maintenant l'onglet **Agrégatd ArcSight Events (Événements ArcSight agrégés**) dans la section Related List (Liste connexe).



c. Facultatif : Pour consigner une note de travail chaque fois qu'un événement est agrégé sur l'incident de sécurité, cochez la case pour activer cette option.
La note de travail indique qu'un nouvel événement corrélé a été ajouté, ainsi qu'un lien vers les détails de l'événement corrélé.

Vous avez mappé avec succès les valeurs d'un événement de corrélation aux champs d'un SIR incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage de génération d'incidents. Vous avez également agrégé des événements de corrélation à des incidents de sécurité existants SIR lorsque les valeurs de champ d'événement correspondent aux critères d'agrégation configurés.

10. Choisissez-en un pour poursuivre la configuration du profil.

Option	Description
Continuer	Le formulaire de mappage s'affiche. **L'aperçu** est sélectionné dans la barre de progression. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements s'affiche ArcSight ESM .
Précédent	Le formulaire Sélection d'événement de corrélation s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements s'affiche.

Prévisualiser l'incident de sécurité pour l'intégration de l'ingestion d'événements ArcSight ESM

Une fois que vous avez terminé l'étape de mappage, prévisualisez les valeurs que vous avez mappées dans un Now Platform Réponse aux incidents de sécurité incident de sécurité (SIR). Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs de corrélation que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin.

Pourquoi et quand exécuter cette tâche

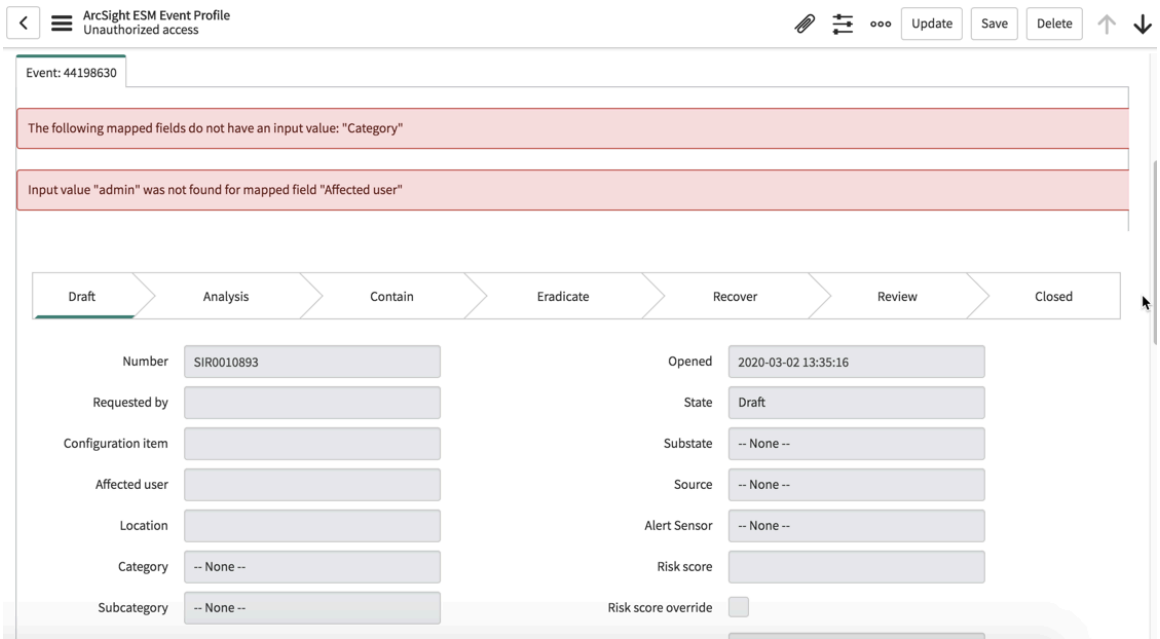
En tant qu'utilisateur disposant du rôle sn_si.admin, prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs contenant des erreurs ou pour renseigner les données manquantes. Si l'aperçu n'est pas terminé, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de sécurité ne sont pas enregistrés en tant qu'incidents réels dans le Réponse aux incidents de sécurité produit.

Procédure

1. Si l'aperçu de l'incident de sécurité n'est pas affiché, cliquez sur **Aperçu** dans la barre de progression.
2. Dans la liste de choix ID d'exemples d'événements, sélectionnez un élément.
   L'incident de sécurité s'affiche. Ne modifiez aucune information dans les champs. Il s'agit d'une vue en lecture seule et un enregistrement de cet incident de sécurité n'est pas enregistré.
3. Examinez le mappage de champs des valeurs d'événements de corrélation sur l'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'image précédente est un exemple d'aperçu avec une erreur de mappage. Dans cet exemple, une valeur de champ de l'événement de corrélation n'a pas de valeur acceptable pour le champ de référence sur le formulaire d'incident SIR. Un message d'erreur s'affiche qui indique qu'une valeur d'entrée est introuvable pour le champ `Catégorie`, qui est un champ de référence avec un ensemble spécifique de valeurs. Par conséquent, cette valeur de champ mappée n'apparaît pas sur le SIR formulaire d'incident de sécurité sans autre modification.

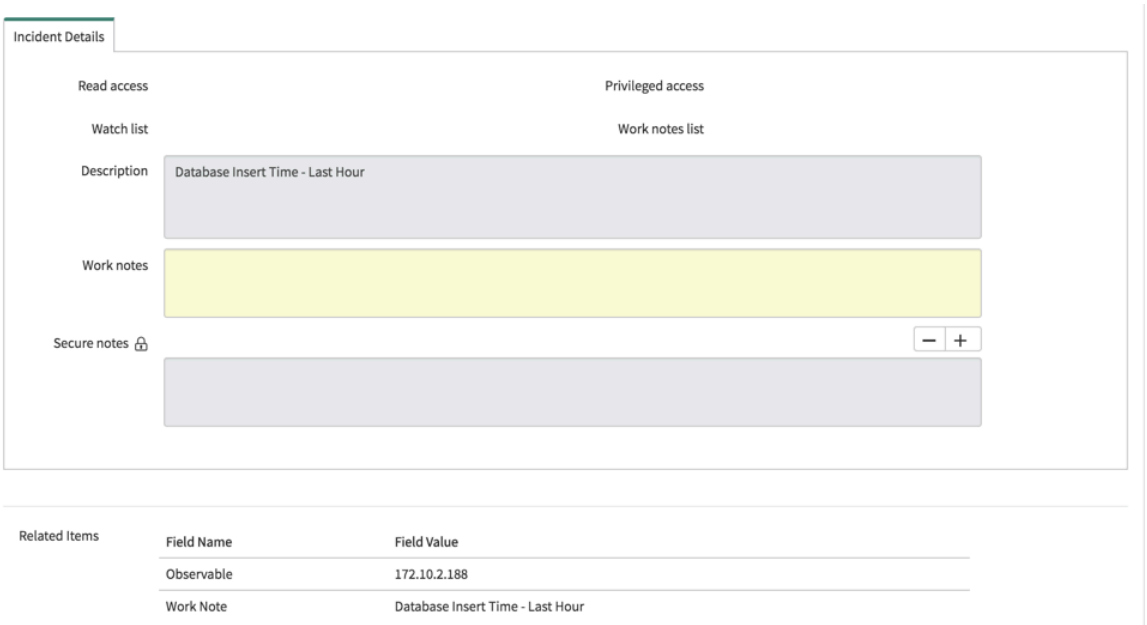
4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

   La figure suivante est un exemple de l'onglet Détails de l'incident dans la moitié inférieure d'un incident de sécurité, une fois que tous les messages d'erreur ont été résolus. Pour cet exemple, les champs Description et Notes de travail ont été mappés, et ces champs sont

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

renseignés avec les valeurs des paires de valeurs extraites des échantillons d'événements ArcSight ESM de corrélation.



Que faire ensuite

Si aucun message d'erreur n'est affiché et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à définir le calendrier.

Créer un calendrier pour ArcSight ESM l'ingestion d'événements

Vous pouvez définir le calendrier d'interrogation ou d'extraction pour les nouveaux événements corrélés. Au cours de cette étape, vous pouvez vérifier les paramètres existants pour la récupération d'événements de corrélation ou modifier la planification selon vos besoins. Cette étape vous permet également de récupérer des événements de corrélation historiques à l'aide d'une plage de dates.

Avant de commencer

Rôle requis : sn_si.admin.

Pourquoi et quand exécuter cette tâche

Vous pouvez choisir d'ingérer des événements de corrélation historiques au cours de l'étape de planification. Vous choisissez également la fréquence à laquelle vous souhaitez interroger les futurs nouveaux événements de corrélation qui correspondent à la configuration du profil.

En tant qu'utilisateur disposant du rôle sn_si.admin, vous configurez ces intervalles d'interrogation pour chaque profil. Les performances de l'intégration d'ingestion ArcSight ESM d'événements de corrélation peuvent être impactées par les différents intervalles d'interrogation. Lors de la planification, vous préférerez peut-être trouver un équilibre entre la réduction de la surcharge d'interrogation sur le serveur et le ArcSight ESM désir d'être averti dès que possible lorsqu'un événement est créé ou mis à jour. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférerez peut-être modifier ce paramètre à une minute si nécessaire.

Extraction d'événements de corrélation nouveaux et mis à jour

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

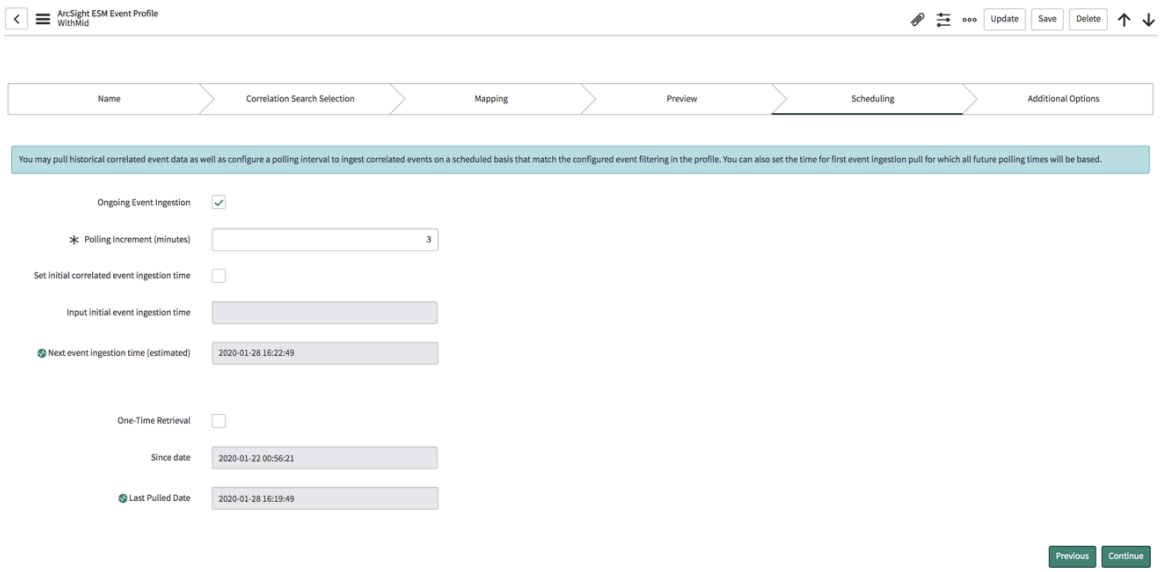
1. Si la page Planification de la barre de progression n'est pas affichée, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les événements de corrélation sont extraits de la console <ArcSight>.

Option	Description
◦ Champ d'ingestion d'événement en cours sélectionné ◦ Champ de récupération ponctuelle effacé	Événement en cours En fonction du paramètre par défaut, l'instance Now Platform effectue une extraction du serveur pour de ArcSight ESM nouveaux événements de corrélation toutes les cinq minutes. Les incidents de sécurité sont créés si des événements de corrélation sont trouvés et si les critères de filtrage de génération d'incident sont respectés. Pour équilibrer les frais généraux d'interrogation d'ingestion afin d'obtenir les données les plus récentes, le paramètre par défaut est de cinq minutes. Toutefois, cette valeur peut être modifiée jusqu'à une minute si nécessaire.
◦ Champ d'ingestion d'événement en cours vide ◦ Champ de récupération ponctuelle sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhaitez une transmission par pull unique pour ingérer des événements de corrélation historiques. Lorsque ce paramètre est configuré, un profil est utilisé une fois pour récupérer des événements de corrélation à partir d'événements historiques basés sur une plage de dates. À droite du champ Depuis date, cliquez sur l'icône Calendrier. Dans le calendrier qui s'affiche, sélectionnez la date à laquelle vous souhaitez commencer à extraire les alertes. À partir de la valeur Date de début, les événements de corrélation sont récupérés jusqu'à la date actuelle. Notez que vous pouvez récupérer des événements jusqu'à sept jours en arrière à partir de la date actuelle. Cette fonctionnalité n'est pas destinée à récupérer des quantités importantes d'événements historiques à des fins d'archivage, mais plutôt une quantité minimale d'événements en cours qui sont activement traités au moment de l'activation du profil. Une fois les événements de corrélation extraits, ce paramètre ne récupérera pas d'autres événements de corrélation pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	ce profil à partir de la date actuelle. Ce paramètre remplit l'incident de sécurité avec tous les événements de corrélation qui sont trouvés pour la plage que vous saisissez.



Par exemple, pour planifier un temps d'ingestion d'un événement de corrélation initial, si vous avez un contrôle de sécurité quotidien ArcSight ESM qui s'exécute une fois par jour à 4 h (heure locale), vous pouvez configurer le profil d'événement de corrélation correspondant dans votre Now Platform instance pour qu'il s'exécute à 4 h 05 (heure locale) afin de capturer immédiatement l'événement de défaillance de sécurité et créer un incident de sécurité. Entrez `04 05 00` dans le champ Ingestion de l'événement initial. Dans le champ Incrémentation (minutes), saisissez `1 440` (24 heures) pour planifier la prochaine ingestion d'événement pendant 24 heures à compter de l'ingestion d'événement initiale. L'heure d'ingestion de l'événement initial et l'heure d'ingestion de l'événement suivant sont affichées dans les champs.

3. Pour configurer les paramètres de cet exemple, procédez comme suit.

a. Une fois la page Planification affichée, cochez la case **Ingestion d'événements en cours** pour activer cette option.

b. Dans le champ Incrémentation (minutes), saisissez `1 440` (24 heures).

c. Cochez la case **Définir le délai d'ingestion de l'événement initial corrélé** pour activer la modification des champs d'ingestion d'événement initial et d'ingestion d'événement suivant.

d. Dans le champ Délai d'ingestion de l'événement initial, saisissez `04 05 00`.
Dans le champ Délai d'ingestion de l'événement suivant (estimé), l'heure de l'ingestion de l'événement suivante s'affiche.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Continuer** pour accéder à la page Options supplémentaires.

> **Remarque :** Le nombre par défaut d'incidents de sécurité qui peuvent être créés et agrégés en une journée, ainsi que la période de temps du flux sont définis dans les paramètres d'intégration ArcSight ESM . Vous pouvez modifier ces paramètres si nécessaire. Consultez ArcSight ESM Paramètres d'intégration pour l'intégration de l'ingestion d'événements pour en savoir plus.

Options supplémentaires : automatisez les mises à jour et la fermeture des événements corrélés en fonction de l'état de SIR l'incident

L'intégration ArcSight ESM dispose d'une interface bidirectionnelle qui permet à la fois les événements de corrélation pour créer des incidents de sécurité, ainsi que la possibilité de mettre à jour les événements de corrélation une fois l'incident de sécurité créé et/ou fermé avec les détails d'incident pertinents tels que le numéro d'incident de sécurité, le groupe d'affectation, SIR l'URL de l'incident, entre autres.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si la page Options supplémentaires de la barre de progression n'est pas affichée, sélectionnez **Options supplémentaires**.
2. Suivez les instructions ci-dessous pour terminer la configuration de mise à jour des événements corrélés lors de la création de l'incident de sécurité.

Option ou champ	Description
Mettre à jour les événements corrélés lors de la création de l'incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour l'étape de l'événement de corrélation dans ArcSight ESM et mettre à jour l'événement avec des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir de l'événement de corrélation. Cela peut se produire pour les événements de corrélation susceptibles de créer un nouvel incident de sécurité ou regrouper des incidents de sécurité existants. **Remarque :** Si cette option n'est pas sélectionnée, l'étape d'événement n'est pas mise à jour lors de la création de l'incident de sécurité.
Mise à jour de l'étape de l'événement corrélé	Sélectionnez une option d'étape dans la liste de choix Mise à jour de l'étape de l'événement corrélé qui affiche toutes les étapes disponibles récupérées à partir du ArcSight ESM serveur.

Étape d'événement corrélé non configurée : si vous n'avez configuré aucune étape d'événement corrélé dans votre Now Platform instance, vous verrez uniquement **l'étape Affecter : configuration initiale** dans la liste de choix Mise à jour de l'étape d'événement corrélé. Pour configurer l'étape, procédez comme suit :

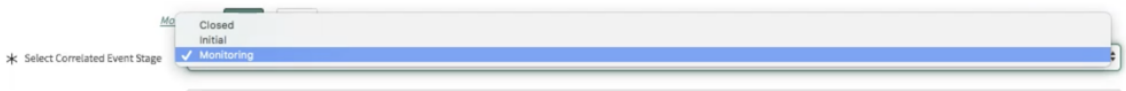
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Entrez un ID de ressource dans le champ Saisir l'ID de ressource de l'étape et cliquez sur **Soumettre**. L'ID de ressource est validé dans la ArcSight ESM console et l'écran suivant s'affiche.



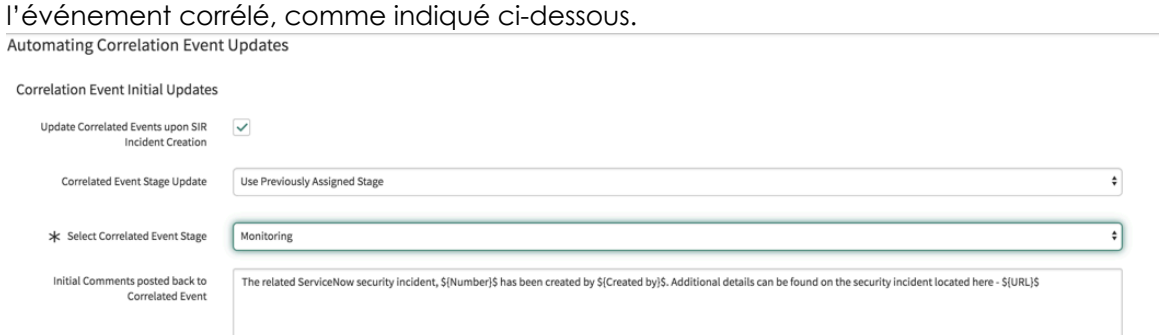
- Cliquez sur **Enregistrer** pour enregistrer la nouvelle étape (**Monitoring**).
- Cliquez sur la liste déroulante Sélectionner l'étape de l'événement corrélé.



- Vous pouvez sélectionner l'étape nouvellement créée dans la liste.

Étape d'événement corrélé déjà configurée : si vous avez déjà configuré l'étape d'événement corrélé, procédez comme suit :

- Sélectionnez **Utiliser l'étape précédemment affectée** dans la liste de choix Mettre à jour l'étape de l'événement corrélé.
- Sélectionnez une étape existante dans la liste de choix Sélectionner l'étape de l'événement corrélé, comme indiqué ci-dessous.



- Commentaires initiaux renvoyés à l'événement corrélé : en plus de mettre à jour la valeur d'étape de l'événement de corrélation, vous pouvez également poster des commentaires sur les annotations d'étape de corrélation. Comme indiqué dans les instructions, vous pouvez modifier le texte par défaut affiché dans la section Commentaires, y compris ajouter ou modifier les variables de substitution en utilisant le format ${nom de champ}$ pour n'importe quel champ du formulaire d'incident de Réponse aux incidents de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez utiliser les étapes par défaut définies dans la ArcSight ESM console ou créer vos propres étapes personnalisées. Pour créer une étape, procédez comme suit :

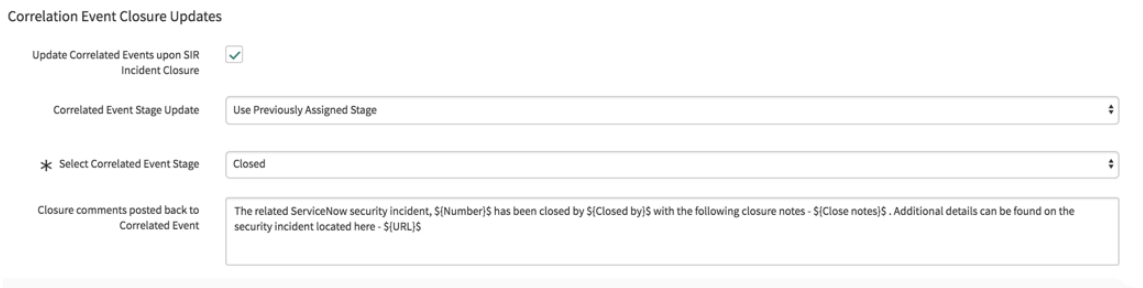
- Dans la ArcSight ESM console, sélectionnez **Fichier** > **Nouveau** > **Étape**. L'onglet Inspecter/Modifier s'affiche.
- Définissez la nouvelle étape et ne cochez pas la case **Utilisateur requis** . Assurez-vous que l'étape est définie correctement et qu'elle se trouve à la bonne position dans le cycle de vie de l'événement.

3. Dans la section Automatisation de la fermeture de l'événement corrélé, vous pouvez définir comment mettre à jour l'incident de sécurité lorsqu'il est fermé.
4. Renseignez les champs du formulaire.

Option ou champ	Description
Mettre à jour les événements corrélés lors de la fermeture de l'incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour l'état de corrélation de l'événement et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est fermé à partir de l'événement corrélé. Cela se produira à la fois pour les événements notables déclencheurs initiaux qui créent l'incident de sécurité ainsi que pour les événements agrégés. **Remarque :** Si cette option n'est pas sélectionnée, l'étape de l'événement ne sera pas mise à jour lorsque l'incident de sécurité sera fermé.
Mise à jour de l'étape de l'événement corrélé	Sélectionnez une option d'étape dans le menu qui affiche toutes les étapes disponibles récupérées à partir du ArcSight ESM serveur. Sélectionnez la valeur d'étape à définir pour tous les événements de corrélation lorsqu'un incident de sécurité doit être fermé. **Remarque :** Les étapes affichées ici sont basées sur les étapes configurées dans la section Mises à jour initiales de l'événement de corrélation.
Sélectionner l'étape de l'événement corrélé	Sélectionnez un état approprié ici.
Commentaires de fermeture renvoyés à l'événement corrélé	En plus de mettre à jour la valeur d'état de l'événement de corrélation, vous pouvez également publier des commentaires de fermeture sur les annotations d'événement de corrélation. Comme indiqué dans les instructions, vous pouvez modifier le texte par défaut affiché dans la section Commentaires, y compris ajouter ou modifier

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	les variables de substitution en utilisant le format ${nom de champ}$ pour n'importe quel champ du formulaire d'incident de Réponse aux incidents de sécurité.



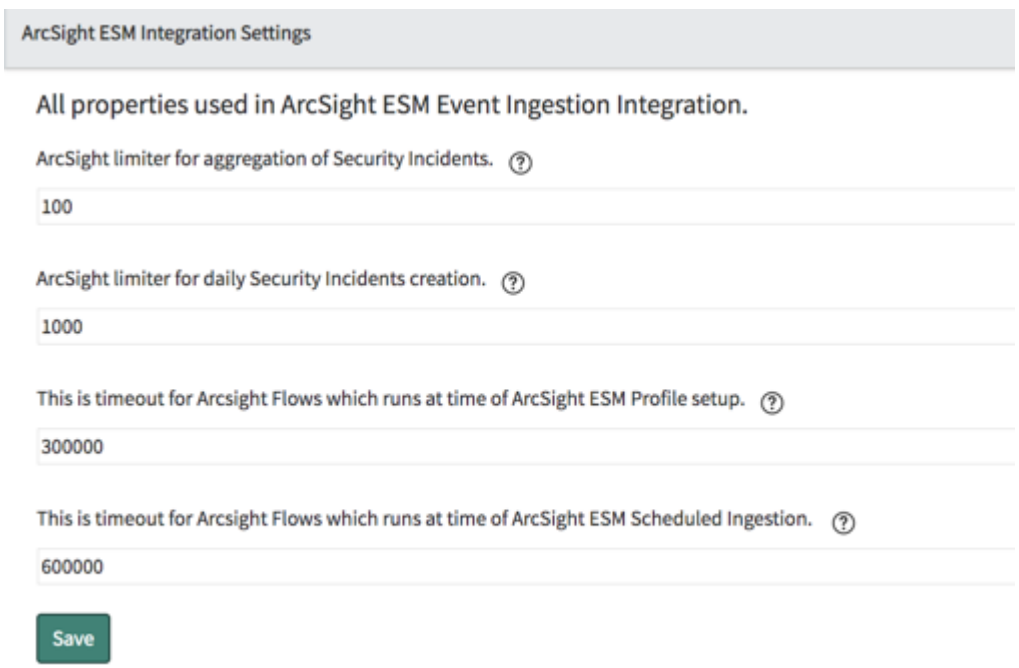
5. Cliquez sur **Terminer** pour terminer la configuration.
   Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Activez ce profil pour extraire des événements de corrélation de la ArcSight ESM console en fonction de votre planification.

ArcSight ESM Paramètres d'intégration pour l'intégration de l'ingestion d'événements

Utilisez cette option pour modifier les paramètres d'ingestion ArcSight ESM par défaut.

Pour modifier les propriétés système, connectez-vous en tant qu'utilisateur ayant le rôle *sn_si.admin* et accédez à **Intégration d'ArcSight ESM** > **Paramètres d'intégration d'ArcSight ESM**.

Les paramètres de configuration par défaut s'affichent. Vous pouvez modifier ces paramètres si nécessaire.



Traduction automatique

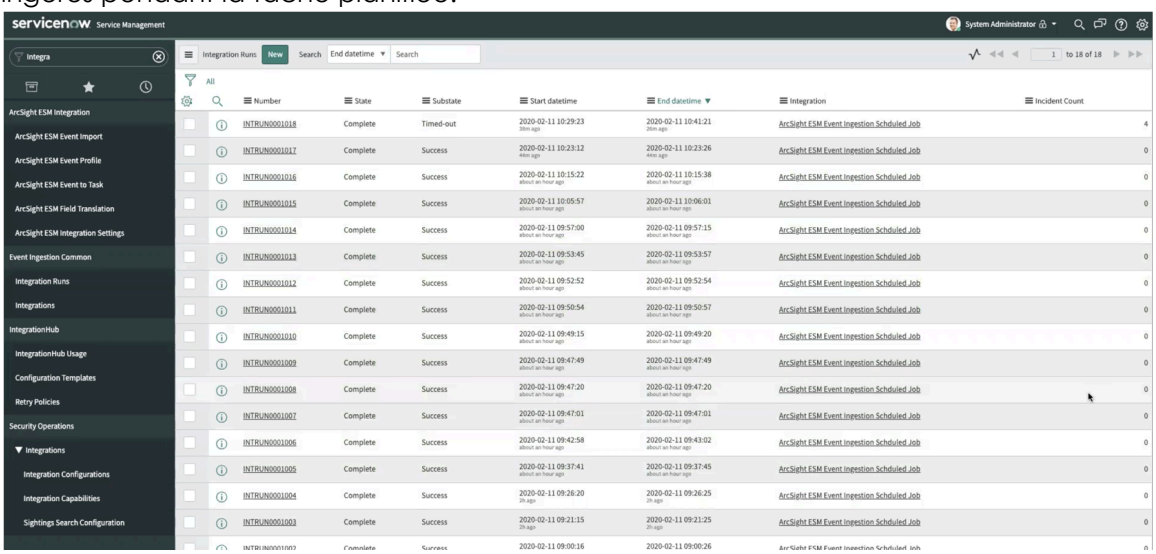
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépanner l'intégration ArcSight ESM de l'ingestion d'événements

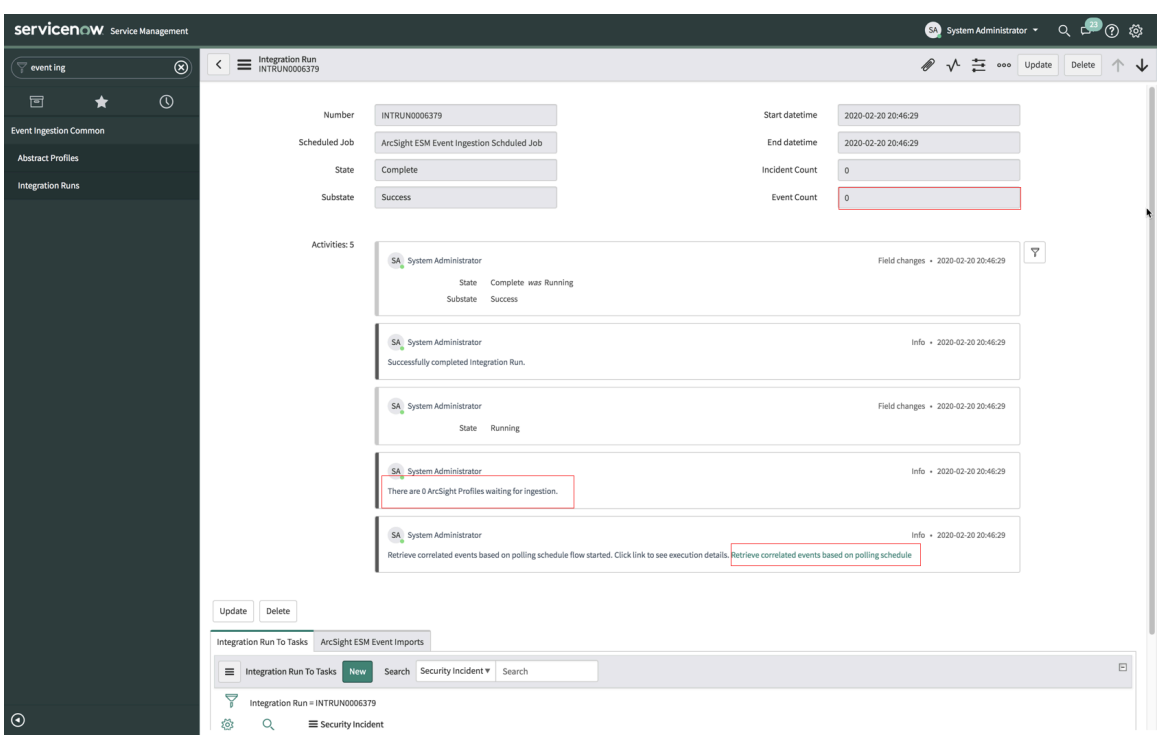
Cette section fournit des informations sur la façon de résoudre les erreurs qui peuvent se produire lors de l'ingestion d'événements.

Exécutions de l'intégration

Accédez à la **Ingestion d'événement commune** > **Exécutions des intégrations**. Une exécution d'intégration a lieu toutes les minutes et capture les détails concernant les événements ingérés pendant la tâche planifiée.



Vous pouvez afficher la liste des exécutions d'intégration et l'état de chaque exécution (Réussite, Expiré, En attente), ainsi que le nombre d'incidents de sécurité créés. Cliquez sur le lien Numéro pour accéder à la page Exécution de l'intégration détaillée.



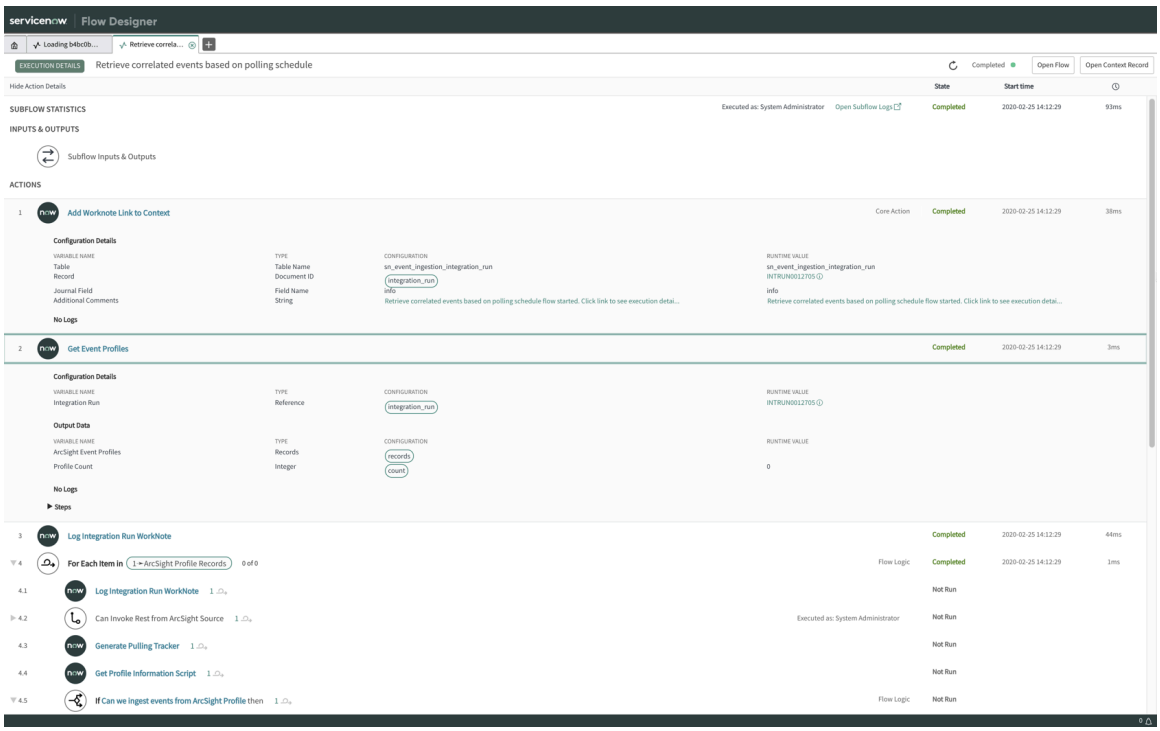
Vous pouvez afficher des détails tels que le nombre d'événements qui ont été ingérés, leur état, l'événement qui a été transformé en incident de sécurité et les différentes tâches qui ont été effectuées pendant l'ingestion. En outre, vous pouvez cliquer sur le lien pour afficher les détails de l'exécution du flux.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails d'exécution du flux

Cliquez sur le lien des détails de l'exécution pour consulter le flux associé à l'ingestion d'événement.



Vous pouvez afficher une exécution étape par étape du flux détaillant les différentes actions et flux secondaires qui ont été exécutés dans le cadre du flux.

Copier le ArcSight ESM profil pour l'intégration de l'ingestion d'événements

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils pour gagner du temps.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

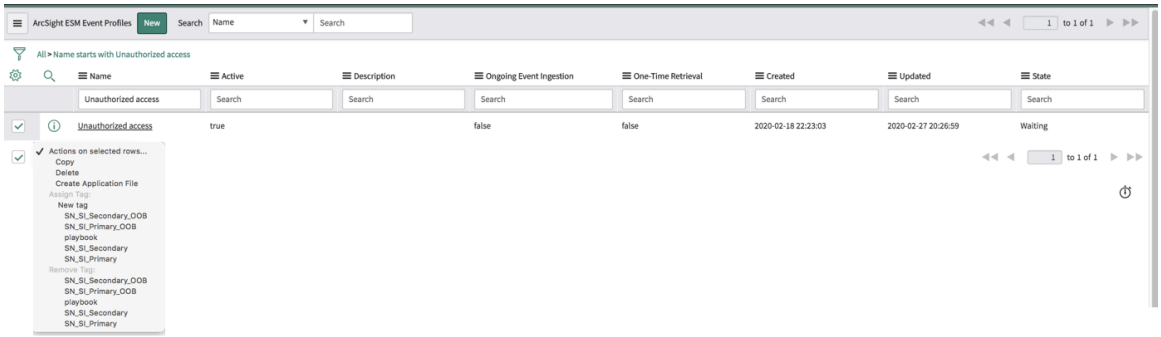
En tant qu'utilisateur disposant du rôle sn_si.admin, si vous copiez un profil, le nom du profil est d'abord modifié pour éviter les profils en double. En outre, le profil copié est désactivé (faux) afin qu'il ne soit pas activé accidentellement avant la fin de la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure

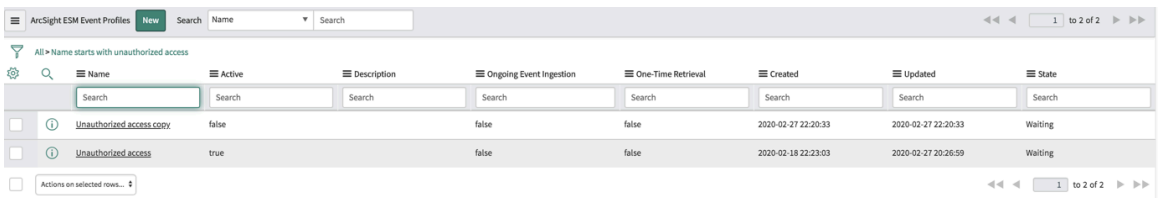
1. Accédez à la **Tout** > **Intégration d'ArcSight ESM** > **Profil d'événement ArcSight ESM**.
2. Dans la liste ArcSight Profiles (Profils ArcSight qui s'affiche), sélectionnez un profil que vous souhaitez copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier (Copier**).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (`vrai`), la copie est désactivée à ce stade (`faux`). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. Notez que l'état de la colonne **Actif** est défini sur faux, car le profil doit être activé.

Utiliser l'éditeur de script pour formater les valeurs d'événements de corrélation pour ArcSight ESM l'intégration

En plus des champs directement mappés à partir des valeurs d'événements de corrélation ingérés, utilisez l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

L'éditeur de script modifie les valeurs d'un ArcSight ESM champ d'événement de corrélation afin que les valeurs prises en charge par l'incident Now Platform SIR de sécurité soient mappées aux champs Catégorie, Élément de configuration (CI), Observable et autres d'incident de sécurité.

Dans certains cas, ArcSight ESM les valeurs d'événements de corrélation sont mappées aux champs de référence tels que les champs Catégorie, Élément de configuration (CI) et Observables sur l'incident de sécurité. En tant qu'utilisateur disposant du rôle sn_si.admin, vous préférez peut-être modifier les valeurs de champ d'événement mappées pour traduire le format ou les valeurs de données afin qu'elles soient conformes aux formats de champ d'incident et aux valeurs attendues. Si vous souhaitez convertir la valeur d'un ArcSight ESM événement de corrélation en une valeur prise en charge par ces champs sur l'incident SIR de sécurité, utilisez l'éditeur de script.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Une fois le formulaire de mappage affiché, cliquez sur le lien pour ouvrir l'éditeur de script.
2. Dans la liste de choix, sélectionnez un champ de destination pour la valeur que vous souhaitez modifier.
3. Dans la section Mappage de champs d'incidents SIR, vous pouvez également cliquer sur l'icône de crochet `[{}]` en regard d'un champ pour ouvrir l'éditeur de script relatif à ce champ.

   Dans certains cas, un include de script peut être approprié pour le champ Élément de configuration. Pour un événement de corrélation, par exemple, une valeur pour l'élément de configuration peut ne pas être mise en correspondance.

   Comme le montre la figure suivante, si une correspondance de nom d'hôte est introuvable dans la Now Platform CMDB pour le champ Élément de configuration, vous pouvez modifier la règle de sorte que, si une adresse IP est trouvée, elle remplisse le champ Élément de configuration.

   L'éditeur s'ouvre avec le champ affiché dans Champ de destination.
4. Entrez toutes les modifications dans le script, puis cliquez sur **Mettre à jour** pour enregistrer vos modifications.
   La ArcSight ESM table Traductions de champ s'affiche.
5. Fermez la table pour revenir au formulaire de mappage.

Utilisation de Concepteur de flux avec ArcSight ESM intégration de l'ingestion d'événements

À l'aide du concentrateur d'intégration et de Flow Designer, plusieurs flux, flux secondaires et actions sont disponibles avec l'intégration ArcSight ESM .

Pour afficher ces flux secondaires, accédez à **Concepteur de flux** > **Concepteur** et cliquez sur l'onglet **Flux secondaires** . La figure ci-dessous montre les flux secondaires importants utilisés pendant la création du profil et la tâche d'ingestion planifiée.



Ces flux secondaires sont répertoriés dans la séquence dans laquelle ils sont exécutés ci-dessous :

- **Validation de la connexion et des informations d'identification** : ce flux secondaire valide ServiceNow la connectivité avec le ArcSight ESM serveur et les informations d'identification spécifiées. Ce flux secondaire est utilisé lorsque vous cliquez sur le bouton **Configurer**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

dans la tuile **ArcSight ESM - Event Ingestion**dans le **Security Operations** > **Intégrations** > **Configuration des intégrations** la page.

- **Obtenir le jeton d'authentification ArcSight** : ce flux secondaire génère le jeton d'authentification ArcSight ESM à partir du nom d'utilisateur et du mot de passe à l'aide du ArcSight ESM service de connexion. Le service de connexion fournit le jeton d'authentification qui peut être utilisé pour appeler n'importe quel autre point de ArcSight ESM terminaison. Ce flux secondaire est utilisé dans tous les autres flux secondaires.
- **Validation de l'ID du visualiseur de requêtes** : ce flux secondaire vérifie si l'ID du visualiseur de requêtes spécifié lors de la création du profil est présent dans le ArcSight ESM serveur.
- **Récupération de la règle de corrélation** : ce flux secondaire récupère les règles de corrélation en fonction de l'ID du visualiseur de requêtes.
- **Obtenir un exemple d'événement** : ce flux secondaire récupère les échantillons d'événements de corrélation à partir du ArcSight ESM serveur. Ces exemples d'événements sont ensuite mappés aux champs d'incident de sécurité dans la section Mappage du profil.
- **Validation de l'ID de ressource d'étape** : ce flux secondaire valide l'ID de ressource d'étape spécifié dans la ArcSight ESM console et extrait le nom de la ressource.
- **Mettre à jour les commentaires d'événements corrélés** : ce flux secondaire met à jour les commentaires d'événements corrélés dans les sections Initial et Fermeture d'incident de la page Options supplémentaires du profil.
- **Récupérer les événements corrélés en fonction du calendrier d'interrogation** : ce flux secondaire exécute la tâche planifiée qui extrait les événements corrélés en fonction de l'intervalle d'interrogation.

Pendant l'exécution, les flux secondaires ci-dessus déclenchent également plusieurs autres flux secondaires et actions directement ou indirectement, comme indiqué ci-dessous.

Flows Subflows Actions Executions Help + New

Can Invoke Rest from ArcSight Source	can_invoke_rest_from_arcsight_source	Security Operations ArcSight ESM Event I...	Published	true	2020-01-07 00:46:32	admin
Check Closure Update Events REST Step St...	check_closure_update_events_rest_step_st...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:08	admin
Check Initial Update Events REST Step St...	check_rest_step_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:55	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:50:26	admin
Correlation Rule Retrieval	correlation_rule_retrieval_5	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:51:40	admin
Finish Profile Event Ingestion	end_process_run	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:53:48	admin
Get Profile Ingestion Information	get_last_run_date	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:54:31	admin
Get Sample Events	get_sample_events	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:55:59	admin
Query Viewer ID Validation	query_viewer_id_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:56:52	admin
Retrieve correlated events based on poll...	retrieve_correlated_events_based_on_poll...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:58:28	admin
Stage Resource ID Validation	get_stage_resource_name	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:00:00	admin
Update Correlated Event	update_correlated_event	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 23:12:18	admin
Update Correlated Event Comments	update_correlated_event_comments	Security Operations ArcSight ESM Event I...	Published	true	2020-02-15 02:08:37	admin
Validate MID Server Status	validate_mid_server_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:03:40	admin

Carbon Black - Intégration de l'enrichissement des incidents

Utilisez l'intégration Carbon Black pour enquêter sur les incidents de sécurité et y répondre à l'aide d'API pour interroger et interagir avec les points de terminaison associés aux incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Trouver des ressources d'intégration Carbon Black - Enrichissement des incidents

- Introduction à l'intégration Carbon Black - Enrichissement des incidents
- Intégration de Security Operations Carbon Black : workflow Obtenir les processus en cours d'exécution
- Intégration de Security Operations Carbon Black : workflow Isoler l'hôte
- Intégration de Security Operations Carbon Black : workflow de suppression de l'isolement de l'hôte

Comprendre les concepts d'intégration

- Types d'intégrations ServiceNow fournies
- Opérations de sécurité Déclencheurs de workflow

Obtenir de l'aide depuis les ressources ServiceNow

- Poser des questions ou y répondre dans la communauté des opérations de sécurité
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client
- Surclassement à Madrid

Introduction à l'intégration Carbon Black - Enrichissement des incidents

L'enrichissement des incidents Carbon Black facilite l'enquête sur un incident de sécurité en interrogeant les journaux à la recherche d'indicateurs potentiellement malveillants. Avant de pouvoir utiliser l'intégration Carbon Black - Enrichissement des incidents, vous devez la télécharger à ServiceNow Store partir du et ajouter l'URL de base du point de terminaison et le serveur MID appropriés.

Avant de commencer

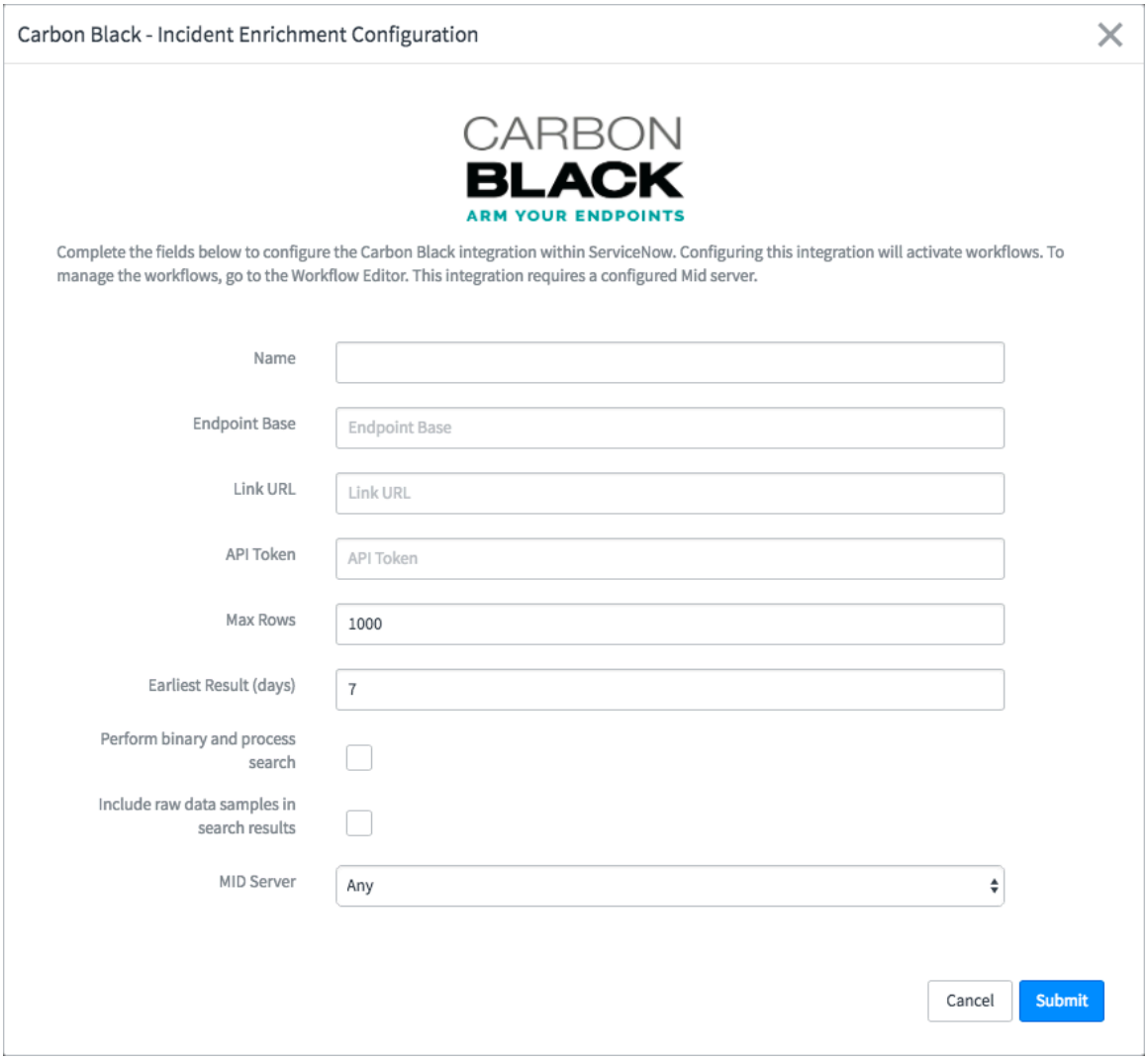
Rôle requis : sn_si_admin

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois le téléchargement terminé, accédez au Carbon Black site Web et obtenez l'URL de base du point de terminaison et le jeton d'API sous votre profil.
3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configuration de l'intégration**.
4. Dans la fiche Carbon Black - Incident Enrichment (Noir carbone - Enrichissement d'incident), cliquez sur **Configure (Configurer)**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
Base du point de terminaison	L'URL du point de terminaison que vous avez acquise à partir du site Carbon Black.
URL de lien	URL du lien qui renvoie à une instance Carbon Black, lorsqu'elle est disponible.
Jeton d'API	Le jeton d'API que vous avez acquis sur le site Carbon Black.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher. La valeur par défaut est de 1 000 lignes.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Effectuer une recherche binaire et de processus	Sélectionnez cette option pour effectuer des recherches binaires afin de trouver des fichiers binaires, tels que des hachages de fichiers, et des recherches de processus pour .exe processus qui peuvent s'être exécutés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend du paramètre que vous définissez sur le **nombre de lignes de la propriété de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	Sélectionnez **N'importe lequel** pour utiliser n'importe quel Serveur MID actif ou sélectionnez un nom de Serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

6. Cliquez sur **Envoyer**.
   La carte de configuration de l'intégration s'affiche.
7. Pour revenir à la liste initiale des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Intégration Carbon Black

L'intégration de Carbon Black vous permet d'enquêter sur les incidents de sécurité et d'y répondre à l'aide d'API pour interroger et interagir avec les points de terminaison associés aux incidents de sécurité.

Explorer

- Intégrations de Réponse aux incidents de sécurité
- Carbon Black - Intégration de l'enrichissement des incidents

Configurer

Lancez-vous avec l'intégration Carbon Black

Utiliser

- Opérations de sécurité Déclencheurs de workflow
- Afficher les éléments affectés pour un incident de sécurité
- Security Operations : workflow Obtenir les processus en cours d'exécution
- Intégration de Security Operations Carbon Black : workflow Obtenir les processus en cours d'exécution
- Afficher les éléments affectés pour un incident de sécurité
- Exécuter une demande de bloc
- Security Operations Integration - Workflow de demande de bloc
- Exécuter Isoler l'hôte

Développer

- ServiceNow Opérations de sécurité Directives de développement de l'intégration
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Intégration de Security Operations Carbon Black : workflow Isoler l'hôte
- Intégration de Security Operations Carbon Black : workflow de suppression de l'isolement de l'hôte

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté des opérations de sécurité
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Lancez-vous avec l'intégration Carbon Black

Carbon Black est un système de sécurité avancé qui s'intègre facilement à Opérations de sécurité . Avant de pouvoir utiliser l'intégration Carbon Black, vous devez télécharger l'intégration à partir du et ajouter la base de point de ServiceNow Store terminaison et le jeton d'API appropriés.

Avant de commencer

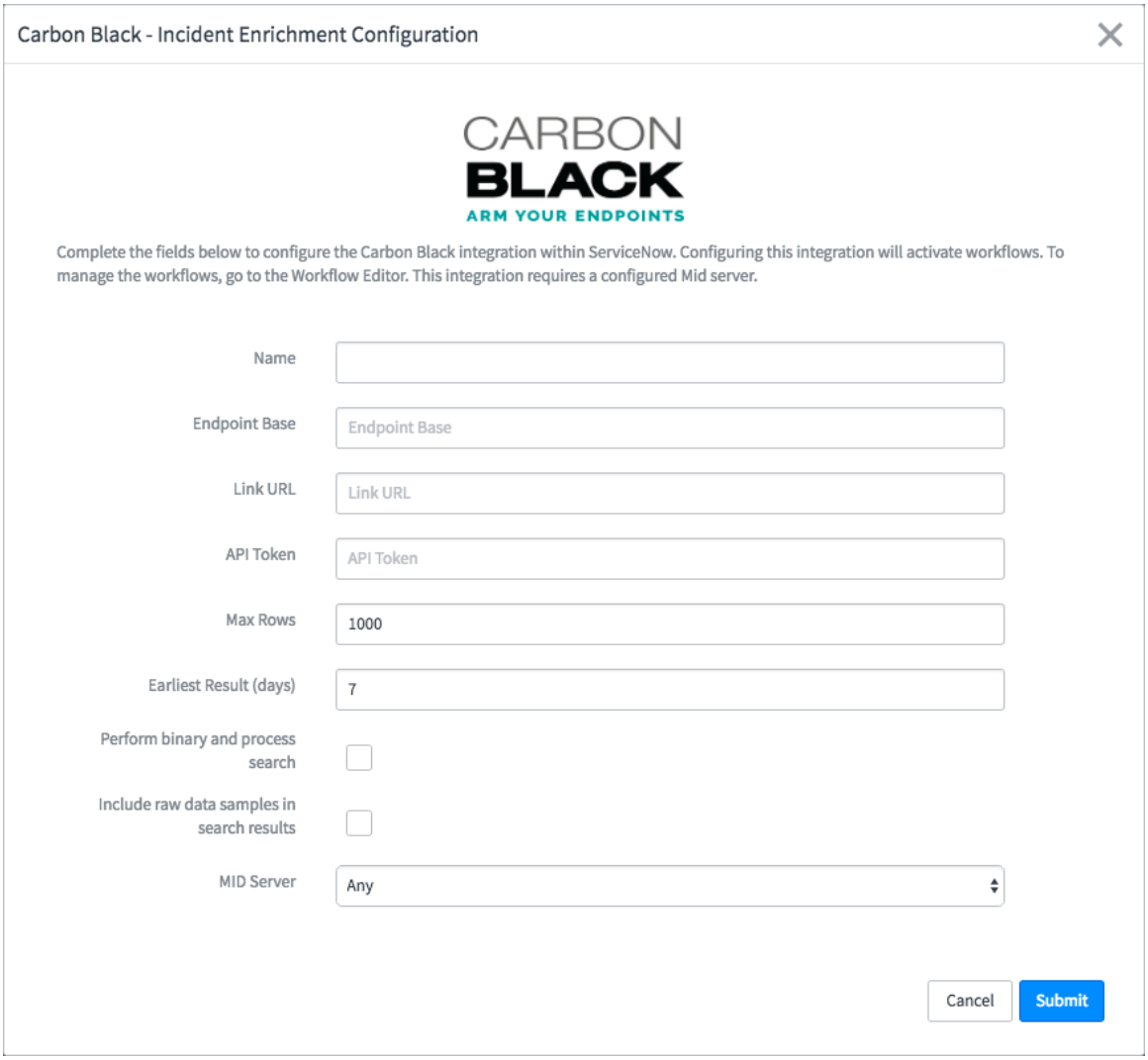
Rôle requis : sn_si_admin

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez au Carbon Black site Web et obtenez l'URL de base du point de terminaison et le jeton d'API sous votre profil.
3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la Carbon Black carte, cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
Base du point de terminaison	La base de point de terminaison que vous avez acquise sur le site Carbon Black.
Jeton d'API	Le jeton d'API que vous avez acquis sur le site Carbon Black.
Utiliser un serveur MID	Cochez cette case si elle n'est pas déjà cochée.
Serveur MID	Sélectionnez **N'importe lequel** pour utiliser n'importe quel Serveur MID actif ou sélectionnez un nom de Serveur MID spécifique.
Activer Isoler l'hôte	Cochez cette case pour permettre aux éléments de configuration sélectionnés d'être isolés de l'onglet de liste connexe **Éléments de configuration** dans un incident de sécurité.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Envoyer**.
   La carte de configuration de l'intégration s'affiche.
7. Pour revenir à la liste initiale des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Anti-robot Check Point - Intégration de l'analyseur d'e-mail

L'intégration Check Point Anti-bot - Analyseur d'e-mails est prise en charge à l'aide d'un analyseur d'e-mails qui utilise les notifications par e-mail de Check Point Anti-bot pour créer des incidents de sécurité et diriger les workflows d'enrichissement et de réponse.

Configurer l'intégration Check Point Anti-bot - Analyseur d'e-mails

L'intégration Check Point Anti-bot - Analyseur d'e-mails utilise des notifications par e-mail pour diriger les workflows d'enrichissement et de réponse.

Avant de commencer

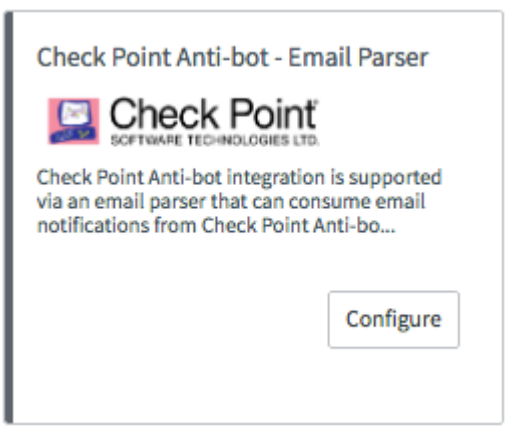
Rôle requis : sn_si_admin

Pourquoi et quand exécuter cette tâche

Un modèle d'analyseur d'e-mails Check Point Anti-bot est fourni pour être utilisé pour l'intégration. Il doit être configuré et activé avant que l'intégration n'ait lieu. La mise à jour de l'analyseur l'active.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.



2. Dans la carte Check Point Anti-bot - Analyseur d'e-mails, cliquez sur **Configurer**.
3. Dans la boîte **de dialogue Check Point Anti-bot - Configuration de l'analyseur d'e-mails** , cliquez sur le lien **Configurer l'analyseur d'e-mails** .
4. Cliquez sur le lien **Check Point Anti-bot** pour modifier les paramètres dans l'analyseur d'e-mail de modèle fourni.
   Renseignez au minimum le champ `L'e-mail provient de` . Pour créer un analyseur d'e-mails, reportez-vous à la section Créer des analyseurs d'e-mails dans Security Operations.
5. Cochez la case **Actif** .
6. Cliquez sur **Mettre à jour** dans le formulaire **Analyseur d'e-mail** .
   L'analyseur d'e-mail est actif. Vous n'avez pas besoin de revenir aux **configurations d'intégration**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Check Point Next Generation Threat Prevention intégration

Ce document décrit les étapes requises pour intégrer les options Check Point Next Generation Threat Prevention (NGTP) à ServiceNow® Réponse aux incidents de sécurité (SIR) afin que les applications fonctionnent correctement ensemble.

Une fois installée et configurée, l'analyste des incidents de sécurité utilise cette intégration pour bloquer les adresses IP, les URL et les domaines malveillants à l'aide des options de liste de demandes de blocs avec les ServiceNow Réponse aux incidents de sécurité produits (SIR). Cette liste de demandes de blocs est configurée sur les passerelles Check Point en tant que flux de renseignements personnalisé. La fonctionnalité Flux de renseignements personnalisés permet d'ajouter des flux de renseignements cybernétiques personnalisés dans le moteur de prévention des menaces de nouvelle génération. Il permet d'extraire les flux d'un serveur tiers, en l'occurrence l'application ServiceNow Réponse aux incidents de sécurité , directement vers Check Point Next Generation Gateway pour qu'ils soient appliqués par les lames Anti-Virus et Anti-Bot. L'analyste de Security Incident Response crée des entrées pour la liste de blocs Check Point à partir d'observables déterminés comme malveillants sur ServiceNow les incidents de sécurité SIR.

Pour la plupart des implémentations, une liste de demandes de blocs est un fichier csv hébergé sur un serveur Web externe. Pour cette intégration, ce serveur Web est votre instance Now Platform, ce qui permet au moteur de prévention des menaces de nouvelle génération Check Point d'extraire la liste des adresses IP, des URL et des domaines à bloquer.

Pour appliquer les observables bloquants sur Check Point Gateway, assurez-vous que la politique de prévention des menaces est configurée avec les lames anti-bot et anti-virus activées. Au fur et à mesure que les entrées de la liste de blocs sont modifiées, le moteur de prévention des menaces importe la liste dynamiquement à l'intervalle configuré et applique la politique sans changement de configuration ni validation sur le pare-feu. Pour cette intégration, Now Platform a créé une table contenant les entrées de la liste de blocs qui sont récupérées par la passerelle de nouvelle génération Check Point autorisée aux intervalles de récupération configurés.

L'intégration comprend les fonctionnalités suivantes :

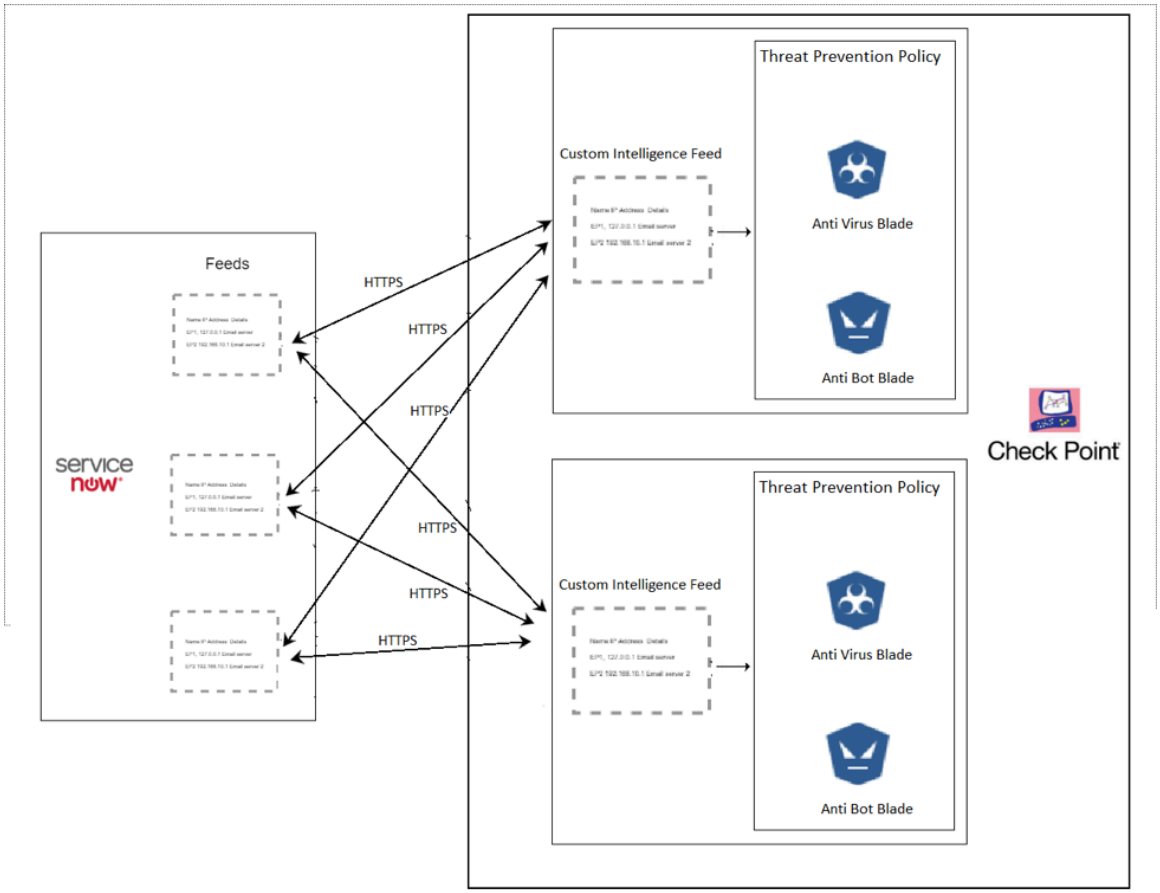
- Flexibilité de création de plusieurs listes de blocs qui s'appliquent à plusieurs passerelles Check Point.
- Rapports détaillés sur les types de sites bloqués (hameçonnage, logiciels malveillants et sites sur liste d'autorisation).
- Balisage des incidents de sécurité de Now Platform avec des entrées de liste de blocs par type d'observable (URL, domaine, adresse IP).
- Configurer les périodes d'expiration de la liste de blocs pour maintenir la taille de la liste de blocs en faisant automatiquement expirer ou en supprimant les entrées plus anciennes.
- Recherche d'entrées de liste de blocs entre différentes listes de blocs.
- Liaison des entrées de liste de blocs aux enregistrements d'observables et aux incidents de sécurité qui incluent des résultats de Threat Intelligence et des détails sur les raisons pour lesquelles une entrée est bloquée.

Diagramme d'architecture d'intégration

Vous trouverez ci-dessous le diagramme d'architecture de haut niveau représentant les composants impliqués et les points d'intégration entre NOW Platform et Check Point Systems.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Le logo Check Point Systems, l'image Anti-Virus Blade et l'image Anti Bot Blade proviennent de Check Point Systems ©. Ils sont la propriété de Check Point Systems.

Modules d'extension

L'intégration nécessite que le module d'extension Réponse aux incidents de sécurité (com.snc.security_incident) soit activé.

Pour installer des modules d'extension Réponse aux incidents de sécurité :

1. Connectez-vous à votre instance avec vos informations d'identification HI.
2. Vérifiez que vous disposez du rôle administrateur (admin).
3. Accédez à la définition>modules d'extension du système dans votre instance.
4. Sélectionnez et cliquez sur Réponse aux incidents de sécurité.

Une fois ces modules d'extension installés, vous pouvez charger le nouveau module d'extension Check Point Integration à partir de ServiceNow Store et suivre les instructions de configuration suivantes.

Versions de système d'exploitation Check Point prises en charge

Cette intégration nécessite le flux d'intelligence personnalisé des lames Check Point et Anti-Bot et Anti-Virus. Ceux-ci sont pris en charge à partir de R80.20 et plus. Installez le correctif de la fonctionnalité d'intelligence personnalisée connue sous le nom de Check Point R80.10 Jumbo HF prendre 121 et plus. Consultez la section Installation de la documentation Check Point Custom Intelligence Feed pour plus d'informations sur la matrice de compatibilité des produits.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Après avoir installé le correctif, assurez-vous que les commandes ci-dessous sont accessibles sur Check Point Gateway. Connectez-vous en SSH à la passerelle et connectez-vous en mode expert.

```
[gw-93440b> expert
[Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

Versions ServiceNow prises en charge

La version San Diego ou une version ultérieure est prise en charge.

Références

Vous trouverez ci-dessous quelques-unes des références Check Point qui sont utiles dans la configuration des prérequis.

1. Fonctionnalité Flux d'intelligence personnalisés - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. Pour configurer les lames Anti-Bot et Anti-Virus, reportez-vous au Guide de l'utilisateur Check Point. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. Pour configurer l'inspection HTTPS sur Check Point, suivez le lien ci-dessous. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

Autorisations et rôles

Les rôles ServiceNow suivants sont requis.

- Administrateur (admin) pour l'installation du module d'extension de l'application d'intégration
- Administrateur d'incident de sécurité (sn_si.admin) pour la création de listes de blocs dans ServiceNow et l'approbation des demandes d'ajout et de désactivation des entrées de liste de blocs.
- Analyste de la sécurité (également appelé ici analyste SOC, sn_si.analyst) pour la création et la gestion des enregistrements d'entrée de liste de blocs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur l'affectation du rôle d'analyste de sécurité, sur le site web de la documentation ServiceNow , accédez à Security operations>Security Incident Response> Affectation d'analystes de sécurité.

Configurer Check Point NGTP

Avant de pouvoir utiliser l'intégration Check Point NGTP , vous devez créer un compte API, configurer des politiques et activer l'intégration.

Créer un compte API pour l'intégration Check Point NGTP

Un rôle de compte API est requis dans votre instance Now Platform pour cette intégration. Le nom d'utilisateur et le mot de passe associés à ce compte sont créés dans Now Platform et saisis dans Check Point, de sorte que Check Point s'authentifie auprès de Now Platform lors de la récupération des entrées de la liste de blocs.

Avant de commencer

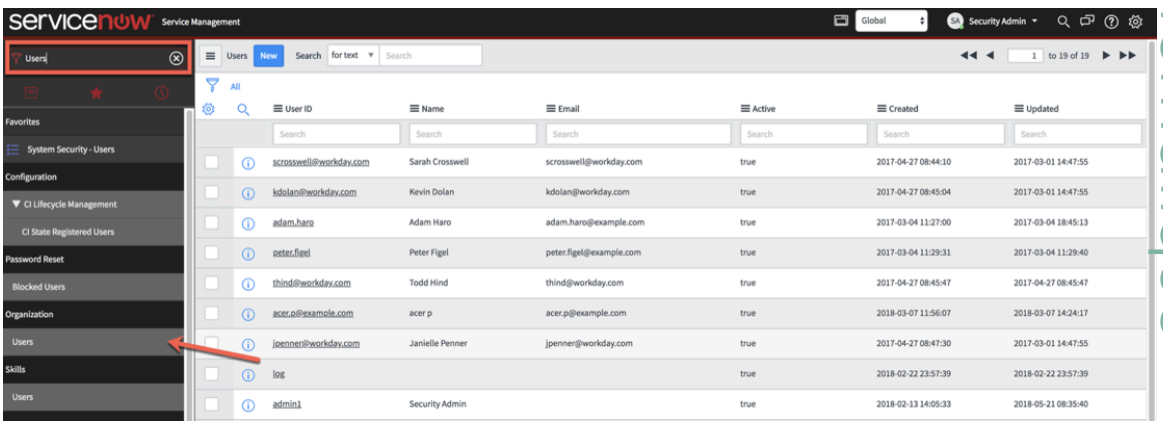
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

L'administrateur Now Platform crée un rôle de compte API (sn_sec_checkpoint.api_account_access). Ce compte est utilisé exclusivement pour saisir les informations d'identification requises pour l'authentification sur Check Point, afin que la passerelle puisse récupérer les listes de blocs à partir de Now Platform. Il s'agit d'un compte d'utilisateur API distinct et unique dans l'instance Now Platform affecté à l'administrateur Check Point.

Procédure

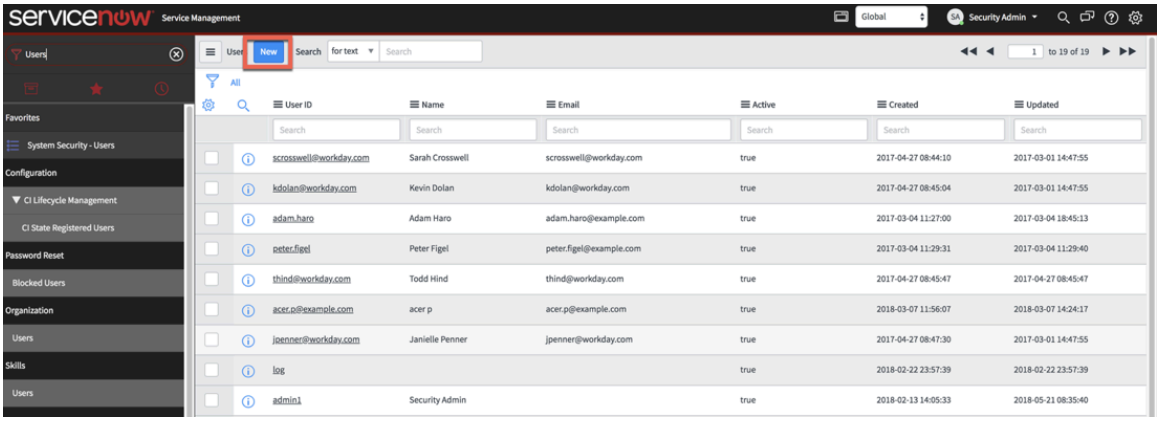
1. Accédez à la **Tout** > **Organisation** > **Utilisateurs**.
2. Cliquez sur le module **Utilisateurs** .



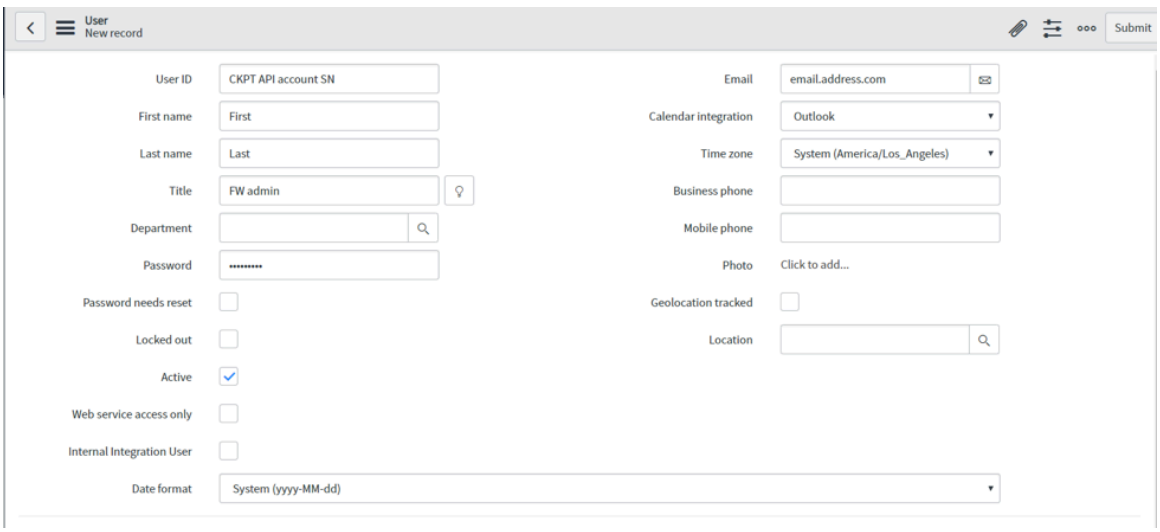
3. Cliquez sur **Nouveau** dans la liste Utilisateurs qui s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Un nouveau formulaire s'affiche.



4. Remplissez le formulaire selon vos besoins.

Remarque : Les valeurs d'ID d'utilisateur, de titre et d'adresse e-mail indiquées dans la table et la figure suivantes sont des exemples de valeurs.

Champ	Description
ID d'utilisateur	ID d'utilisateur unique pour le rôle dans votre instance Now Platform. Cet ID d'utilisateur est entré dans le champ **Nom d'utilisateur** de la section **Authentification client** de la passerelle Check Point de configuration de la liste de blocs. Un exemple est le compte d'API CKPT SN.
Prénom	Personne que vous affectez
Nom	Personne que vous affectez
Titre	Fonction, par exemple administrateur du télétravail.
Mot de passe	Mot de passe unique créé pour ce rôle. Ce mot de passe est entré dans le champ **Mot de passe** de la section **Authentification client** de la configuration de la liste de blocs sur la passerelle Check Point.
E-mail	Adresse e-mail unique

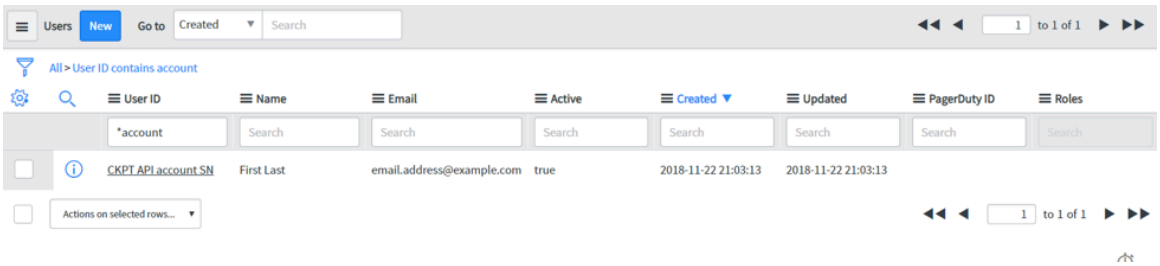
5. Cliquez sur **Envoyer**.

Traduction automatique

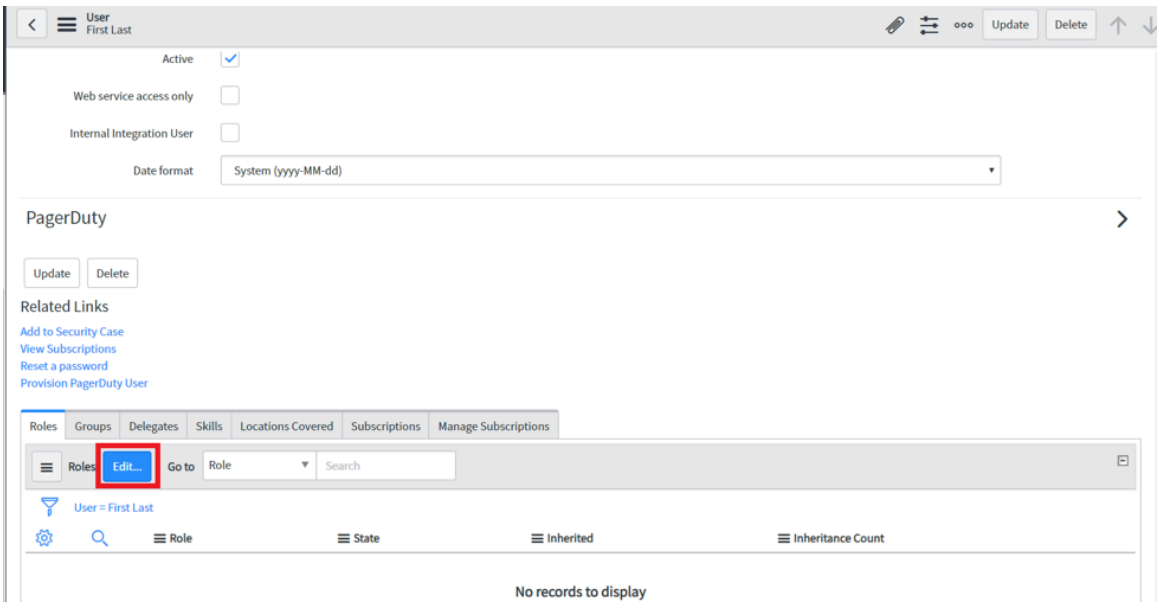
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois soumis, vous pouvez affecter le rôle.

6. Dans la liste Utilisateurs, dans la colonne ID d'utilisateur, cliquez sur le nom de l'ID d'utilisateur que vous avez entré, par exemple le compte CKPTAPI SN.



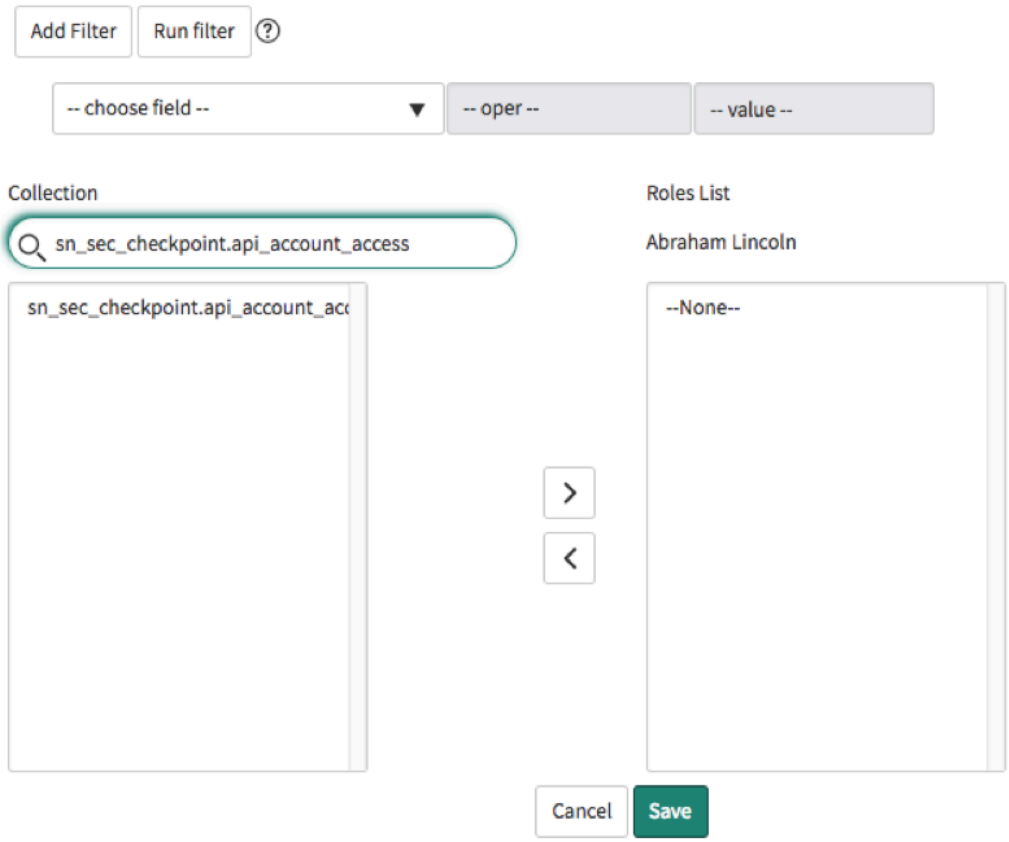
7. Dans l'enregistrement ouvert de la section **Rôles**, cliquez sur Modifier.



8. Sur le formulaire **Modifier les membres** qui s'affiche, saisissez sn_sec_checkpoint.api_account_access dans le champ **Collecte** .

Traduction automatique

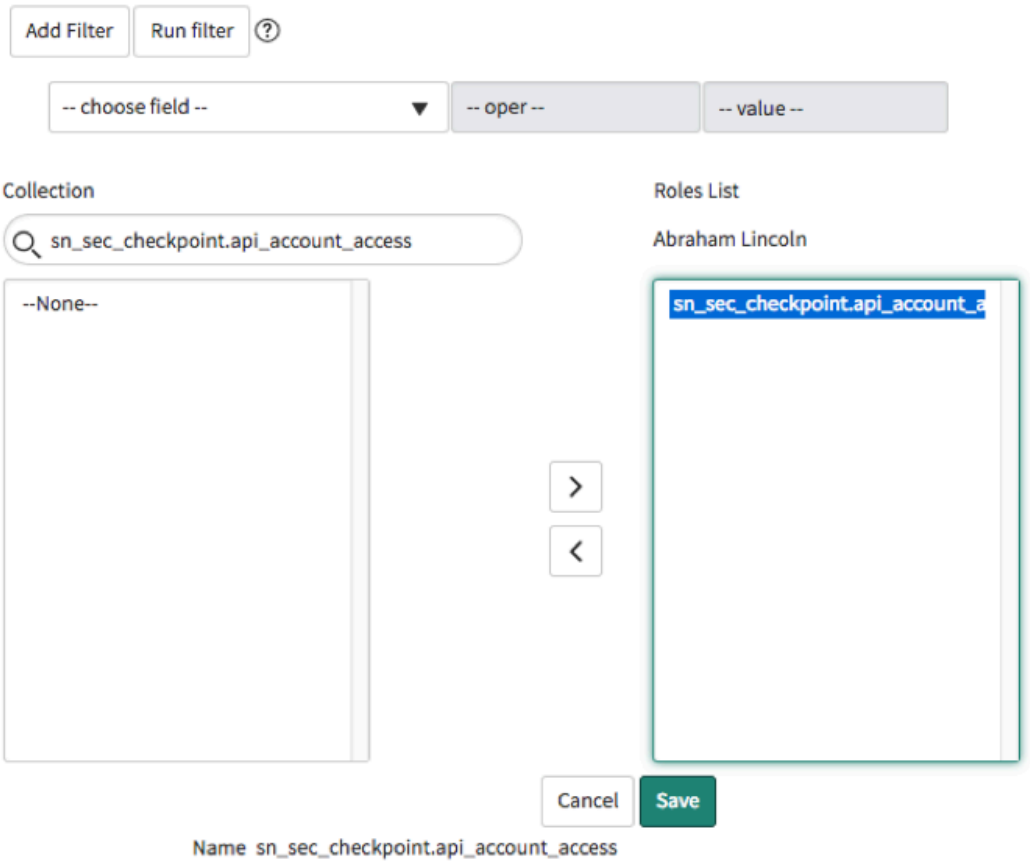
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Dans la colonne **Collection** , sélectionnez, puis déplacez sn_sec_checkpoint.api_account_access vers la **liste des rôles**.
10. Cliquez sur **Enregistrer**.
11. Accédez à **Utilisateurs** et, dans la colonne **Utilisateur** de la liste, cliquez sur le nom de l'ID que vous avez créé pour le rôle (compte d'API CKPT SN).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





12. L'enregistrement utilisateur s'affiche. Cet enregistrement vérifie que le compte d'utilisateur a été affecté.

Configurer l'intégration Check Point NGTP

Pour configurer l'intégration Check Point Next Generation Threat Prevention , procédez comme suit. Cela permettrait de s'assurer que les conditions préalables au fonctionnement de l'intégration sont en place.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

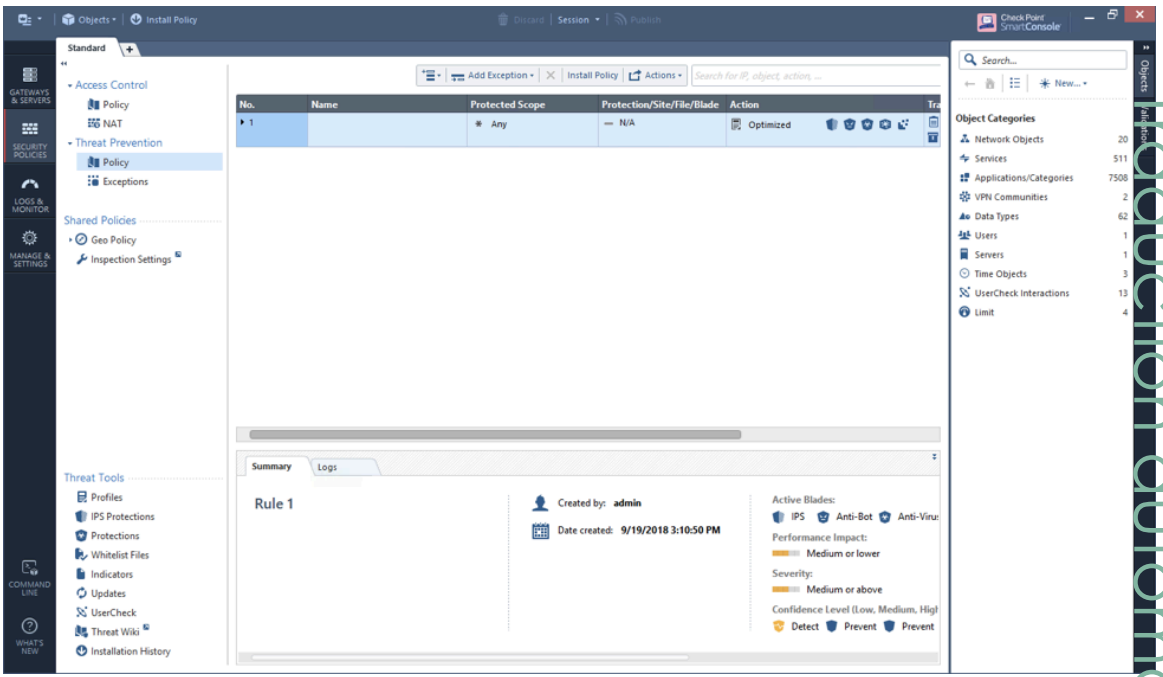
Procédure

1. Vérifiez que la politique de prévention des menaces est configurée avec les lames anti-bot et anti-virus activées.
   Reportez-vous au Guide de l'utilisateur Check Point mentionné dans la section Référence pour obtenir des informations détaillées sur la configuration des lames Anti-Bot et Anti-Virus.

   Remarque : Les images de cette rubrique sont privilégiées et exclusives et sont utilisées avec l'autorisation de Check Point Software Technologies, Ltd.

   a. Connectez-vous à **la Smart Console**.

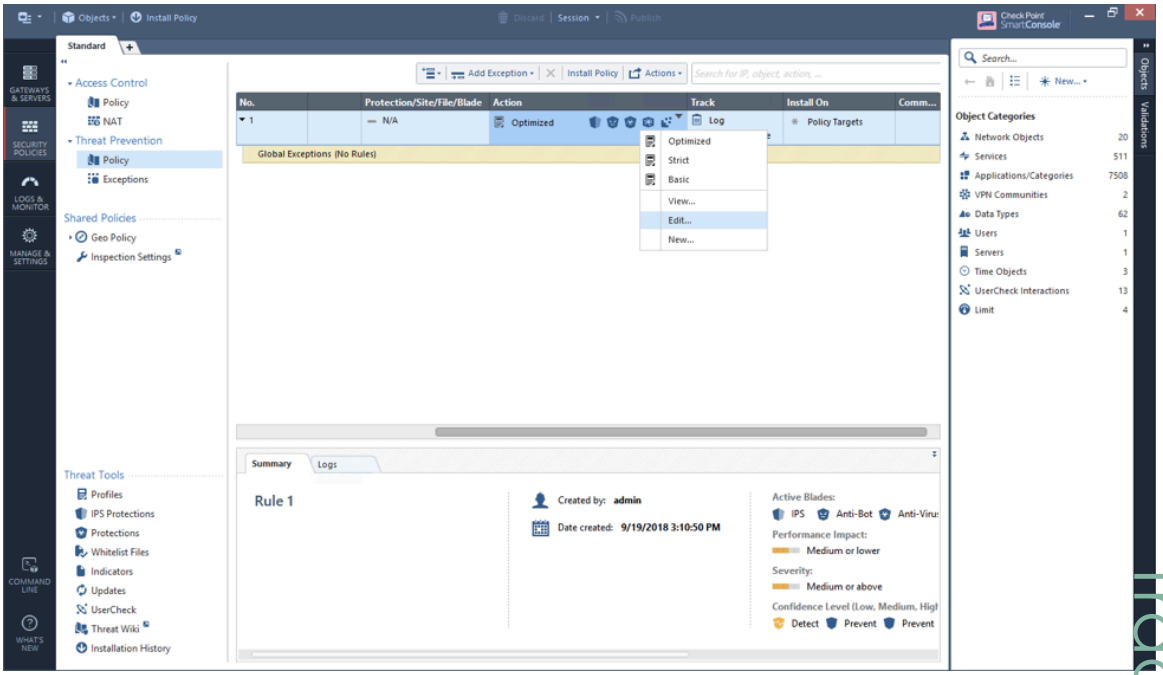
   b. Accédez à la **Politiques de sécurité** > **Prévention des menaces** > **Politique**.



   c. Ouvrez la politique de prévention des menaces en mode de modification.

Traduction automatique

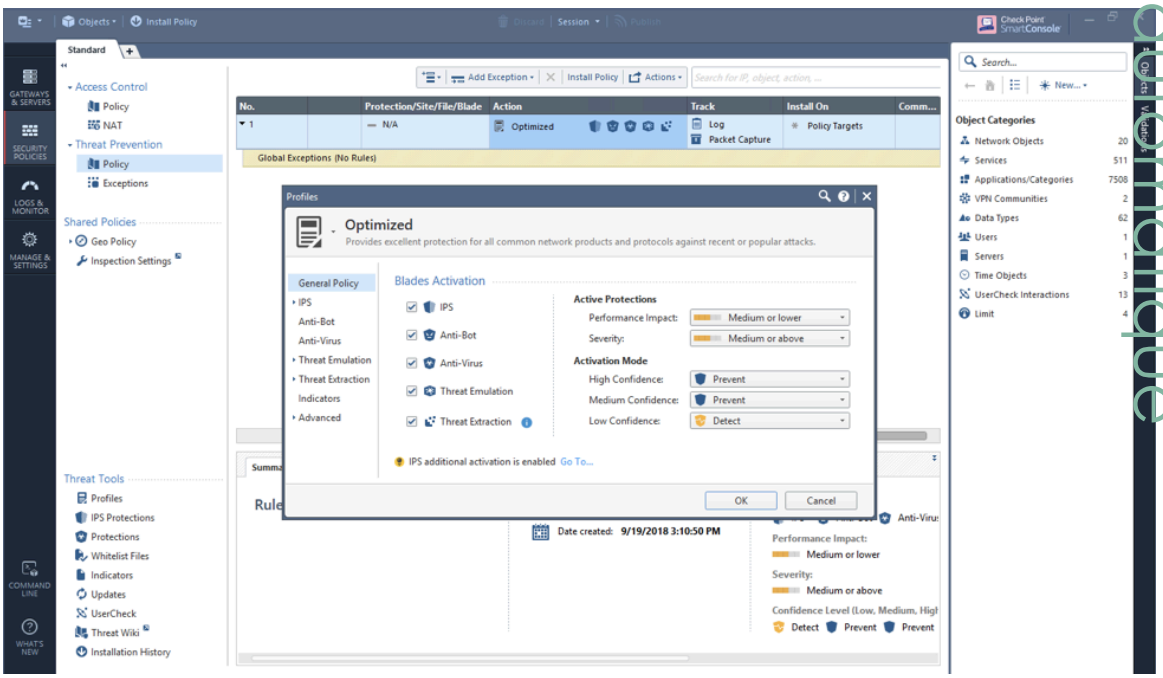
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Protections actives → La gravité doit être « moyenne ou supérieure »

e. Le mode d'activation → confiance élevée doit être « Prévenir »

f. Lames Activation à Anti-Virus et Anti-Bot doivent être sélectionnées.



g. Publiez les changements (le cas échéant) et installez la politique.

2. S'ils ne sont pas déjà configurés, des flux d'intelligence personnalisés doivent être ajoutés après l'activation des lames Anti-bot et Anti-virus.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

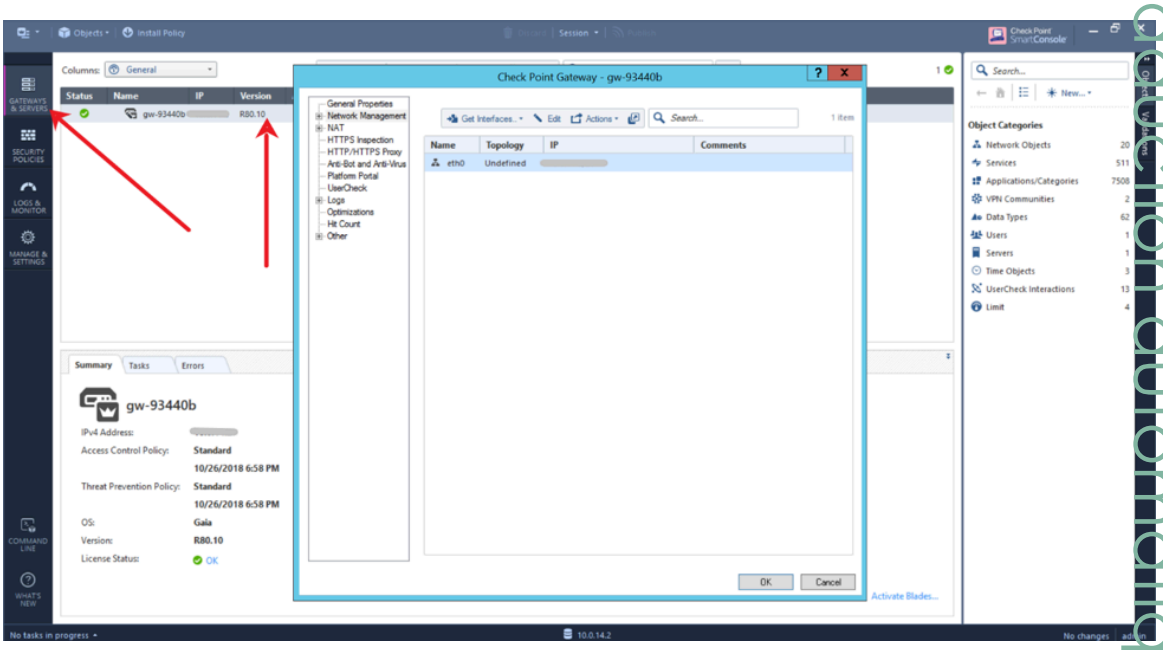
Reportez-vous à la section Installation de la documentation de la fonctionnalité Flux d'intelligence personnalisé Check Point. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

3. Si ce n'est pas déjà fait, configurez la passerelle Check Point pour acheminer tout le trafic Internet via un proxy HTTP (si vous configurez l'inspection HTTPS).

> **Remarque :** Pour le blocage d'URL sur Check Point NGTP, certains paramètres doivent être vérifiés. Le trafic Internet HTTPS utilise le protocole SSL (Secure Sockets Layer) et est crypté pour garantir la confidentialité des données. Cependant, HTTPS peut cacher le trafic malveillant qui aurait dû être bloqué. Pour que Check Point Gateway bénéficie d'une visibilité sur le trafic HTTPS, acheminez le trafic via un proxy HTTP ou configurez une inspection HTTPS (recommandé). Cette section détaille les étapes à suivre pour configurer un proxy HTTP sur Check Point Gateway.

a. Connectez-vous à **la Smart Console**.

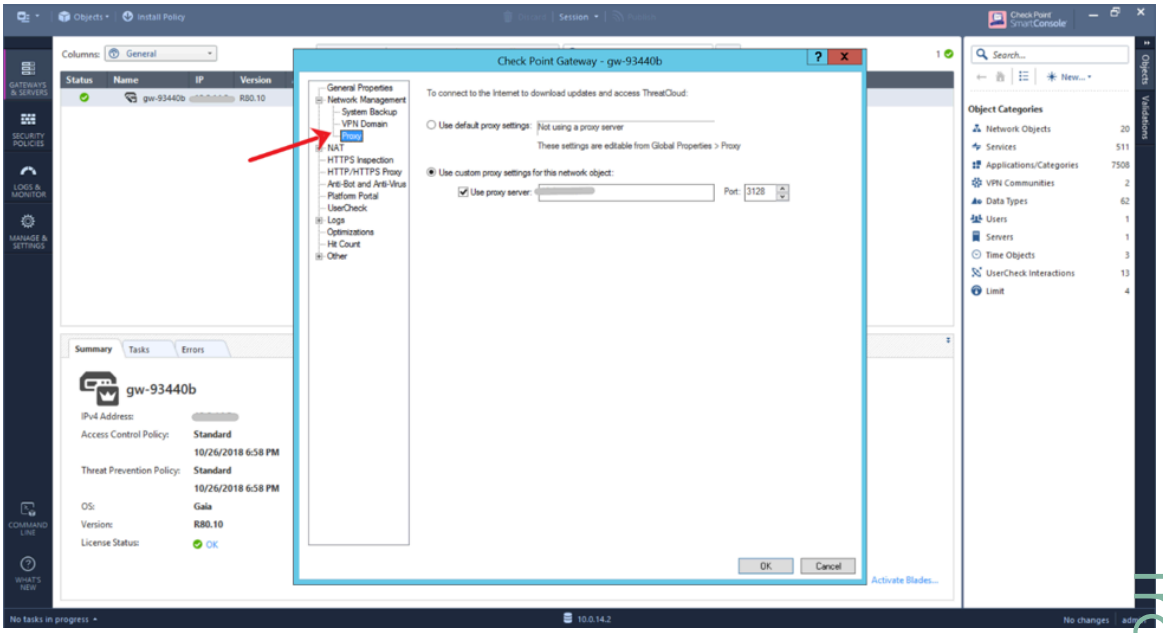
b. Accédez à **Serveurs et passerelles**, puis double-cliquez sur le serveur applicable.



c. Accédez à la **Gestion du réseau** > **Proxy**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Fournissez les détails du proxy à utiliser pour acheminer le trafic HTTP.

e. Assurez-vous que les demandes HTTP du point de terminaison client passent par le proxy HTTP.

4. Si ce n'est pas déjà fait, activez l'inspection HTTPS (si le proxy HTTP est configuré). Lorsque la majeure partie du trafic est via SSL, il est recommandé d'utiliser le panneau d'inspection HTTPS. Cela rend le trafic transparent pour GW. Activez l'inspection HTTPS sur Check Point Gateway, comme suit.

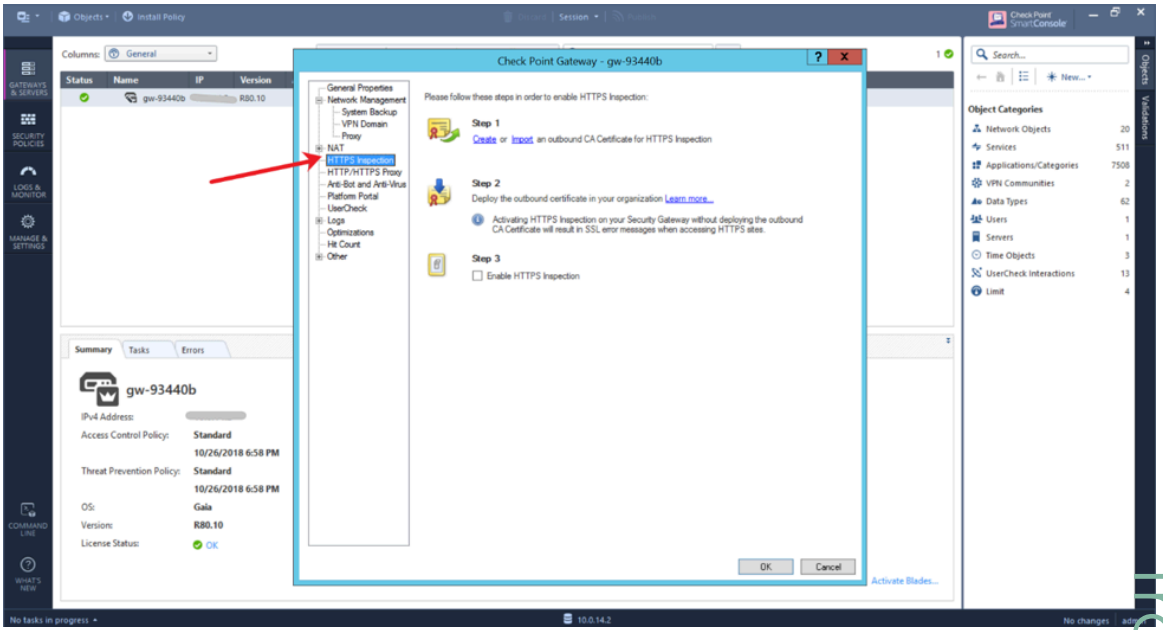
a. Connectez-vous à **la Smart Console**.

b. Accédez à **Serveurs et passerelles**, puis double-cliquez sur le serveur applicable.

c. Accédez à **l'inspection HTTPS**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Suivez les étapes de configuration de l'inspection HTTPS dans le Guide de l'utilisateur Check Point.

Activer l'intégration Check Point NGTP

Si vous n'avez pas installé l'application, suivez les instructions pour l'installer.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer l'application.
2. Accédez à la **Applications système** > **Applications**.
3. Cliquez sur l'onglet **Téléchargements** .
   La liste des applications disponibles pour l'installation s'affiche.
4. Localisez l'application Check Point Next Generation Threat Prevention , sélectionnez-la et cliquez sur **Installer**.
   Votre application est automatiquement installée sur votre instance.

Utilisation de listes de blocs

L'intégration ServiceNow Check Point Next Generation Threat Prevention prend en charge les listes de blocs qui acceptent les observables d'adresse IP, d'URL et de domaine.

ServiceNow La liste de blocs configurée est un fichier CSV hébergé sur un serveur Web externe, qui, pour cette intégration, est l'instance Now Platform. Le flux d'intelligence personnalisé est configuré sur Check Point Gateway, qui extrait les adresses IP, les URL et les domaines de Now Platform à des intervalles préconfigurés.

Cette intégration prend en charge trois types de listes de blocs :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Adresse IP (inclut une adresse IP individuelle (IPv4 uniquement) pour la liste de blocs et des blocs CIDR (plages) d'adresses pour la liste d'autorisation).
- URL
- Domaine

Observables pris en charge par l'intégration Check Point NGTP

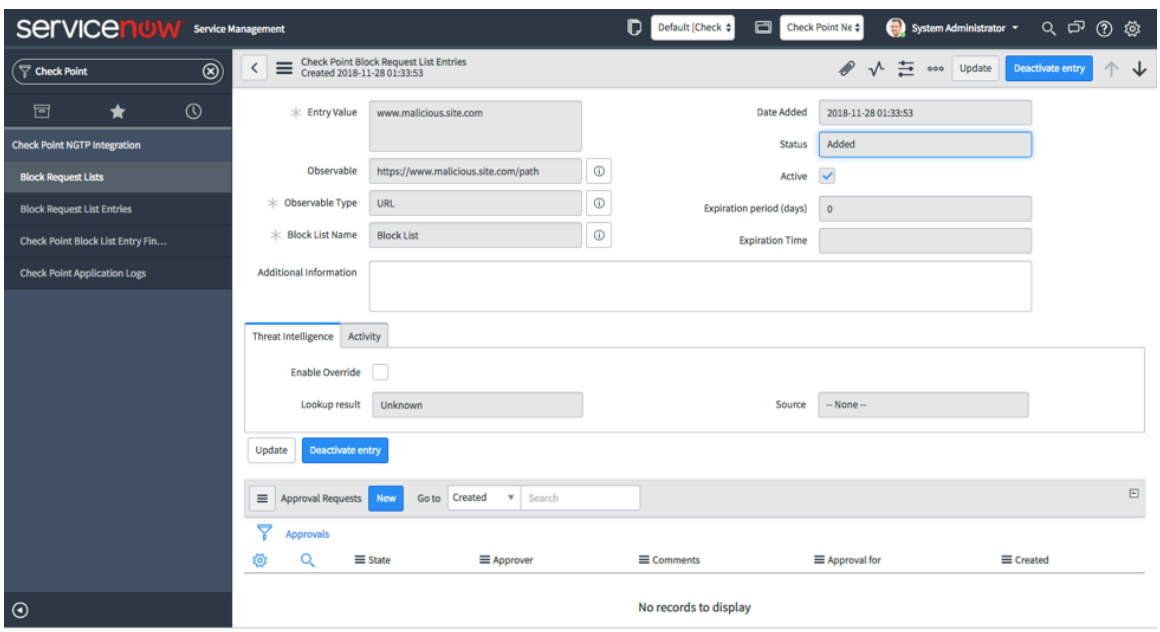
Cette section répertorie les descriptions des observables pris en charge par cette intégration et des exemples de formats pour chaque type.

Type d'observable	Exemples	Description
Domaine	• example.com • mail.example.com	Les caractères génériques ne sont pas pris en charge.
Adresse IP	95.153.103.54 (IPv4)	Représente une adresse d'interface unique et distincte. L'intégration ne prend en charge que les formats IPv4 et CIDR (le format CIDR n'est pris en charge qu'à des fins de liste d'autorisation). À des fins de liste d'autorisation, l'intégration prend en charge les observables d'adresses IP qui incluent des plages CIDR (Classless Inter-Domain Routing), par exemple, 95.153.100.0/22. **Remarque :** Un message d'erreur s'affiche lorsque vous essayez d'associer une seule adresse IP à une liste de blocs que vous avez déjà autorisée à répertorier dans le cadre d'une plage CIDR. Par exemple, l'adresse unique 95.153.103.54 fait partie de la plage CIDR représentée par 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• https://www.example.com • http://www.example.com	Description : les URL HTTPS sont formatées par l'application pour découper le chemin à partir de l'URL

Traduction automatique

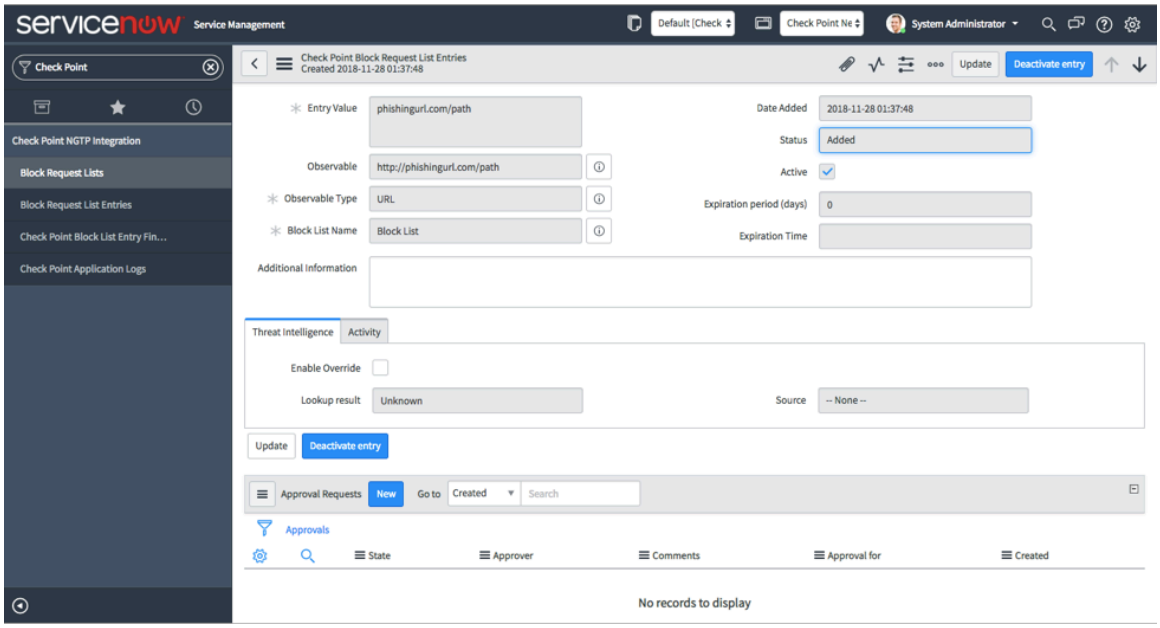
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type d'observable	Exemples	Description
		et conserver le nom de domaine uniquement. Check Point NGTP s'appuie sur la requête HTTP CONNECT pour évaluer le trafic Web et appliquer le blocage. Pour la demande HTTPS CONNECT, l'URL entière n'est pas visible dans la demande et seul le nom de domaine est visible. Lorsqu'un utilisateur bloque une URL HTTPS avec un chemin d'accès spécifique (exemple : https://www.example.com/path), l'application supprime automatiquement le chemin d'accès (www.example.com). L'application conserve la relation entre l'observable d'origine et l'URL formatée. Vous trouverez ci-dessous la capture d'écran de l'entrée de la liste de blocs qui montre l'URL formatée et l'observable d'origine.



Pour les URL HTTP avec un chemin spécifique (par exemple, http://www.example.com/path), Check Point bloquerait l'URL spécifiée, car l'URL entière est visible dans la demande CONNECT.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Créer une liste de blocs pour l'intégration Check Point NGTP

Créez une liste de blocs dans votre instance Now Platform. Une fois approuvées et activées, vous pouvez créer des entrées pour ces listes de blocs à partir d'observables identifiés comme malveillants sur les incidents Now Platform Security Incident Response (SIR) et demander l'approbation pour les bloquer.

Avant de commencer

Rôle requis : administrateur d'incident de sécurité (sn_si.admin)

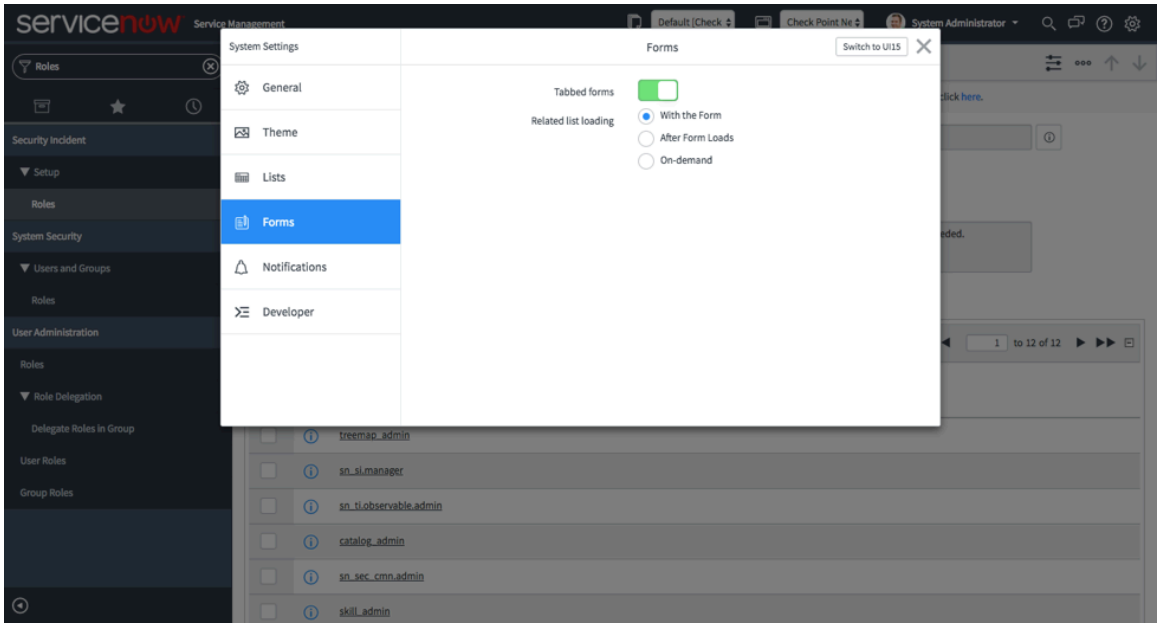
Pourquoi et quand exécuter cette tâche

Créez la liste de blocs sur votre instance Now Platform afin que Check Point puisse importer les objets (adresses IP, URL, domaines) inclus dans la liste. Le flux d'intelligence personnalisé est configuré sur Check Point Gateway qui extrait les adresses IP, les URL et les domaines de la Now Platform à un intervalle préconfiguré. Pour garantir le blocage des observables, la politique de prévention des menaces doit être configurée avec les lames anti-bot et anti-virus activées.

Remarque : Les figures de cette rubrique s'affichent lorsque **les formulaires à onglets** sont désactivés dans les paramètres système.

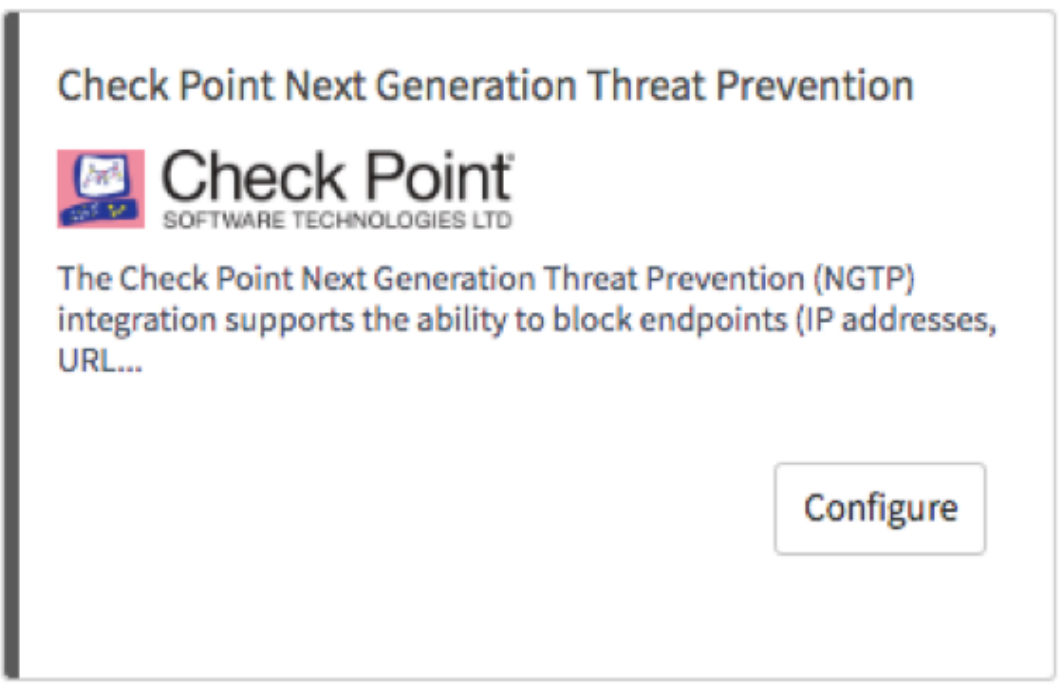
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Procédure

1. Une fois l'installation de l'application terminée, accédez à **Intégrations** > **Configurations d'intégration**.
2. Localisez la carte **Check Point Next Generation Threat Prevention** et cliquez sur **Configurer**.

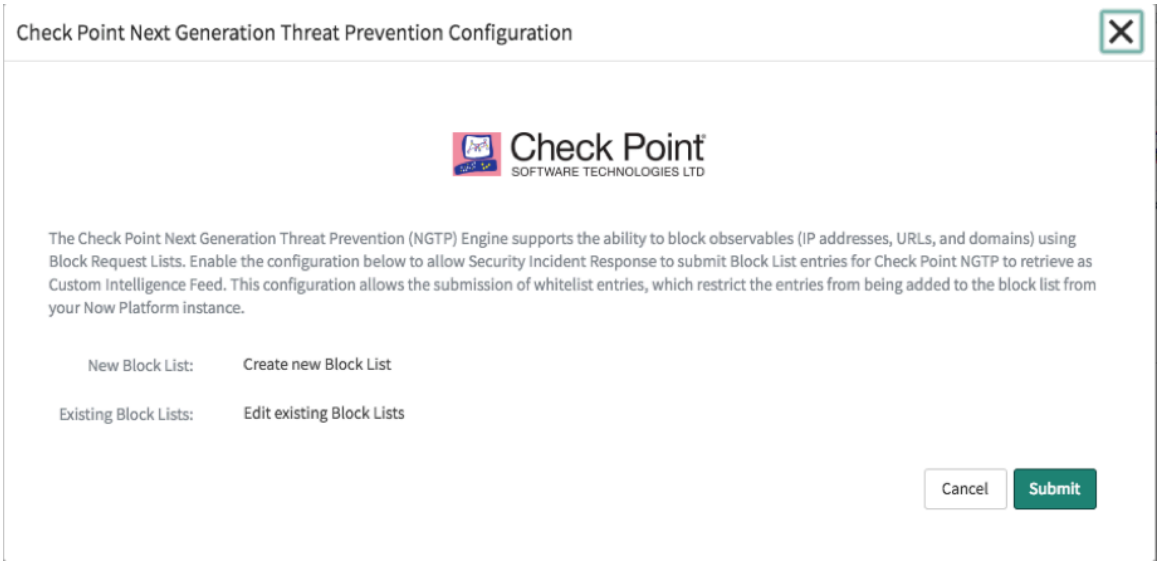


Remarque : Contenu privilégié et propriétaire utilisé avec l'autorisation de Check Point Software Technologies, Ltd.

3. Cliquez sur **Créer une nouvelle liste de blocs**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom de la liste de demandes de blocs Check Point. Incluez le type d'observable (URL, IP, domaine) dans ce champ afin que l'analyste de sécurité puisse facilement reconnaître l'intention de la liste de blocs par son nom. Le nom doit également indiquer clairement à quelle politique de pare-feu ces objets de liste de blocs sont mappés. Voici quelques exemples de noms de liste de blocs : adresse IP de programme malveillant sortante ou URL de hameçonnage sortante.
Actif	Cette case est décochée par défaut pour indiquer que la liste de blocs est inactive. Lorsqu'elle est inactive, la liste de blocs ne peut pas recevoir d'entrées supplémentaires. Lorsque la case est cochée (lorsque la demande de changement est fermée ou que la demande de changement n'est pas générée), la liste de blocs est activée et disponible pour les entrées de liste de blocs.
Balise d'affichage	La case à cocher est sélectionnée par défaut pour baliser automatiquement l'observable et l'enregistrement d'incident de sécurité associé si l'observable est bloqué sur la liste de blocs. Lorsque cette option est cochée, le champ « Marquer pour les observables » est disponible sur le formulaire. **Remarque :** Un nom de balise est créé par défaut à partir de la valeur que vous saisissez dans le champ Nom avec un préfixe Check Point, par exemple, Check Point-Malware OutBound IP. Vous pouvez modifier le nom et la couleur de la balise. Le nom de la balise est affiché dans le champ « Balise pour les observables », une fois la liste de blocs enregistrée.

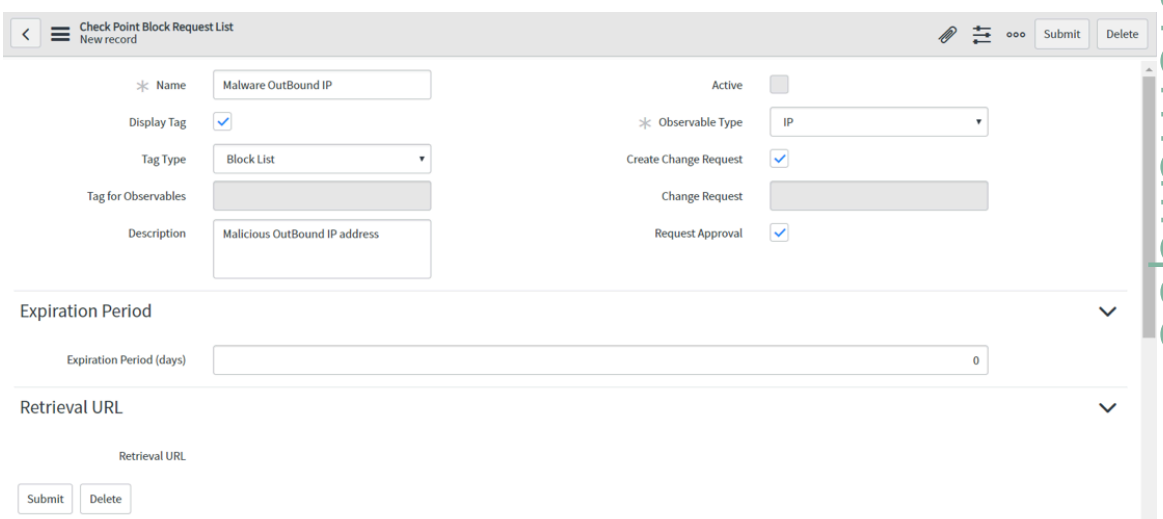
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Lorsque la case est décochée, aucune balise n'est créée et le champ « Balise pour les observables » n'est pas disponible sur le formulaire.
Type d'observable	Sélectionnez un type d'observable accepté par cette liste de blocs dans la liste : adresse IP (y compris CIDR pour la liste d'autorisation), URL ou domaine.
Type de balise	Balises disponibles dans la liste. Une liste de blocs est une liste d'observables que vous souhaitez que Check Point Next Generation Threat Prevention bloque. Une liste d'autorisation est une liste d'observables que vous ne souhaitez en aucun cas bloquer dans Check Point Next Generation Threat Prevention. Par défaut, la couleur de la balise de la liste de blocs est le noir et la couleur de la balise de la liste d'autorisation est le gris. Vous pouvez changer la couleur.
Créer une demande de changement	Cette case à cocher est sélectionnée par défaut pour créer automatiquement une demande de changement et des tâches de changement dans votre instance Now Platform, qui sont jointes à l'enregistrement de liste de blocs. La demande de changement est utilisée pour configurer l'URL de récupération de la liste de blocs dans la passerelle de pare-feu de nouvelle génération Check Point. Cette option est recommandée si votre administrateur de pare-feu utilise également Now Platform pour les modifications de politique ou de règle de pare-feu. Si vous créez une demande, une fois qu'elle est fermée, la liste de blocs est automatiquement activée. Décochez la case pour activer manuellement la liste de blocs après avoir reçu un avis par e-mail de l'administrateur du pare-feu indiquant que le flux d'intelligence personnalisé a été configuré sur toutes les passerelles Check Point. Lorsque la case à cocher Créer une demande de changement est désactivée, le champ Demande de changement n'est plus disponible.
Demander l'approbation	Cette case à cocher est sélectionnée par défaut pour demander des approbations pour l'activation/la suppression d'entrées de liste de blocs des listes de blocs. L'approbation est demandée aux utilisateurs ayant le rôle Administrateur d'incident de sécurité (sn_si.admin). La demande d'approbation sera envoyée par e-mail aux approbateurs. Une fois l'approbation acceptée, l'entrée sera activée sur cette liste de blocage. Lorsque la case n'est pas cochée, les entrées de cette liste de blocs ne suivent pas le workflow d'approbation et sont directement activées sur la liste de blocs.
Balise pour l'observable	Ce champ n'est affiché que si la case Balise d'affichage est cochée. Le champ est automatiquement renseigné après l'enregistrement de la liste

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

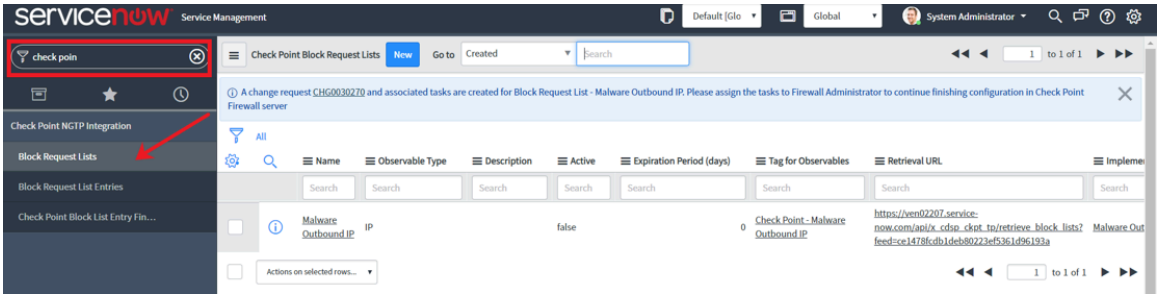
Champ	Description
	de blocs avec une valeur par défaut dans le champ Nom. Si la liste de blocs est créée avec le nom « URL de programme malveillant », le nom de balise dérivé est « Liste de blocs – URL de programme malveillant »
Demande de changement	Lorsque la case à cocher Créer une demande de changement est sélectionnée, le numéro de la demande de changement s'affiche sur l'instance Now Platform une fois la liste de blocs enregistrée. Lorsque la case à cocher Créer une demande de changement est désactivée, ce champ n'est pas affiché.
Description	Description de la liste de blocs Check Point. Le nom contient généralement les types de sites et d'observables que vous vous attendez à voir sur cette liste de blocs, et vous pouvez utiliser ce champ pour plus de détails.
Période d'expiration (jours)	Période d'expiration de la liste de blocs. 0 (la valeur par défaut) indique que l'entrée de la liste de blocs n'expire jamais. Si vous modifiez cette valeur, cette entrée est active pendant le nombre de jours que vous entrez. Vous pouvez entrer une valeur minimale de 1, soit 24 heures, et il n'y a pas de valeur maximale.
URL de récupération	L'URL de récupération sera générée automatiquement, une fois la liste de blocs enregistrée. Pour configurer cette liste de blocs sur les passerelles Check Point, vous devez utiliser cette URL. Une fois cette URL configurée, Check Point extrait les observables à bloquer au format CSV.



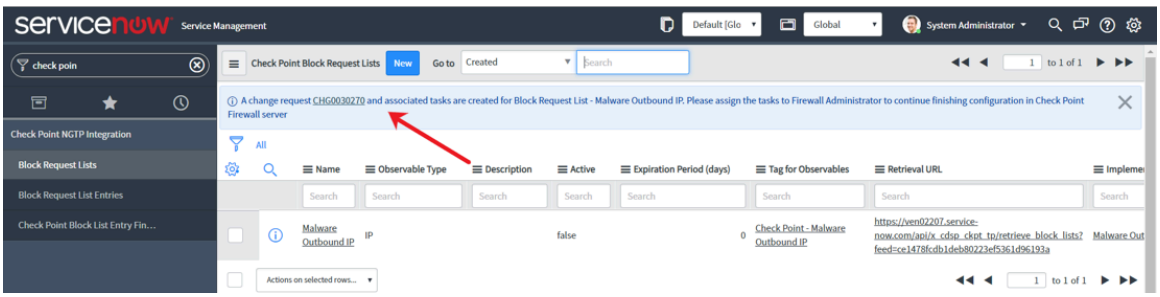
5. Cliquez sur **Envoyer**.
6. Si la liste de demandes de blocs Check Point n'est pas affichée, accédez à **Intégration Check Point NGTP** > **Listes de demandes de blocs**.

Traduction automatique

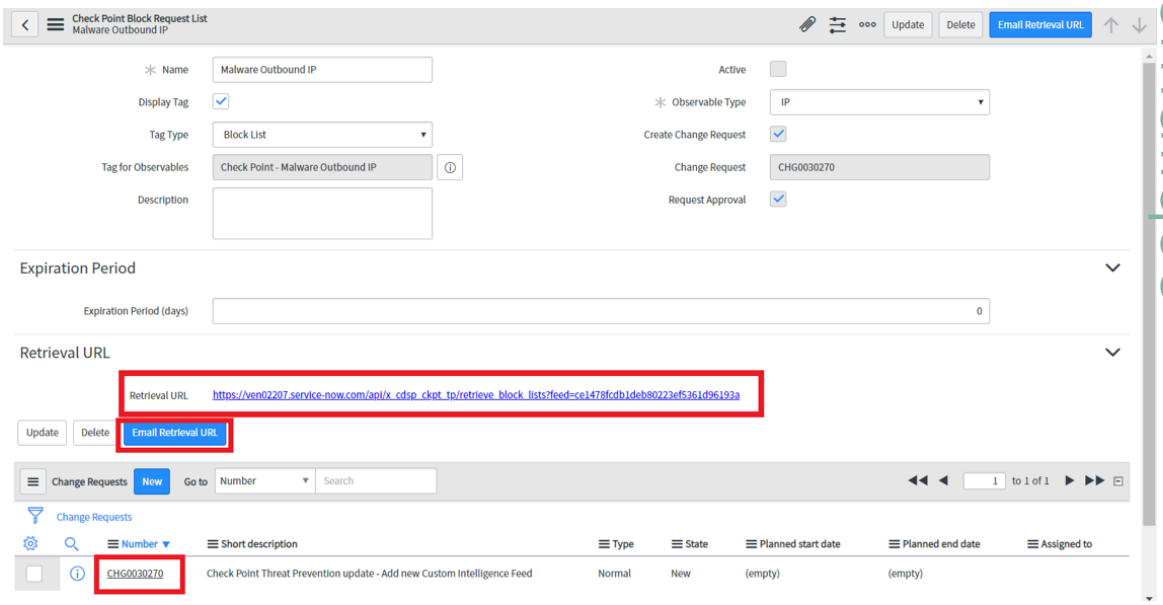
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La nouvelle liste de blocs s'affiche. Le statut de la liste de blocs est toujours inactif (faux), ce qui signifie que la liste de blocs n'est pas disponible pour accepter des entrées. Si l'option Créer une demande de changement a été configurée, un message s'affiche indiquant qu'une demande de changement et des tâches ont été créées dans votre instance Now Platform.



7. Dans la colonne **Nom** , cliquez sur un élément pour ouvrir l'enregistrement. L'enregistrement de la liste de blocs s'affiche. Cet exemple montre une liste de blocage d'adresses IP sortantes de programme malveillant. Les champs, options et liens suivants sont affichés dans le nouvel enregistrement après soumission et décrits dans la table suivante.



Champ	Description
URL de récupération d'e-mail	Envoie par e-mail un message indiquant que le lien de blocage est disponible pour configuration à l'administrateur de pare-feu Check Point.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL de récupération	Cette URL est utilisée pour configurer un flux de renseignements personnalisé sur les passerelles Check Point. **Remarque :** Si vos paramètres système sont définis sur Formulaires à onglets, ce lien s'affiche dans l'onglet Informations de récupération de la liste de blocs au bas de l'enregistrement.
Demande de changement de Now Platform	Un lien vers l'enregistrement de demande de changement s'affiche dans la section Demandes de changement lorsqu'elle est configurée, et le numéro de la demande s'affiche dans le champ Demande de changement.
Mettre à jour	Modifiez les données et mettez à jour les champs modifiables.
Supprimer	Supprimer l'enregistrement.

8. Créez et ajoutez d'autres listes de blocs selon vos besoins.
   Les listes de blocs sont affichées sur la page Listes de demandes de blocs Check Point.

Que faire ensuite
Activez la liste de demandes de blocs manuellement ou avec une demande de changement Now Platform.

Activer une liste de blocs pour l'intégration Check Point NGTP

Une fois que la liste de blocs a été créée dans votre Now Platform et que l'URL est disponible, l'administrateur Check Point configure la liste de blocs en tant que flux d'intelligence personnalisé sur toutes les passerelles Check Point Next Generation. Avant de pouvoir accepter les entrées de la liste de blocs, celle-ci doit être configurée dans Check Point et activée dans Now Platform.

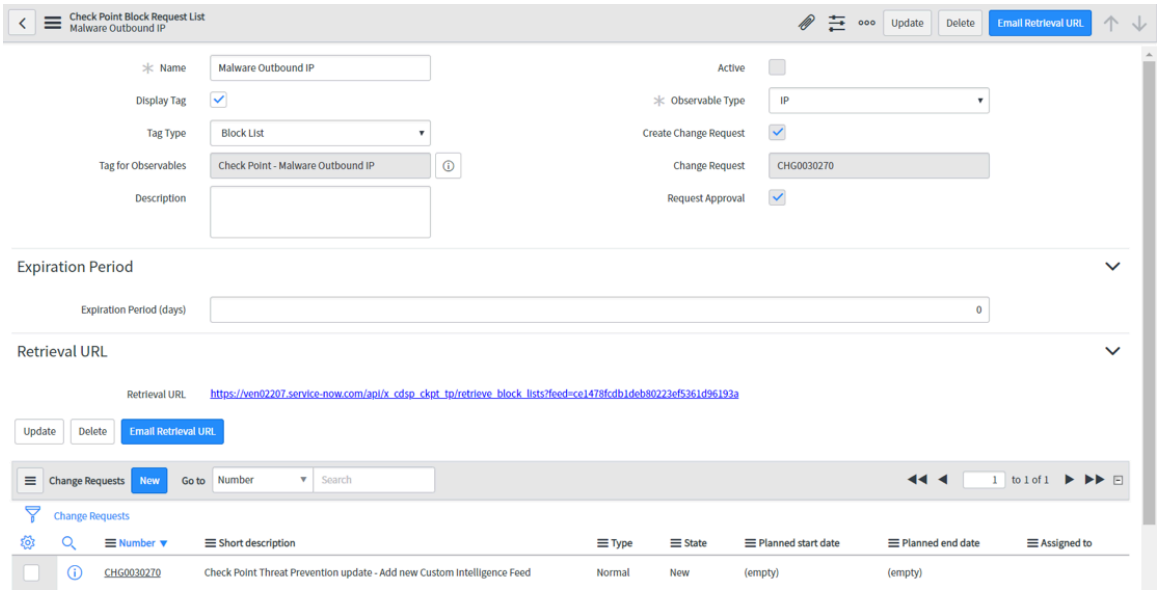
Avant de commencer
Rôle requis : administrateur d'incident de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche
Une fois la liste de blocs configurée, en tant qu'administrateur des incidents de sécurité, vous pouvez activer la liste de blocs manuellement ou la liste de blocs est automatiquement activée lorsqu'une demande de changement Now Platform est terminée. La demande de changement doit être approuvée et passée de l'état inactif à l'état actif avant de pouvoir accepter les entrées de la liste de blocs.

Procédure

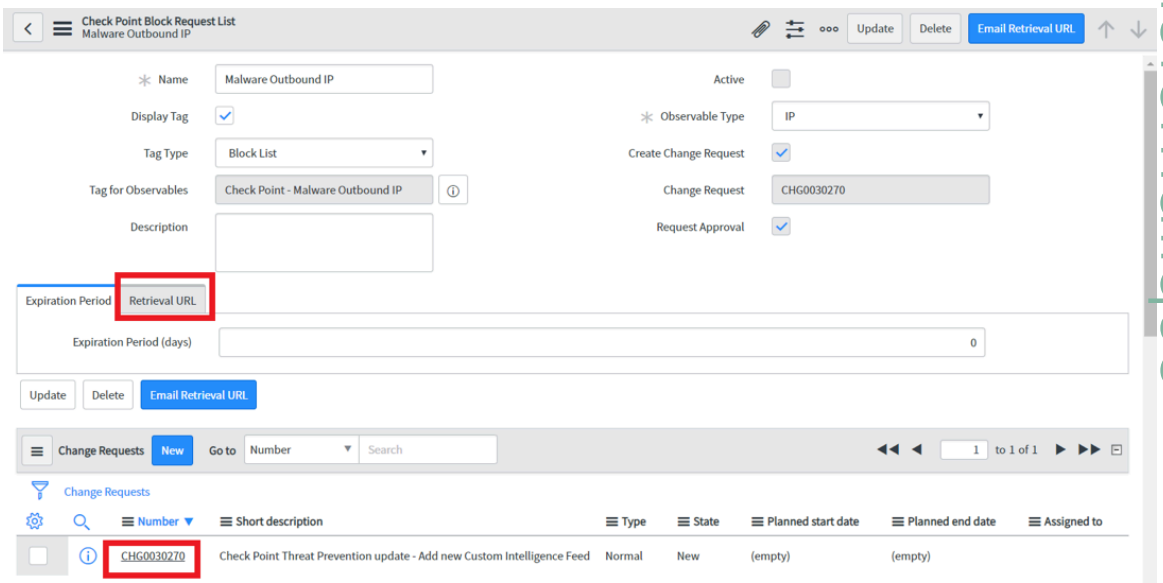
1. Accédez à la **Tout** > **Intégration Check Point NGTP** > **Listes de demandes de blocs**et sélectionnez le module **Listes de demandes de blocs** .
2. Dans la liste **Listes de demandes de blocs Check Point** qui s'affiche, sélectionnez votre nouvelle liste de blocs dans la colonne **Nom** .
3. Sur l'enregistrement qui s'affiche, notez le bouton **URL de récupération d'e-mail** , le lien d'URL de récupération de la liste de blocs actif et, s'il est configuré, la demande de changement Now Platform dans la section Demandes de changement.
   Notez également que la case Actif n'est pas cochée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Une fois les formulaires à onglets désactivés dans les paramètres système, l'URL de récupération de la liste de blocs apparaît dans la section URL de récupération.

4. Cliquez sur l'onglet URL de récupération de la **liste de blocs** pour afficher l'URL de récupération.
   La figure suivante montre l'URL de récupération de la liste de blocs affichée sous la forme d'un onglet avec des formulaires à onglets sélectionnés dans les paramètres de votre système. Le lien vers la demande de changement (CH0030270) s'affiche également.



5. Pour terminer la configuration et déplacer la liste de blocs d'inactive à active, vous devez choisir l'une des options suivantes pour avertir l'administrateur de pare-feu que l'URL de récupération est disponible.

Option	Description
Cliquez sur URL de récupération d'e-mail.	URL de récupération de la liste de blocs d'e-mails directement à l'administrateur du pare-feu. Cette option permet à

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	l'administrateur de pare-feu de terminer la configuration sur la plateforme Check Point. Choisissez cette option si l'administrateur du pare-feu n'utilise pas Now Platform.
Complétez la demande de changement Now Platform et affectez les tâches de configuration à l'administrateur de pare-feu.	Cette option n'est disponible que si l'administrateur de pare-feu pour Check Point utilise également Now Platform et que les processus de gestion des changements et d'approbation de Now Platform sont configurés. **Remarque :** Les utilisateurs ayant le rôle d'administrateur d'incident de sécurité (sn_si.admin) peuvent approuver la demande de changement Now Platform. Une fois les tâches de configuration terminées et la demande de changement fermée, la liste de blocs est activée automatiquement.

Que faire ensuite
Après avoir notifié l'administrateur du pare-feu que l'URL de récupération est disponible et avoir confirmé que la liste de blocs a été configurée dans Check Point, en tant qu'administrateur d'incident de sécurité, l'étape suivante consiste à activer la liste de blocs. Soit vous activez la liste de blocs manuellement, soit, si la configuration est configurée, vous utilisez le formulaire de demande de changement Now Platform pour activer la liste de blocs. La liste de blocs est automatiquement activée lorsque la demande de changement est fermée.

Configurer une liste de blocs en tant que flux de renseignements personnalisé sur l'intégration Check Point NGTP

L'administrateur du pare-feu doit configurer le flux d'intelligence personnalisé correspondant à la liste de blocs créée dans la Now Platform.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Cette tâche doit être effectuée sur chacune des passerelles Check Point NGTP. L'administrateur du pare-feu aurait besoin de l'accès SSH des serveurs de passerelle. Si votre organisation dispose de processus d'approbation et de gestion des changements dans la Now Platform, vérifiez que l'option d'envoi/réception d'e-mail est activée. L'administrateur du pare-feu aurait besoin de l'URL de récupération de la liste de blocs et des informations d'identification de l'utilisateur ServiceNow avec le rôle Check Point API Account Access Role (sn_sec_checkpoint.api_account_access).

Si l'administrateur de pare-feu n'utilise pas la NOW Platform, l'administrateur d'incident de sécurité NOW peut fournir les informations requises par e-mail. Si l'administrateur de pare-feu utilise la Now Platform, la demande de changement associée à la liste de blocs peut également être affectée à l'administrateur de pare-feu. Cette demande de changement contient les informations requises pour configurer le flux de renseignements personnalisé.

Pour plus d'informations sur la configuration du flux de renseignements personnalisé sur les passerelles Check Point, consultez : https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Vérifiez que l'option d'envoi/réception d'e-mail est activée dans votre instance Now Platform en accédant à **Propriétés d'e-mail** > **Administration** > **Propriétés d'e-mail**.
2. Sous Configuration des e-mails sortants, vérifiez que **l'envoi d'e-mail** et la **réception d'e-mail** sont sélectionnés.
3. Modifiez SSH en Check Point Gateway avec le mode expert.
4. Exécutez la commande pour ajouter un flux de renseignements personnalisé.
   L'exécution de la commande est interactive et demande le format du flux et le mot de passe.
   - Lorsque vous êtes invité à indiquer le format du flux, saisissez « cp_csv »
   - Lorsque vous êtes invité à saisir le mot de passe d'utilisateur de la Now Platform avec accès à l'API

   L'exécution de la commande avertissait que le certificat de serveur (plate-forme NOW) n'était pas approuvé par la machine et invitait à ajouter le certificat de sécurité de serveur au magasin de confiance de la machine. Entrez **Y**.

   Le message « État :Réussite » s'affiche, confirmant que le flux a bien été ajouté.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

Soumettre les entrées de la liste de blocs d'un incident de sécurité pour l'intégration Check Point NGTP

Les observables joints à un enregistrement d'incident de sécurité sont soumis pour approbation en tant qu'entrées de liste de blocs à différentes listes de blocs. Un processus d'approbation facultatif pour les entrées de la liste de blocs fait partie du workflow préconfiguré. La passerelle importe les entrées de la liste de blocs (adresses IP, URL, domaines) qui sont incluses dans les listes de blocs.

Avant de commencer

Rôle requis :

- L'analyste des incidents de sécurité (sn_si.analyst) doit soumettre des entrées de liste de blocs.
- L'administrateur d'incident de sécurité (sn_si.admin) pour approuver les entrées de la liste de blocs. Cette autorité peut être affectée selon les besoins de votre organisation.

Pourquoi et quand exécuter cette tâche

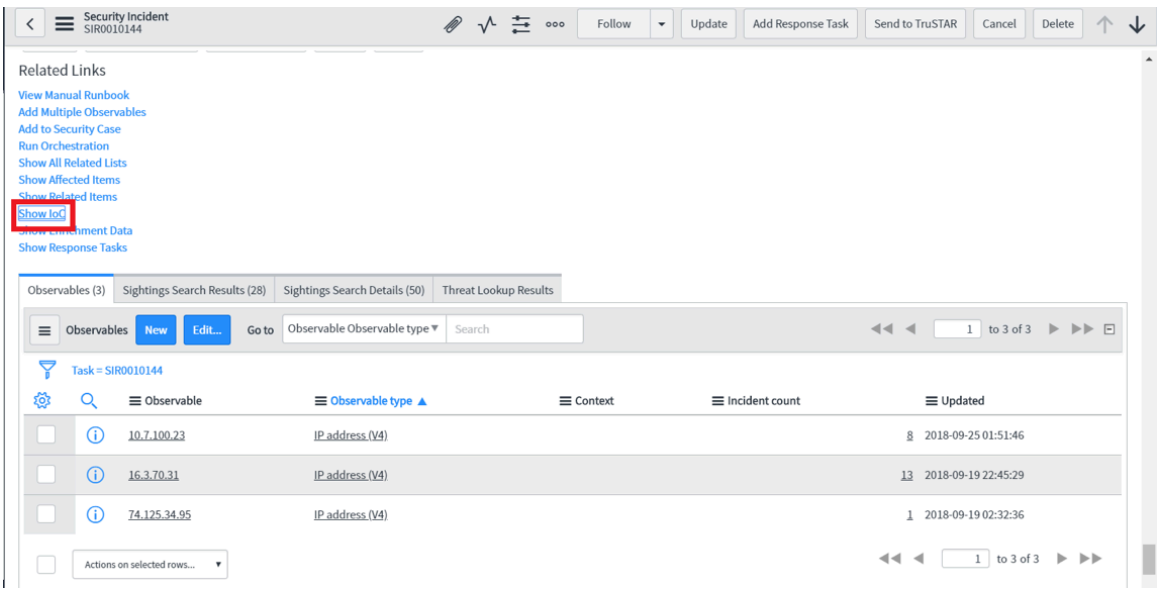
Les utilisateurs ayant le rôle sn_si.analyst soumettent des entrées de bloc en demandant un blocage des observables joints à un enregistrement d'incident de sécurité. Une fois

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

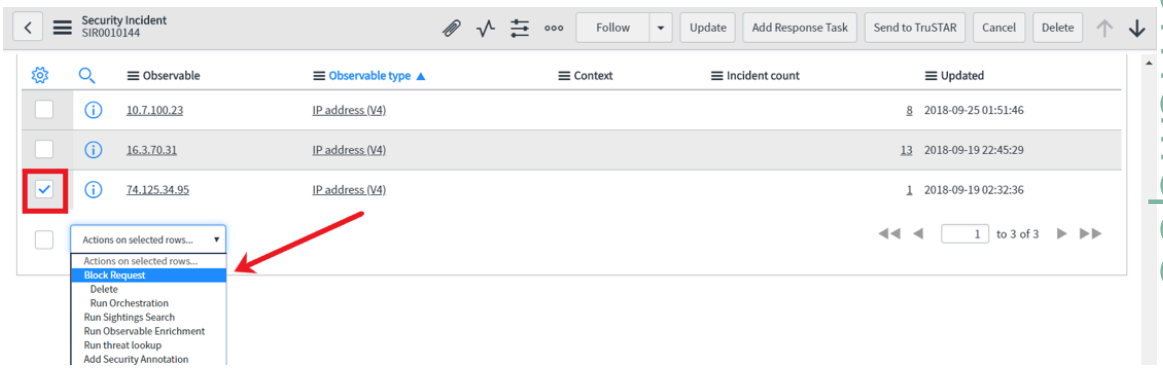
soumise, une entrée de liste de blocs avec l'état En attente est générée et envoyée pour approbation. L'exemple suivant montre une demande de bloc pour un observable d'URL.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents**et cliquez sur un enregistrement d'incident de sécurité pour l'ouvrir.
2. Cliquez sur le lien connexe **Afficher IoC** .



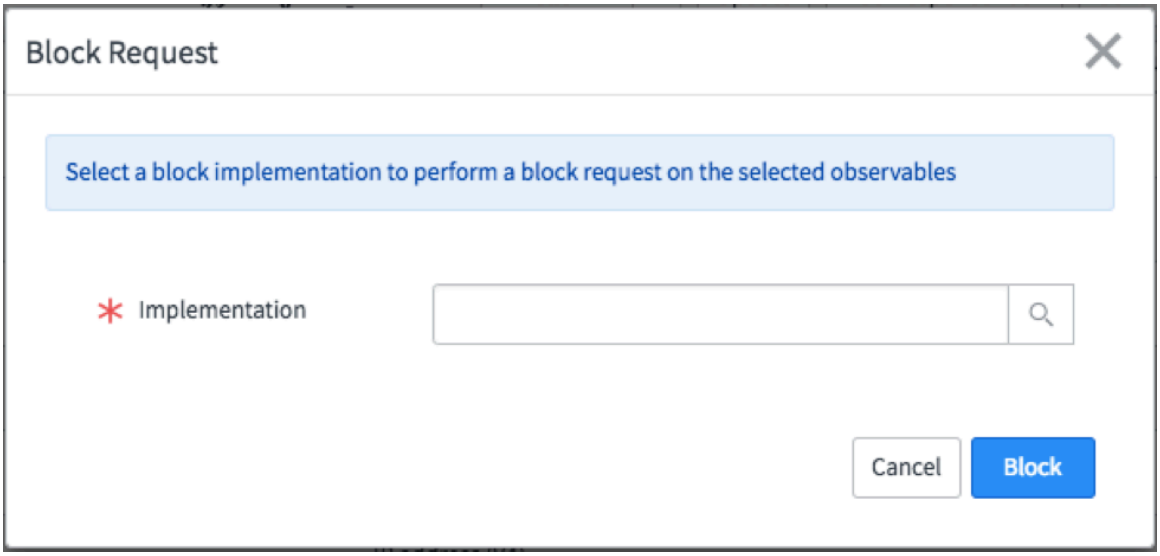
3. Dans la liste connexe Observables, sélectionnez les observables que vous souhaitez bloquer et, dans la liste **Actions sur les lignes sélectionnées** , sélectionnez **Bloquer la demande**.



4. Dans la boîte de dialogue qui s'affiche, cliquez sur l'icône de recherche ( )

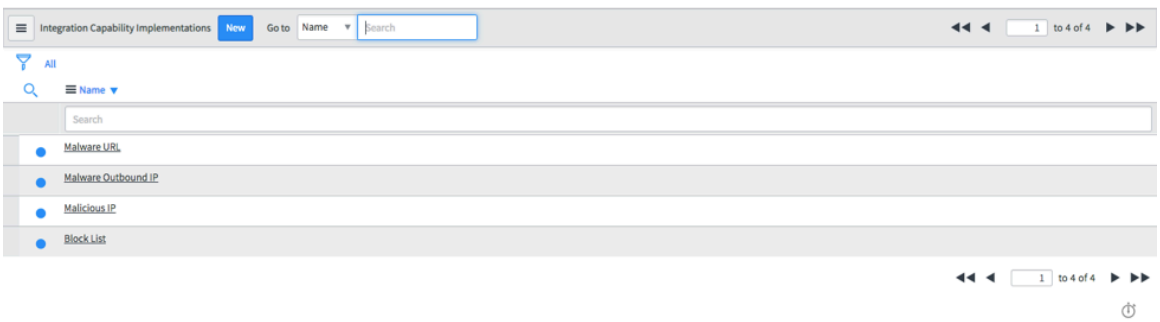
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

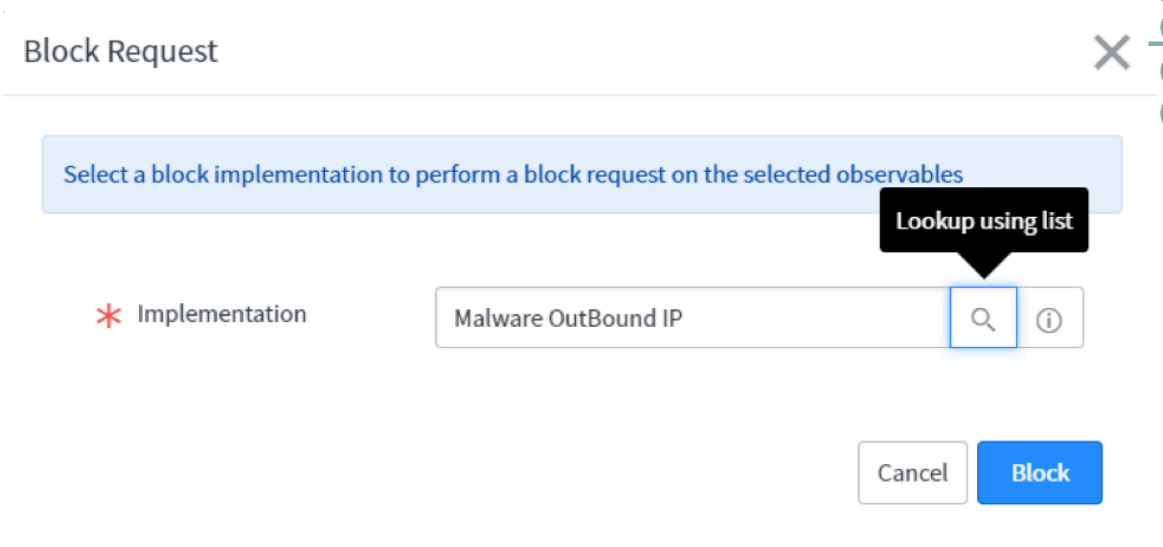


5. Dans la liste, sélectionnez la liste de blocs à laquelle vous souhaitez joindre cette entrée.

Remarque : Pour cet exemple, le type d'observable d'entrée (IP) doit correspondre au type d'observable de la liste de blocs (IP).



6. Dans la boîte de dialogue Demande de bloc avec le nom de la liste de blocs affiché dans le champ Implémentation, cliquez sur **Bloquer**.

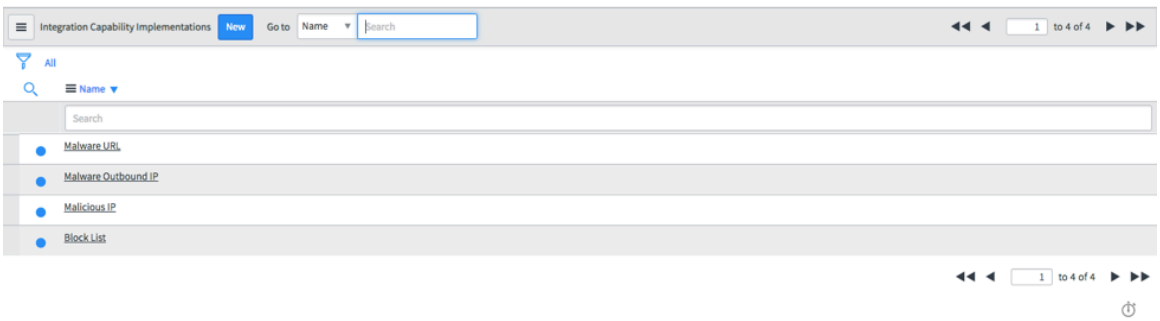


Traduction automatique

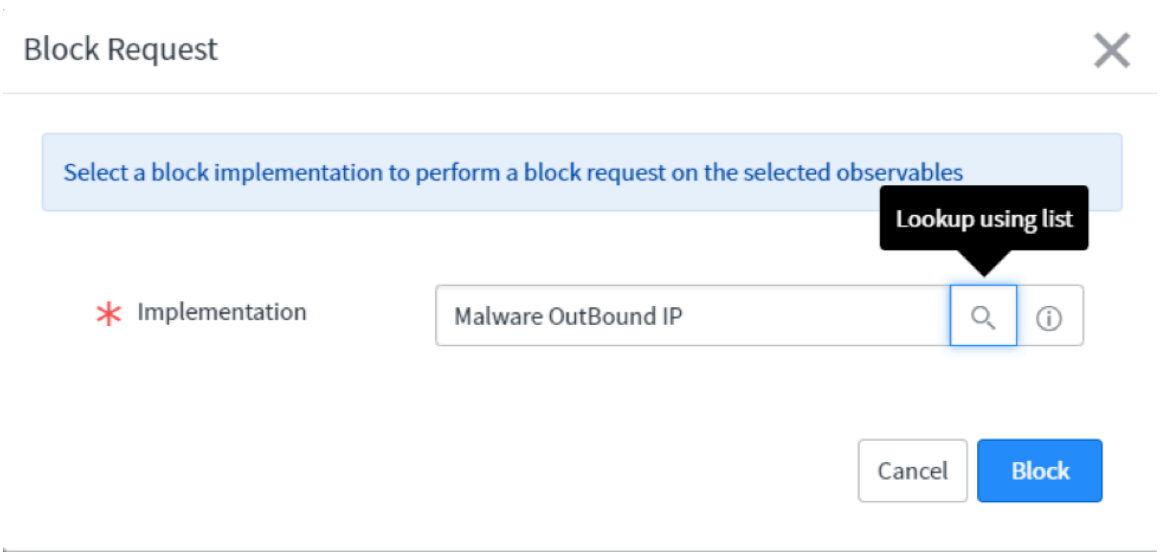
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Dans la liste qui s'affiche, sélectionnez la liste de blocs à laquelle vous souhaitez joindre cette entrée.

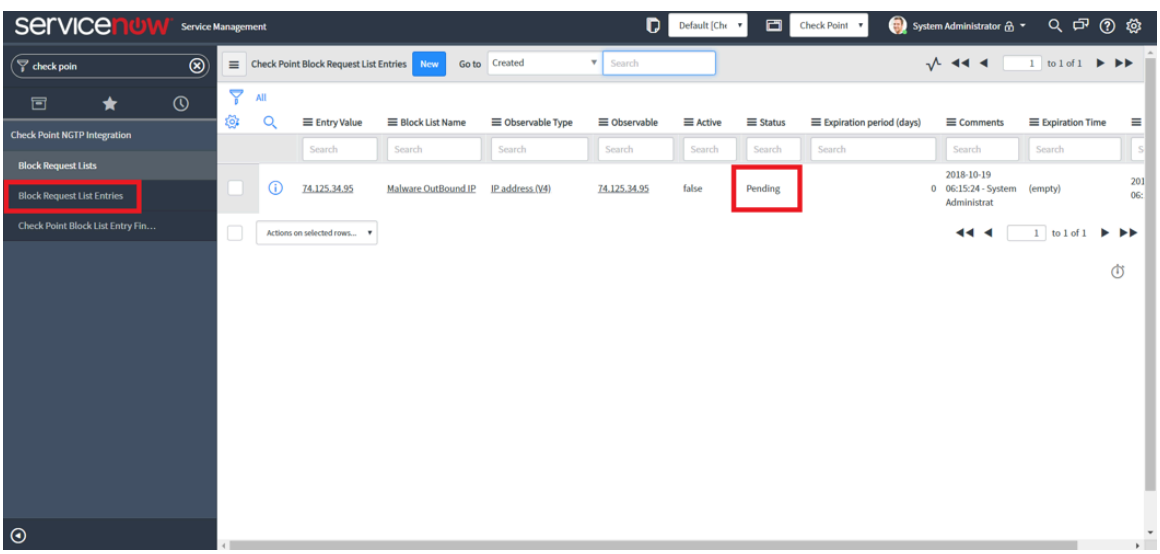
   Remarque : Pour cet exemple, le type d'observable d'entrée (IP) doit correspondre au type d'observable de la liste de blocs (IP).



8. Dans la boîte de dialogue Demande de bloc avec le nom de la liste de blocs affiché dans le champ **Implémentation** , cliquez sur **Bloquer**.



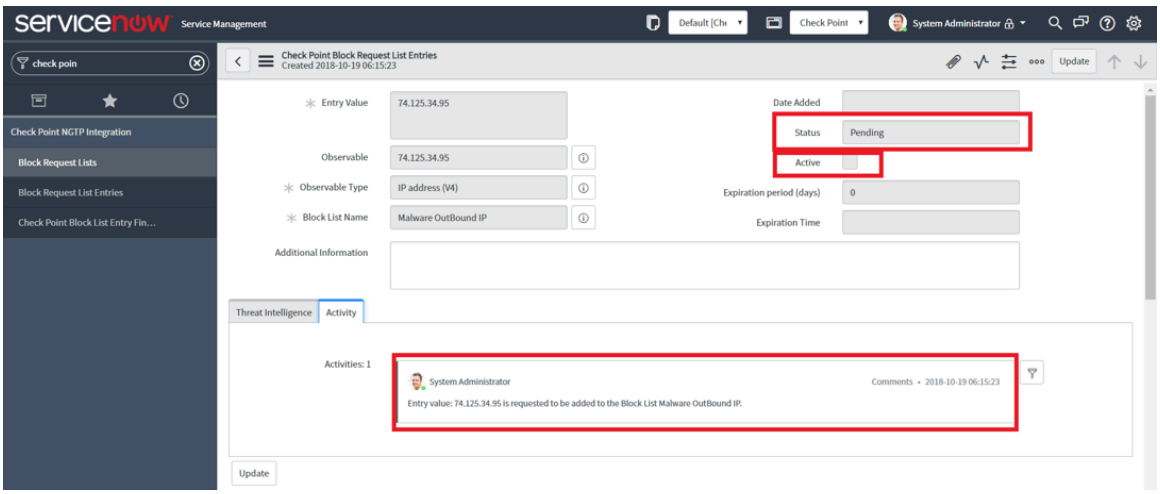
9. Accédez à la **Intégration Check Point NGTP** > **Entrées de la liste de demandes de blocs**, puis cliquez sur **Entrées de la liste de demandes de bloc.**



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Dans la liste Check Point Request List Entries (Entrées de la liste de demandes de blocs Check Point), cliquez sur votre observable dans la colonne **Valeur d'entrée** pour ouvrir l'enregistrement.
    Pour cet exemple, l'enregistrement de **74.125.34.95** s'affiche.



L'état est En attente, la case Actif est décochée et les notes de travail indiquent qu'il existe une demande d'ajout de l'observable. Cette demande d'entrée de liste de blocs est prête à être approuvée.

L'icône en regard du champ Observable est un lien vers la table Observable de Now Platform.

La valeur du champ Observable (74.125.34.95) est liée à la table Observable et correspond au format qui a été apporté à partir de l'événement de déclenchement de l'incident de Réponse aux incidents de sécurité.

Soumettre des entrées de liste de blocs directement à partir de la table d'entrée de la liste de blocs

Pour les observables déterminés comme malveillants et non associés à un incident de sécurité Now Platform spécifique, vous soumettez des entrées de liste de blocs à partir de la liste de blocs.

Avant de commencer

Rôle requis : administrateur d'incident de sécurité (sn_si.analyst)

Pourquoi et quand exécuter cette tâche

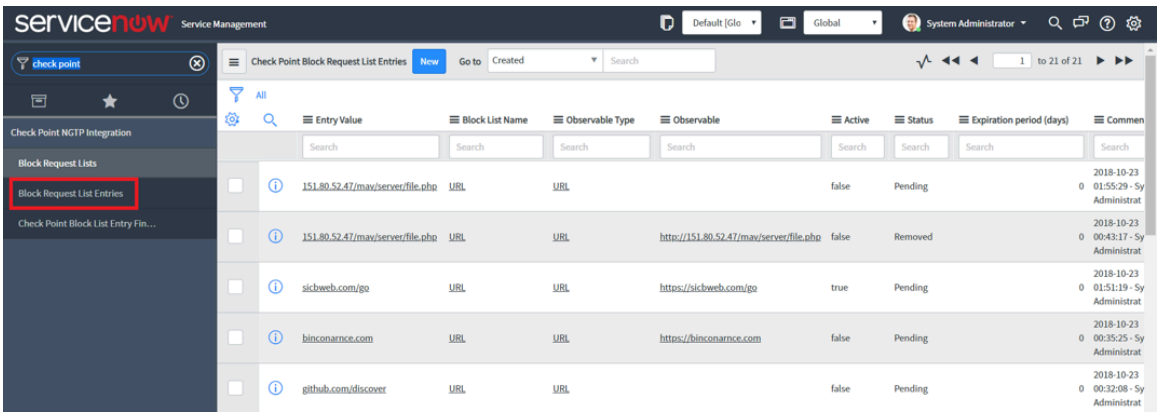
Lorsque vous souhaitez bloquer un observable que vous avez déterminé comme malveillant ou autoriser un observable que vous avez déterminé comme non malveillant et que l'observable n'est pas associé à un enregistrement d'incident de sécurité Now Platform spécifique, vous soumettez les entrées de la liste de blocs directement à partir de la liste de blocs. Des exemples de ces types d'entrées de liste de blocs peuvent être des URL ou des domaines pour des sites spécifiques.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

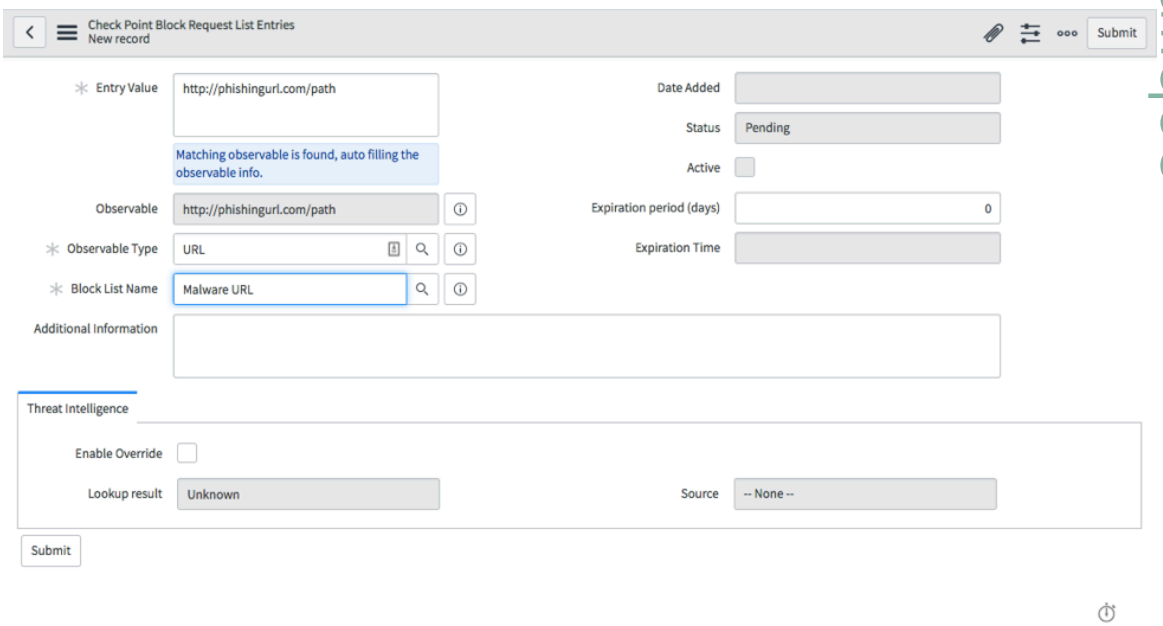
Procédure

1. Accédez à la **Tout** > **Intégration Check Point NGTP** > **Entrées de demande de bloc**.



2. Cliquez sur le module **Listes de demandes de blocs** .
3. Dans la liste Entrées de la liste de demandes de blocs Check Point, cliquez sur **Nouveau**.
4. Dans le champ **Valeur d'entrée** , entrez une valeur pour votre observable.
   Les deux résultats possibles de cette entrée :
   - Les champs restants du formulaire sont remplis automatiquement.
   - Un observable correspondant est trouvé et un message s'affiche indiquant qu'un observable correspondant existe. Sélectionnez la liste de blocs à laquelle vous souhaitez joindre cette entrée, puis cliquez sur Soumettre. Sélectionnez la liste de blocs à laquelle vous souhaitez joindre cette entrée avant de définir la période d'expiration.

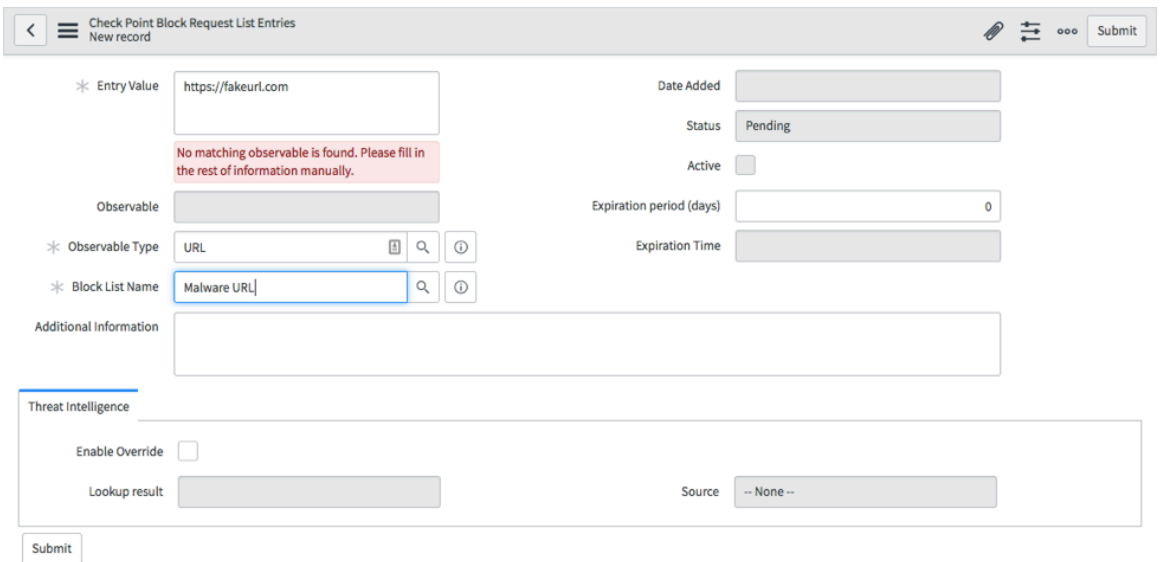
   Un message s'affiche pour vous demander de remplir le formulaire. Aucun observable correspondant n'a été trouvé et vous devez remplir le formulaire. Une fois que vous l'avez terminée, sélectionnez la liste de blocs à laquelle vous souhaitez joindre l'observable et cliquez sur Soumettre. Un enregistrement d'observable est créé. La figure suivante montre un exemple d'observable de domaine existant et comment les champs sont remplis automatiquement.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur l'icône de recherche pour sélectionner la liste de blocs à laquelle vous souhaitez joindre l'entrée.
6. Cliquez sur **Envoyer**.
7. Si vous avez configuré une approbation par e-mail dans votre workflow, une demande d'approbation par e-mail est envoyée.
   Si un message s'affiche vous demandant de remplir manuellement le reste des informations, renseignez les champs.



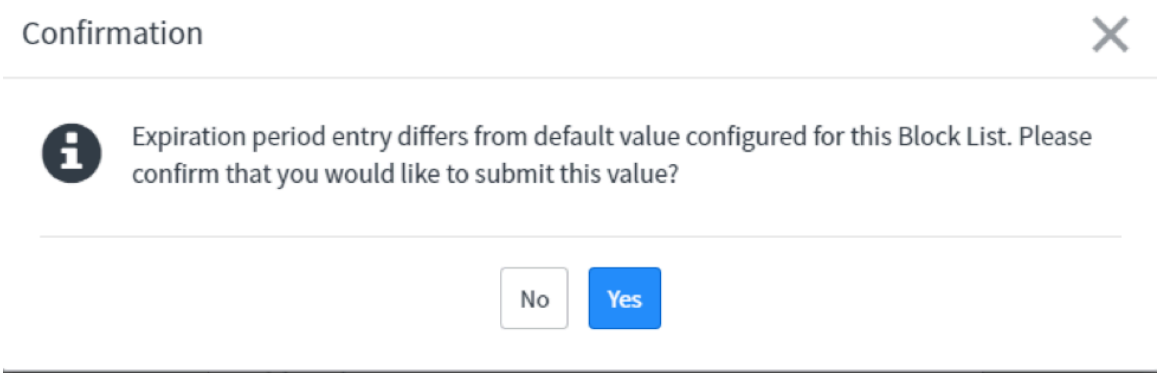
Champ	Description
Type d'observable	Type d'observable pris en charge à partir de la boîte de dialogue.
Nom de la liste de blocs	Liste de blocs dont vous souhaitez l'entrée. **Remarque :** Sélectionnez la liste de blocs à laquelle vous souhaitez joindre l'entrée avant de définir la période d'expiration.
Activer le remplacement (sélectionné par défaut)	Rechercher un résultat ou une source. Une fois configuré, elle vous permet d'entrer un résultat de recherche et la source utilisée pour trouver les résultats. Ces champs sont généralement renseignés lors de la création d'un enregistrement d'incident de sécurité. Dans ce cas, il n'y a pas de recherche de résultat ou de source, et vous renseignez ces champs manuellement.
Rechercher un résultat	Sélectionnez **Inconnu** ou **Malicieuse**.
Source	Source qui effectue une recherche de menace sur l'entrée de la liste de blocs, par exemple, ThreatCrowd...
Période d'expiration	La période d'expiration héritée de la liste de blocs par défaut. Vous pouvez remplacer cette valeur, mais uniquement lors de la création de l'entrée. 0 indique que l'entrée de la liste de blocs n'expire jamais.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si vous modifiez cette valeur, cette entrée est active pendant le nombre de jours que vous entrez. Vous pouvez entrer une valeur minimale de 1, mais il n'y a pas de valeur maximale. Par exemple, si vous saisissez 30 jours à 14 h 01 le 1er mai, l'entrée Liste de blocs expirera à 14 h 01 le 31 mai. Toutefois, le planificateur vérifie les entrées expirées à 00h00 tous les jours et change l'état de l'entrée en « expiré » à 00h00 le 1er juin.

8. Cliquez sur **Envoyer**.
   Si vous avez modifié la période d'expiration par défaut de l'entrée de la liste de blocs, une boîte de dialogue de confirmation d'avertissement s'affiche indiquant que la période diffère de la liste de blocs sélectionnée.

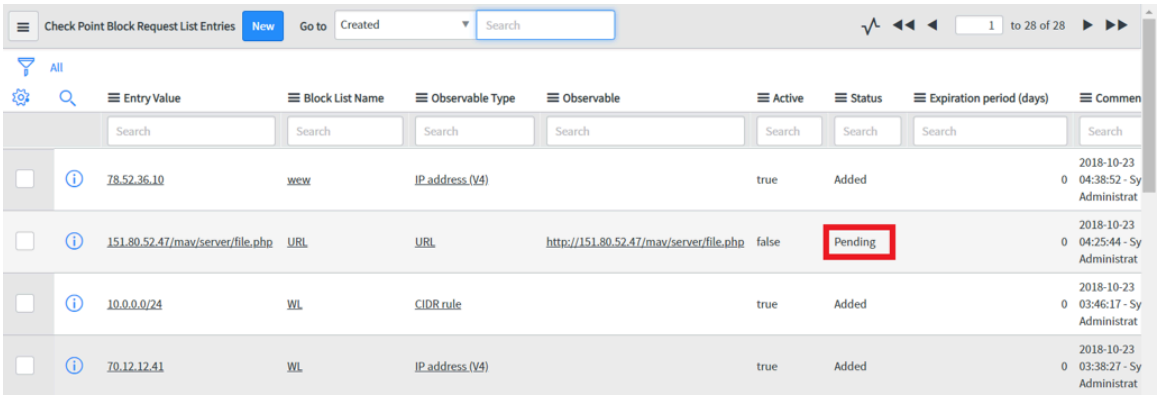


Option	Description
Oui	Confirme votre remplacement d'expiration, enregistre l'enregistrement et vous renvoie aux entrées de la liste de blocs Check Point. Si vous avez configuré une approbation par e-mail dans votre workflow, une demande d'approbation par e-mail est envoyée.
Non	Annule le remplacement. À ce stade, vous pouvez modifier la valeur de la **période d'expiration**. Après avoir modifié la valeur, cliquez sur Soumettre pour revenir à la liste Entrées de blocs Check Point.

9. Si ce n'est pas le cas, accédez aux entrées de la **liste de demandes de blocs Check Point** et notez que l'état de l'entrée est **En attente**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'entrée est maintenant prête pour approbation.

Approuver les entrées de la liste de blocs pour l'intégration Check Point NGTP

Un processus d'approbation des entrées de la liste de blocs fait partie du workflow préconfiguré. Vous approuvez les entrées de la liste de blocs avant que les entrées ne soient activées sur les listes de blocs. Une fois que vous avez approuvé l'entrée de la liste de blocs, la passerelle récupère l'entrée et votre observable est bloqué à partir de ce moment-là.

Avant de commencer

- L'approbation des entrées de la liste de blocs est affectée par défaut à l'administrateur d'incident de sécurité (sn_si.admin), mais cette autorité peut être affectée selon les besoins de votre organisation. Dans l'exemple suivant, l'administrateur de Now Platform dispose d'un pouvoir d'approbation.

Rôle requis : sn.si.admin

Pourquoi et quand exécuter cette tâche

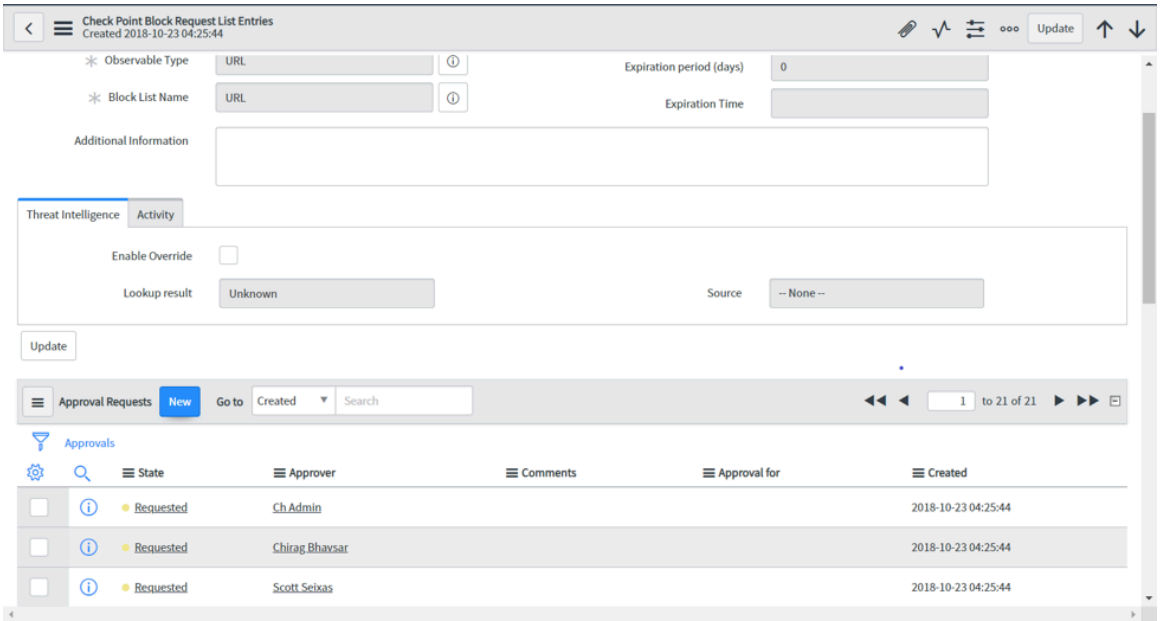
Lorsque le processus d'approbation est activé, une entrée de la liste de blocs n'est pas activée ou désactivée sur la liste de blocs tant qu'elle n'est pas approuvée.

Procédure

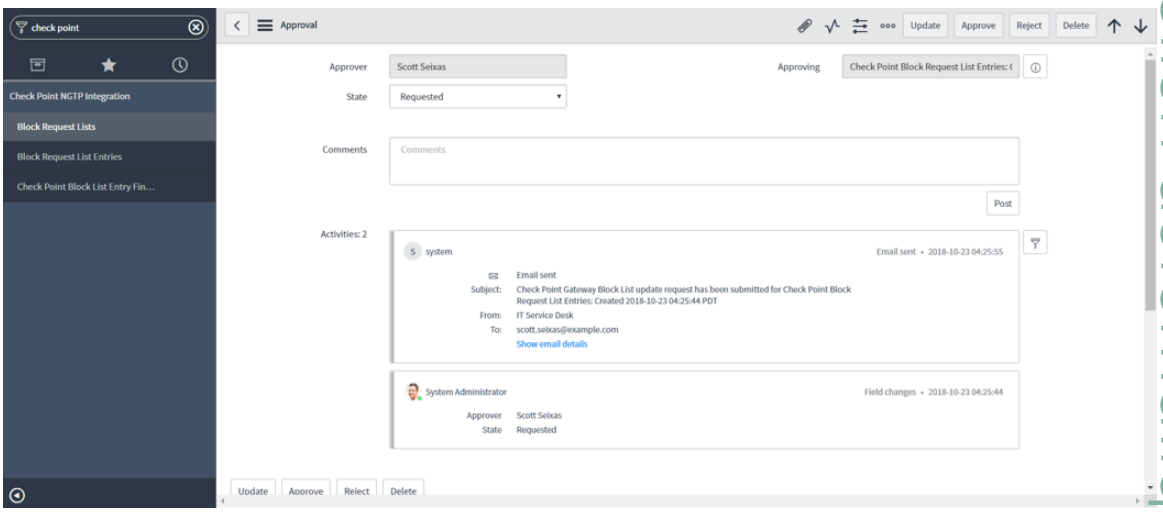
1. Accédez à la **Tout** > **Intégration Check Point NGTP** > **Entrées de la liste de demandes de blocs**et ouvrez l'enregistrement Entrée de la liste de blocs.
2. Dans l'enregistrement Entrée de la liste de blocs, faites défiler jusqu'à la section **Demandes d'approbation** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans Demandes d'approbation, cliquez sur un élément de la colonne **État** pour l'ouvrir. L'enregistrement de l'approbation s'affiche.



4. Choisissez une option pour approuver l'entrée de la liste de blocs.

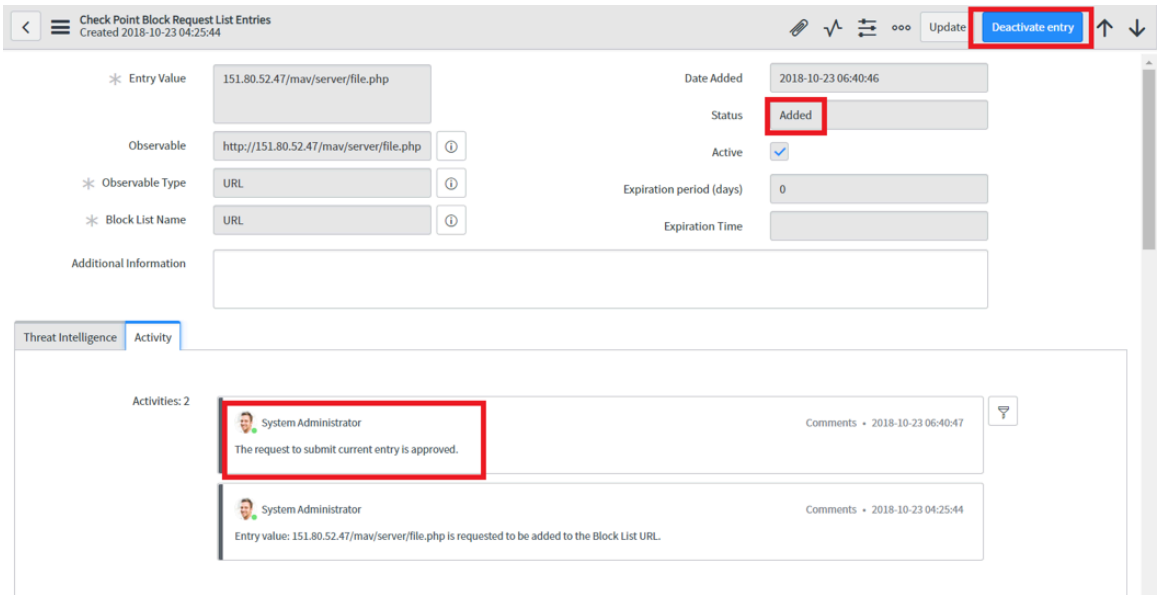
Option	Description
Approuver	Sur l'enregistrement d'entrée, le champ État devient Ajouté et la case Actif est cochée. Le bouton Désactiver est affiché et actif. Les notes de travail montrent que la demande d'entrée de la liste de blocs a été approuvée.
Refuser	Sur l'enregistrement d'entrée, le champ État devient Rejeté et la case Actif est décochée, ce qui indique que l'entrée n'est pas bloquée sur la passerelle.

Traduction automatique

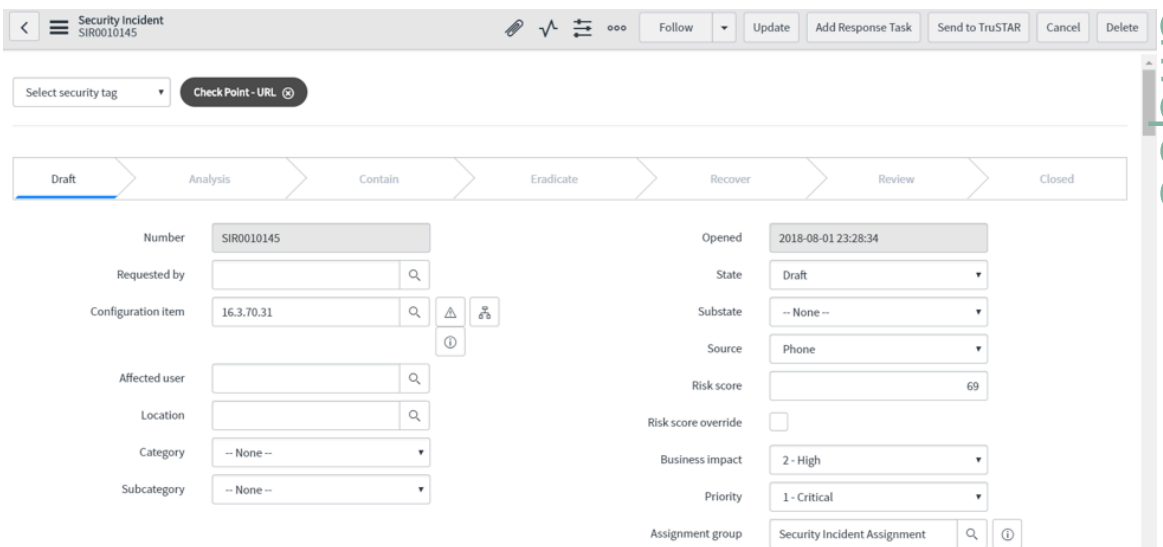
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Les notes de travail montrent que la demande d'entrée de liste de blocs a été rejetée.

Une fois que vous avez approuvé l'entrée de la liste de blocs et qu'elle est activée, le pare-feu de nouvelle génération Check Point récupère l'entrée de la liste de blocs après l'intervalle de récupération suivant. Une fois l'entrée récupérée, l'observable est bloqué à partir de ce moment-là. Dans la figure suivante, notez que la case Actif est cochée, que l'état est Ajouté et que les notes de travail indiquent que la demande a été approuvée.



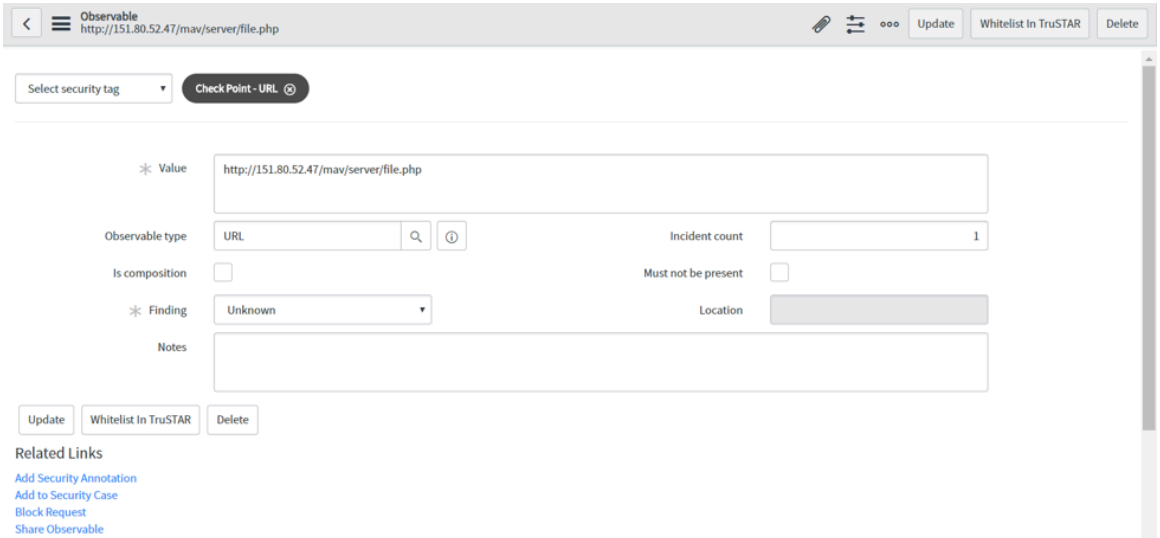
Une fois l'entrée de la liste de blocs approuvée et activée, l'enregistrement d'incident de sécurité est marqué d'une balise de sécurité. La balise s'affiche en haut de l'enregistrement.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La balise de sécurité est également affichée sur l'enregistrement de l'observable.



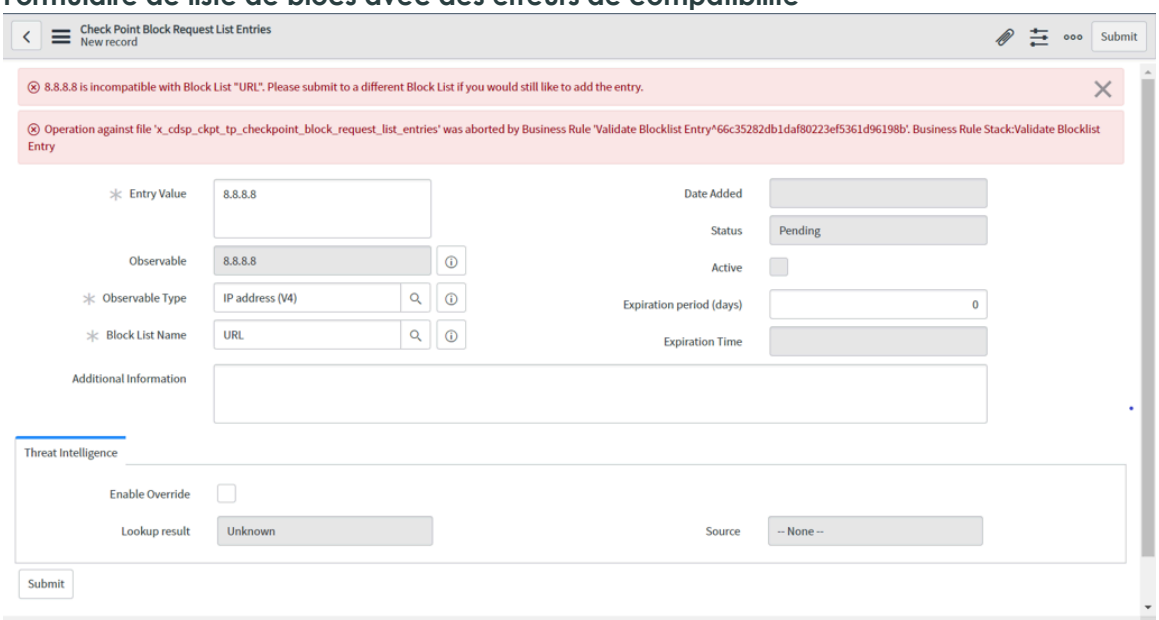
Exceptions d'entrée de la liste de blocs pour l'intégration Check Point NGTP

Il existe des restrictions pour l'ajout d'entrées de liste de blocs à des listes de blocs. En cas de conflits de doublons, de compatibilité ou CIDR (routage inter-domaine sans classe) lorsque vous essayez d'ajouter des entrées de liste de blocs à des listes de blocs, des messages d'erreur s'affichent pour vous aider à résoudre ces erreurs.

Exception de compatibilité

Chaque liste de blocs n'accepte que les entrées compatibles avec son type d'observable. Si vous créez une liste de blocs de domaine et que vous essayez d'y attacher un observable d'adresse IP, un message d'erreur incompatible s'affiche. Par exemple, une liste de blocs de domaine ne peut accepter que les observables de domaine, comme illustré dans la figure suivante.

Formulaire de liste de blocs avec des erreurs de compatibilité

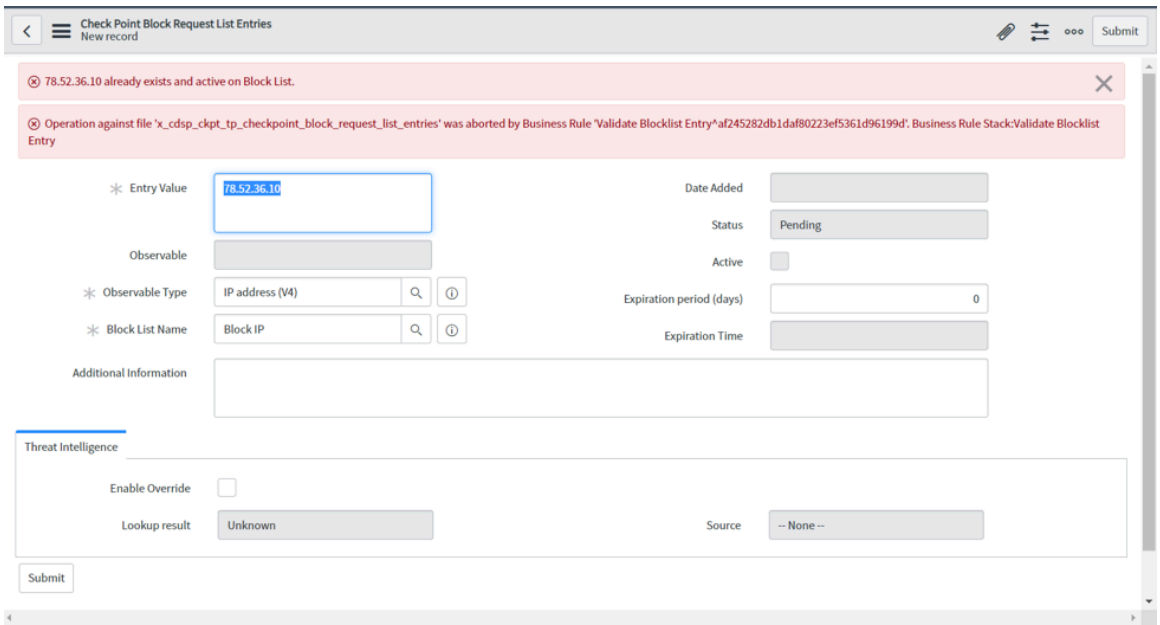


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

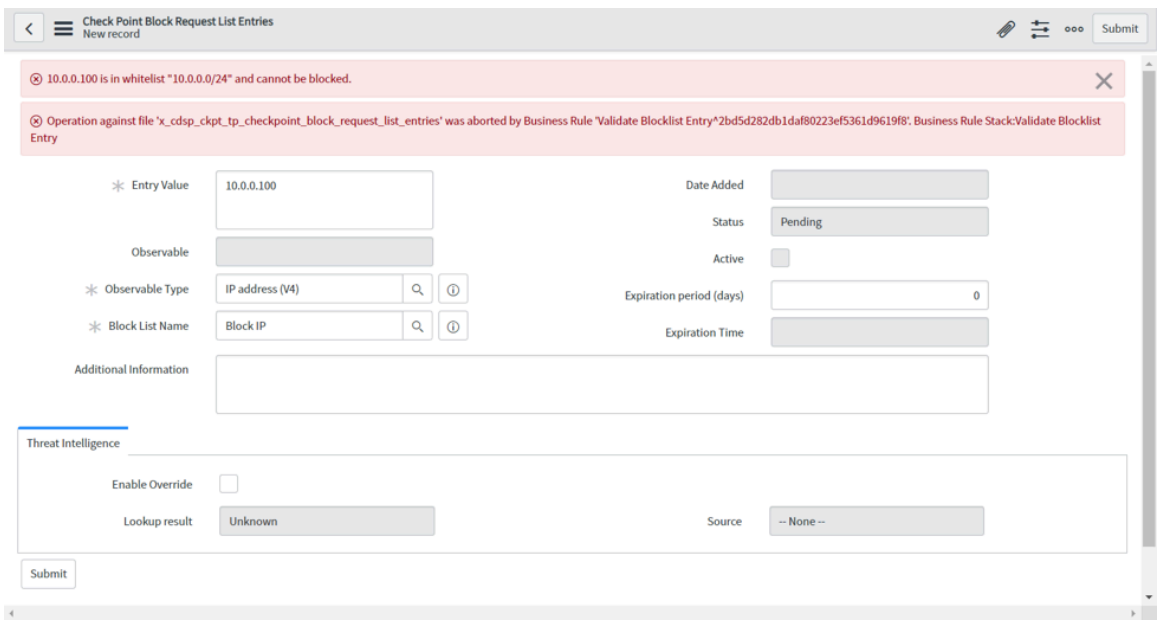
Exception de duplication

Un observable ne peut pas être activé sur plusieurs listes de blocs du même type d'observable. Si un observable d'URL est déjà activé sur une liste de blocs d'URL et que vous tentez d'activer le même observable sur une liste de blocs d'URL de hameçonnage, un message d'erreur de duplication s'affiche.



Exception CIDR (Classless Inter-Domain Routing)

Si vous tentez d'associer une seule adresse IP à une liste d'autorisation et que cette adresse IP fait partie d'un observable CIDR déjà sur une liste de blocs ou liste d'autorisation, une erreur de conflit CIDR s'affiche. Cette erreur indique que l'adresse IP unique est déjà incluse dans la liste de blocs ou la liste d'autorisation dans le cadre de l'observable CIDR. Par exemple, 192.168.24.25 fait partie du bloc CIDR 192.168.0.0/22.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modifier le nom de la balise de sécurité pour l'intégration Check Point NGTP

Si la case Afficher la balise est cochée lors de la création de l'enregistrement Liste de blocs, vous pouvez modifier les noms des balises et les couleurs des balises de sécurité. Les balises de sécurité vous aident à suivre les observables qui sont déjà bloqués.

Avant de commencer

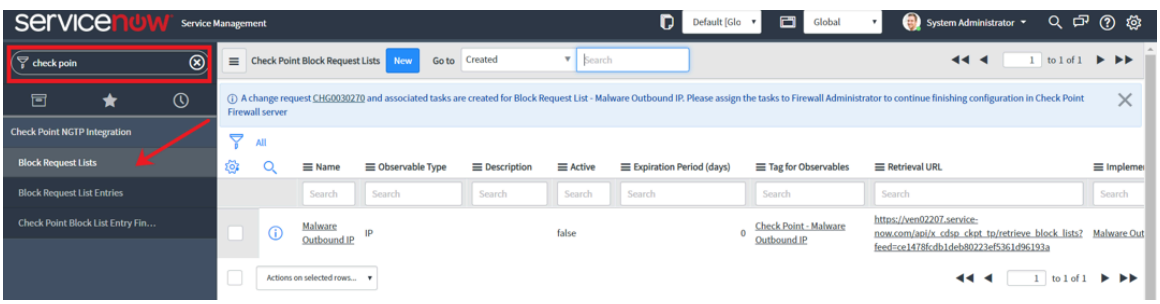
Rôle requis : sn.si.admin

Pourquoi et quand exécuter cette tâche

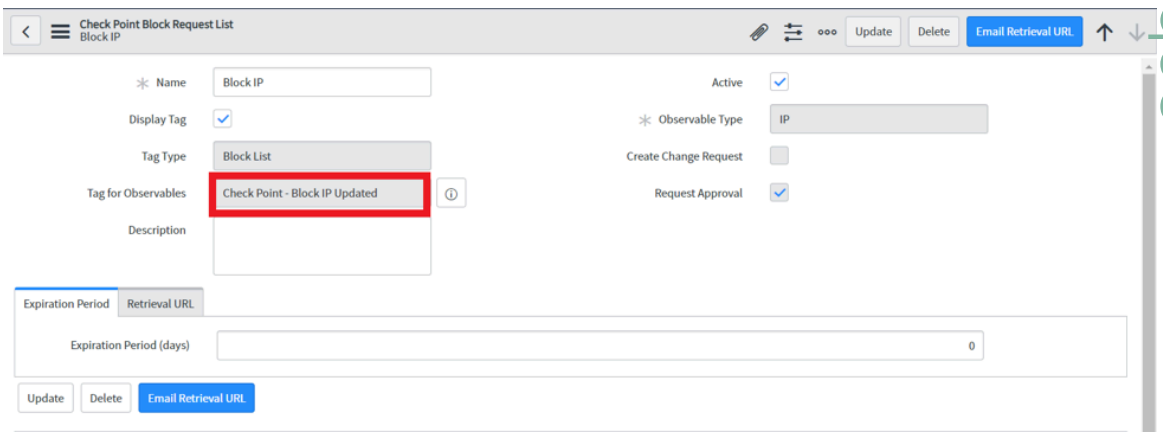
Les balises de sécurité vous aident à identifier rapidement quels incidents de sécurité ont des observables sur une liste de bloc. Les balises vous aident également à identifier si un observable est déjà bloqué ou s'il a été supprimé d'une liste de blocs. Par défaut, la couleur de la balise de sécurité est noire pour les entrées de la liste de blocs et grise pour les entrées de la liste d'autorisation. Vous pouvez modifier les noms et les couleurs des balises pour vous aider à reconnaître plus facilement certaines balises.

Procédure

1. Accédez à la **Tout** > **Intégration Check Point NGTP** > **Configuration de la liste de demandes de blocs**.



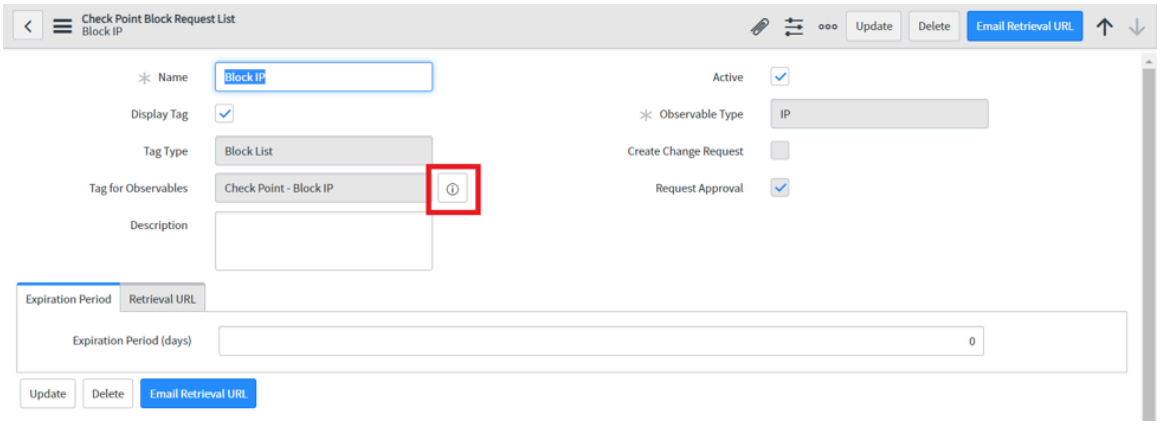
2. Cliquez sur un élément dans la colonne **Nom** pour l'ouvrir.
   L'enregistrement de la liste de blocs s'affiche. Par défaut, le nom de la balise de sécurité est la même que celle que vous avez saisie dans le champ Nom de la liste de blocs lorsque vous l'avez créée. Par défaut, le nom inclut également un préfixe de liste de blocs, par exemple, Liste de blocs – URL malveillantes de programmes malveillants.



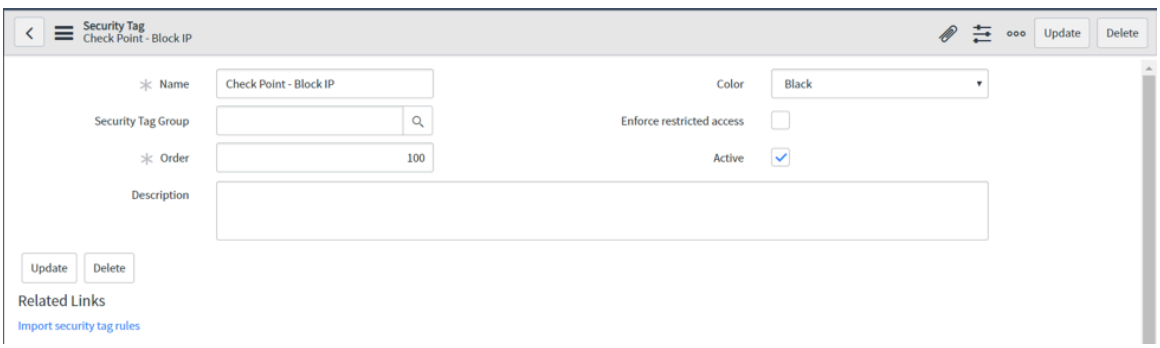
3. Cliquez sur l'icône d'informations en regard de Balise pour les observables, puis Ouvrir l'enregistrement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

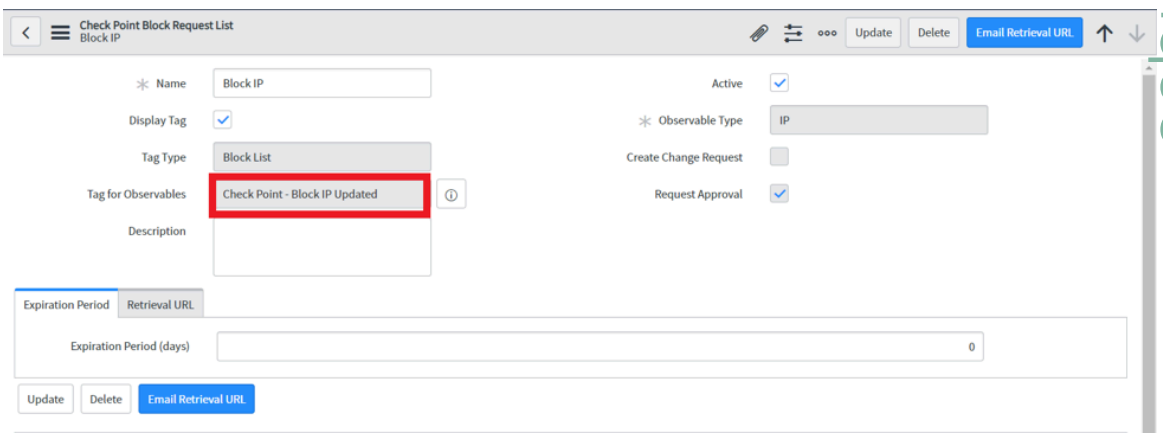


Le formulaire de balise de sécurité s'affiche.



4. Dans le champ **Nom** , modifiez le nom de la balise de sécurité.
5. Cliquez sur **Mettre à jour**.
   L'enregistrement de la liste de blocs mis à jour s'affiche avec le nom de balise modifié.

> **Remarque :** Dans l'exemple suivant, Sortant a été ajouté au nom de la balise. Conservez le préfixe Check Point dans le nom de votre nouvelle balise pour vous aider à identifier qu'elle est associée à l'intégration de pare-feu de nouvelle génération de Check Point.

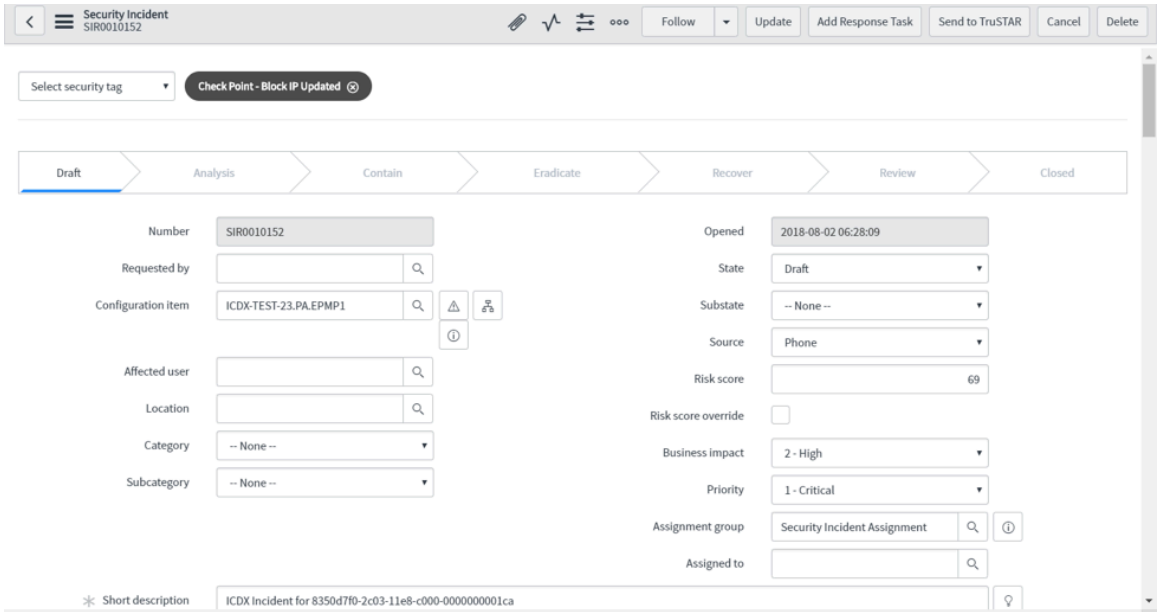


Les balises de sécurité sont affichées pour chaque type d'observable (IP, URL, domaine) sur l'enregistrement d'incident de sécurité et l'enregistrement de l'observable chaque fois que l'observable est ajouté à la liste de blocs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats



Si un observable a déjà été ajouté à une liste de blocs et qu'une balise de sécurité est affichée sur un incident de sécurité pour cet observable, la balise de sécurité de la liste de blocs est également affichée automatiquement sur tous les enregistrements d'incident de sécurité ultérieurs qui sont créés. Cette duplication vous indique que l'observable figure déjà sur une liste de blocs. Vous n'avez pas besoin d'ajouter cet observable et de le bloquer à nouveau.

Lorsqu'un observable n'est plus bloqué, une balise de sécurité n'est pas affichée sur l'enregistrement d'incident de sécurité ou l'enregistrement de l'observable. Dans ce cas, aucune balise de sécurité n'indique que la date d'expiration de l'observable est dépassée ou que l'observable a été désactivé d'une liste de blocs.

Désinstaller l'intégration Check Point NGTP

Si vous souhaitez désinstaller Check Point NGTP l'intégration de votre instance Now Platform et supprimer tous les restes de l'intégration, consultez le site de documentation ServiceNow pour obtenir des instructions sur la désinstallation d'applications.

Rôle requis : admin

Intégration de l'hôte CrowdStrike Falcon

L'intégration CrowdStrike Falcon Host vous permet de transférer les observables d'un incident de sécurité dans une liste de surveillance, ce qui leur permet de générer des alertes supplémentaires. Cette intégration est une implémentation du workflow CrowdStrike Falcon Host - Publier dans la liste de surveillance.

Explorer Intégrations de Réponse aux incidents de sécurité	Configurer Démarrer l'intégration CrowdStrike Falcon Host
Utiliser	Développer

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

• Effectuer des recherches sur les observables • Activité Publier dans la liste de surveillance	• ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide • Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service et assistance client	

Démarrer l'intégration CrowdStrike Falcon Host

La fonctionnalité de configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration CrowdStrike Falcon Host . Avant de pouvoir utiliser l'intégration CrowdStrike Falcon Host , vous devez la télécharger à ServiceNow Store partir du , puis ajouter un nom d'utilisateur et un mot de passe.

Avant de commencer

- Si vous mettez à niveau CrowdStrike Falcon Host l'intégration à partir d'une version précédente, vous devez supprimer la configuration existante et en configurer une nouvelle. La nouvelle intégration prend en charge l'authentification OAuth2. Cette mise à jour nécessite que vous saisissiez **l'ID du client API** et le **secret du client API** pour vous authentifier et terminer la configuration.
- Dans les **périmètres de l'API** du CrowdStrike Falcon Host portail, activez le paramètre de **lecture** et **d'écriture** pour **les IOC (indicateurs de compromission).**

Rôle requis : sn_si_admin

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Dans la carte CrowdStrike Falcon Host, cliquez sur **Configurer**.
4. Renseignez les champs du formulaire pour finaliser la configuration :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de l'hôte CrowdStrike Falcon

Champ	Description
Nom	Nom de l'intégration, par exemple `demo-1`.
ID client API	L'ID client que vous obtenez à partir de la section des paramètres de votre profil de compte dans CrowdStrike Falcon Host le portail.
Secret client API	Clé secrète du client que vous obtenez à partir de la section des paramètres de votre profil de compte dans CrowdStrike Falcon Host le portail.

5. Cliquez sur **Envoyer**.

Résultats

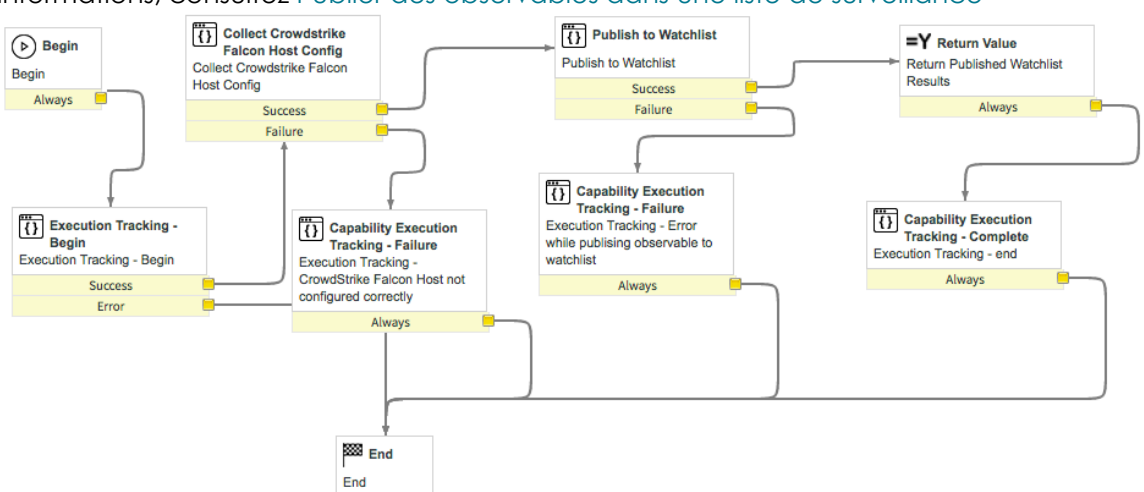
Une fois configurée, l'intégration CrowdStrike Falcon Host peut être sélectionnée pour publier des observables dans des listes de surveillance au format Réponse aux incidents de sécurité.

CrowdStrike Falcon Host pour Security Operations : workflow de publication dans la liste de surveillance

Le workflow **CrowdStrike Falcon Host pour Security Operations : publier dans la liste de surveillance** est utilisé pour spécifier la liste de surveillance pour la génération d'alertes ou d'événements. Les alertes et les événements sont affichés dans le système CrowdStrike Falcon Host en fonction de la façon dont il est configuré.

Workflow Publier dans la liste de surveillance

Ce workflow est déclenché lorsque Intégration de Security Operations : aptitude Publier dans la liste de surveillance vous sélectionnez un ou plusieurs observables associés à un incident de sécurité et que vous utilisez l'action d'interface utilisateur Publier dans la liste de surveillance pour pousser les observables vers une liste de surveillance. Les observables peuvent ensuite être utilisés pour générer des alertes supplémentaires. Pour plus d'informations, consultez Publier des observables dans une liste de surveillance tierce.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les activités spécifiques à cette intégration sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Collecter l'activité de configurations de l'hôte CrowdStrike Falcon

L'activité **de workflow Collecter les configurations de l'hôte CrowdStrike Falcon** rassemble des informations de configuration à utiliser dans le workflow.

L'activité **Collecter la configuration de l'hôte CrowdStrike Falcon peut** être utilisée avec n'importe quel workflow pour collecter les paramètres de configuration de l'hôte CrowdStrike Falcon.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Configuration réussie. .
Échec	Une erreur s'est produite lors de la tentative de vérification de la configuration. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
user_name	Nom d'utilisateur de l'hôte CrowdStrike Falcon
mot de passe	Mot de passe de l'hôte CrowdStrike Falcon

Activité Publier dans la liste de surveillance

L'activité de workflow **Publier dans la liste de surveillance** pousse les observables d'un incident de sécurité dans une liste de surveillance pour générer des alertes ou des événements. Les alertes et les événements sont affichés dans le système CrowdStrike Falcon Host en fonction de la façon dont il est configuré.

L'activité **Publier dans la liste de surveillance** peut être utilisée avec n'importe quel workflow pour publier des observables dans une liste de surveillance.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Configuration réussie. .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats (suite)

Résultat	Description
Échec	Une erreur s'est produite lors de la tentative de vérification de la configuration. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
observables	La liste des observables à partir de Réponse aux incidents de sécurité.
user_name	Le nom d'utilisateur de la personne responsable de l'intégration de CrowdStrike Falcon Host.
mot de passe	Le mot de passe de la personne responsable de l'intégration de CrowdStrike Falcon Host.
task_sys_id	L'identificateur système pour cette tâche de publication dans la liste de surveillance.
CapabilityExecutionId	Nom de l'option associée.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
statut	État de l'activité de publication.

CrowdStrike Falcon Insight pour Opérations de sécurité l'intégration

Avec l'intégration CrowdStrike Falcon InsightOpérations de sécurité , vous pouvez effectuer des actions de rattrapage sur les points de terminaison en temps réel, utiliser des profils pour recueillir des détails sur l'hôte et effectuer des requêtes ou des actions spécifiques sur le point de terminaison à l'aide du Now Platform Réponse aux incidents de sécurité produit.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Le CrowdStrike Falcon Insight for Opérations de sécurité integration fonctionne avec le Now Platform afin que vous puissiez obtenir des informations supplémentaires sur le champ d'application d'un incident. capture toutes les activités d'événement CrowdStrike Falcon Insight de point de terminaison pertinentes, vous pouvez l'utiliser pour vous concentrer sur les Now Platform enquêtes et les actions de rattrapage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
ServiceNow site web de la documentation produit	Site web de la documentation produit ServiceNow
CrowdStrike Falcon Insight pour Opérations de sécurité	Mise en route de l'intégration CrowdStrike Falcon Insight

Mise en route de l'intégration CrowdStrike Falcon Insight

Vous pouvez activer et configurer l'interface CrowdStrike Falcon Insight de confidentialité avec votre instance et Réponse aux incidents de sécurité votre Now Platform produit.

Avant de commencer

Rôle requis : administrateur

Avant de pouvoir l'utiliser CrowdStrike Falcon Insight pour l'intégration Opérations de sécurité , vous devez le télécharger à ServiceNow Storepartir du fichier .

Pourquoi et quand exécuter cette tâche

Liste de vérification

Tâche de configuration	Description
Affectez et vérifiez les rôles requis Now Platform et Réponse aux incidents de sécurité .	Ces rôles sont requis pour la configuration et la vérification des résultats attendus : • Le rôle administrateur installe l'intégration à partir du ServiceNow Store rôle sn_si.admin et lui attribue le rôle. • Le rôle sn_si.admin configure l'intégration, crée et active les profils, puis attribue le rôle sn_si.analyst. • Le rôle sn_si.analyst répond aux incidents de sécurité, lance manuellement les profils et peut soumettre des demandes d'actions telles que l'isolement de l'hôte et la suppression de l'isolement de l'hôte pour un groupe approuvé.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant de configurer cette intégration.	Le module d'extension Programme d'installation du ServiceNow Hub d'intégration pack Entreprise [com.glide.hub.integrations.enterprise] est requis. Ce module d'extension permet l'exécution des actions et des flux du Centre d'intégration : Le Réponse aux incidents de sécurité module d'extension

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	(com.snc.security_incident) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si ces applications ne sont pas déjà installées, vous devez installer et activer chaque application une par une dans l'ordre suivant pour garantir une installation fluide : **1.** Réponse aux incidents de sécurité Dépendance (com.snc.si_dep) **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Orchestration de support de sécurité **5.** Renseignements sur les menaces Prise en charge commune **6.** Trusted Security Circles **7.** Opérations de sécurité Assistant de configuration **8.** Réponse aux incidents de sécurité
Configurez un groupe d'approbation.	Une aptitude d'approbation facultative est disponible pour isoler les ordinateurs hôtes, les restaurer sur le réseau et lancer des recherches de perceptions. Pour activer cette option, vous devez obtenir l'approbation préalable du rôle sn_si.admin avant que les ordinateurs hôtes ne soient isolés et restaurés sur votre réseau, ou lorsque des recherches de perceptions sont effectuées. Si vous avez besoin d'un niveau supplémentaire de contrôle sur ces actions, activez l'option **Exiger l'approbation** lors de la configuration du profil. L'autorité d'approbation est affectée à l'utilisateur ayant le rôle sn_si.admin. Vous pouvez également réaffecter cette autorité d'approbation à un groupe d'approbation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
Attribuez et vérifiez les rôles de la plateforme CrowdStrike Falcon.	Les rôles suivants sont requis sur la plateforme CrowdStrike Falcon pour la configuration de l'intégration : • Le rôle d'administrateur Falcon est nécessaire pour afficher, créer ou modifier des clients ou des clés d'API. • Le rôle Répondeur en temps réel – Administrateur est requis pour créer et exécuter des scripts personnalisés. • Le rôle Répondeur en temps réel – Intervenant actif est requis pour créer et exécuter des scripts personnalisés.
Vérifiez que les scripts personnalisés, les rôles et les autorisations sont activés dans la plateforme CrowdStrike Falcon.	Cette intégration utilise les scripts personnalisés de CrowdStrike pour quelques-unes des fonctionnalités d'enrichissement. • Vérifiez que les rôles Intervenant en temps réel – Administrateur et Répondeur en temps réel – Intervenant actif sont disponibles. • Vérifiez que l'option **de politique Par défaut (Windows)** est activée dans Configuration > politiques de réponse dans l'interface utilisateur de CrowdStrike Falcon. • Vérifiez que la **réponse en temps réel** et **les scripts personnalisés** sous la fonctionnalité En temps réel sont activés dans l'interface utilisateur de CrowdStrike Falcon.
Générer des clients et des clés d'API dans la plateforme CrowdStrike Falcon.	Créez les clients ou les clés de l'API CrowdStrike dans la plateforme CrowdStrike Falcon à utiliser dans la configuration de l'intégration Now Platform .

Créer un client d'API CrowdStrike et générer les clés

Créez le client d'API CrowdStrike et générez l'ID client et la clé que vous utilisez pour configurer l'intégration CrowdStrike Falcon Insight .

Avant de commencer

Rôle requis : administrateur de CrowdStrike Falcon

Procédure

1. Sur la plateforme CrowdStrike Falcon, accédez aux **clients et aux clés d'API**.
2. Dans la table Clients d'API OAuth2, cliquez sur **Ajouter un nouveau client d'API**.
3. Saisissez les détails suivants pour définir votre client d'API :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom du client	Entrez le nom du client. Ce champ est obligatoire.
Description	Saisissez la description du nom du client.
Périmètres de l'API	Il est nécessaire de définir les champs d'application. **Important :** Assurez-vous d'activer le compte API et assurez-vous que les champs d'application suivants sont activés pour le compte API : ◦ Activer les champs d'application de lecture et d'écriture pour l'API des hôtes ◦ Activer le périmètre de lecture pour l'API d'indicateurs

4. Cliquez sur **Ajouter** pour enregistrer le client d'API et générer l'ID client et la clé secrète.

Installer et configurer CrowdStrike Falcon Insight

Installez et configurez l'application CrowdStrike Falcon Insight for à Opérations de sécurité partir de ServiceNow Store sur votre Now Platform instance.

Avant de commencer

Rôle requis : administrateur

Remarque : Vous ne pouvez associer une aptitude qu'à un seul profil. Vous ne pouvez pas associer une aptitude à plusieurs profils. Lorsque vous configurez des serveurs CrowdStrike, vous ne pouvez pas réutiliser une aptitude CrowdStrike avec plusieurs profils qui partagent le serveur CrowdStrike. Vos profils peuvent avoir la même fonctionnalité CrowdStrike, chaque profil doit utiliser son propre serveur CrowdStrike.

Procédure

1. Téléchargez l'intégration pour Opérations CrowdStrike Falcon Insight de sécurité à partir de et ServiceNow Store installez-le.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette d'intégration CrowdStrike Falcon InsightOpérations de sécurité , puis cliquez sur **Configurer**.
4. Renseignez les champs du formulaire pour finaliser la configuration :

CrowdStrike Falcon Insight Configuration

Champ	Description
Nom	Nom de l'intégration, par exemple `demo-1`.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL de l'API CrowdStrike Falcon Insight	URL de base qui héberge l'API CrowdStrike. Entrez l'URL avec le protocole HTTPS. Par exemple, https://api.crowdstrike.com.
ID client	L'ID client que vous obtenez à partir de la section des paramètres de votre profil de compte dans le CrowdStrike Falcon Insight portail.
Secret client	Clé secrète du client que vous obtenez à partir de la section des paramètres de votre profil de compte dans le CrowdStrike Falcon Insight portail.



5. Cliquez sur **Envoyer**.

Résultats

Une fois l'intégration validée et soumise, elle est enregistrée sous forme de vignette sur la page Intégrations de sécurité. Vous pouvez afficher le CrowdStrike Falcon Insight module dans le navigateur d'application.

Créer un groupe d'approbation

Créez un groupe d'approbation pour l'intégration CrowdStrike Falcon InsightOpérations de sécurité , qui peut approuver les demandes d'isolement des ordinateurs hôtes, de restauration sur le réseau et de lancement des recherches de perceptions.

Avant de commencer

Vous ne pouvez pas réaffecter l'autorité d'approbation à un groupe, sauf si un groupe d'approbation est disponible dans votre instance.

Remarque : L'option d'approbation de la configuration du profil s'affiche uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Groupes**.
2. Dans la liste des groupes, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Groupe d'approbation

Champ	Description
Nom	Nom du groupe que vous voyez lorsque vous soumettez une demande d'approbation.
E-mail de groupe	Liste de distribution d'e-mails ou adresse e-mail du point de contact du groupe, par exemple le gestionnaire de groupe.
Responsable	Nom du gestionnaire de groupe. Cliquez sur l'icône de recherche pour afficher la liste.
Parent	Nom du groupe parent, s'il est associé à un parent.
Type	Catégories de groupes.
Fournisseurs	vendor_manager rôle que vous affectez aux utilisateurs dans le processus de gestion des fournisseurs de votre organisation.
Description	Informations supplémentaires sur le groupe.

4. Cliquez sur **Envoyer**.
   Le nouveau groupe s'affiche dans la liste Groupes.

   Ce groupe est disponible pour traiter les demandes lorsque vous activez l'option **Exiger une approbation** pendant la configuration de ce profil.

   Pour surveiller et traiter les demandes soumises par les utilisateurs disposant du rôle sn_si.analyst, chaque membre du groupe d'approbation accède à l'onglet **Mes approbations** dans le Now Platform.

Que faire ensuite

L'étape suivante consiste à installer et configurer l'application CrowdStrike Falcon Insight à partir de ServiceNow Store.

Créer un profil d'aptitude pour l'intégration CrowdStrike Falcon Insight

Créez un profil et sélectionnez les CrowdStrike Falcon Insight options que vous souhaitez qu'il exécute.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Réfléchissez aux raisons pour lesquelles vous souhaitez créer un profil avant d'y ajouter CrowdStrike Falcon Insight des options. Le tableau suivant répertorie les options que vous

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

devez ajouter à un profil lorsque vous souhaitez que le profil effectue certaines requêtes ou actions.

Vous pouvez créer un profil unique qui exécute des requêtes pour obtenir des détails sur le système, répertorie les utilisateurs connectés, extrait les services en cours d'exécution, extrait les processus en cours, extrait les statistiques réseau, isole l'hôte et supprime l'hôte isolé. Vous pouvez également créer plusieurs profils, chacun ayant sa propre aptitude.

Remarque : Les options Isoler l'hôte, Supprimer l'isolement et Obtenir un fichier ne peuvent pas être fusionnées avec d'autres options lors de la création d'un profil.

Types de profils et options requises de CrowdStrike Falcon Insight

Objectif du profil	Options de CrowdStrike
Collecter les détails de l'hôte et les utilisateurs connectés	• **Obtenir les détails de l'hôte** • **Obtenir les utilisateurs connectés**
Extraire les statistiques, les processus et les services réseau en cours d'exécution pour un hôte	• **Obtenir les statistiques réseau** • **Obtenir les processus en cours d'exécution** • **Obtenir les services d'exécution**
Isoler un hôte	**Isoler l'hôte**
Supprimer l'isolement d'un hôte	**Supprimer l'isolement**
Obtenir un fichier à partir d'un point de terminaison hôte	**Obtenir un fichier**

Procédure

1. Accédez à la **Tout** > **Intégration de CrowdStrike Falcon Insight** > **Profils des aptitudes de CrowdStrike**.
2. Cliquez sur **Nouveau**.
3. Sur le formulaire, renseignez les champs.

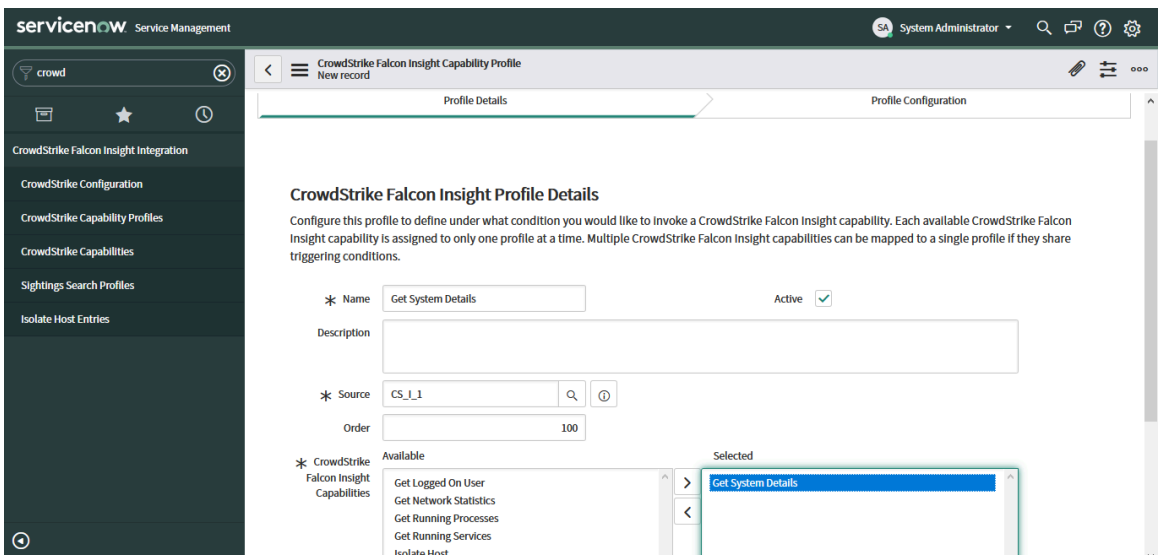
Champ	Description
Nom	Nom du nouveau profil d'aptitude. Ce nom vous aide à identifier le type de profil et est également le nom par défaut de la balise de sécurité associée à ce profil.
Actif	Indique si le profil est actif ou non. Lorsque le profil est actif, il se déclenche automatiquement lorsqu'un incident de sécurité correspondant aux conditions de filtrage spécifiées dans la configuration est créé.
Description	Description unique du profil d'aptitude.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Nom du serveur. Vous ne pouvez afficher que les serveurs précédemment configurés à partir de la liste.
Ordre	Priorité du flux. La valeur de ce champ indique l'ordre dans lequel les flux sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux doté du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400. Par défaut : 100
Options de CrowdStrike Falcon Insight	Fonctionnalités du profil CrowdStrike Falcon Insight. Sélectionnez les options que vous souhaitez pour ce profil dans la colonne **Disponible** dans la colonne **Sélectionné**.

L'exemple suivant montre un formulaire complet pour un profil avec l'option Obtenir les détails du système.



4. Cliquez sur **Suivant**.

Que faire ensuite

Vous pouvez maintenantconfigurer votre profil. Assurez-vous d'avoir passé en revue les concepts de configuration des profils et des conditions de déclenchement avant de configurer le profil.

Configurer les profils et les incidents de sécurité pour l'intégration CrowdStrike Falcon Insight

Configurez les paramètres de votre profil afin que le profil se déclenche uniquement dans les conditions que vous définissez.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Définissez les conditions qui déclenchent automatiquement les CrowdStrike Falcon Insight options que vous avez sélectionnées pour le profil. Vous pouvez également sélectionner un autre champ d'entrée pour le champ Élément de configuration (CI). Dans cet autre champ, vous pouvez définir des conditions de filtrage afin que seuls les incidents de sécurité liés à votre événement déclencheur déclenchent automatiquement le profil.

Remarque : Accédez à la page Configuration du profil uniquement après avoir saisi les détails du profil. Pour plus d'informations, consultez Créer un profil d'aptitude pour l'intégration de CrowdStrike Falcon Insight.

Procédure
1. Sur la page Configuration du profil, examinez et configurez les sections suivantes :

Définir un critère d'incident (automatisation)

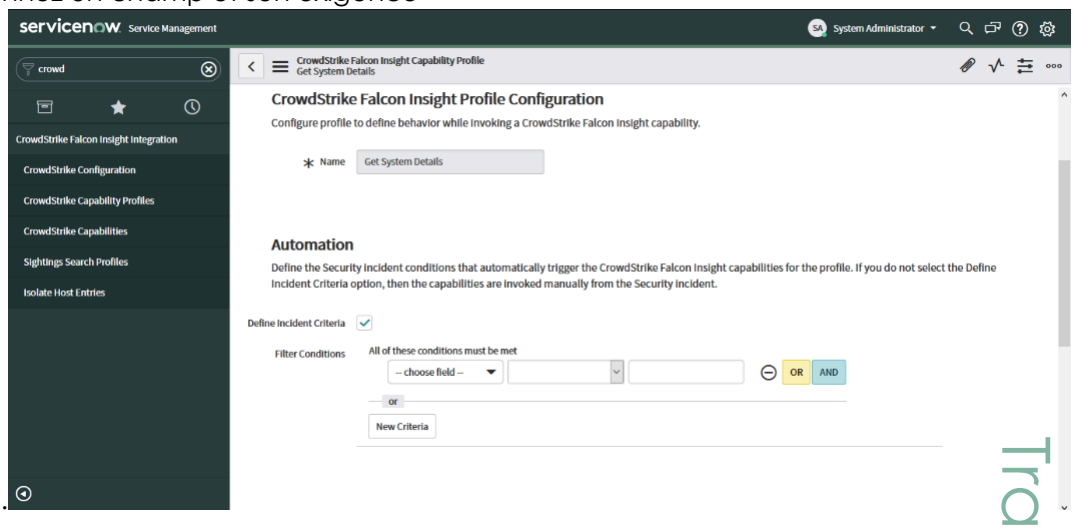
Définissez les conditions d'incident de sécurité qui déclenchent automatiquement les CrowdStrike Falcon Insight options du profil. Si vous ne sélectionnez pas l'option **Définir des critères d'incident** , les options sont invoquées manuellement à partir de l'incident de sécurité.

Traduction automatique

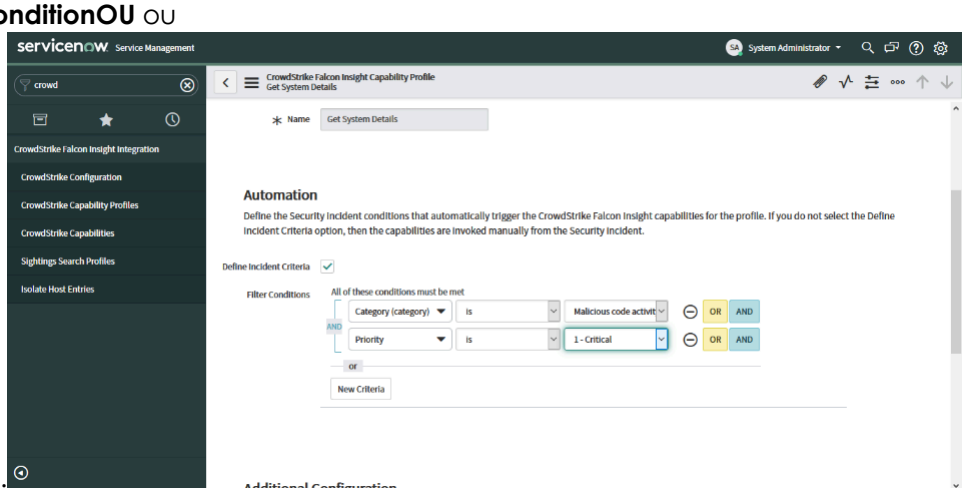
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Sélectionnez l'option **Définir les critères d'incident** .

b. Pour définir les conditions, dans la section Conditions de filtre, sélectionnez un champ et son exigence correspondante.



c. Dans le champ **Nouveau critère**, saisissez les nouveaux critères, puis définissez **la conditionOU** ou ET.

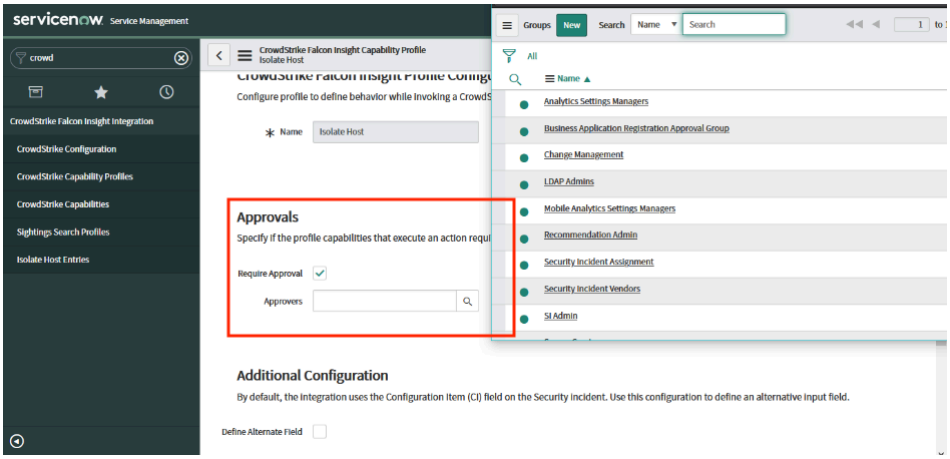


Approbations

Pour fournir un niveau de contrôle supplémentaire lorsque vous utilisez les options de CrowdStrike Falcon Insight, sélectionnez l'option **Exiger l'approbation** . L'option d'approbations de la configuration du profil s'affiche uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte.

Remarque : L'autorité d'approbation est affectée à l'utilisateur ayant le rôle sn_si.admin. Vous pouvez également réaffecter cette autorité d'approbation à un groupe d'approbation. Pour plus d'informations, consultez Configurer un groupe d'approbation.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Configuration supplémentaire

Sélectionnez un autre champ sur l'incident de sécurité pour afficher toutes les données CI correspondantes que vous trouvez lors de l'analyse de vos actifs. Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité.

a. Sélectionnez l'option **Définir un autre champ** .

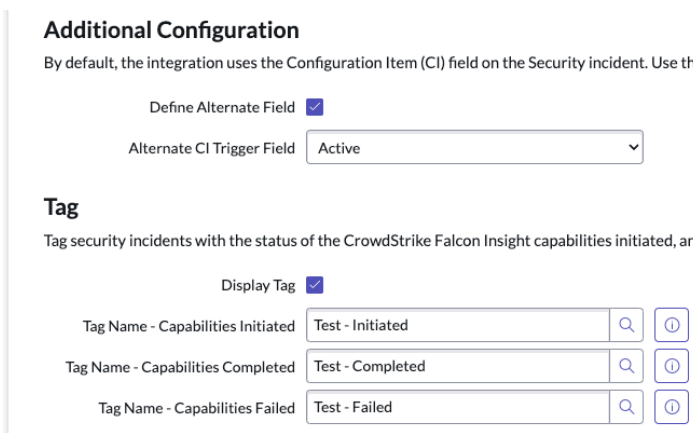
b. Dans le **champ Autre déclencheur de CI**, sélectionnez un champ d'entrée.

> **Remarque :** Pour plus d'informations, consultez Comprendre le fonctionnement des conditions de déclenchement avec un élément de configuration pour un profil.

Balises

Pour baliser les incidents de sécurité avec les CrowdStrike Falcon Insight balises Options-Initié, Capacités-Terminées et Capacités-Échouées, sélectionnez l'option **Afficher les balises** . Par défaut, cette option est désactivée pour tous les profils.

> **Remarque :** Ces balises sont fournies avec le système de base. Vous pouvez créer vos propres balises si nécessaire.



2. Cliquez sur **Terminé**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comment fonctionnent les conditions de déclenchement avec un élément de configuration pour un profil

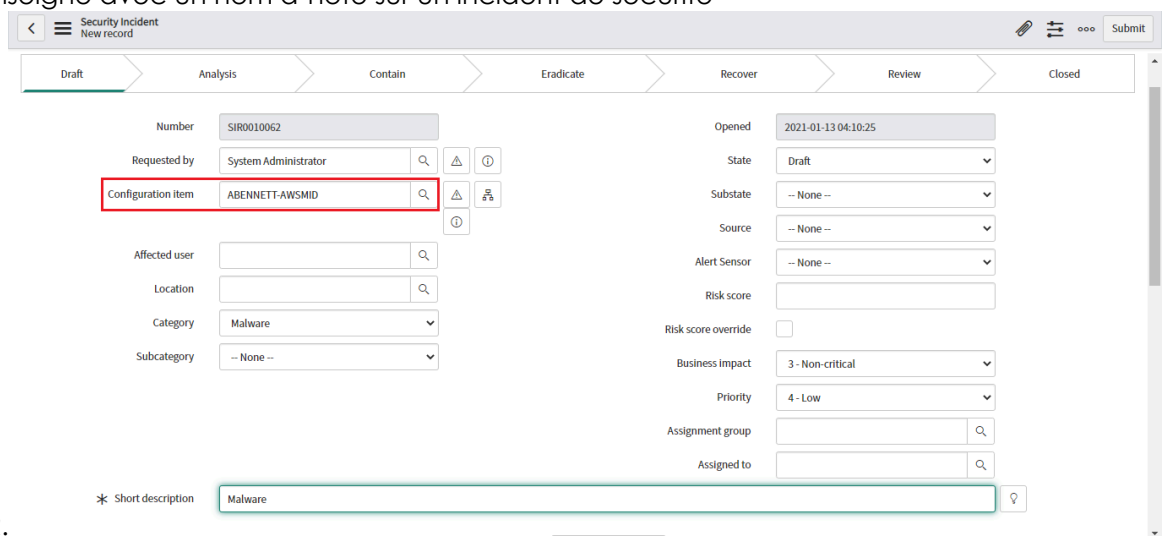
Vous pouvez configurer les paramètres du profil afin qu'un profil s'exécute uniquement lorsqu'un ensemble de conditions spécifiques est satisfait ou vous pouvez configurer un profil pour rechercher des valeurs de champ spécifiques sur un incident de sécurité.

Après avoir créé un profil et sélectionné les CrowdStrike Falcon Insight options sur lesquelles vous souhaitez que le profil s'exécute, vous pouvez définir des conditions de déclenchement afin que votre profil s'exécute automatiquement lorsque les valeurs de champ par défaut correspondent à l'incident Now Platform de sécurité.

Par défaut, l'intégration utilise le champ **Élément de configuration** (CI) sur un incident de sécurité. Ce champ est utilisé pour faire correspondre vos ID d'actifs avec les informations stockées dans la Now Platform base de données. Lorsqu'un incident de sécurité SIR est créé par un événement de sécurité et qu'un profil est activé, vos actifs sont analysés à la recherche d'une valeur correspondante sur le nom d'hôte ou une adresse IP.

Lorsqu'une valeur correspondante est trouvée dans la base de données, ces données sont collectées à partir de la console et extraites vers votre CrowdStrike Falcon InsightNow Platform instance où elles sont affichées sur les listes connexes d'un incident de sécurité.

L'exemple suivant montre un champ d'élément de configuration renseigné avec un nom d'hôte sur un incident de sécurité



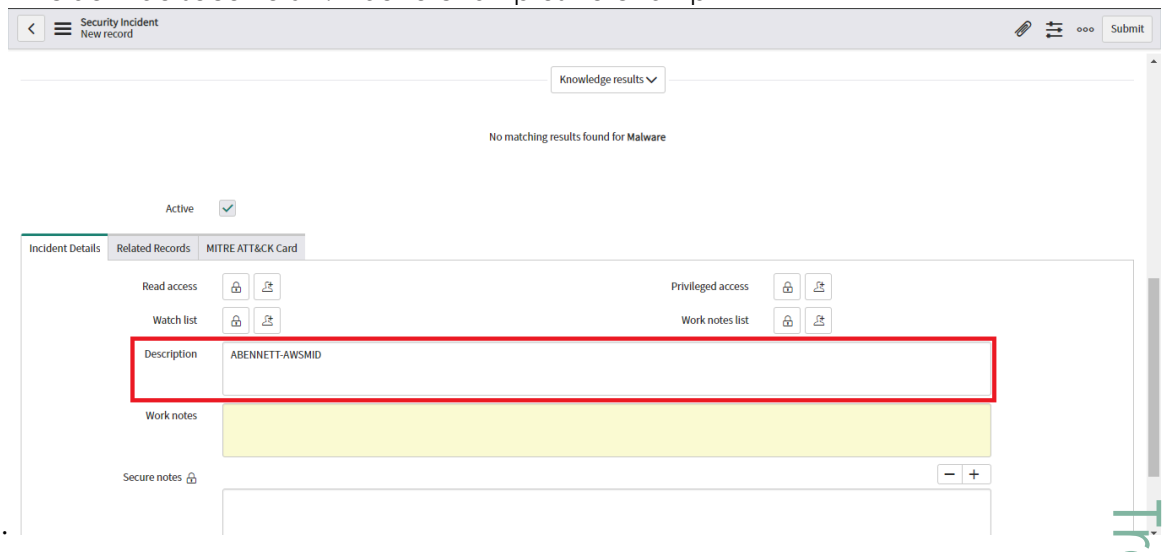
SIR.

Lorsque le champ **Élément de configuration** (CI) n'est pas renseigné avec un nom d'hôte ou une adresse IP qui correspond à la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour afficher toutes les données CI correspondantes que vous trouvez lors de l'analyse de vos actifs.

Lors de la configuration du profil, vous pouvez sélectionner un autre champ **de déclenchement CI** pour l'identification du point de terminaison afin de vous assurer que les données CI issues de la CrowdStrike Falcon Insight recherche sont renseignées sur l'incident de sécurité associé. Vous pouvez sélectionner n'importe quel champ de l'incident de sécurité comme champ de déclenchement CI alternatif, y compris les champs personnalisés que vous créez. Si le champ CI n'est pas renseigné pour l'incident de sécurité associé lors de la création de l'incident, sélectionnez l'autre champ CI pour vous assurer que vos profils sont déclenchés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'exemple suivant montre un autre champ renseigné avec un nom d'hôte sur un incident de sécurité SIR. L'autre champ est le champ **Description** .



Vérifier les CrowdStrike Falcon Insight conditions de déclenchement du profil

Testez le profil et vérifiez que les filtres de condition de déclenchement que vous avez configurés fonctionnent comme prévu.

Avant de commencer

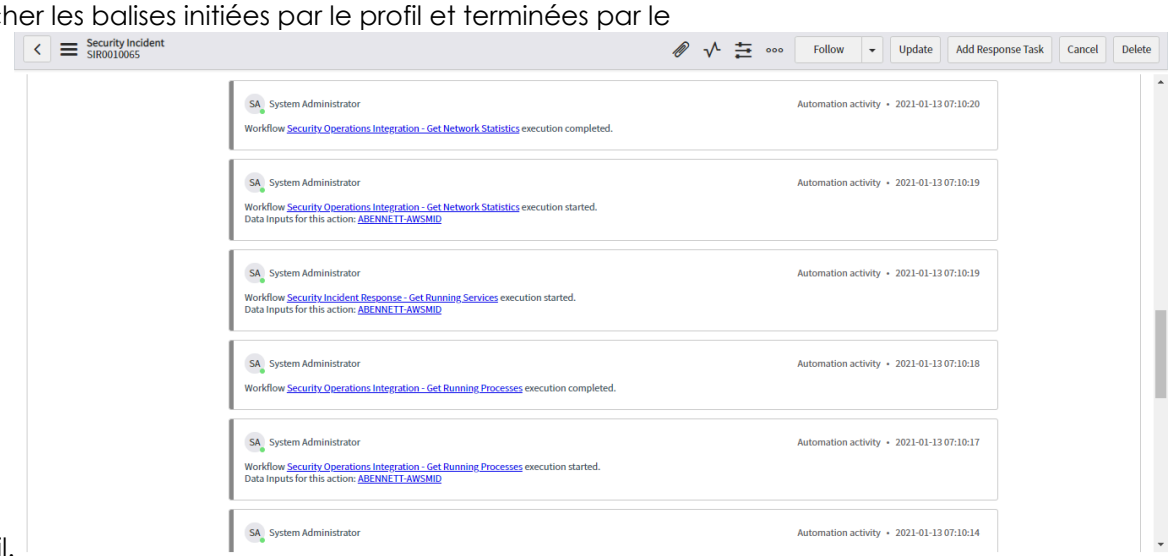
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Activez le profil basé sur les conditions de déclenchement configurées que vous avez spécifiées afin de pouvoir afficher les résultats de la requête dans les Now Platform incidents de sécurité.

Procédure

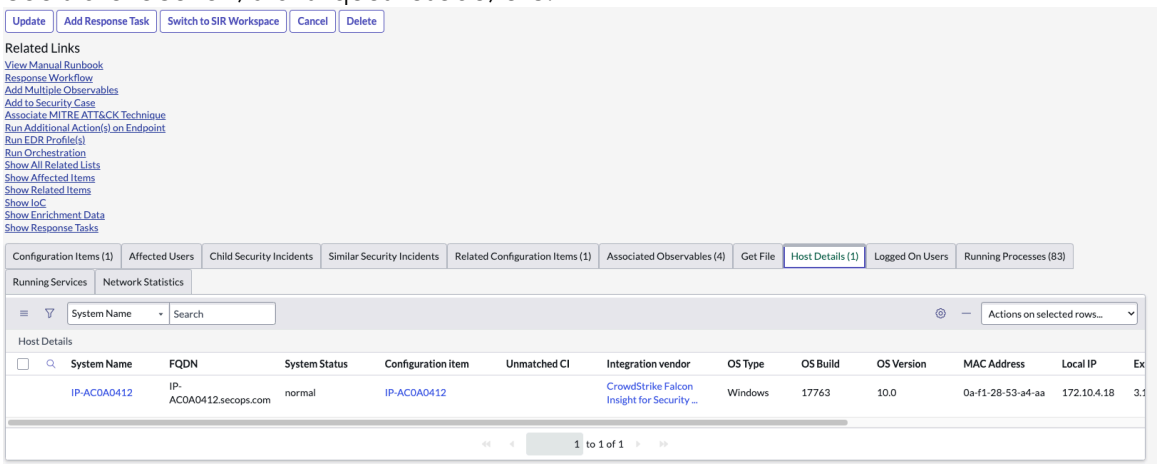
1. Accédez à la **Tout** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez **Nouveau** pour créer un incident de sécurité.
3. Pour créer un incident de sécurité, renseignez les informations requises et cliquez sur **Enregistrer**.
4. Passez en revue la section Notes de travail et activités pour afficher les balises initiées par le profil et terminées par le profil.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Passez en revue les détails dans les listes connexes Détails tels que Obtenir le fichier, Détails de l'hôte CrowdStrike Falcon Insight , Utilisateurs connectés, Processus en cours, Services en cours d'exécution, Statistiques réseau, etc.



Déclencher manuellement un CrowdStrike Falcon Insight profil à partir d'un incident de sécurité

Déclenchez un profil manuellement après avoir examiné un incident de sécurité.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

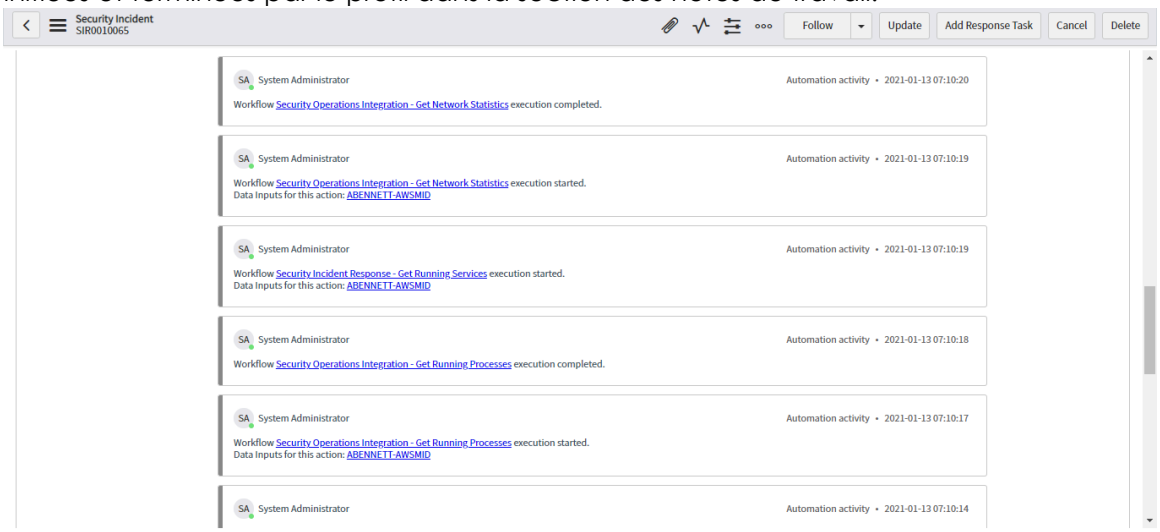
Une fois que vous avez activé le profil, en fonction des conditions de déclenchement configurées, vous pouvez afficher les résultats de la requête dans les Now Platform incidents de sécurité. CrowdStrike Falcon Insight vous permet également d'exécuter des options individuelles sur des éléments de configuration (CI) sans utiliser de profil.

Procédure

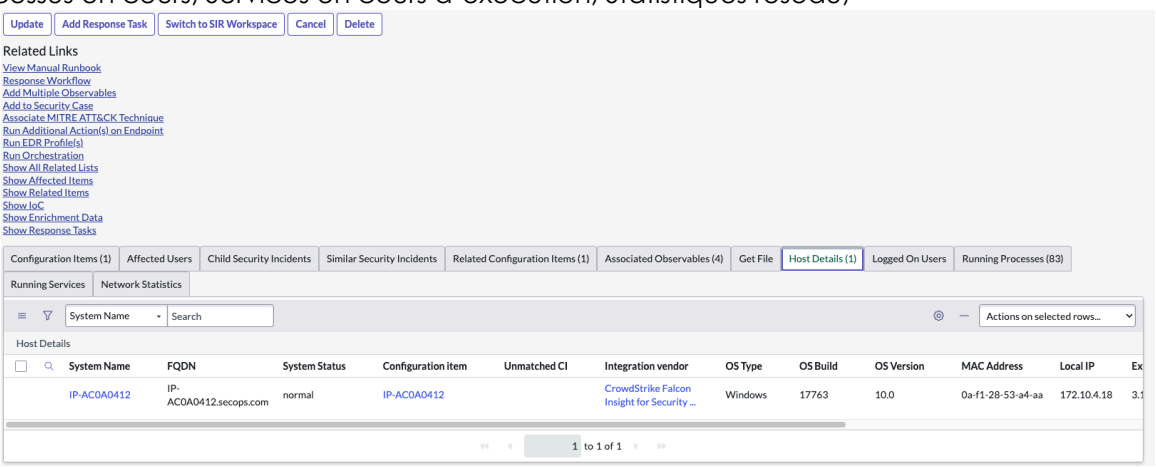
1. Accédez à la **Tout** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les CrowdStrike Falcon Insight informations.
3. Dans la section des listes connexes, sélectionnez **Exécuter le(s) profil(s) EDR**.
4. Parcourez et sélectionnez un profil dans la liste des profils disponibles.
5. Sélectionnez **Inclure le CI connexe** pour exécuter ce profil sur tous les CI connexes du profil.
   Par exemple, si cinq CI sont associés à l'incident de sécurité, le profil sélectionné s'exécute sur les cinq CI.
6. Cliquez sur **Envoyer**.
   Le profil sélectionné est déclenché manuellement. Vous pouvez passer en revue la section des notes de travail et des activités, ainsi que les balises

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

initiées et terminées par le profil dans la section des notes de travail.



7. Les résultats apparaissent sous la forme de listes connexes telles que Obtenir un fichier, Détails de l'hôte, Utilisateurs connectés, Processus en cours, Services en cours d'exécution, Statistiques réseau, etc.



8. Pour exécuter des options individuelles sur un CI, procédez comme suit :

   a. Dans la liste connexe Éléments de configuration, sélectionnez le CI requis.

   b. Cliquez sur la liste déroulante **Actions sur les lignes sélectionnées...** , puis sélectionnez l'aptitude requise que vous souhaitez exécuter pour le CI sélectionné. Par exemple, Isoler l'hôte.

   c. Recherchez l'implémentation de l'aptitude requise pour le CI à l'aide de l'option de recherche et sélectionnez **Isoler l'hôte de CrowdStrike Falcon Insight**.

   d. Cliquez sur **Isoler l'hôte** pour l'exécuter sur le CI sélectionné.

Créer et configurer un profil pour la recherche de perception

Utilisez la recherche de perceptions pour CrowdStrike Falcon Insight localiser les ordinateurs infectés sur le réseau de votre organisation et pour traiter les tickets de Security Incident Response.

Avant de commencer

Rôle requis : sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Sélectionnez un ou plusieurs observables et effectuez une recherche de perception manuelle pour CrowdStrike Falcon Insight déterminer la récurrence d'une menace dans le temps.

Procédure

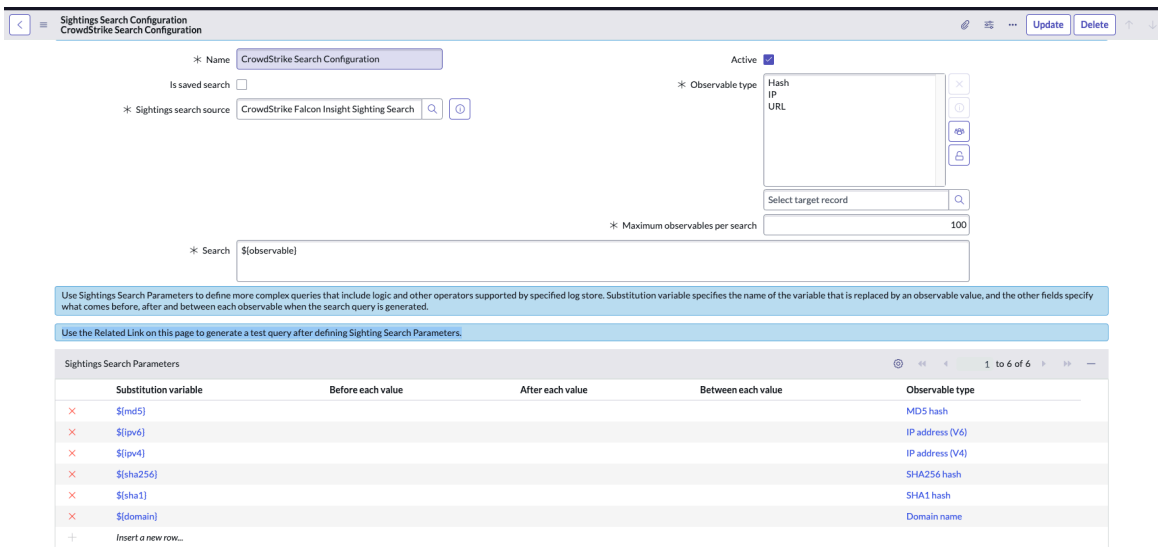
1. Accédez à la **Tout** > **Intégration de CrowdStrike Falcon Insight** > **Profils de recherche de perception**.
2. Cliquez sur **Nouveau**.
3. Configurez ce profil pour déterminer les serveurs à rechercher pour une option de recherche CrowdStrike Falcon Insight spécifique.
4. Renseignez les champs du formulaire :

Champ	Description
Nom	Nom du profil de recherche de perceptions.
Est une recherche enregistrée	La configuration de recherche enregistrée est créée si vous sélectionnez cette option.
Source de recherche de perceptions	La source de la recherche d'observations. Sélectionnez la **recherche d'observation de CrowdStrike Falcon Insight** comme source.
Actif	Option permettant d'indiquer si l'élément supplémentaire est actif ou non.
Type d'observable	L'intégration de CrowdStrike Falcon Insight prend en charge les types d'observables suivants : ◦ Hachage ◦ IP ◦ URL La recherche de perception est prise en charge pour les types d'observables suivants : ◦ Nom du domaine ◦ Adresse IP (V4) ◦ Adresse IP (V6) ◦ Hachage MD5 ◦ Hachage SHA1 ◦ Hachage SHA256
Nombre maximum d'observables par recherche	Nombre maximal d'observables que vous pouvez afficher à partir d'une requête de recherche.
Rechercher	La chaîne de recherche par défaut est `$(observable),` mais vous pouvez définir votre propre requête de recherche en

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	spécifiant les paramètres pris en charge par l'intégration CrowdStrike Falcon Insight .
Paramètres de la recherche de perceptions	Paramètres pour définir des requêtes plus complexes qui incluent la logique et d'autres opérateurs pris en charge par le magasin de journaux spécifié Vous pouvez utiliser les liens connexes en bas de la page pour générer une requête de test après avoir défini des paramètres de recherche de perceptions.



5. Cliquez sur **Envoyer**.
   La configuration est terminée et vous pouvez invoquer la recherche de perceptions à partir de l'incident Now Platform de sécurité.
6. Pour vérifier la configuration et exécuter une recherche de perception, effectuez les étapes suivantes :

   a. Ouvrez un incident de sécurité, faites défiler jusqu'au bas de l'incident de sécurité, puis cliquez sur **Afficher toutes les listes connexes**.

   b. Si vous sélectionnez un ou plusieurs éléments de configuration (CI) dans les listes connexes Processus **en cours d'exécution** .

   > **Remarque :** Si vous exécutez une recherche de perception pour un CI à partir de la liste connexe Processus en cours, il s'agira uniquement d'une recherche de perception de hachage de processus.

   c. Cliquez sur la liste déroulante **Actions sur les lignes sélectionnées...** , puis sélectionnez **Exécuter la recherche d'observations CrowdStrike**.

   d. Rechercher le profil de recherche de perception requis à l'aide de l'option de recherche.

   e. Sélectionnez le profil de recherche de perception requis, puis cliquez sur **Soumettre**.

Traduction automatique

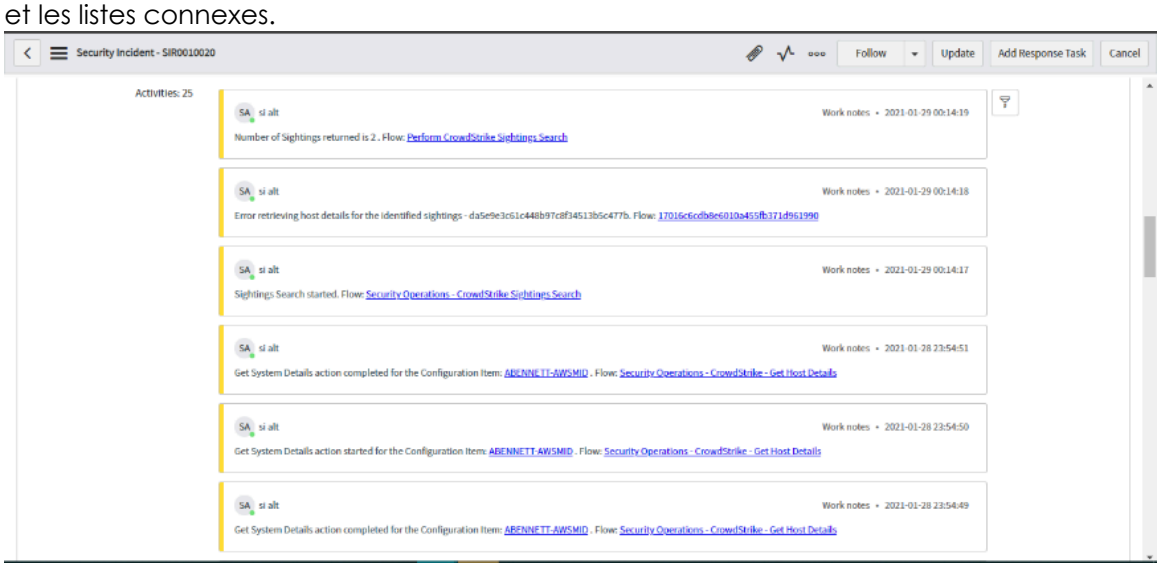
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Si vous sélectionnez un ou plusieurs observables dans les listes connexes **Observables associés** .

g. Cliquez sur la liste déroulante **Actions sur les lignes sélectionnées...** , puis sélectionnez **Exécuter la recherche de perceptions**.

h. Dans la fenêtre contextuelle, sélectionnez une valeur aléatoire et cliquez sur **Rechercher**.

i. Une fois la recherche terminée, validez les résultats et les détails dans les notes de travail et les listes connexes.



j. Sélectionnez l'onglet **Observations** pour afficher les détails de la perception.

k. Cliquez sur l'icône **Aperçu** à côté du CI pour afficher plus d'informations sur les détails d'observation CrowdStrike.

l. Cliquez sur les **détails de la recherche de perceptions** pour afficher les détails de la recherche de perceptions, puis cliquez sur l'onglet **Résultats de recherche de perceptions** pour obtenir les résultats de la recherche.

Configurer et déclencher des actions supplémentaires dans CrowdStrike Falcon Insight

L'intégration CrowdStrike Falcon Insight prend en charge l'exécution d'actions supplémentaires telles que l'expression régulière (regex). L'intégration CrowdStrike Falcon Insight fournit 40 actions supplémentaires avec le système de base.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tout** > **Intégration de CrowdStrike Falcon Insight** > **Actions supplémentaires de CrowdStrike**.
2. Cliquez sur **Nouveau** pour créer votre propre action supplémentaire ou sélectionnez une action existante fournie avec le système de base.
   Par exemple, créons une action supplémentaire.
3. Renseignez les champs du formulaire.

Traduction automatique

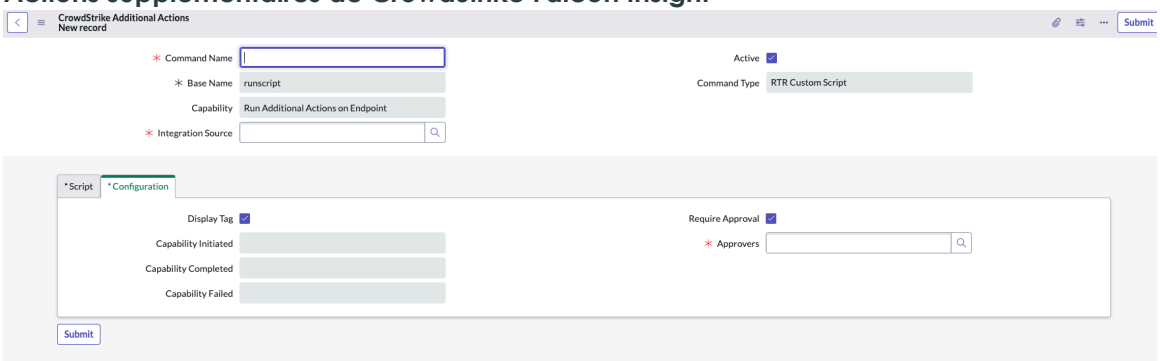
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom de la commande	Nom de la commande pour l'action supplémentaire. Par exemple, reg set.
Nom de base	Nom de base de l'action supplémentaire. Ce champ est défini par défaut. Par exemple, reg.
Option	Nom de l'aptitude pour l'action supplémentaire. Ce champ est défini par défaut. Par exemple, Exécuter des actions supplémentaires sur le point de terminaison.
Source d'intégration	Source de l'action supplémentaire. Par exemple, Intégration de CrowdStrike Falcon Insight.
Actif	Option permettant d'indiquer si l'élément supplémentaire est actif ou non.
Type de commande	Type de commande pour l'action supplémentaire. Ce champ est défini par défaut. Par exemple, Script personnalisé RTR.
Script	◦ **Type de système d'exploitation** : option permettant de sélectionner le type de système d'exploitation pour votre script. Sélectionnez l'une des options suivantes : ▪ **Windows** ▪ **Mac OS X** ▪ **Linux** ▪ **Aucun** ◦ **Script** : option permettant d'entrer dans votre script si vous avez sélectionné l'un des systèmes d'exploitation suivants, à l'exception de l'option Aucun.
Configuration	◦ **Balise d'affichage** : option permettant d'afficher la balise de la configuration. Vous pouvez sélectionner la balise pour les champs suivants : ▪ Aptitude : initiée. Par exemple, reg set - Initiated. ▪ Aptitude : terminée. Par exemple, reg set - Completed. ▪ Aptitude : échec. Par exemple, reg set - Failed. ◦ **Exiger l'approbation** : option permettant de sélectionner un approbateur ou un groupe devant approuver la configuration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

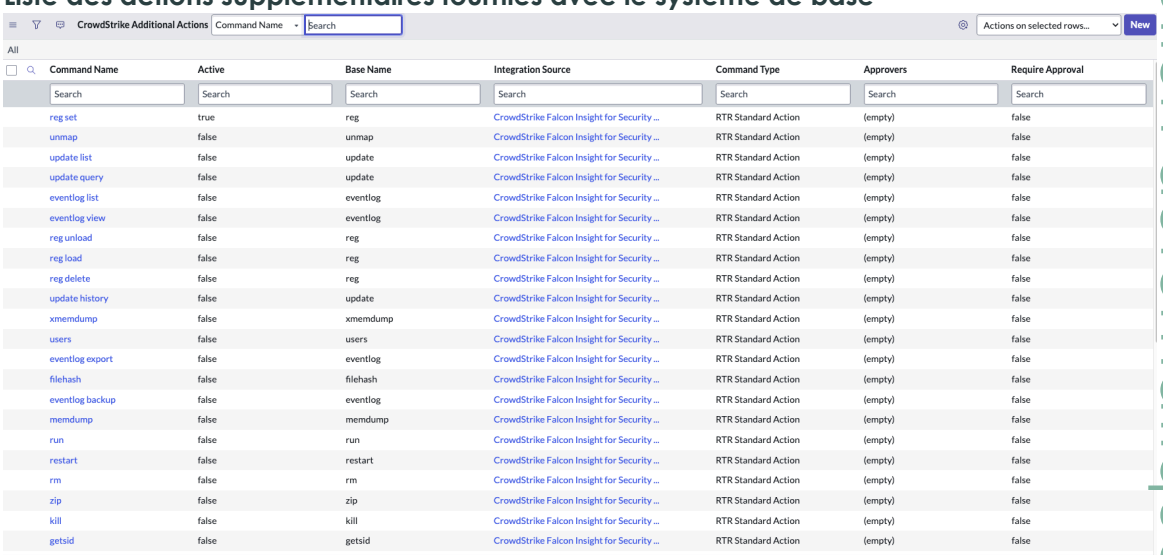
Actions supplémentaires de CrowdStrike Falcon Insight



4. Cliquez sur **Envoyer**.
5. Vous pouvez également choisir parmi les actions supplémentaires existantes suivantes. Le système de base fournit 40 actions supplémentaires que vous pouvez utiliser pour effectuer des configurations supplémentaires.

   Remarque : Assurez-vous d'ouvrir la liste des actions supplémentaires CrowdStrike et définissez l'action supplémentaire requise sur **vrai**, sinon l'action supplémentaire ne sera pas disponible dans l'espace de travail.

Liste des actions supplémentaires fournies avec le système de base



6. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
7. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec l'exécution des actions supplémentaires sur le point de terminaison.

   a. Dans la section Liens connexes, cliquez sur **Exécuter des actions supplémentaires sur le point de terminaison**.

   b. Parcourez et sélectionnez l'aptitude requise.
   Par exemple, cliquez sur Reg **Set** capability.

   c. Sélectionnez **Inclure le CI connexe** pour exécuter les actions supplémentaires sur tous les CI connexes du point de terminaison.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Vous pouvez définir la **sous-clé** pour exécuter les actions supplémentaires sur le point de terminaison.
Cette sous-clé peut être une clé HKLM/logicielle/nouvelle.

8. Pour lancer l'exécution d'actions supplémentaires sur le point de terminaison, cliquez sur **Exécuter une action supplémentaire**.
9. Affichez les activités d'automatisation de l'exécution et validez-les.
10. Validez l'état de l'action sur les listes connexes Actions supplémentaires sur le point de terminaison.

Utilisation de l'intégration CrowdStrike Falcon Insight dans Analyst Workspace

Utilisez l'intégration CrowdStrike Falcon Insight pour tirer parti des CrowdStrike Falcon Insight options de l'espace de travail d'analyste SIR.

Avant de commencer
Rôle requis : sn_si.admin

Avant d'utiliser CrowdStrike Falcon Insight l'intégration dans l'espace de travail Réponse aux incidents de sécurité, vous devez la ServiceNow Store télécharger et la configurer. Pour plus d'informations, consultez Mise en route de l'intégration CrowdStrike Falcon Insight.

Pourquoi et quand exécuter cette tâche
Vous pouvez utiliser l'intégration CrowdStrike Falcon Insight pour effectuer des actions de rattrapage sur les points de terminaison en temps réel, utiliser des profils pour recueillir des détails sur l'hôte et effectuer des requêtes ou des actions spécifiques sur le point de terminaison à l'aide de l'espace Réponse aux incidents de sécurité de travail.

L'intégration CrowdStrike Falcon Insight permet aux analystes d'utiliser les options suivantes CrowdStrike Falcon Insight dans l'espace de Réponse aux incidents de sécurité travail Analyst :

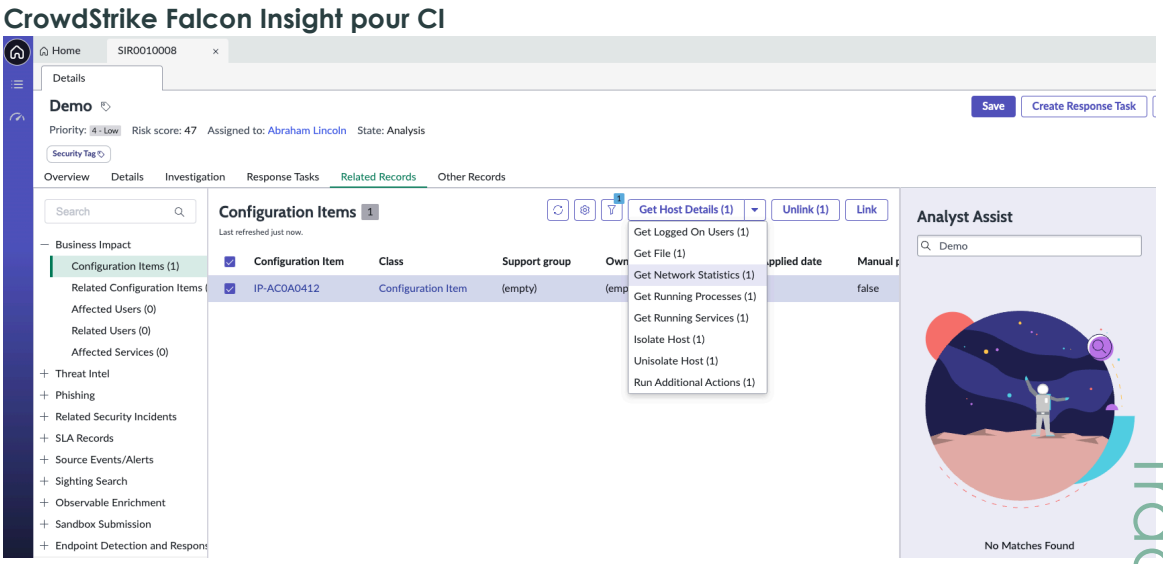
- **Obtenir les détails de l'hôte**
- **Obtenir les utilisateurs connectés**
- **Obtenir les statistiques réseau**
- **Obtenir les processus en cours d'exécution**
- **Obtenir les services d'exécution**
- **Isoler l'hôte**
- **Supprimer l'isolement**
- **Obtenir un fichier**

Procédure

1. Dans l'espace de travail SIR, ouvrez l'incident de sécurité requis et sélectionnez l'onglet **Enregistrements connexes** .
2. Vous pouvez utiliser les options de CrowdStrike Falcon Insight figurant sur la liste connexe Impact sur l'entreprise à des fins d'analyse.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Sélectionnez un **élément de configuration**, puis choisissez une aptitude dans la liste déroulante.



b. Sélectionnez l'implémentation de **CrowdStrike Falcon Insight** et cliquez sur **Soumettre**. L'option Obtenir les statistiques réseau est invoquée sur le CI. Vous pouvez afficher les notes de travail pour les résultats et les conclusions.

3. Vous pouvez utiliser les options de CrowdStrike Falcon Insight de la liste connexe **Endpoint Detection and Reponse (EDR)** pour l'analyse.

a. Dans la liste connexe PEPT (Endpoint Detection and Reponse), choisissez un EDR dans la liste.

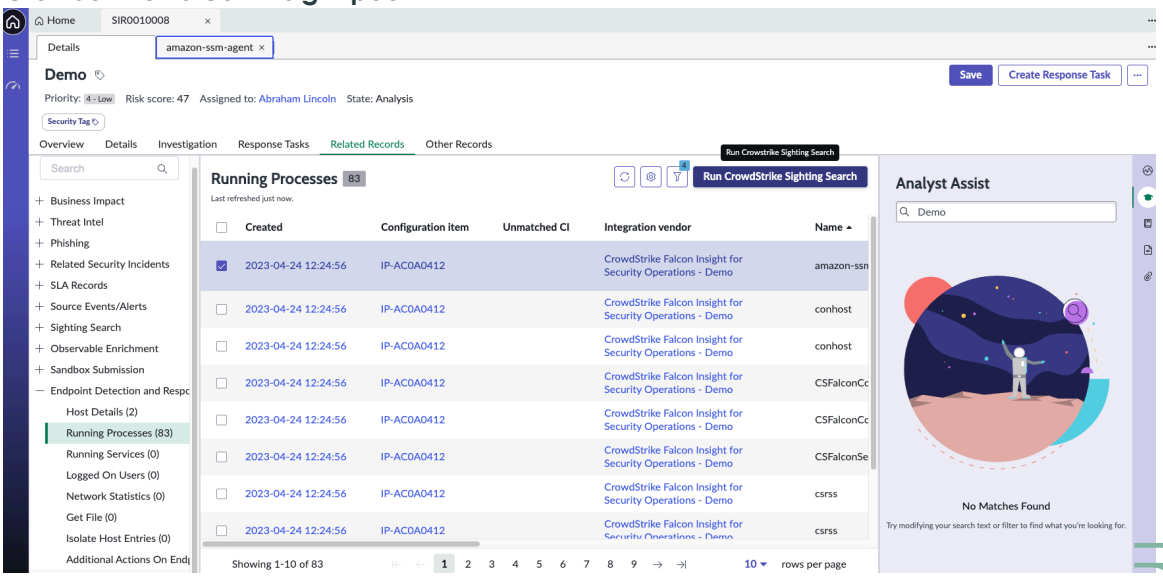
b. Cliquez sur un processus en cours particulier pour afficher les détails du processus en cours d'exécution de CrowdStrike Falcon Insight.

c. Pour exécuter une recherche d'observation CrowdStrike Falcon sur un processus en cours particulier, sélectionnez le processus en cours et cliquez sur **Exécuter l'observation CrowdStrike**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

CrowdStrike Falcon Insight pour EDR



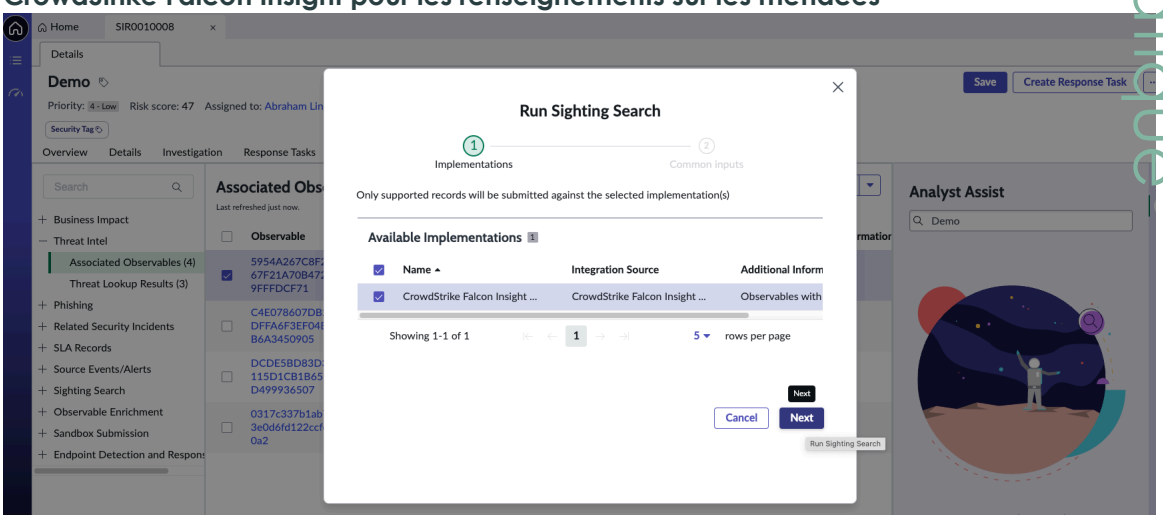
d. Sélectionnez l'implémentation de **CrowdStrike Falcon Insight** et cliquez sur Exécuter la **recherche**.
Ensuite, une recherche de perception de hachage est exécutée sur le processus en cours sélectionné. Vous pouvez afficher les notes de travail pour les résultats et les conclusions.

4. Vous pouvez utiliser les options de CrowdStrike Falcon Insight sur **Threat Intelligence** pour l'analyse.

a. Dans le groupe Threat Intel, sélectionnez un **observable**, puis choisissez une CrowdStrike Falcon Insight aptitude dans la liste déroulante.

b. Sélectionnez l'implémentation de **CrowdStrike Falcon Insight** et cliquez sur **Suivant**.

CrowdStrike Falcon Insight pour les renseignements sur les menaces



c. Dans la fenêtre contextuelle Sélectionner la date/heure, sélectionnez une valeur aléatoire et cliquez sur **Soumettre**.
Ensuite, une recherche d'observation est exécutée sur l'observable sélectionné. Vous pouvez afficher les notes de travail pour les résultats et les conclusions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration de CrowdStrike Falcon X Sandbox pour Security Operations

Avec l'intégration CrowdStrike Falcon X SandboxOpérations de sécurité , vous pouvez soumettre des fichiers et des URL dans le cadre du processus de réponse aux incidents de sécurité afin d'effectuer une analyse détaillée des menaces et CrowdStrike Falcon X Sandbox des logiciels malveillants.

L'intégration CrowdStrike Falcon X Sandbox vous fournit un environnement virtuel isolé à la demande dans lequel vous pouvez effectuer l'analyse de programme malveillant et fournir des résultats à l'incident ServiceNow de sécurité via l'intégration.

Lorsque vous soumettez vos incidents de programme malveillant, ils sont conservés dans le cadre de l'enregistrement de l'incident de sécurité. Vous pouvez utiliser ces enregistrements pourrésoudre un incident ou d'autres incidents et automatiser la soumission des fichiers et des URL.

L'intégration prend en charge l'automatisation des playbooks de réponse aux hameçonnages et aux programmes malveillants, ce qui permet au personnel de votre Opérations de sécurité centre d'être plus productif et efficace dans la réponse aux incidents de sécurité.

Avantages clés

Grâce à cette intégration, vous pouvez effectuer les opérations suivantes :

- Automatisez la soumission de fichiers et d'URL à partir d'e-mails d'hameçonnage signalé par les utilisateurs (URP), d'e-mails, de pièces jointes et d'autres incidents de sécurité.
- Soumettez ou soumettez manuellement des fichiers et des URL précédemment analysés pour une analyse mise à jour.
- Créez plusieurs configurations de soumission qui appliquent CrowdStrike Falcon X Sandbox automatiquement des paramètres de soumission tels que le système d'exploitation, le type d'analyse et les options d'exécution.
- Analysez les résultats relatifs aux programmes malveillants et aux menaces dans un rapport au format HTML au sein de l'incidentSIR. Vous pouvez afficher lesrésultats de la recherche et l'historique des indicateurs pour les fichiers et les URL qui ont été analysés plusieurs fois.
- Marquez ServiceNow les incidents avec l'état de traitement de la soumission, ainsi que les résultats de la recherche de menaces.

Voir aussi

Identificateur de document	Titre de document
CrowdStrike Falcon X Sandbox	CrowdStrike Falcon Sandbox FAQ
ServiceNow site web de la documentation produit	Site web de la documentation produit ServiceNow

Démarrer l'intégration CrowdStrike Falcon X Sandbox

Activez et configurez l'interface CrowdStrike Falcon X Sandbox avec votre instance et Réponse aux incidents de sécurité votre ServiceNow produit.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Avant de pouvoir utiliser l'intégration CrowdStrike Falcon X Sandbox pour Security Operations, vous devez la télécharger à partir du ServiceNow Store.
- Passez en revue la liste de vérification de configuration suivante et vérifiez que vous avez effectué toutes les tâches pour une intégration fluide CrowdStrike Falcon X Sandbox .

Rôle requis : admin, sn_si.admin

Liste de vérification

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform AND Réponse aux incidents de sécurité .	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • L'administrateur (admin) installe l'intégration sandbox à partir de l'App Store ServiceNow et attribue le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Le sn_si.admin crée et modifie la configuration et les paramètres globaux, puis affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). • L'analyste des incidents de sécurité (sn_si.analyst) répond aux incidents de sécurité, notamment en soumettant des fichiers et des URL à la boîte de dialogue et en analysant les résultats de soumission.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant de configurer cette intégration.	Cette intégration est prise en charge sur Paris et Orlando mises en production. Assurez-vous que ces modules d'extension dépendants sont installés. Ces modules d'extension permettent l'exécution d'actions et de Hub d'intégration flux : • ServiceNow Étape d'action du Centre d'intégration : REST (com.glide.hub.action_step.rest) • ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **Remarque :** Si vous ne trouvez pas de module d'extension, vous devrez peut-être le demander au ServiceNow personnel. Pour demander un module d'extension, suivez les étapes présentées dans Demander un module d'extension .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	Le Réponse aux incidents de sécurité module d'extension (com.snc.security_incident) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité Dépendance (com.snc.si_dep) **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Orchestration de support de sécurité **5.** Renseignements sur les menaces Support commun (requis pour que vousutilisiez les options d'intégration Sandbox) **6.** Trusted Security Circles **7.** Opérations de sécurité Assistant de configuration **8.** Réponse aux incidents de sécurité Pour plus d'informations sur la configuration de votre Now Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une application Security Operations et Activer une application ServiceNow Store.
Vérifiez que vous disposez d'une licence pour la clé API privée Falcon Sandbox et obtenez la CrowdStrike Falcon X Sandbox clé API complète.	Cette intégration prend uniquement en charge le cloud privé Falcon Sandbox. **Remarque :** Cette version ne prend pas en charge l'intégration de Falcon X. CrowdStrike Falcon X Sandbox offre une clé API restreinte auto-signée et une clé API complète mise à niveau. Utilisez la clé API

Traduction automatique

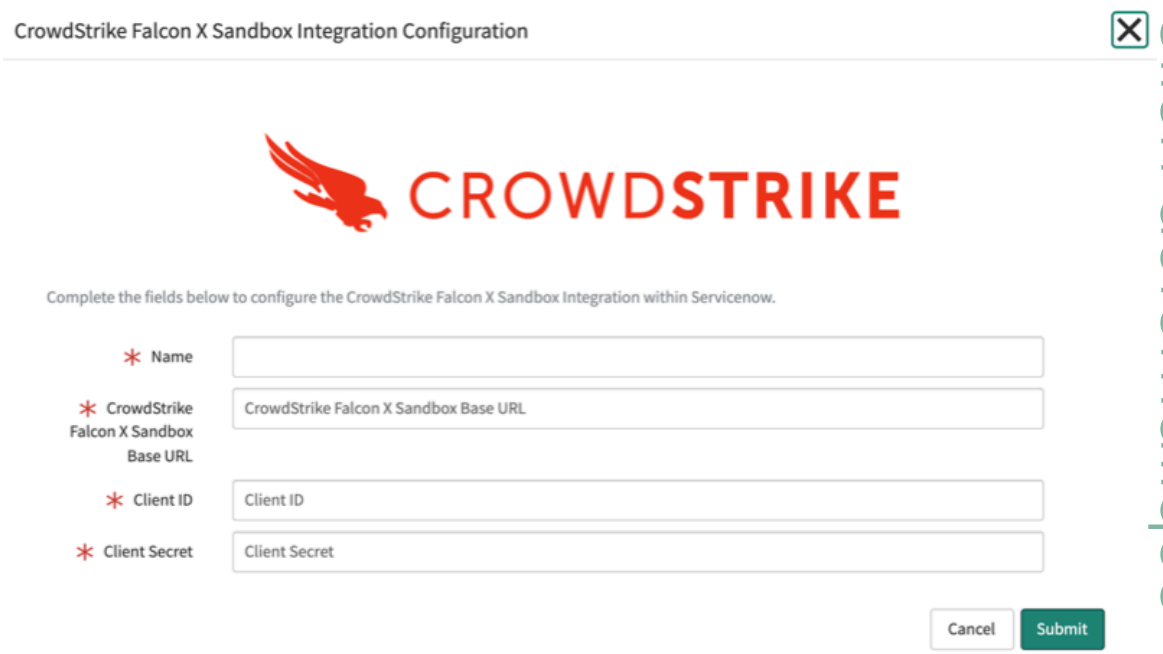
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	complète pour cette intégration , car elle permet un accès illimité aux soumissions automatisées. Pour plus d'informations, consultez la base de connaissances CrowdStrike Falcon Sandbox .

Procédure

1. Téléchargez l'intégration de CrowdStrike Falcon Sandbox for Security Operations à partir du ServiceNow Store.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette d'intégration CrowdStrike Falcon X Sandbox , puis cliquez sur **Configurer**.



4. Entrez les détails suivants pour terminer la configuration :

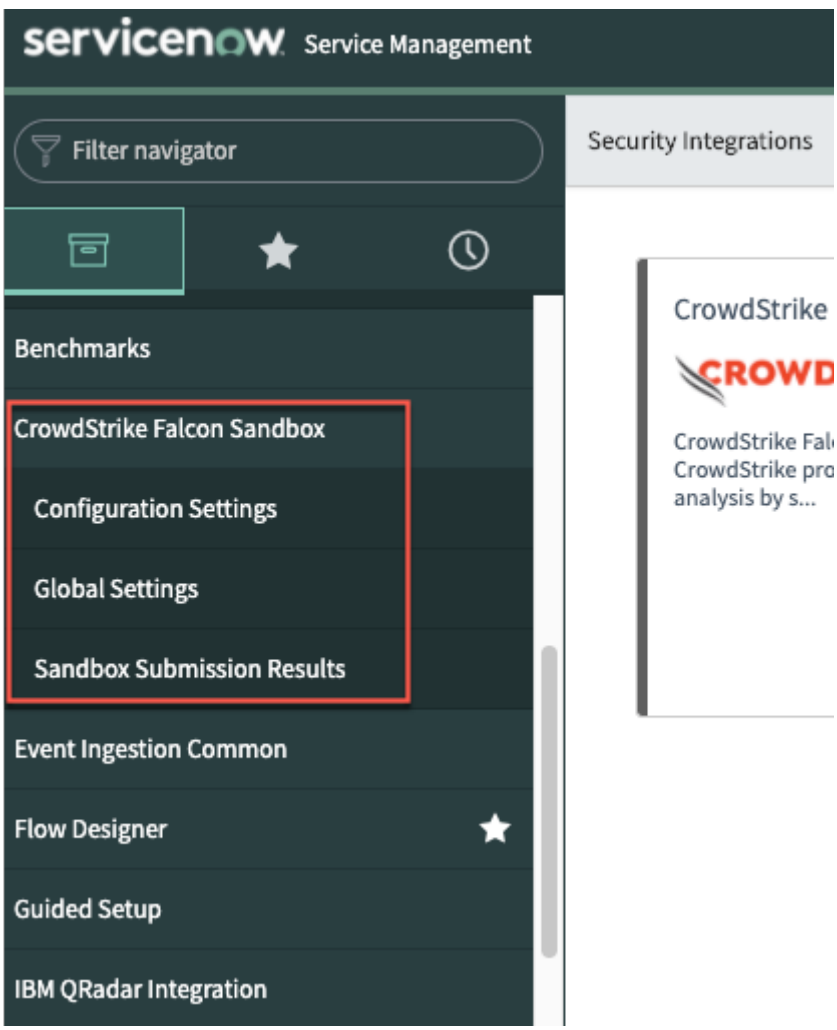
Champ	Description
Nom	Nom de cette intégration, par exemple : `demo-1`. Bien qu'il s'agisse d'un nom unique pour identifier la configuration sand box, vous ne pouvez configurer qu'une seule intégration par instance ServiceNow.
CrowdStrike Falcon Sandbox Base URL	S et l'URLde base de la boîte de dialogue Cette URL est disponible une fois que

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	vous avez configuré le sandbox.Par exemple, `https:// servicenow.falcon-sandbox.com` est une URL de base.
ID client	ID client de l'API OAuth2. Pour plus d'informations, reportez-vous à la section Clients et clés d'API .
Secret client	Clé secrète du client de l'API OAuth2. Pour plus d'informations, reportez-vous à la section Clients et clés d'API .

5. Cliquez sur **Envoyer**.
   Une fois le bac à sable validé et soumis, il est enregistré sous forme de vignette sur la page Intégrations de sécurité. Vous pouvez maintenant afficher le module Sandbox dans le navigateur d'application.



Que faire ensuite

Une fois l'intégration terminée, l'étape suivante consiste à configurer les configurations de soumission de Sandbox.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les configurations de soumission à Sandbox

Configurez la configuration Sandbox pour définir l'environnement d'analyse et les options d'exécution pour vos soumissions d'enregistrements d'incidents de sécurité pour l'analyse de programme malveillant.

Avant de commencer

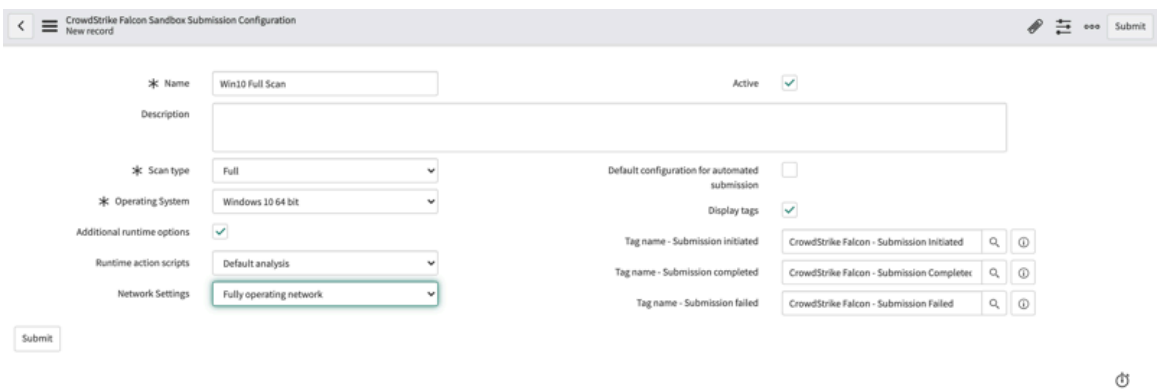
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Avant de pouvoir soumettre des fichiers ou des URL à l'utilisation CrowdStrike Falcon X Sandbox de l'intégration, vous devez configurer au moins une configuration de soumission. La configuration de la soumission définit le système d'exploitation Sandbox, le type d'analyse, les options de temps d'exécution et d'autres caractéristiques de gestion des incidents. Vous pouvez créer plusieurs configurations pour utiliser les différentes options disponibles dans l'environnementCrowdStrike Falcon X Sandbox.

Procédure

1. Accédez à la **Tout** > **Bac à sable CrowdStrike Falcon X** > **Paramètres de configuration**.
2. Cliquez sur **Nouveau**.



3. Renseignez les champs suivants pour créer une configuration pour un **type d'analyse** complète.

Champ	Description
Nom	Nom unique pour la configuration de la soumission. Ce nom apparaît aux analystes lorsqu'ils soumettent un fichier. Il est important de s'assurer que le nom est descriptif et facile à distinguer des autres configurations (par exemple, Win 10 Full Scan). Si le nom n'est pas unique, une erreur s'affiche et les noms d'enregistrements de configuration en double ne sont pas enregistrés.
Type d'analyse	Speut être saisi en tant que **Complet**. Un type **d'analyse rapide** fournit une analyse des menaces limitée.

Traduction automatique

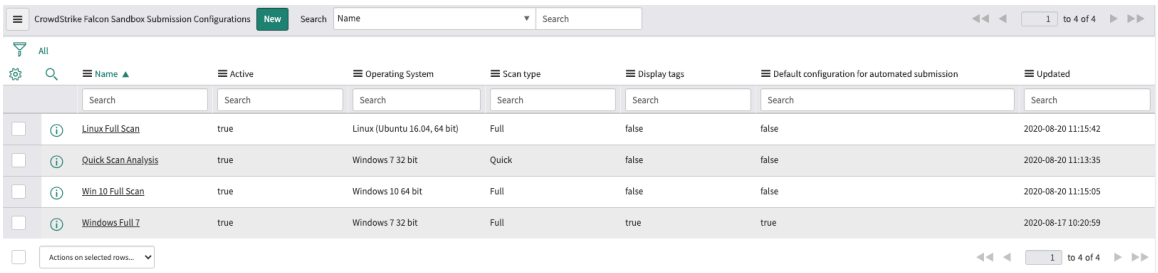
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Système d'exploitation	Unenvironnement de machine virtuelle nalysis dans lequel le sandbox analyse le fichier ou l'URL.
Actif	Peut être sélectionnée lors de la soumission manuelle de fichiers ou d'URL.
Configuration par défaut pour la soumission automatisée	Option qui est effacée par défaut. La sélection de cette option permet à cette configuration d'être disponible pour automatiser les soumissions d'analyse de programme malveillant. **Remarque :** Vous ne pouvez avoir qu'une seule configuration de soumission active comme configuration par défaut pour les soumissions automatisées.
Balises d'affichage	Option qui est effacée par défaut. Lorsque vous sélectionnez cette option, des balises s'affichent pour indiquer l'état d'une soumission de fichier ou d'URL. Le traitement de l'analyse peut prendre plusieurs minutes. Les balises d'affichage sont soumission initiée, soumission terminée ou soumission échouée.
Options Runtime supplémentaires	Option qui est effacée par défaut. Lorsque vous sélectionnez cette option, des paramètres d'exécution supplémentaires pris en charge par Sandbox sont disponibles.
Scripts d'action Runtime	Option qui vous permet d'utiliser un script decommande qui simule le comportement humain et interagitavec le fichier ou l'URL pendant l'analyse. https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ Voir CrowdStrike Falcon X Sandbox la documentation pour plus de détails.
Paramètres réseau	Option qui vous permet de sélectionner le type de paramètres réseau utilisés lors de la soumission d'une URL ou d'un fichier à Sandbox.

4. Cliquez sur **Envoyer**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois la configuration envoyée, elle est enregistrée en tant qu'enregistrement sur la page Paramètres de configuration. La configuration doit être **Actif** pour être utilisée dans les soumissions de set box.



Que faire ensuite

Une fois que vous avez configuré les soumissions de sandbox, l'étape suivante consiste à soumettre manuellement des fichiers ou des ULR à Sandbox

.

Soumettre manuellement les fichiers ou les URL au bac à sable (Sandbox)

Vous pouvez soumettre manuellement un fichier ou une URL à un bac à sable lorsque certains critères d'incident, tels que la catégorie Hameçonnage, sont remplis.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

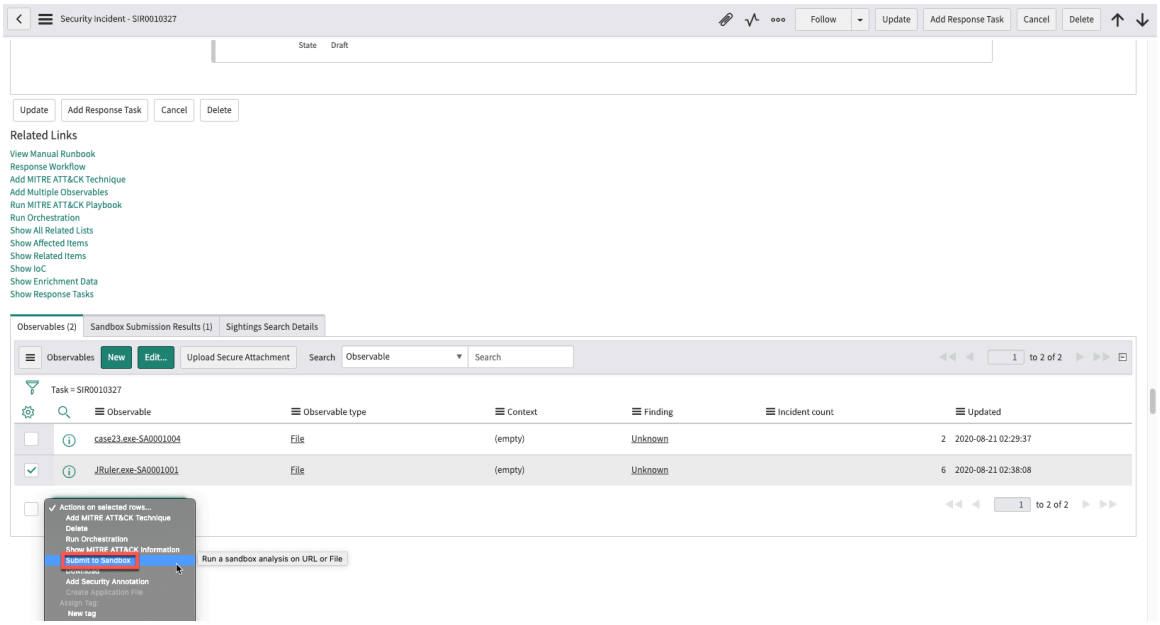
Après avoir examiné l'incident de sécurité et le fichier ou l'URL, vous pouvez sélectionner l'option **Soumettre au bac à sable** pour effectuer une analyse de programme malveillant.

Procédure

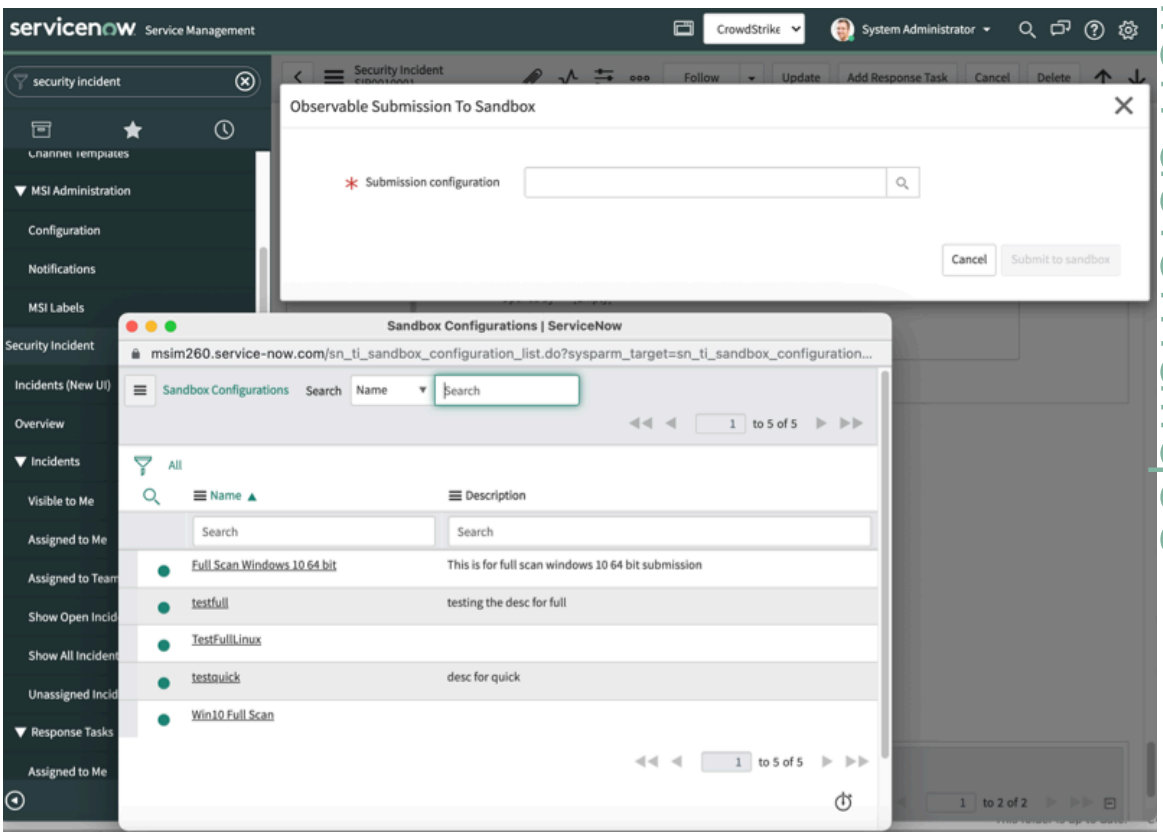
1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents** et ouvrez un incident de sécurité auquel vous souhaitez soumettre un enregistrement de type observable de fichier ou d'URL.
2. Cliquez sur le lien connexe **Afficher IoC** .
3. Dans l'onglet **Observables** , sélectionnez un ou plusieurs enregistrements pour lesquels vous souhaitez effectuer une analyse des menaces ou des programmes malveillants, puis cliquez sur **Soumettre au bac à sable**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



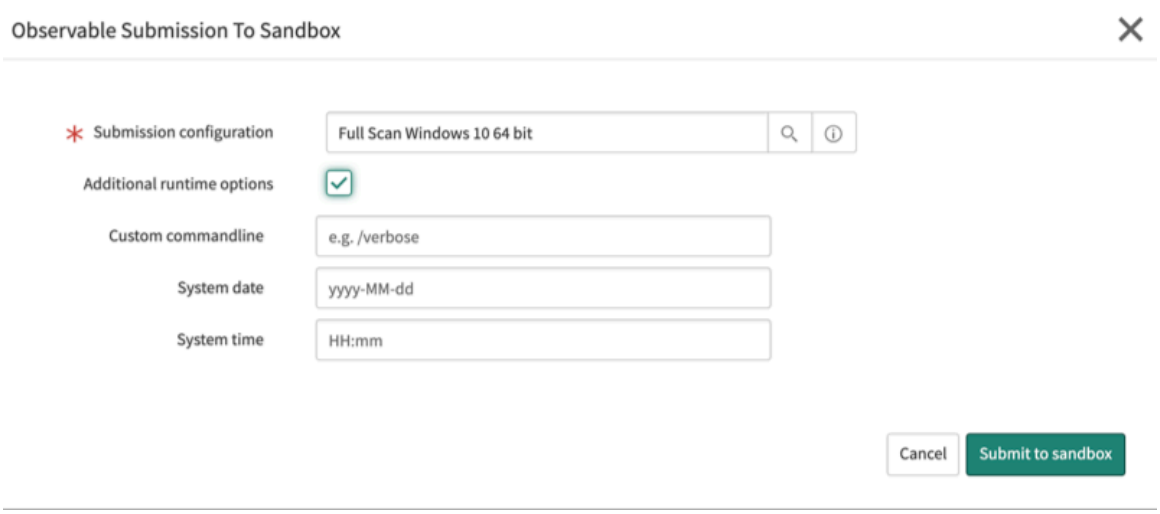
4. Lorsque le filtre Soumission de fichier s'affiche, sélectionnez votre configuration de bac à sable préférée dans **Configuration de soumission**, puis cliquez sur **Soumettre au bac à sable**.



5. Facultatif : Sélectionnez **Options d'exécution supplémentaires** si vous souhaitez fournir d'autres options personnalisées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Champ	Description
Ligne de commande personnalisée	Ligne de commande d'application normale ou opération spéciale.
Date du système	Date système au format aaaa-MM-jj.
Heure du système	Heure du système au format HH :mm.

Une fois que vous avez initié la soumission, vous pouvez afficher les notes de travail pour voir l'état de votre soumission. Pour plus d'informations sur l'état de la soumission ou pour analyser les résultats, consultez les résultats de soumission du **bac à sable**.

Remarque : Dans CrowdStrike Falcon X Sandbox, l'analyse rapide n'est pas prise en charge pour les URL. Si les notes de travail contiennent trop d'informations, vous pouvez utiliser l'option Filtre pour accéder aux notes de travail requises qui vous intéressent.

Que faire ensuite

Lorsque vous soumettez les observables au bac à sable pour l'analyse de programme malveillant, affichez les résultats de soumission du bac à sable pour passer aux étapes suivantes sur les menaces potentielles.

Automatiser CrowdStrike les soumissions Falcon Sandbox à l'aide de Flow Designer

L'intégration CrowdStrike Falcon X Sandbox inclut des modèles de flux créés à l'aide de qui fonctionnent avec les Concepteur de flux enregistrements d'incidents de sécurité.

Avant de commencer

- Vérifiez que vous avez créé une configuration de soumission Sandbox et que vous avez activé une configuration comme **configuration par défaut pour la soumission automatisée**. Lorsque le flux est déclenché, la soumission du bac à sable se produit sur votre configuration par défaut.

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Ces flux sont principalement conçus pour vous aider à démarrer lorsque vous souhaitez automatiser les soumissions de fichiers ou d'URL dans le cadre de votre workflow de réponse aux incidents.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous activez un exemple de flux, vos pièces jointes de fichier d'hameçonnage sont automatiquement envoyées si vous définissez les incidents de sécurité comme hameçonnage dans votre échantillon de flux. Vous pouvez également soumettre tous les fichiers .exe lorsque ce type de fichier est joint à un enregistrement d'observable.

Vous pouvez modifier ces exemples de flux pour déclencher une soumission automatisée dans différentes conditions, catégories, conditions composées, etc.

L'intégration sandbox se compose de deux flux du système de base qui sont désactivés par défaut.

- **Envoyer le fichier lorsque la catégorie est Hameçonnage** : ce flux soumet un fichier au bac à sable pour analyse de programme malveillant lorsque la catégorie d'incident de sécurité est définie comme hameçonnage. Vous devez joindre un fichier à l'enregistrement de l'observable sur l'incident de sécurité. Si vous utilisez la fonctionnalité User Reported Phishing (URP), toute pièce jointe à un e-mail est automatiquement analysée et ajoutée à l'enregistrement d'incident SIR en tant qu'enregistrement d'observable. Aucune autre action n'est requise pour automatiser la soumission.
- **Soumettre lorsque le type de fichier de l'observable est exe** : ce flux soumet un fichier au bac à sable pour analyse de programme malveillant lorsque l'observable d'incident de sécurité est un exe. Comme pour le flux de catégorie d'hameçonnage, vous devez joindre un fichier à un enregistrement d'observable sur l'incident de sécurité. Vous pouvez le faire manuellement en chargeant le fichier ou automatiquement si une pièce jointe d'e-mail d'hameçonnage, ou un autre mécanisme qui crée l'incident, est associé aux enregistrements observables.

Lorsque les flux sont configurés et que les conditions d'incident satisfont aux paramètres, les soumissions de bac à sable se déclenchent automatiquement lorsque vous examinez l'incident de sécurité. Examinez la note de travail qui indique qu'une soumission a été lancée, qu'une balise apparaît si activée dans la configuration et qu'un enregistrement des résultats de soumission est en attente.

L'intégration sandbox contient également plusieurs flux secondaires. Les flux secondaires sont des composants internes des options globales de soumission d'intégration. Vous pouvez personnaliser et modifier les flux secondaires en fonction de vos critères de sécurité.

Vous pouvez faire référence aux flux secondaires pour résoudre les problèmes liés aux soumissions de bac à sable. Un enregistrement d'exécution est créé chaque fois que vous appelez un flux secondaire. Cet enregistrement indique à quel endroit du flux une erreur particulière s'est produite et vous permet de résoudre le problème.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration de Sandbox : workflows multiples

Flows | Subflows | Executions | Help | + New

All > Application Name contains Sandbox

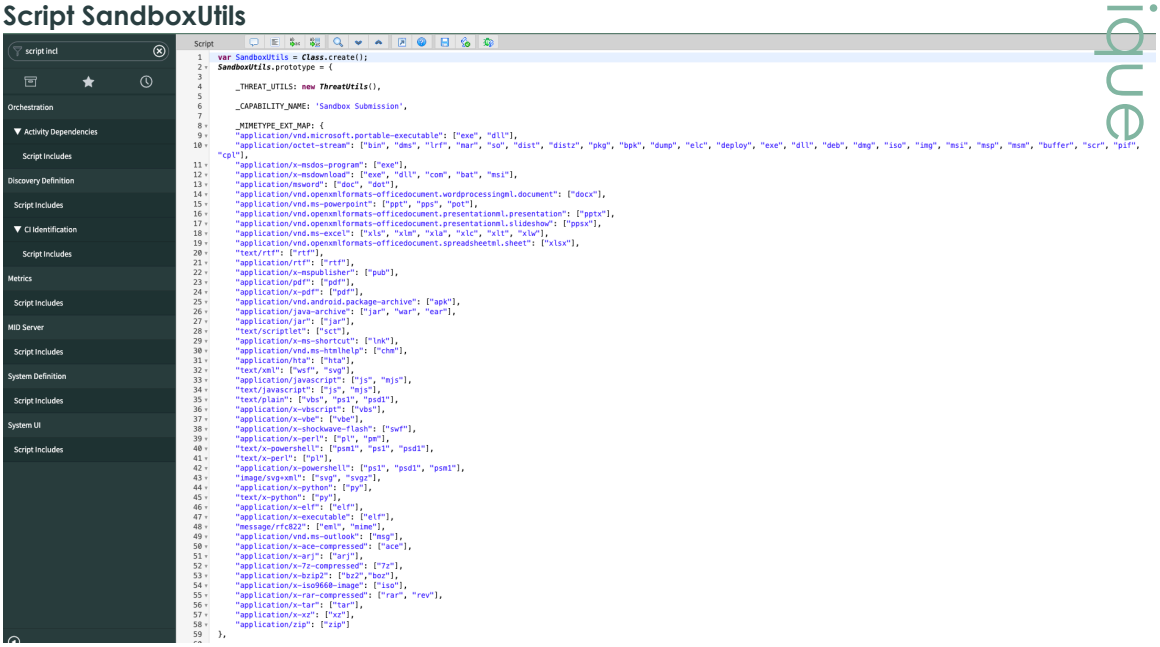
Name ▲	Internal name	Application	Status	Active	Updated	Updated by
Search	Search	*Sandbox	Search	Search	Search	Search
Add submission status tag on SIR	add_submission_status_tag_on_sir	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 12:33:57	admin
Aggregate Additional Runtime Options	aggregate_additional_runtime_options	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 08:47:54	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-18 02:52:33	admin
CrowdStrike Falcon Sandbox Poll Submission	crowdstrike_falcon_sandbox_polling	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-02 05:11:53	admin
CrowdStrike Falcon Sandbox Submission	submit_file_to_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:17:57	admin
CrowdStrike Falcon Submission Results	crowdstrike_falcon_submission_results	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:30:16	admin
CrowdStrike Polling Quick/Full Scan	crowdstrike_polling_quickfull_scan	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 20:23:07	admin
Fetch Environment Ids from Sandbox	fetch_environment_ids_from_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-25 07:45:54	admin
Submit File or URL to CrowdStrike Quick ...	submit_fileurl_to_crowdstrike	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 19:04:42	admin
Submit File/URL to Sandbox	submit_fileurl_to_sandbox	Security Operations CrowdStrike Falcon S...	Draft	true	2020-05-25 07:50:18	admin
Submit Observable for Automated submission	submit_observable_for_automated_submission	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-06 06:15:35	admin

Actions on selected rows... | 1 to 11 of 11

Remarque :

- Si vous choisissez de personnaliser les flux par défaut, vous devez vérifier que le flux secondaire Soumettre l'observable pour la soumission automatisée est inclus dans votre flux pour déclencher les soumissions automatiques.
- Vous pouvez personnaliser et définir vos extensions de fichier pour un exe. Créer une copie du flux **Soumettre lorsque le type de fichier pour l'observable est exe** et apporter des modifications à la copie. Le type de contenu et les extensions de fichier sont mappés dans le script SandboxUtils . Pour accéder aux includes de script, accédez à **Définitions du système > Includes de script** et recherchez SandboxUtils.

Script SandboxUtils

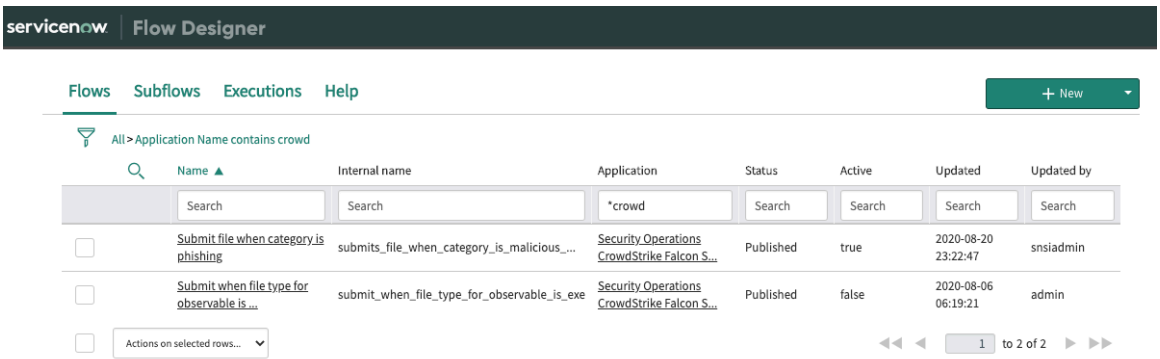


Traduction automatique

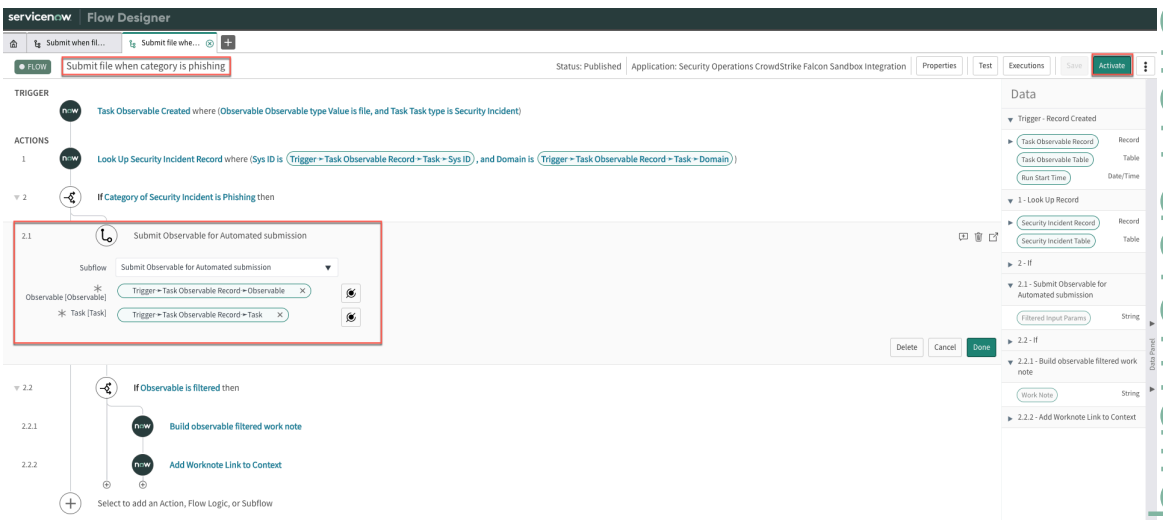
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Concepteur de flux** > **Concepteur** > **Flux**.
2. Filtrez les flux par type **d'application** .
   Par exemple, *crowd filtre les deux CrowdStrike Falcon X Sandbox flux.



3. Sélectionnez un flux pour afficher les détails.
   L'exemple ci-dessous montre le fichier Soumettre lorsque la catégorie est flux d'hameçonnage.



4. Cliquez sur **Activer** , puis sur **OK** lorsque le message de confirmation s'affiche.

Que faire ensuite

Après avoir configuré les flux de soumission automatisés, vous pouvez afficher les résultats de soumission du bac à sable pour analyser toutes les menaces.

Surveiller les résultats de soumission dans le bac à sable

Les résultats de toutes les soumissions de Sandbox sont affichés dans l'onglet Résultats de soumission de **Sandbox** pour chaque incident de sécurité.

Avant de commencer

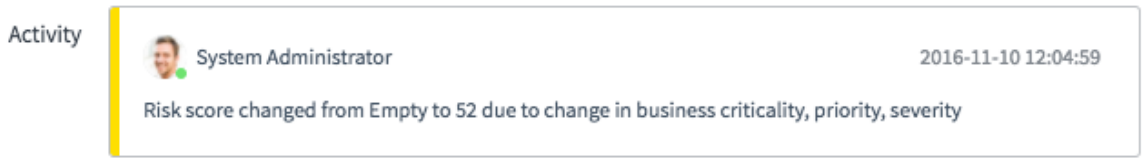
Rôle requis : sn_si.analyst

Traduction automatique

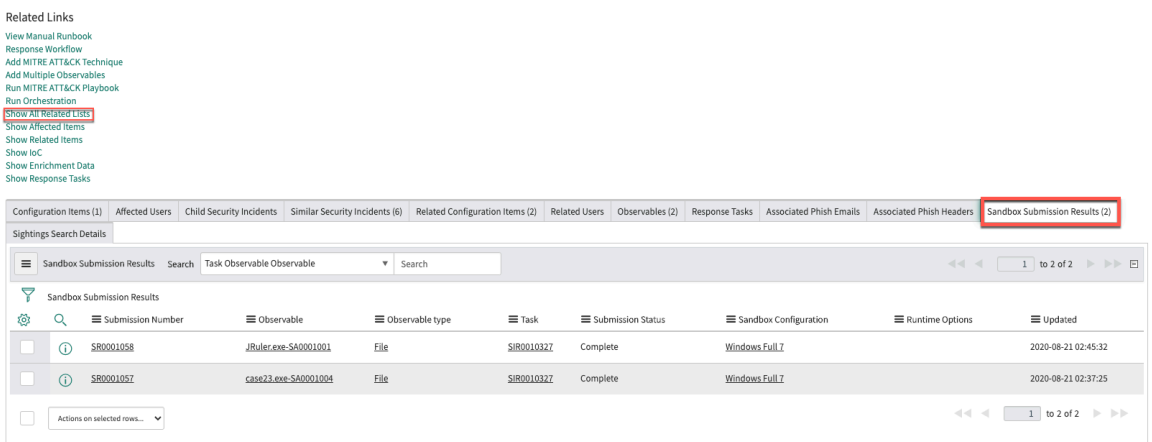
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez l'incident de sécurité sur lequel vous travaillez et vérifiez que la soumission de s andbox est correcte.



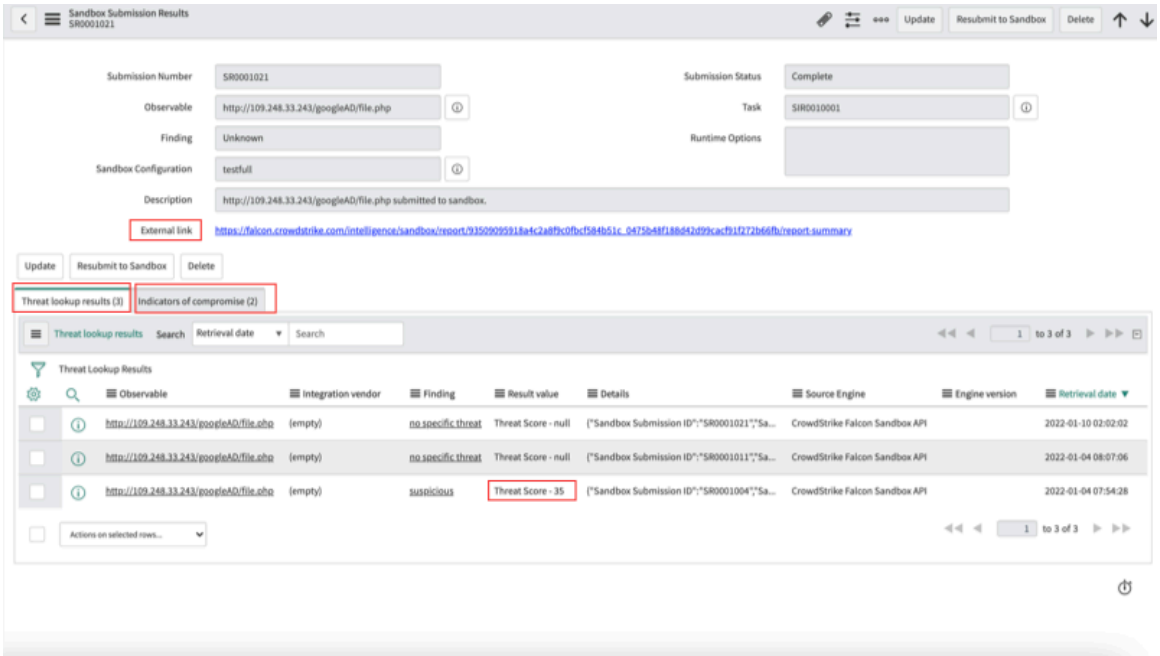
2. Passez en revue les notes du travailpour plus d'informations et découvrez comment procéder si vous ne pouvez pas vérifier que l'analyse est réussie.
3. Cliquez sur le lien des résultats complets dans les notes de travail ou, en bas de l'incident de sécurité, accédez à **Afficher toutes les listes connexes**> **Résultats de soumission du bac à sable**.
   Les résultats sont affichés dans l'onglet Résultats de soumission du bac à sable.



4. Cliquez sur Ouvrir n'importe quel enregistrement pour afficher l'analyse complète de set de boîte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



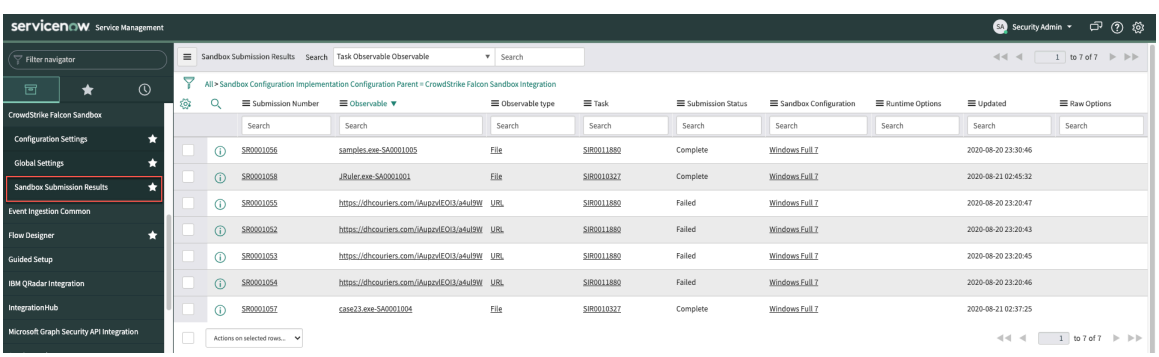
5. Facultatif : Cliquez sur **Resubmit to Sandbox (Soumettre à nouveau au bac à sable**) pour traiter à nouveau l'observable.

Résultats

- **L'onglet Résultats de la recherche de menace** fournit l'évaluation de la menace, y compris les résultats de malveillance, les scores de menace et des détails supplémentaires. Cesdétails sont fournis dans la structure de format standard de recherche de menaces pour toutes les ServiceNow intégrations de recherche de menaces.
- L'onglet **Indicateurs de compromission** fournit les résultats malveillantsou suspects avec les scores de confiance. Les scores de confiance sont similaires aux autres informations d'indicateur stockées dans la ServiceNow plateforme. Les indicateurs classés comme informatifs ne sont pas inclus dans cet onglet.
- Cliquez sur **Lien externe** pour afficher les résultats du bac à sable dans le CrowdStrike Falcon X Sandbox portail.

> **Remarque :** Cette option nécessite que vous ayez le CrowdStrike Falcon X Sandbox rôle pour afficher les résultats.

Vous pouvez également surveiller les résultats de soumission des andbox pour tous les incidents de sécurité en accédant à **Bac à sable CrowdStrike Falcon** > **Résultats de soumission du bac à sable**.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Marquer les incidents de sécurité avec l'état de soumission Sandbox

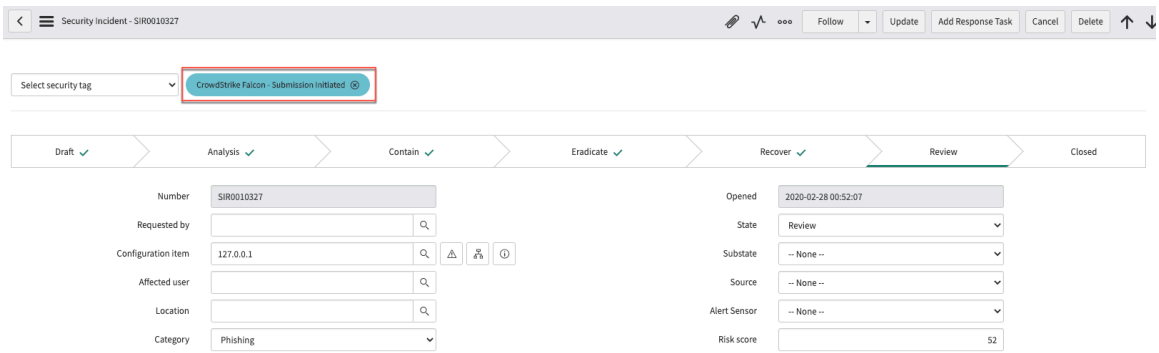
Vous pouvez éventuellement baliser les incidents de sécurité avec les balises Soumission initiée et Soumission terminée.

Lorsque vous sélectionnez l'option **Afficher les balises** dans la configuration de la soumission Sandbox, les balises s'affichent pour indiquer l'état d'une soumission de fichier ou d'URL. La vérification de l'état de cette façon est utile car le traitement de l'analyse de la boîte et de l'environnement peut prendre plusieurs minutes.

Les balises d'affichage sont appelées soumission initiée, soumission terminée et soumission échouée.

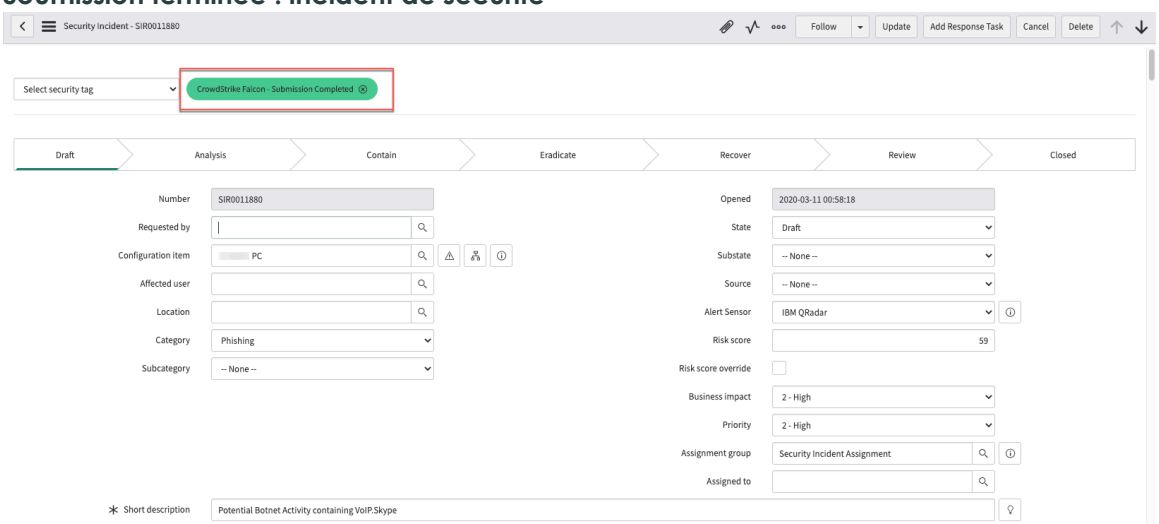
L'exemple suivant montre un incident de sécurité où la soumission a été initiée.

Soumission initiée : incident de sécurité



L'exemple suivant montre un incident de sécurité où la soumission a été terminée.

Soumission terminée : incident de sécurité



Passer en revue les paramètres globaux sandbox

Si vous rencontrez des problèmes avec les résultats de soumission des fichiers ou des URL, passez en revue et modifiez les paramètres globaux de laboîte à outils.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **CrowdStrike Falcon Sandbox** > **Paramètres globaux**.
2. Passez en revue et modifiez les paramètres selon les besoins.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Limite de taille de fichier (Mo)	Limite de taille de fichier de chargement de bac à sable en mégaoctets. **Remarque :** La limite de taille de fichier de 256 Mo est configurée par défaut. N'augmentez pas la valeur au-delà de 256 Mo. Toutefois, vous pouvez réduire la limite de taille de fichier maximale pour éviter de soumettre des fichiers volumineux.
Délai maximal pour les résultats de soumission (minutes)	Délai maximal pour la soumission des résultats à partir du sandbox. **Remarque :** Le délai par défaut est de 30 minutes. Si vos résultats prennent plus de 30 minutes, vous pouvez augmenter le temps. Vous pouvez également afficher les résultats dans le portail sandbox.

3. Cliquez sur **Enregistrer** .

Intégration de l'enrichissement des incidents Elasticsearch

L'intégration Elasticsearch d'enrichissement d'incident recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer Intégrations de Réponse aux incidents de sécurité	Configurer • Commencez avec l'intégration de l'enrichissement Elasticsearch des incidents • Créer des enregistrements de configuration de recherche d'observations
Utiliser • Exécuter une recherche d'observations • Security Operations Integration - Workflow de recherche de perceptions • Security Operations - Workflow de recherche de perceptions Elasticsearch	Développer • ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté des opérations de sécurité
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Commencez avec l'intégration de l'enrichissement Elasticsearch des incidents

Elasticsearch est un moteur de recherche et d'analyse distribué et RESTful qui s'intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l'intégration Elasticsearch d'enrichissement d'incident, vous devez la télécharger à ServiceNow Store partir du et ajouter l'URL de base API et les informations d'identification de connexion appropriées.

Avant de commencer

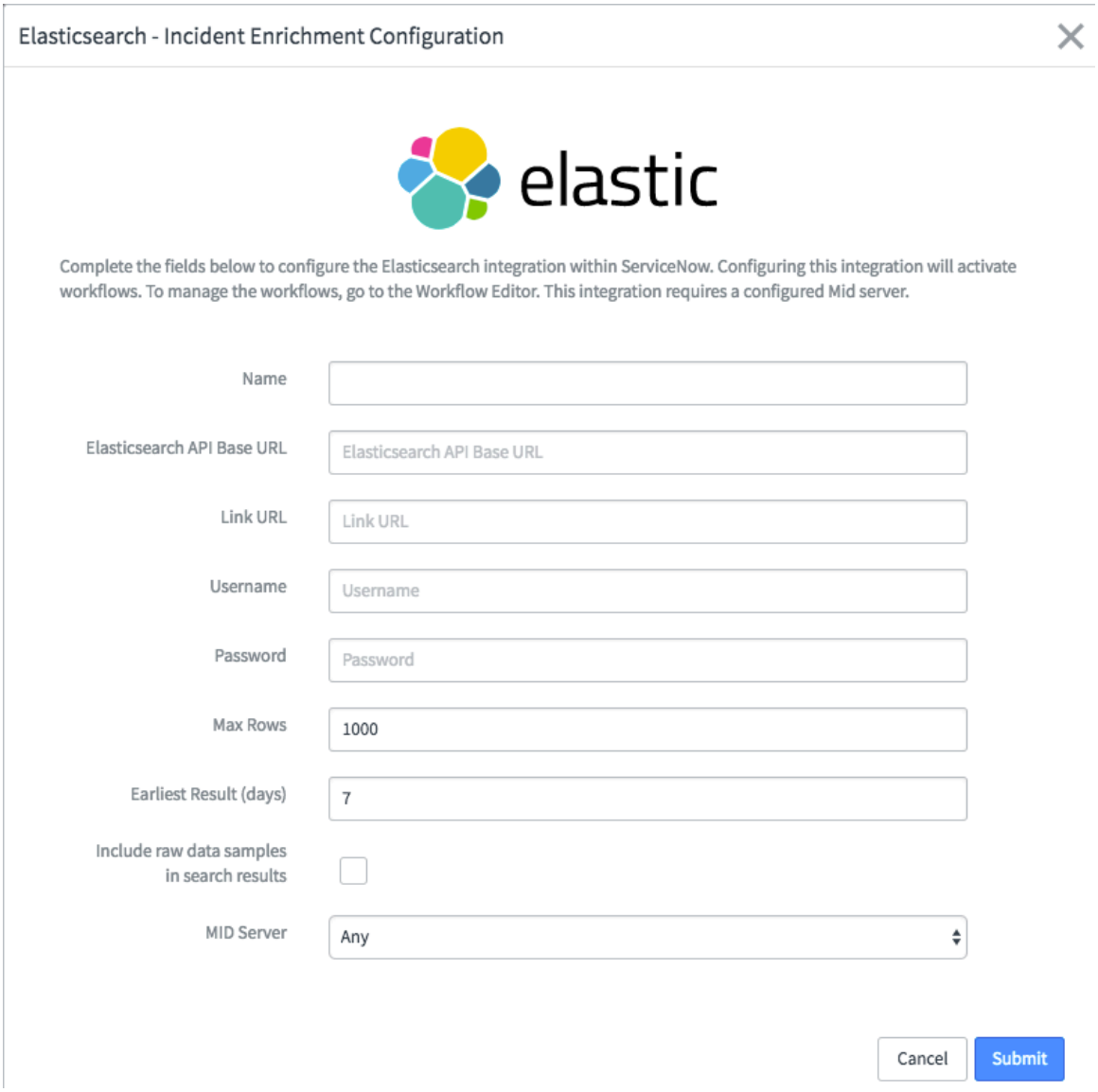
Rôle requis : sn_si.admin

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à Elasticsearch l'URL de base de l'API sous votre profil Elasticsearch et obtenez-la.
3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Sur la carte Enrichissement d'incident Elasticsearch , cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
URL de base de l'API Elasticsearch	L'URL de base que vous avez acquise à partir du Elasticsearch site.
URL de lien	[Facultatif] Liens vers une instance Kibana, lorsqu'ils sont disponibles
Nom d'utilisateur	Votre nom d'utilisateur Intel Elasticsearch .
Mot de passe	Votre mot de passe Intel Elasticsearch .
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend du paramètre que vous définissez sur le **nombre de lignes de la propriété de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	Sélectionnez **N'importe lequel** pour utiliser n'importe quel Serveur MID actif ou sélectionnez un nom de Serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

6. Cliquez sur **Envoyer**.
   La carte de configuration de l'intégration s'affiche.
7. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
8. Pour revenir à la liste initiale des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Résultats

Une fois configurée, l'intégration Elasticsearch d'enrichissement d'incident peut être sélectionnée pour publier des observables dans des listes de surveillance dans Réponse aux incidents de sécurité.

Intégration de sécurité des points de terminaison FireEye

FireEye Endpoint Security (série HX) permet aux entreprises d'inspecter et d'analyser les menaces connues et inconnues sur les terminaux.

Aujourd'hui, les attaquants expérimentés contournent les défenses traditionnelles sur lesquelles la plupart des équipes de sécurité s'appuient depuis des années pour protéger leurs terminaux. Même lorsqu'une défense traditionnelle arrête une menace connue, elle ne peut pas déterminer ce que cette menace essayait de faire. FireEye HX Endpoint Security aide votre équipe de sécurité à traquer et à arrêter les menaces avancées connues et inconnues contre vos terminaux.

L'intégration de Gold Standard Security Incident Response à FireEye HX, permet aux analystes de sécurité d'enquêter plus facilement et efficacement sur les incidents de sécurité et d'y remédier en un instant, sans avoir à naviguer entre les outils. Vous pouvez utiliser l'imbrication du réseau pour effectuer des actions de rattrapage sur les points de terminaison, implémenter des profils pour recueillir des détails spécifiques sur l'hôte et effectuer des requêtes ou des actions spécifiques sur le point de terminaison.

Fonctionnalités principales

- Capacité d'effectuer des actions d'enrichissement de l'hôte pour recueillir plus de détails sur le point de terminaison, tels que les détails de l'hôte, les statistiques réseau, les détails des utilisateurs, les détails des fichiers, les détails des processus et les détails du service.
- Capacité à effectuer une recherche de sécurité d'entreprise pour identifier les observables potentiellement malveillants sur les points de terminaison et à prendre des mesures correctives.
- Capacité à collecter le triage et l'acquisition de données pour une inspection et une analyse approfondies des terminaux.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Limitations

Voici les limites connues de cette intégration :

1. La valeur du champ Application MID doit être saisie manuellement.
2. Isoler l'hôte et Obtenir les services d'exécution ne peuvent pas être exécutés sur l'agent Linux.
3. Supprimer l'isolement ne prend pas en charge l'agent Linux.
4. Triage Acquisition ne prend pas en charge l'agent Linux.
5. Les utilisateurs doivent configurer les liens connexes Afficher les données d'enrichissement. Il n'est pas disponible prêt à l'emploi.
6. Pour la recherche d'observations, seules cinq recherches actives peuvent être présentes à la fois. Les observations restantes seront mises en file d'attente et commenceront après la fin de l'une des observations en cours.
7. Les perceptions sont disponibles prêtes à l'emploi, qui seront fausses actives par défaut.
8. Le hachage n'est pas pris en charge pour obtenir l'exécution des processus.

Configurer votre instance Now Platform pour l'intégration FireEye

Vérifiez et passez en revue la procédure de configuration suivante pour configurer l'instance Now Platform pour l'intégration FireEye.

Avant de commencer

Rôle requis : administrateur Now Platform (sn_si.admin)

La section suivante répertorie les tâches de configuration qui doivent être effectuées dans votre instance Now Platform avant d'installer l'application pour l'intégration FireEye.

Vérifiez que vous avez effectué les tâches suivantes avant d'installer l'application à partir de ServiceNow Store.

Tâche	Description
Vérifiez que vous avez affecté les rôles NowPlatform et Réponse aux incidents de sécurité (SIR) requis.	Les rôles suivants sont requis : 1. Un utilisateur disposant du rôle d'administrateur système (admin) est requis pour installer l'application pour l'intégration. 2. Un utilisateur disposant du rôle d'administrateur d'incident de sécurité (sn_si.admin) est requis pour configurer l'intégration, créer, activer et supprimer des profils. 3. L'utilisateur ayant le rôle d'analyste des incidents de sécurité (sn_si.analyste) est requis pour travailler avec les incidents de sécurité. Un utilisateur disposant de ce rôle peut initier n'importe laquelle des options disponibles dans l'intégration.
Vérifiez que vous avez installé et configuré un serveur MID.	Configurer Serveur MID : un Serveur MID dans votre instance NowPlatform est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	nécessaire pour gérer les fichiers et vous connecter au service FireEye déployé au sein du réseau de votre organisation. Pour plus d'informations sur les MID Servers, voir https://docs.servicenow.com
Vérifiez que les applications principales de ServiceNow qui sont requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application.	Les applications suivantes doivent être installées et activées à partir de ServiceNow Store avant d'installer cette application. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour garantir une installation fluide : **1.** Prise en charge de Security Incident Response **2.** Base de support de la sécurité **3.** Security Support Common **4.** Réponse aux incidents de sécurité **5.** Support commun de Threat Intelligence **6.** ServiceNow Integration Hub Enterprise Pack Installer
Avant d'activer l'option d'approbation pour les profils, vérifiez que vous avez créé un groupe d'approbation.	Un workflow d'approbation facultatif est disponible pour isoler les ordinateurs hôtes, les restaurer sur le réseau, obtenir des fichiers et exécuter des actions supplémentaires sur le point de terminaison. Si votre organisation souhaite un niveau supplémentaire de contrôle sur ces actions, activez l'option Exiger l'approbation pendant la configuration des profils. En l'absence de profil, si une aptitude est invoquée directement à partir de la liste connexe, les approbations peuvent être gérées à partir du module de paramètres par défaut FireEye. En tant qu'administrateur de sécurité, vous pouvez configurer l'approbation tout en configurant les profils et les paramètres par défaut. Un groupe d'approbation doit être disponible dans la liste Groupes de votre instance.

Traduction automatique

Procédure

1. Accédez à la **Administration utilisateurs** > **Groupes**.

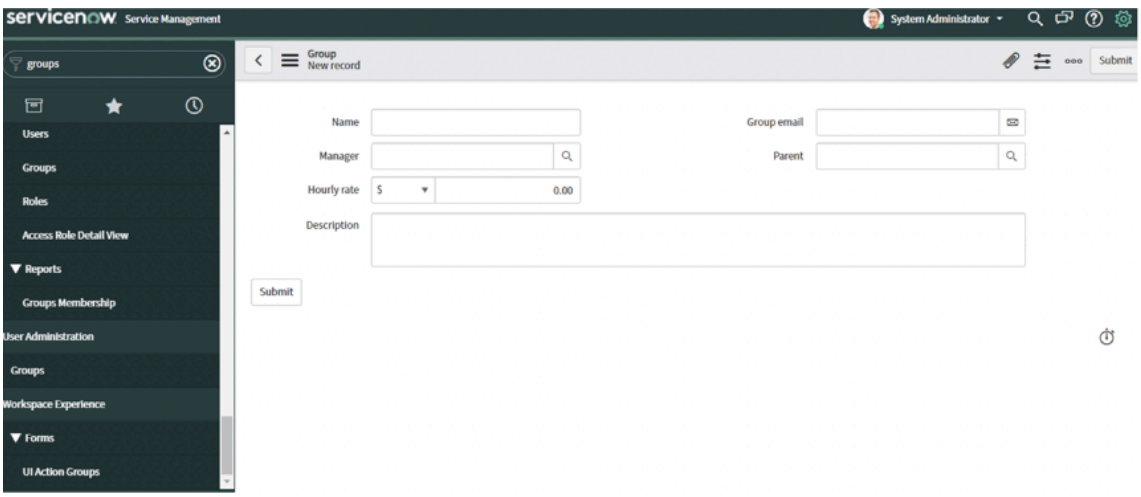
2. Cliquer sur **Nouveau** dans la liste Groupes.

3. Remplissez le formulaire avec les détails suivants :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom du groupe qui s'affiche lorsqu'une demande d'approbation est soumise.
E-mail de groupe	(Facultatif) Liste de distribution des e-mails de groupe ou adresse e-mail du point de contact, tel que le gestionnaire de groupe.
Responsable	(Facultatif) Nom du gestionnaire de groupe. Cliquez sur l'icône de recherche pour afficher la liste.
Parent	(Facultatif) Nom du groupe parent, s'il est associé à un parent.
Taux horaire	(Facultatif) Montant payé pour chaque heure travaillée.
Description	(Facultatif) Informations supplémentaires sur le groupe.

4. Cliquer sur **Soumettre**.



Le nouveau groupe s'affiche dans la liste Groupes. Vous avez créé un groupe d'approbation avec succès. Ajoutez des utilisateurs à votre nouveau groupe, selon vos besoins, qui peuvent approuver les demandes soumises par l'analyste de sécurité. Un utilisateur hérite des rôles de tous les groupes auxquels il appartient. Vous pouvez également affecter des rôles directement à un utilisateur.

Pour surveiller et traiter les demandes soumises par les utilisateurs disposant du rôle sn_si.analyst, chaque membre du groupe d'approbation doit accéder à Mes approbations dans Now Platform. Les approbateurs peuvent également trouver les demandes soumises spécifiquement pour l'intégration de FireEye sous les approbations FireEye.

Que faire ensuite

L'étape suivante consiste à installer et configurer l'application à partir de ServiceNow Store.

Configuration des paramètres d'horodatage pour l'acquisition du triage

Configurez et vérifiez les paramètres d'horodatage avant la procédure d'installation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : administrateur d'incident de sécurité Now Platform (sn_si.admin)

Avant d'installer l'application FireEye, vous devez effectuer certaines conditions préalables sur FireEye.

L'acquisition du triage peut être demandée avec une entrée de champ « Autour de l'horodatage » ou « Standard ». Autour de l'horodatage demande des informations collectées pendant une durée spécifiée avant l'horodatage jusqu'à une durée spécifiée après l'horodatage. L'horodatage correspond à l'heure à laquelle l'événement qui a généré l'alerte s'est produit. Si vous sélectionnez Standard, l'appliance Endpoint Security demande des informations à l'hôte pour toutes les données relatives à un événement.

Lorsqu'un utilisateur d'Endpoint Security demande une collecte de triage basée sur une date et une heure spécifiques, l'agent renvoie des informations pour une plage de temps spécifiée avant et après l'alerte. Les paramètres d'horodatage contrôlent la longueur de la fenêtre pour la collecte de triage. Les paramètres d'horodatage s'appliquent uniquement aux événements d'URL d'agent (événements de surveillance d'URL) et de clé de registre (événements de clé réglementaire).

Vous pouvez utiliser l'onglet Paramètres d'horodatage pour spécifier la durée avant et après l'horodatage pendant laquelle les informations sont collectées. Les paramètres d'horodatage peuvent être compris entre 0 et 86 400 secondes. La valeur par défaut pour les deux paramètres est de 600 secondes.

Vous pouvez utiliser l'onglet Paramètres d'horodatage de la page Paramètres de triage automatique pour spécifier la durée avant et après l'horodatage pendant laquelle les informations sont collectées. L'horodatage correspond à l'heure à laquelle l'événement qui a déclenché l'alerte s'est produit.

Procédure

1. Accédez à la **Interface utilisateur Web de la sécurité du point de terminaison**.
2. Sélectionner **Administrateur** > **Paramètres de triage**.
3. Cliquer sur **Paramètres d'horodatage** de l'onglet **Paramètres de triage automatique** la page.
4. Spécifiez la durée avant et après l'horodatage pour laquelle les informations sont nécessaires.
5. Entrez le nombre de secondes avant l'horodatage spécifié pour lequel les informations sont nécessaires.
6. Entrez le nombre de secondes après l'horodatage pendant lesquelles les informations sont nécessaires.
7. Cliquer sur **Enregistrer**.

> **Remarque :** Vous pouvez rétablir les paramètres par défaut de toutes les valeurs de la page en cliquant sur **Rétablir les valeurs par défaut**, puis en cliquant sur Enregistrer.

- **Zone d'espace d'acquisition**: la page Acquisitions indique la quantité d'espace disque restante pour les acquisitions.
- **Définition de limites d'utilisation du disque pour les acquisitions :**
  - Les triages, les acquisitions de fichiers et les acquisitions de données peuvent s'accumuler au fil du temps et utiliser une quantité croissante d'espace disque. Pour contrôler cela, vous pouvez leur allouer un certain nombre d'espace disque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dix pour cent de l'espace disque que vous spécifiez est réservé aux acquisitions automatiques de triage. Lorsque l'espace d'acquisition total alloué est dépassé, les triages automatiques les plus anciens sont supprimés.

- Lorsque la taille totale du disque des acquisitions terminées dépasse une limite spécifiée, le dispositif Endpoint Security supprime les acquisitions terminées les plus anciennes jusqu'à ce que suffisamment d'espace disque soit libéré pour ramener le total sous la limite spécifiée. Les acquisitions qui ne sont pas encore finalisées ne sont pas concernées.
- Le dispositif Endpoint Security supprime automatiquement les acquisitions si un administrateur, un analyste ou un enquêteur utilise l'interface utilisateur Web d'Endpoint Security pour supprimer manuellement l'agent associé.

Pour définir des limites d'utilisation du disque pour des acquisitions complètes à l'aide de l'interface utilisateur Web :

- Accédez à **l'interface utilisateur Web de la sécurité des points de terminaison**.
- Sélectionner **Limites d'utilisation du disque** à partir de l' **Administrateur** menu.
- Dans l' **Limite d'espace d'acquisition** , spécifiez la quantité maximale d'espace disque (en Go) qui peut être utilisée pour stocker le triage, les fichiers et les acquisitions de données. Les valeurs valides et les valeurs par défaut varient en fonction de votre modèle d'appliance Endpoint Security. Les valeurs appropriées pour votre modèle sont affichées sur la page Limites d'utilisation du disque.
- Cliquer sur **Enregistrer**.

Remarque : Tous les paramètres mentionnés sont respectés et en cas de défaillances ou d'erreurs, Now Platform renvoie simplement ces erreurs.

Installer l'application et configurer une source pour l'intégration

Installez et configurez l'application à partir de ServiceNow Store sur votre instance Now Platform.

Avant de commencer

Rôle requis : administrateur NowPlatform (admin)

Remarque : Un Serveur MID actif est obligatoire pour configurer une source.

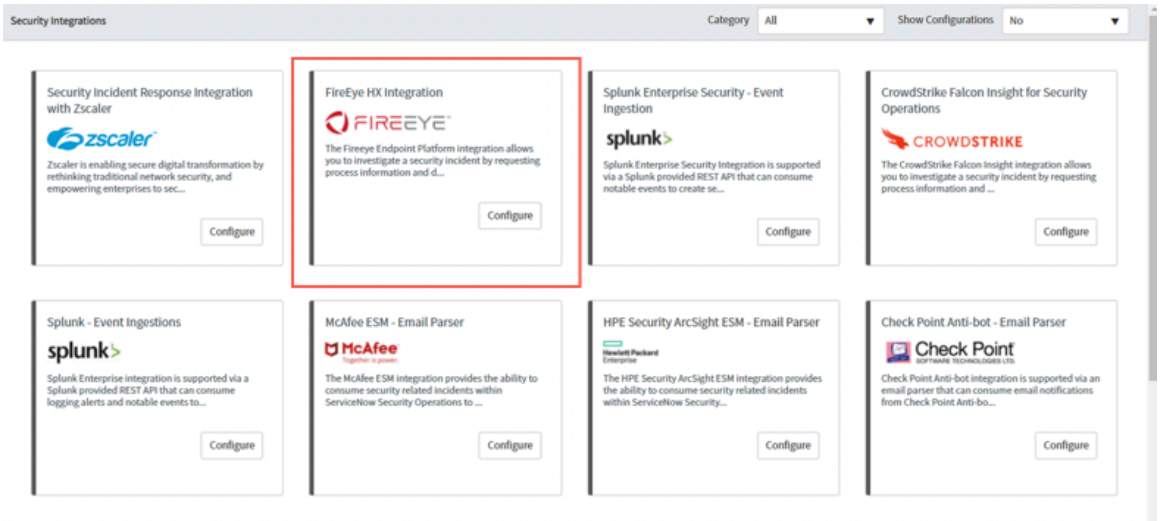
Téléchargez l'intégration de Réponse aux incidents de sécurité avec FireEye HX l'application à partir du ServiceNow Store et installez-la.

Une fois l'application correctement installée, procédez comme suit pour la configurer :

Procédure

1. Accédez à la **Intégrations** > **Configurations d'intégration**.
2. Sélectionnez le **Configurations d'intégration** permettant d'afficher les intégrations disponibles et de localiser le module **FireEye (en anglais seulement)** carreau.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



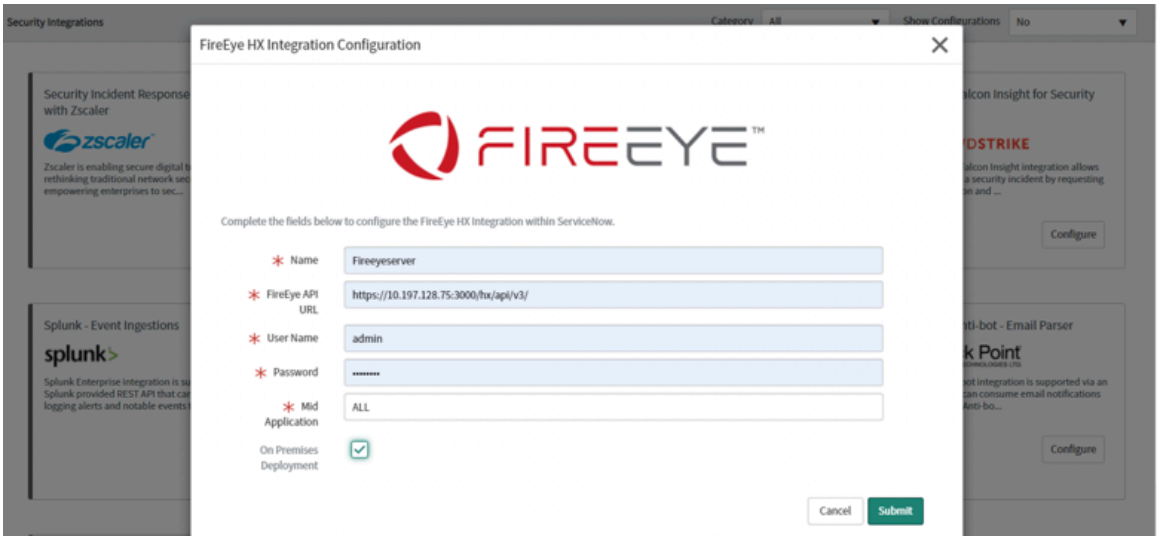
3. Cliquer sur **Configurer** sur la vignette FireEye.

4. Renseignez les informations suivantes pour configurer l'intégration FireEye :

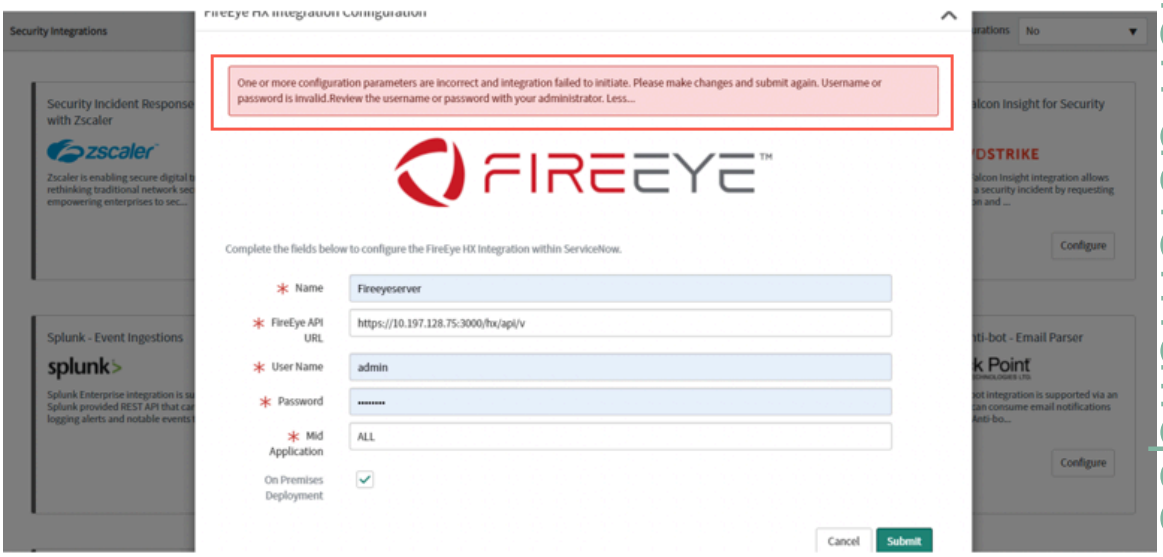
Champ	Description
Nom	Nom de la configuration FireEye. Ce nom est utilisé pour identifier la source ainsi que les informations d'identification et la configuration associées. Ce nom vous aide à distinguer les informations d'identification et les comptes et à identifier chaque source pour éviter les conflits avec les profils.
URL D'API	URL de base hébergeant l'API FireEye.
Noms d'utilisateur	Saisissez le nom d'utilisateur du compte FireEye.
Mot de passe	Saisissez le mot de passe du compte FireEye.
Application MID	Application MID configurée dans votre environnement. Le MID Server est nécessaire pour traiter les fichiers zip pour certaines des options d'enrichissement. Par défaut, ce sera TOUT. Les utilisateurs doivent fournir manuellement un nom d'application valide.
Déploiement sur site	La valeur par défaut est désactivée. Si vous utilisez la version cloud de FireEye, vérifiez que la case n'est pas cochée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquer sur **Soumettre**.
   La liste des configurations FireEye s'affiche avec votre nouvel enregistrement de configuration. Vous avez terminé la configuration d'un serveur FireEye. Si vous ne parvenez pas à vous connecter au FireEye ou si vos informations d'identification sont incorrectes, un message d'erreur de validation s'affiche, comme illustré dans la figure suivante. Vérifiez que vos informations d'identification sont correctes et réessayez.



Traduction automatique

Paramètres par défaut FireEye

Vous trouverez ci-dessous les paramètres de configuration supplémentaires une fois l'installation terminée.

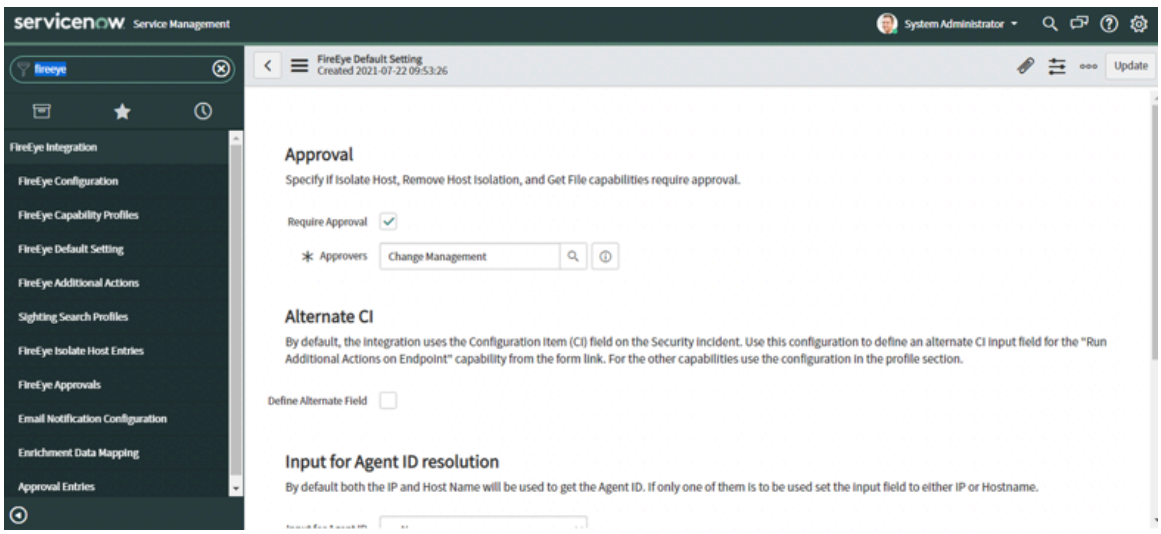
Une fois l'installation terminée, vous trouverez le module Paramètres par défaut de FireEye dans le menu de navigation de gauche. Il contient les paramètres par défaut des différentes fonctionnalités de FireEye.

Configurations supplémentaires

Les paramètres de configuration supplémentaires sont les suivants :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. **Approbation**: cette approbation s'applique spécifiquement aux options Isoler l'hôte, Supprimer l'isolement de l'hôte et Obtenir un fichier lorsqu'elles sont déclenchées directement à partir de la liste connexe et en l'absence de profils leur correspondant. S'il existe un/des profil(s) existant(s) pour ces options, la configuration d'approbation dans le profil sera honorée.
   - **Exiger l'approbation :** Lorsque vous activez l'option Exiger l'approbation, le champ Approbateurs est disponible sur le formulaire.
   - **Approbateurs**: liste des groupes d'approbateurs. Après avoir soumis une demande, le groupe doit obtenir l'approbation du groupe.
2. **CI alternatif**: si vous cochez cette case, la liste des champs disponibles pour transmettre un CI alternatif à l'aptitude s'affiche. Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité. Cette configuration ne s'applique qu'à l'aptitude « Exécuter des actions supplémentaires sur le point de terminaison ». Utilisez donc cette configuration pour définir un autre champ d'entrée CI pour l'aptitude « Exécuter des actions supplémentaires sur le point de terminaison » uniquement. Pour les autres options, utilisez la configuration dans la section des profils. Si les profils ne définissent pas d'autre CI, les options sélectionnent le champ CI à partir du formulaire d'incident de sécurité.
3. **Entrée pour la résolution de l'ID de l'agent**: par défaut, l'adresse IP et le nom d'hôte sont utilisés pour obtenir l'ID de l'agent. Si un seul d'entre eux doit être utilisé, définissez le champ d'entrée sur IP ou Nom d'hôte.

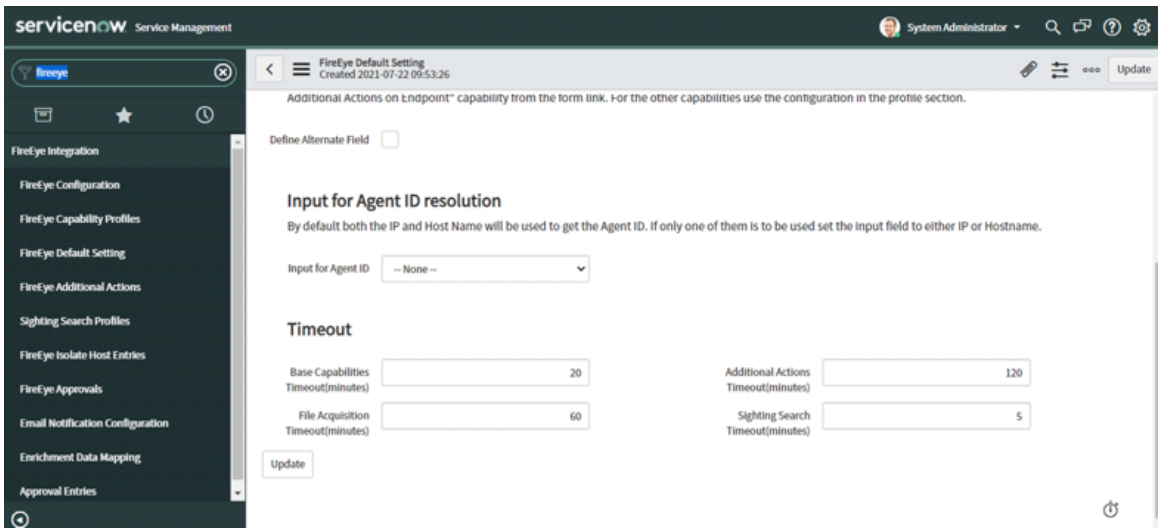


4. **Délai d'expiration**:
   - **Délai d'expiration des options de base (minutes) :** Les options Enrichissement, Isoler l'hôte et Supprimer l'isolement de l'hôte échoueront si aucune réponse n'est restituée dans le temps imparti.
   - **Délai d'expiration de l'action supplémentaire (minutes) :** L'aptitude Exécuter des actions supplémentaires sur le point de terminaison échoue si aucune réponse n'est restituée dans le temps imparti.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Délai d'expiration de l'acquisition du fichier (minutes) :** L'aptitude d'obtention de fichier échouera si aucune réponse n'est restituée dans le temps imparti.
- **Délai d'expiration de la recherche de perception (minutes) :** La recherche sera interrompue passé le délai défini.



Créer un nouveau profil d'aptitude pour l'intégration du point de terminaison FireEye

Créez un profil et sélectionnez les FireEye HX options que vous souhaitez qu'il exécute.

Avant de commencer

Rôle requis : administrateur d'incident de sécurité Now Platform (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Les profils sont créés pour regrouper les capacités et aideraient les analystes à effectuer facilement l'enquête/la correction.

Voici la liste des fonctionnalités que vous pouvez ajouter au(x) profil(s) :

1. Obtenir les détails de l'hôte
2. Obtenir les utilisateurs connectés
3. Obtenir les statistiques réseau
4. Obtenir l'exécution des processus
5. Obtenir les services d'exécution
6. Obtenir un fichier
7. Isoler l'hôte
8. Supprimer l'isolement

Vous ne pouvez pas associer les options Obtenir un fichier, Isoler l'hôte et Supprimer l'isolement de l'hôte avec d'autres options lors de la création d'un profil. Les profils pour ceux-ci doivent être créés individuellement. D'autre part, Obtenir les détails du système, Obtenir les utilisateurs connectés, Obtenir les statistiques réseau, Obtenir les processus en cours d'exécution et Obtenir les services d'exécution peuvent être regroupés. Vous pouvez créer des profils individuellement ou en les matraquant en totalité ou en parties selon vos besoins. Une fois qu'une option est incluse dans un profil, elle ne peut pas être incluse dans un autre profil.

Pour créer un profil d'aptitude, procédez comme suit :

Traduction automatique

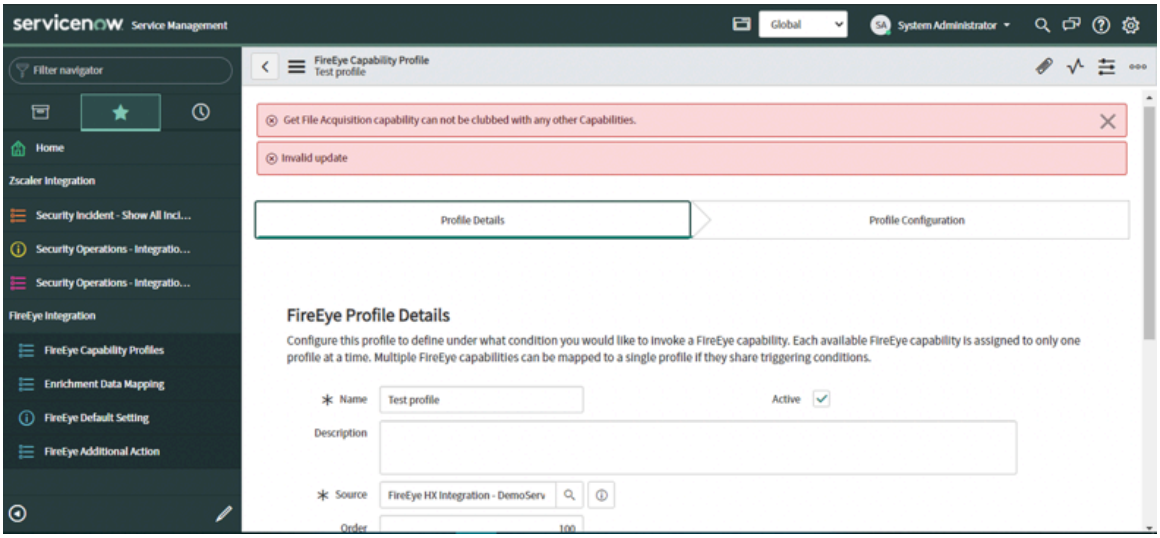
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Intégration de FireEye** > **Profils d'aptitude FireEye**.
   La liste des profils d'aptitude s'affiche.
2. Cliquer sur **Nouveau**.
3. Renseignez les champs du formulaire.

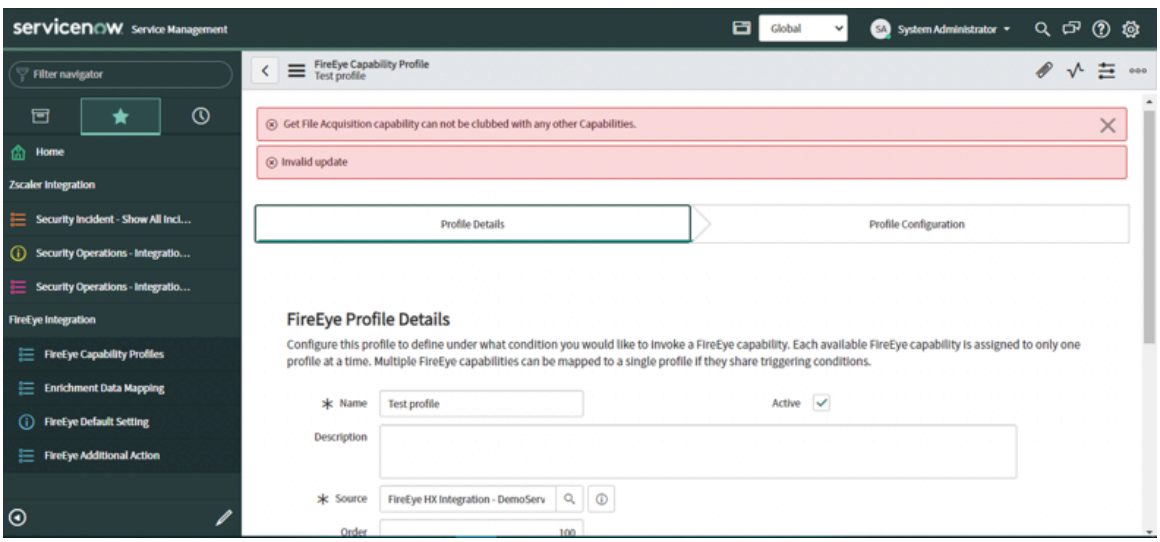
Nom	Nom du profil d'aptitude FireEye HX . Ce nom vous permet d'identifier le type de profil et de le décrire.
Description	Informations supplémentaires sur le profil qui le décrivent plus en détail.
Source	Nom de la FireEye HX source. Seules les sources configurées sont disponibles dans la liste de choix.
Options FireEye HX	Options du FireEye HX profil. Sélectionnez les options que vous souhaitez pour ce profil dans la colonne Disponible et déplacez-les vers la colonne Sélectionné.
Ordre	Priorité du flux. La valeur par défaut est 100. La valeur de ce champ indique l'ordre dans lequel les flux sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux doté du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400.
Actif	Cela indique que le profil est actif. Lorsque le profil est actif, il se déclenche automatiquement lorsqu'un incident de sécurité correspondant aux conditions de filtrage spécifiées dans la configuration est créé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La figure suivante est un exemple de formulaire rempli pour les détails du profil avec l'option Obtenir les détails de l'hôte.

4. Cliquer sur **Suivant** pour passer à la configuration du profil.



Remarque : Les options Isoler l'hôte, Supprimer l'isolement de l'hôte et Obtenir un fichier ne peuvent pas être associées à d'autres options.

Traduction automatique

Que faire ensuite

L'étape suivante consiste à configurer votre profil. Avant de configurer les paramètres du profil, il est préférable d'examiner les concepts de configuration des profils et des conditions de déclenchement. Pour plus d'informations, consultez Comprendre le fonctionnement des conditions de déclenchement avec un élément de configuration pour un profil.

Comprendre le fonctionnement des conditions de déclenchement avec un élément de configuration

Une fois que vous avez créé un profil et sélectionné les fonctionnalités FireEye que vous souhaitez que le profil exécute, configurez les paramètres du profil afin qu'il ne s'exécute que lorsqu'un ensemble de conditions spécifiques est rempli.

Vous pouvez définir des conditions de déclenchement afin que le profil s'exécute automatiquement chaque fois qu'un incident de sécurité correspondant à la condition de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

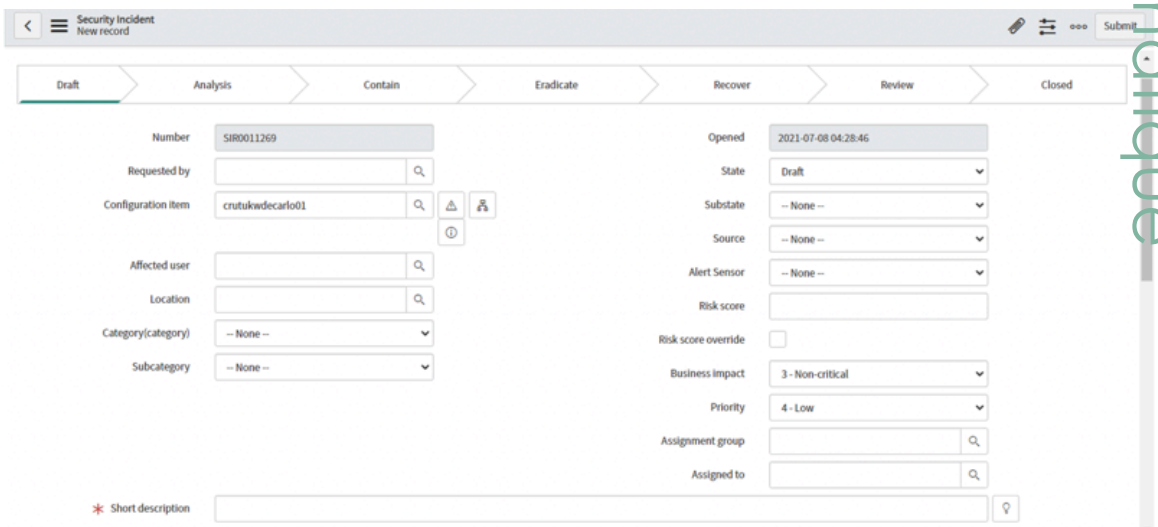
déclenchement est créé. Si la condition de déclenchement n'est pas définie, ces profils peuvent être exécutés manuellement en cliquant sur le formulaire « Exécuter le(s) profil(s) EDR » sur l'incident de sécurité, puis en sélectionnant le profil.

Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité. Cette valeur permet de faire correspondre les ID de vos actifs avec les informations stockées dans la CMDB de Now Platform. Lorsqu'un incident de sécurité est créé et qu'un profil est exécuté automatiquement ou manuellement, la CMDB effectue une recherche pour récupérer le nom d'hôte et/ou l'adresse IP en fonction de la valeur du champ CI. Le nom d'hôte et/ou l'adresse IP sont utilisés pour résoudre l'ID FireEye HX de l'agent afin d'identifier le point de terminaison.

Dans l'idéal, une valeur correspondante est trouvée dans la base de données et les données sont collectées à partir de la FireEye HX console pour l'actif correspondant. Les données des différentes options sont extraites dans votre instance Now Platform et affichées dans les listes connexes d'un incident de sécurité. Lorsque le champ Élément de configuration (CI) n'est pas renseigné sur l'incident de sécurité avec un nom d'hôte ou une adresse IP qui correspond à la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité contenant soit le nom d'hôte, soit l'adresse IP pour effectuer la résolution de l'ID de l'agent.

Au cours de l'étape de configuration de la configuration du profil, vous pouvez sélectionner un autre champ CI pour l'identification du point de terminaison afin de vous assurer que vous êtes en mesure d'identifier le point de terminaison sur FireEye HX. Vous pouvez sélectionner n'importe quel champ de l'incident de sécurité comme champ de déclenchement CI alternatif, y compris les champs personnalisés que vous créez. En sélectionnant ce champ CI alternatif comme copie de sauvegarde, vous vous assurez que vos profils s'exécutent même si le champ CI n'est pas renseigné pour l'incident de sécurité associé lors de la création de l'incident.

Remarque : Les autres champs CI ne sont pris en compte que pour les options qui peuvent être ajoutées à un profil. Pour toutes les actions supplémentaires, le CI alternatif est sélectionné dans la page des paramètres par défaut.



Configurer les profils et les incidents de sécurité pour l'intégration FireEye HX

Après avoir créé un profil et sélectionné les FireEye HX fonctionnalités que vous souhaitez que le profil exécute, configurez les paramètres de sorte que le profil ne puisse être invoqué que dans les conditions définies.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_si.admin

Configurez le profil de manière à ce qu'il s'exécute uniquement lorsque les conditions que vous spécifiez sont remplies. Sélectionnez un autre champ d'entrée pour le champ Élément de configuration (CI), si nécessaire, et définissez les conditions de filtrage afin que le profil puisse être déclenché automatiquement lors de la création d'un incident de sécurité répondant aux conditions de déclenchement.

Remarque : Vous pouvez accéder au modèle suivant : **Configuration du profil** page qu'après avoir saisi le **Détails du profil**.

Procédure

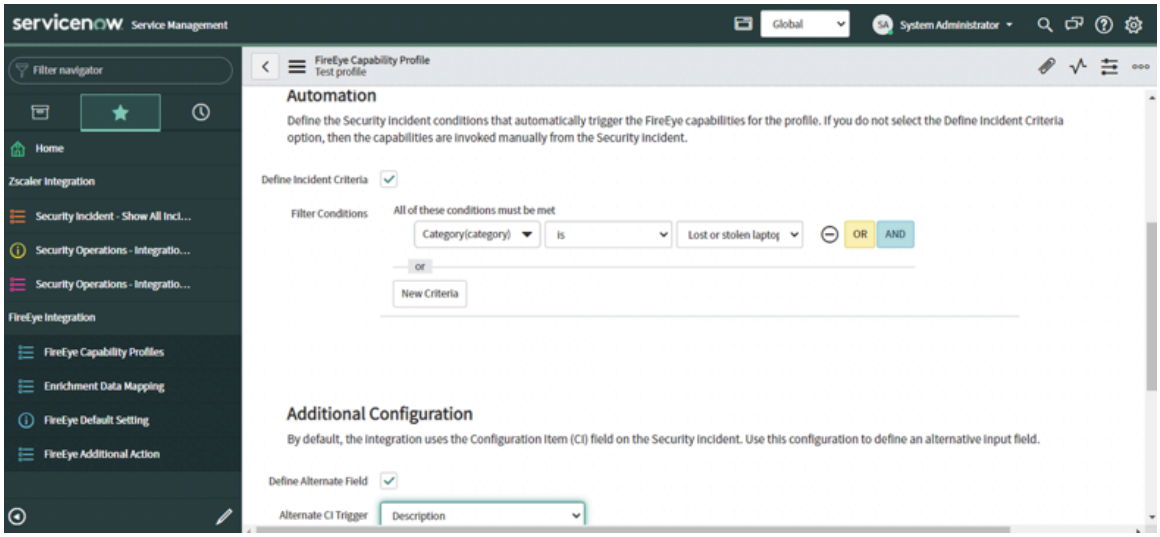
1. Accédez à la **Intégration de FireEye** > **Profils d'aptitude FireEye**.
2. Cliquer sur **Suivant** sur le **Détails du profil** après avoir renseigné la section Détails du profil.
3. Examinez et configurez les sections suivantes :
   - **Définir un critère d'incident (automatisation)**: définir les conditions d'incident de sécurité qui déclencheraient automatiquement les FireEye HX options du profil. Si vous ne sélectionnez pas l'icône **Définir un critère d'incident** , le profil et les options sous-jacentes peuvent être invoqués manuellement à partir de l'incident de sécurité.
     - Sélectionner **Définir un critère d'incident** Option permettant de déclencher FireEye HX automatiquement les options dans le profil.
     - Dans l' **Conditions de filtre**, sélectionnez le champ requis.
     - Vous pouvez ajouter **Nouveau critère** et définissez également la condition OU ou ET.

       Remarque : Isoler l'hôte, Supprimer l'isolement de l'hôte, Obtenir le fichier ne peuvent pas être déclenchés automatiquement.

   - **Configuration supplémentaire**: lorsque le champ Élément de configuration (CI) n'est pas renseigné sur l'incident de sécurité avec un nom d'hôte ou une adresse IP qui correspond à la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour interroger les FireEye HX API.
     - Sélectionnez le **Définir un autre champ** Option permettant de définir un autre champ d'entrée.
     - Sélectionner le champ d'entrée dans le **Champ de déclenchement CI alternatif**.

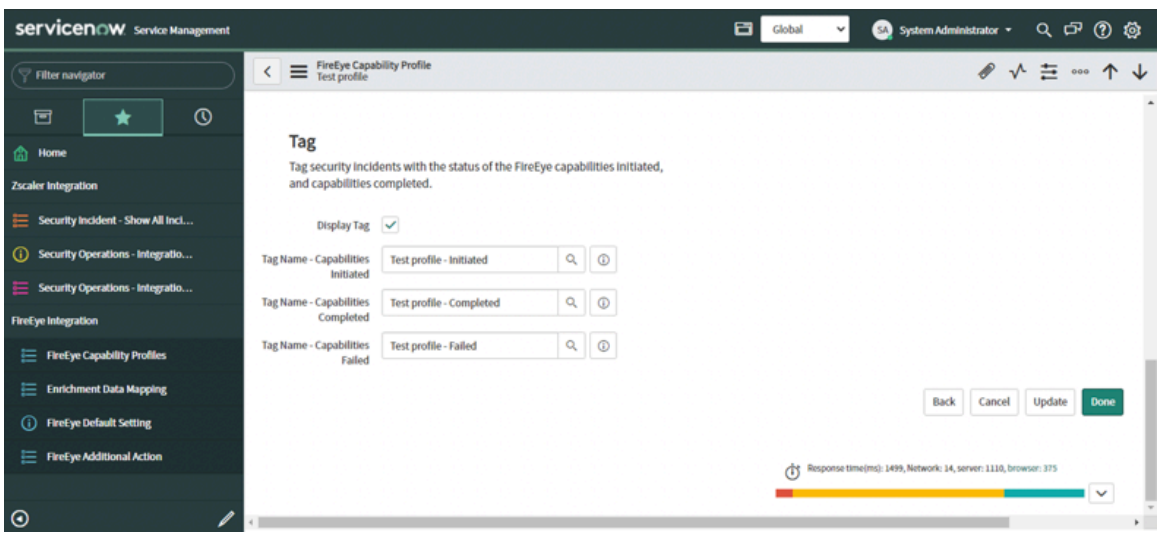
       Remarque : Pour plus d'informations, consultez Comprendre le fonctionnement des conditions de déclenchement avec un élément de configuration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



◦ **Balises**: vous pouvez éventuellement baliser les incidents de sécurité avec le profil initié, le profil terminé et les FireEye HX balises ayant échoué.

Sélectionnez le **Balise d'affichage** Case à cocher pour activer le marquage des incidents de sécurité, le nom du profil est préfixé lors de l'activation de la balise. Par défaut, cette option est désactivée pour tous les profils.

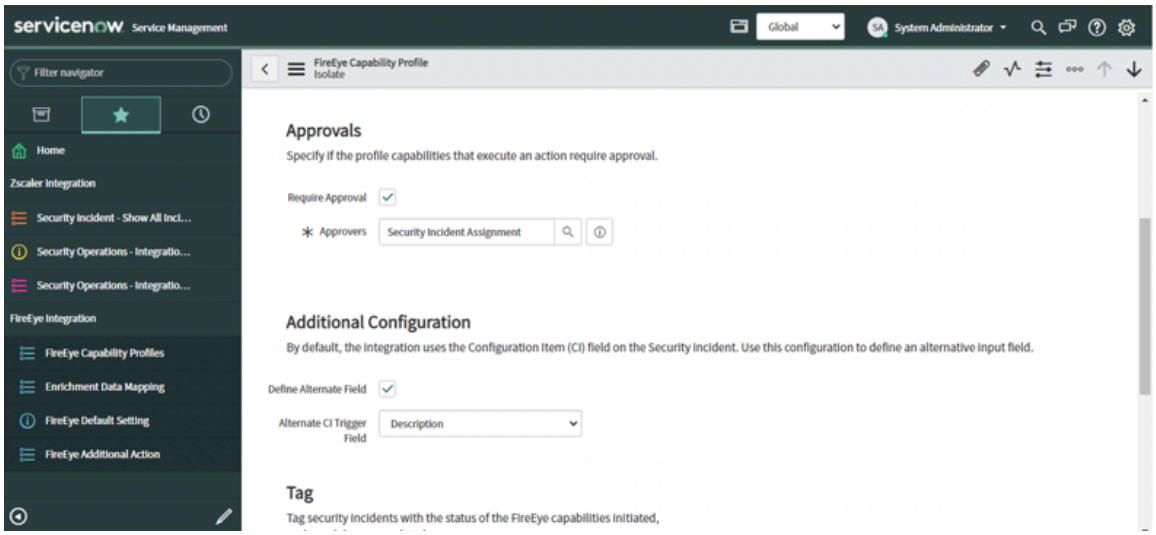


◦ **Approbations**: sélectionnez l'icône **Exiger l'approbation** Case à cocher pour fournir un niveau de contrôle supplémentaire lors de l'utilisation des FireEye HX options d'isolement des ordinateurs hôtes, de restauration sur le réseau et d'obtention des fichiers.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'option d'approbation de la configuration du profil s'affiche uniquement pour les options Isoler l'hôte, Supprimer l'isolement de l'hôte et Obtenir un fichier.



4. Cliquez sur **Terminé**.
5. Vérifiez les FireEye HX conditions de déclenchement.

Vérifier les filtres de condition de déclenchement

Testez le profil et vérifiez que les filtres de condition de déclenchement que vous avez configurés fonctionnent comme prévu.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

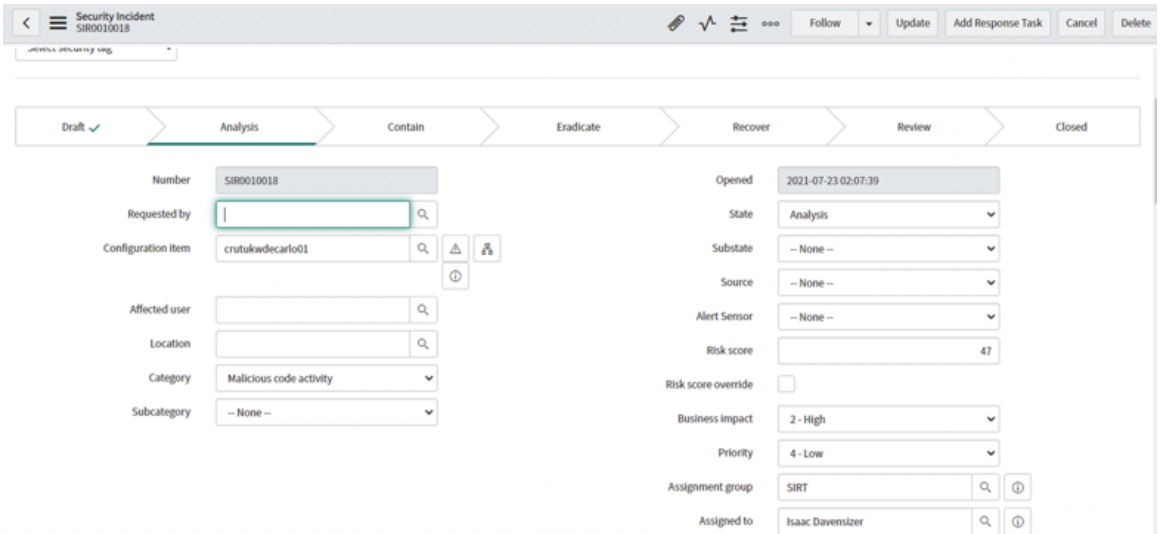
Une fois que vous avez activé le profil, en fonction des conditions de déclenchement configurées, vous pouvez afficher les résultats de la requête dans les incidents de sécurité de Now Platform.

Procédure

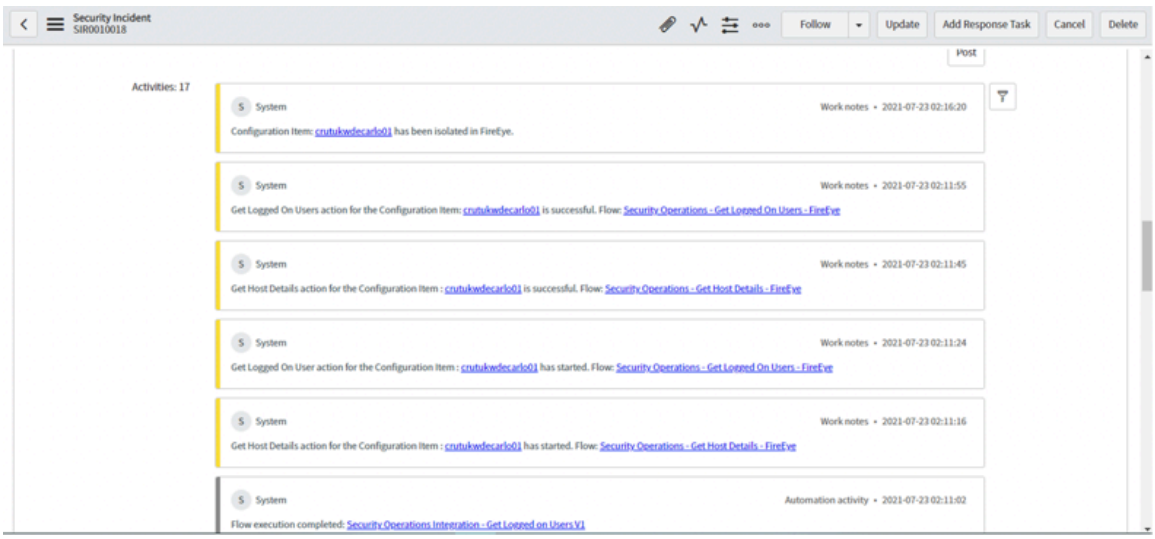
1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionner **Nouveau** pour créer un nouvel incident de sécurité.
3. Fournissez les conditions de filtre telles qu'indiquées dans le profil d'aptitude pour déclencher le profil respectif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquer sur **Enregistrer**.



5. Passez en revue la section des notes de travail et des activités.

6. Affichez le profil initié, le profil terminé ou les balises échouées du profil.

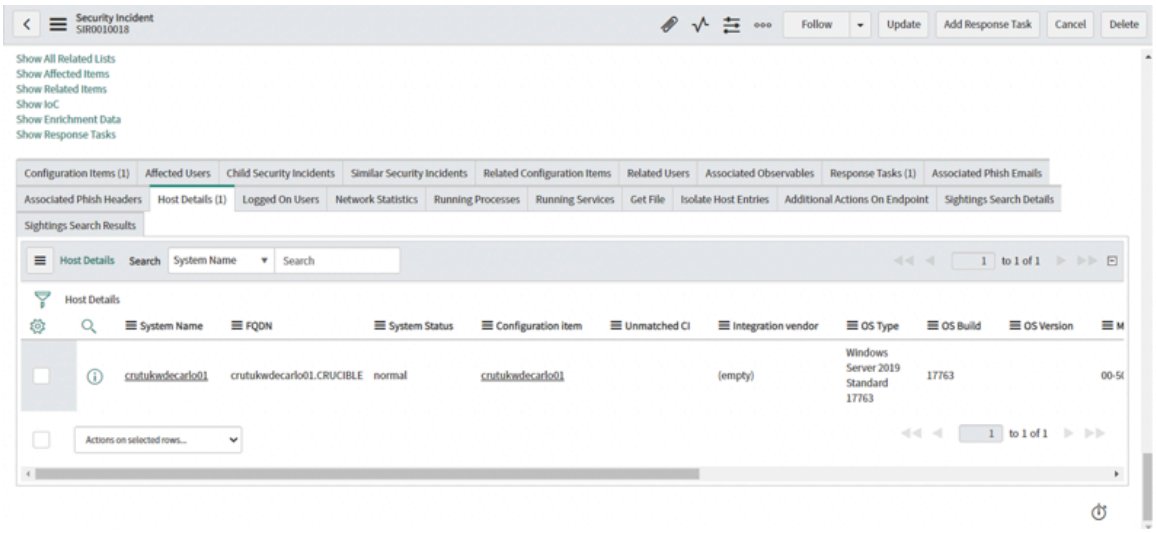
7. Cliquer sur **Afficher toutes les listes connexes**.

8. Cliquez sur une liste connexe (onglet).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, Détails de l'hôte.



Déclencher un profil d'aptitude FireEye à partir des liens connexes

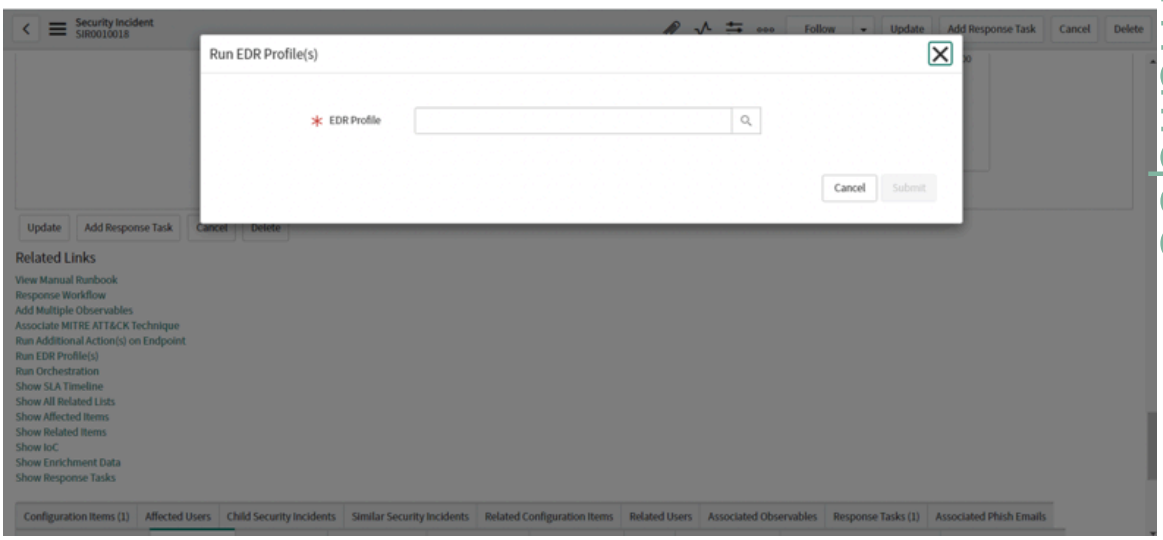
Déclenchez manuellement un profil d'aptitude après avoir examiné un incident de sécurité à partir des liens connexes.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Procédure

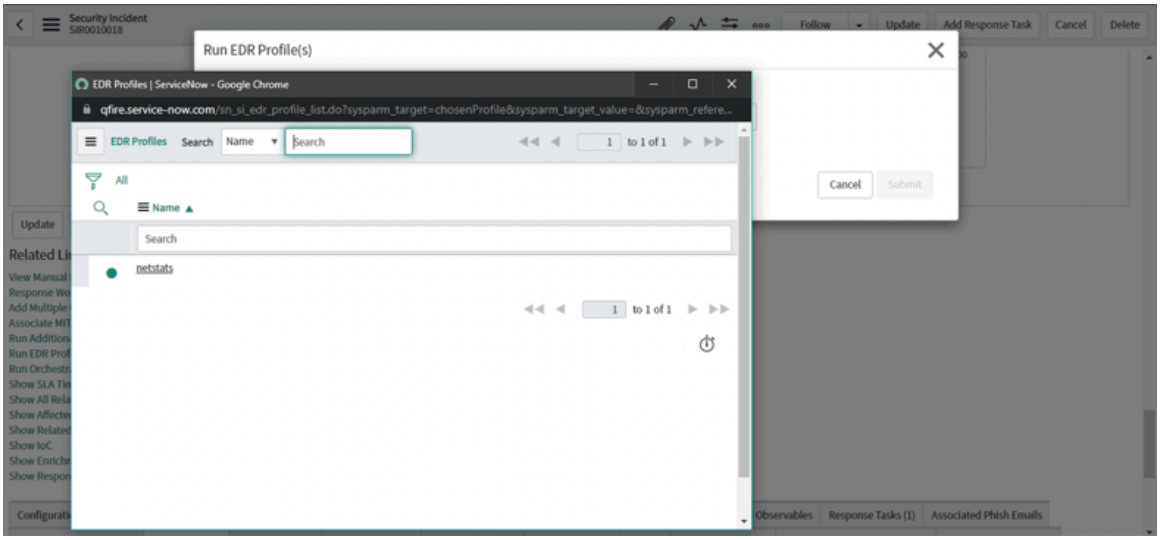
1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner.
3. Cliquer sur **Exécuter le(s) profil(s) EDR**dans la section Liens connexes.

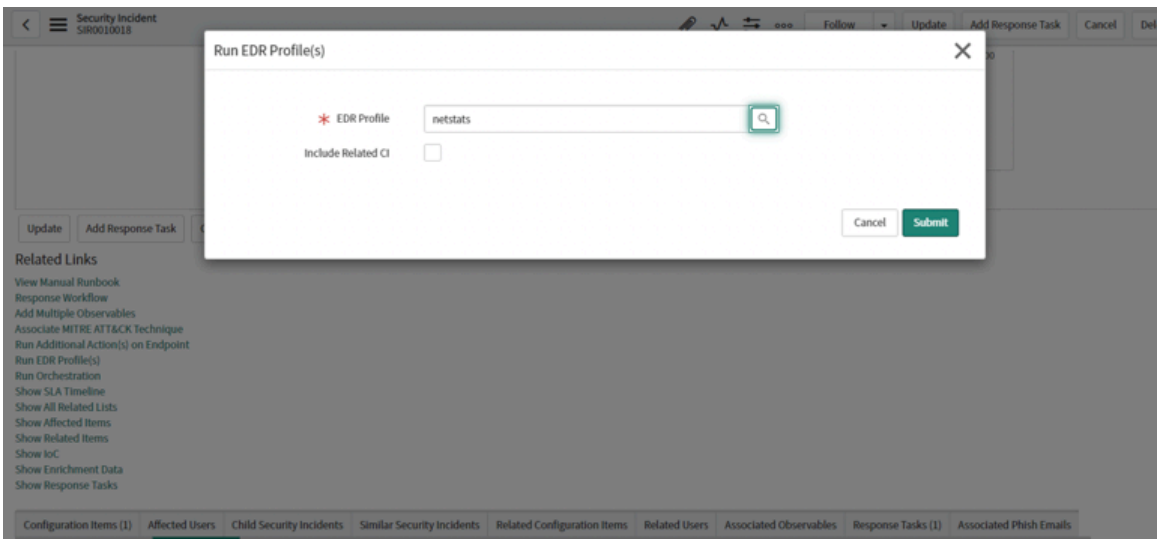


4. Parcourez et sélectionnez un profil dans la liste des profils disponibles, puis cliquez sur **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





5. Le profil sélectionné est déclenché manuellement.

6. Passez en revue la section des notes de travail et des activités.

7. Affichez les balises et consultez les listes connexes pour les données.

> **Remarque :** En plus d'exécuter le profil pour le CI ou le CI alternatif de l'incident de sécurité, vous pouvez également exécuter le profil pour les valeurs CI présentes dans la liste connexe Élément de configuration en cochant Inclure le CI connexe dans la boîte de dialogue. Cette opération permet également de récupérer les données des valeurs CI présentes dans la liste connexe. Vous pouvez également exécuter le profil uniquement pour les valeurs CI présentes dans la liste connexe.

Déclencher un profil d'aptitude FireEye à partir de la liste connexe Élément de configuration

Déclenchez manuellement un profil d'aptitude à partir de la liste connexe des éléments de configuration.

Avant de commencer

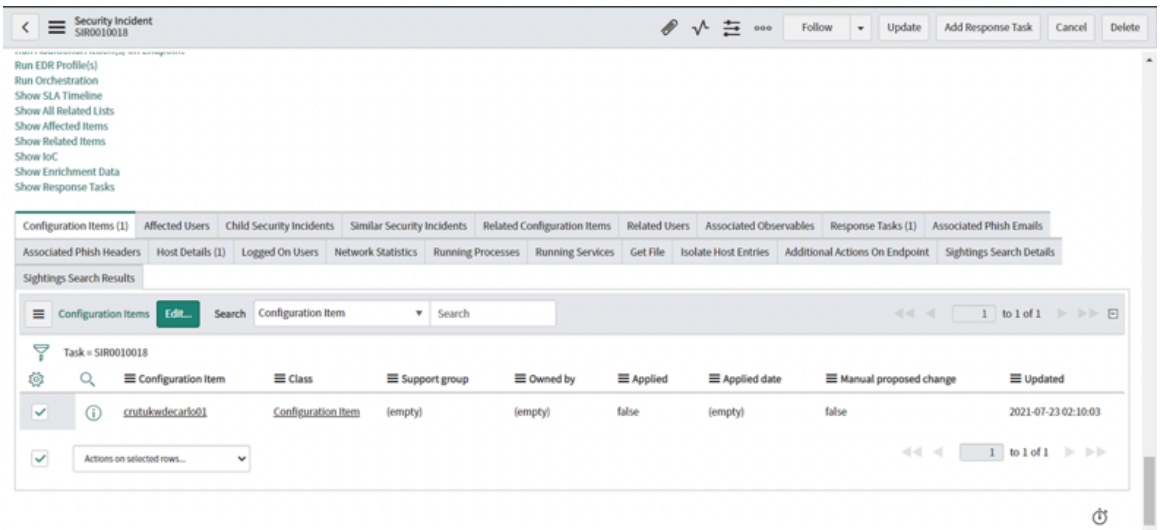
Rôle requis : sn_si.admin, sn_si.analyst

Traduction automatique

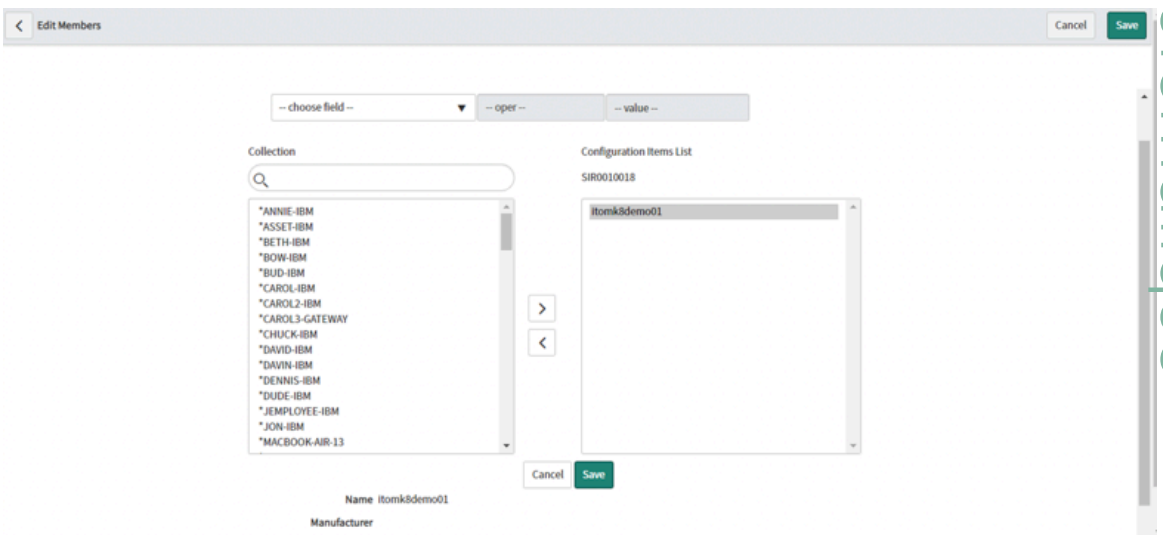
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les FireEye HX informations.
3. Cliquer sur **Afficher toutes les listes connexes** dans la section Listes connexes.
4. Cliquez sur **ID d'élément de configuration** liste connexe.



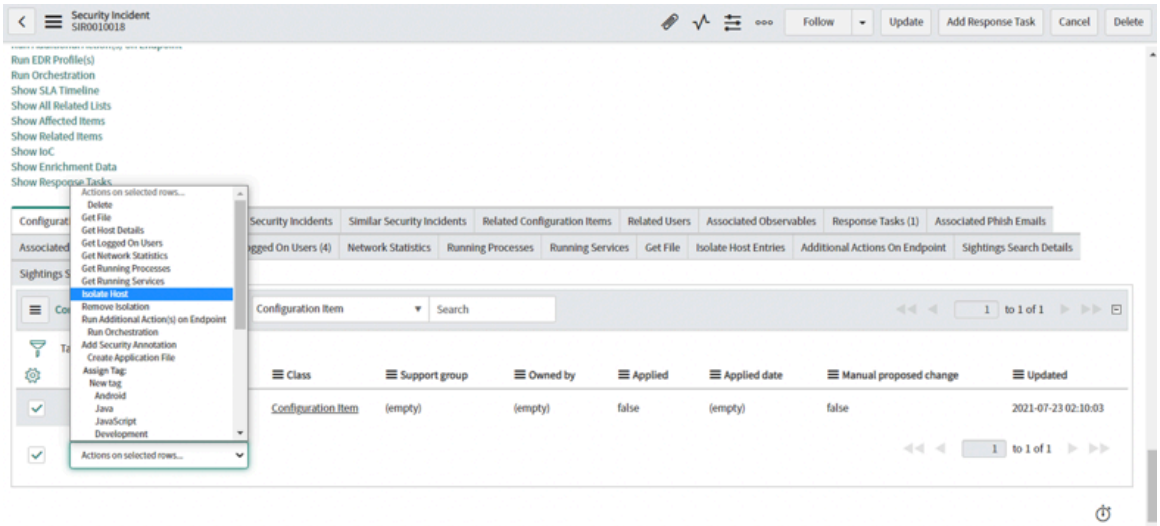
5. Cliquer sur **Modifier** pour ajouter les éléments de configuration disponibles, si les valeurs ne sont pas déjà présentes, puis cliquez sur **Enregistrer**.



6. Sélectionnez le ou les éléments de configuration ajoutés puis, dans Actions sur les lignes sélectionnées, sélectionnez une option.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. L'aptitude sélectionnée est déclenchée manuellement.

8. Passez en revue la section des notes de travail et des activités.

9. Affichez les balises et vérifiez les données dans les listes connexes.

FireEye : capacité d'obtention de fichier

Les demandes d'acquisition de fichiers demandent à un agent Endpoint Security d'obtenir un fichier à partir de son point de terminaison hôte. Les acquisitions de fichiers sont utilisées pour l'analyse statique ou dynamique de compromissions potentielles ou vérifiées, ainsi que pour la conservation de preuves lors d'enquêtes sur les menaces internes. L'option Obtenir un fichier doit être créée sous la forme d'un profil distinct.

Avant de commencer

Rôle requis : administrateur

Déclenchement de l'obtention d'un profil de fichier et de la création d'un profil d'aptitude FireEye HX avec **Obtenir un fichier** capacité.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.

2. Sélectionnez l'incident de sécurité que vous souhaitez examiner.

3. Cliquer sur **Exécuter le(s) profil(s) EDR**dans la section Liens connexes.

4. Parcourez et sélectionnez Obtenir un profil de fichier dans la liste des profils disponibles.

5. Fournissez l'attribut **Nom de fichier** et **Chemin d'accès au fichier**.

> **Remarque :** Entrez le nom du fichier que vous souhaitez acquérir. Spécifiez un nom de chemin d'accès précis ou une autre variable d'environnement Windows appropriée basée sur le chemin d'accès. Vous devez spécifier les noms de la lettre du lecteur ou du chemin d'accès. Différents points de terminaison peuvent avoir des mappages de lecteur différents. Si vous spécifiez explicitement un nom de dossier, vous pouvez terminer le chemin d'accès par une barre oblique inverse. Toutefois, la barre oblique inverse finale n'est pas obligatoire.

6. Cliquer sur **Soumettre**.

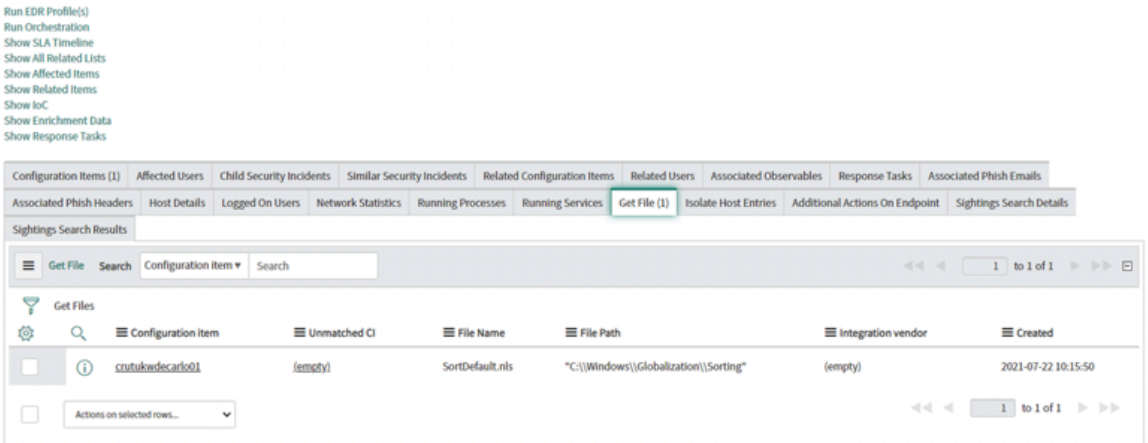
7. Passez en revue la section des notes de travail et des activités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Afficher les balises et vérifier les résultats dans le **Obtenir un fichier** liste connexe.

Remarque : L'option Obtenir un profil de fichier est maintenant déclenchée manuellement.



Pour examiner une acquisition de fichier téléchargé :

- Ouvrez le fichier d'acquisition .zip fichier.
- Entrez le mot de passe requis pour ouvrir le fichier. Le mot de passe peut être consulté en passant la souris sur le lien de téléchargement dans FireEye HX la console. Suivez les étapes ci-dessous pour afficher le mot de passe :
  - Connectez-vous à la console FireEye HX.
  - Accédez à la **Acquisitions** et filtrer par Type d'acquisition – Fichier.
  - Sélectionnez l'enregistrement souhaité.

    Remarque : Vous pourrez voir les détails du fichier acquis sur l'onglet de droite.

  - Passez la souris sur le **Télécharger** lien disponible en haut pour obtenir le mot de passe.

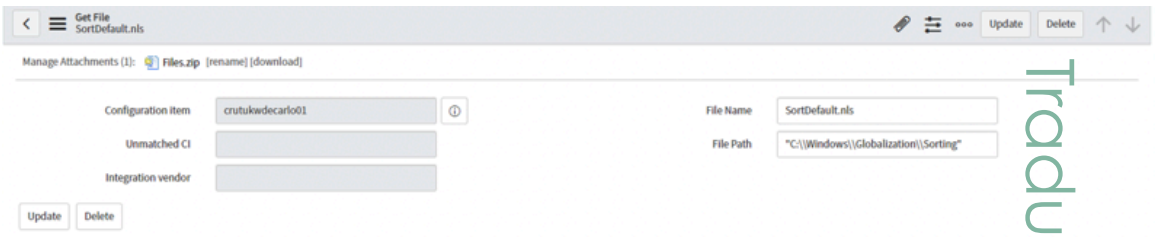
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

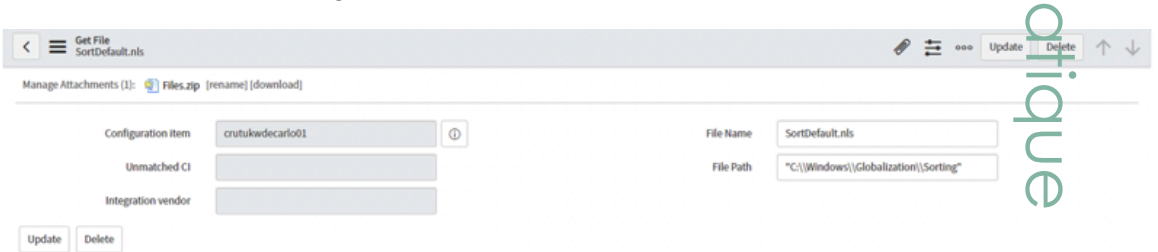
- Ouvrez et vérifiez les fichiers contenus dans le fichier .zip à l'aide de n'importe quel éditeur texte ou XML.

Remarque :

- Il est recommandé d'ajouter manuellement le fichier récupéré en tant qu'observable, afin qu'il puisse être suivi en tant que preuve par rapport à l'incident de sécurité. Cela permettra également de visualiser les fichiers à l'avenir, en cas d'oubli ou de modification du mot de passe.
- La taille de fichier maximale prise en charge pour l'action Obtenir un fichier est de 1 024 Mo, et cette valeur peut être configurée en changeant **com.glide.attachment.max_taille**et le délai d'expiration par défaut est de 60 minutes et peut être configuré à partir de la FireEye HX page Paramètres par défaut.



- L'obtention du fichier peut également être déclenchée à partir de la liste connexe des éléments de configuration.



Traduction automatique

Actions supplémentaires FireEye sur le point de terminaison

L'intégration FireEye prend en charge l'exécution d'actions supplémentaires au-delà des actions de référence.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ces actions comprennent l'acquisition de triage et l'acquisition de données. Prêts à l'emploi, deux acquisitions de données sont prises en charge :

- Script détaillé de l'enquête complète
- Script standard des détails de l'enquête

De plus, l'acquisition de triage est également prise en charge dès le départ. Ces trois éléments sont créés par défaut en même temps que la source. Les clients peuvent également créer leurs propres actions, c'est-à-dire des acquisitions de données à partir du module d'actions supplémentaires FireEye. [1] La taille de fichier maximale prise en charge pour les actions supplémentaires FireEye est de 1 024, et cette valeur peut être configurée en modifiant **com.glide.attachment.max_taille**et le délai d'expiration par défaut est de 120 minutes et peut être configuré à partir de la page Paramètres par défaut FireEye.

Script détaillé de l'enquête complète

Permet de collecter tous les artefacts d'investigation et d'investigation à partir du point de terminaison, mais c'est l'option la plus coûteuse. Cette configuration est idéale pour les situations où il n'y aura qu'une seule fenêtre pour collecter des données à partir du point de terminaison en question et où la possibilité d'acquérir plus de données ne peut pas être garantie ultérieurement. Utilisez donc cette action avec prudence.

Script standard des détails de l'enquête

Active les options les plus courantes de collecte d'artefacts d'investigation et d'expertise à partir d'un point de terminaison. Destiné à être l'outil de réponse principal lorsque vous soupçonnez qu'un point de terminaison peut être compromis et que vous devez effectuer une analyse approfondie de ce point de terminaison. Vise à trouver un équilibre entre la collecte des données les plus pertinentes et les plus précieuses tout en évitant les options coûteuses qui peuvent être collectées plus tard une fois qu'une enquête plus approfondie s'avère nécessaire.

Acquisition du triage

Les collections de triage contiennent des informations provenant du cache de vérification ainsi que des informations d'audit judiciaire supplémentaires, telles que l'historique des téléchargements d'URL, l'historique des téléchargements de fichiers, les listes de processus et de ports et les informations système standard. Vous souhaiterez peut-être examiner ces informations lorsqu'un trafic réseau anormal est détecté et vous souhaitez plus de visibilité sur les actions des points de terminaison.

Gestion des scripts d'acquisition de données sur FireEye

Les demandes d'acquisition de données (parfois appelées demandes de réponse en direct) vous permettent d'acquérir toutes les données dont vous avez besoin à partir d'un seul point de terminaison en cours d'exécution. À l'aide de la page Scripts d'acquisition de données de FireEye, vous pouvez créer, modifier, copier et supprimer les scripts d'acquisition de données utilisés pour les demandes d'acquisition de données.

Accéder à la page Scripts d'acquisition de données sur FireEye

Pour accéder à la page Scripts d'acquisition de données :

1. Accédez à l'interface utilisateur Web Endpoint Security.
2. Sélectionnez Scripts d'acquisition de données dans le menu Administrateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Création d'un script sur FireEye

Pour créer un script d'acquisition de données :

1. Sélectionner **Scripts d'acquisition de données** > **Administrateur** de l'interface utilisateur Web d'Endpoint Security.
2. Cliquer sur **Créer un script**.
3. Entrez un nom pour le nouveau script dans le champ **Nom du script** champ.
4. Vous pouvez également entrer une description du script.
5. Sélectionnez le système d'exploitation auquel le script s'applique. Vous ne pouvez sélectionner qu'un seul système d'exploitation dans la boîte de dialogue Créer un script.
6. Cliquer sur **Créer** pour démarrer la définition de script.
7. Sélectionner un type de données d'acquisition dans le **Ajouter un type d'acquisition**dans la liste déroulante et cliquez sur **Ajouter**. Les options pour le type d'acquisition que vous avez demandé apparaissent à droite de la liste de scripts.
8. Fournissez des valeurs pour les options de type d'acquisition ou utilisez les valeurs par défaut déjà sélectionnées. L'interface utilisateur Web ne vous avertit pas et ne supprime pas les onglets, les espaces ou les caractères indésirables (tels que \n) dans vos spécifications.
9. Répétez les 2 étapes précédentes pour demander des données supplémentaires pour le script d'acquisition de données. Certains types de données d'acquisition ne sont disponibles qu'une seule fois pour un script, tandis que d'autres peuvent être spécifiés plus d'une fois. Après l'ajout d'un type d'acquisition à un script, la liste des types d'acquisition disponibles dans le **Ajouter un type d'acquisition**La liste déroulante s'ajuste en conséquence.
10. Pour supprimer un type de données d'acquisition du script, cliquez sur l'icône x ( ) dans l'onglet d'acquisition sur le côté gauche de la page.

Remarque : Cette intégration ne prend pas en charge **Autoriser les modifications avant l'acquisition** lors de la création de scripts. Assurez-vous donc que la case n'est pas cochée.

Exportation d'un script à partir de FireEye

Vous pouvez exporter un script d'acquisition de données vers un fichier JSON. Pour exporter un script d'acquisition de données :

1. Sélectionner **Scripts d'acquisition de données** > **Administrateur** de l'interface utilisateur Web Endpoint Security.
2. Sélectionnez Scripts d'acquisition de données dans le menu Administrateur.
3. Sélectionnez le script que vous souhaitez exporter sur le côté gauche de la page.
4. sélectionner **Actions** > **Exporter le script**.
5. Un fichier JSON est téléchargé sur votre ordinateur. Le nom du fichier JSON inclut le système d'exploitation, ce qui vous permet de déterminer facilement quels scripts sont destinés à quel système d'exploitation.

Création d'une nouvelle action d'acquisition de données dans Now Platform

Pour créer une action, procédez comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Intégration de FireEye** > **Actions supplémentaires FireEye**. La liste des actions supplémentaires FireEye s'affiche.
2. Cliquer sur **Nouveau**. Le formulaire de la nouvelle action s'affiche.
3. Remplissez le formulaire.

Nom de l'action	Nom de l'action FireEye exécutée. Ce nom vous aide à identifier le type d'action et à le décrire.
Achat	Une acquisition permet d'obtenir les données à analyser. Il s'agit d'un champ en lecture seule, dont la valeur par défaut est Acquisition de données.
Source	Nom de la source FireEye. Seules les sources configurées sont disponibles dans la liste de choix.
Option	Il s'agit d'un champ en lecture seule, renseigné avec l'option Exécuter une ou plusieurs actions supplémentaires
Type d'acquisition	Type d'action d'acquisition qui doit être obtenue et analysée.
Actif	Cela indique que l'action est active.
Exiger l'approbation	Lorsque vous activez l'option Exiger l'approbation, le champ Approbateurs est disponible sur le formulaire. Après avoir soumis une demande, le groupe doit obtenir l'approbation du groupe.
Balise d'affichage	Type de système d'exploitation tel que Windows, Mac, Linux pour l'ajout de scripts. **Remarque :** Un seul type de système d'exploitation est actuellement pris en charge. Vous ne pouvez créer qu'une seule action par système d'exploitation. Pour les autres systèmes d'exploitation, créez de nouvelles actions selon les besoins.
Scripts	Le script importé de FireEye doit être fourni pour le type de système d'exploitation sélectionné. Un seul script peut être ajouté à chaque type de système d'exploitation.

4. Cliquer sur **Soumettre**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déclenchement des acquisitions de données à partir d'un incident de sécurité

Les actions supplémentaires créées peuvent être exécutées via le lien connexe appelé **Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison** sur l'incident de sécurité.

Remarque : **Autoriser les modifications avant l'acquisition** La fonctionnalité FireEye n'est pas prise en charge pour les actions supplémentaires sur le point de terminaison.

Créer et configurer un profil pour la recherche de perceptions avec l'intégration FireEye

Configurez le profil de recherche de perceptions à l'aide de la procédure suivante.

Avant de commencer

Rôle requis : administrateur d'incident de sécurité Now Platform (sn_si.admin)

Chaque fois qu'une source est créée, des configurations de recherche de perceptions individuelles pour cinq types (Fichier, IP (v4), MD5, SHA1 et SHA256) seront créées et inactives par défaut. Vous devez l'activer avant d'utiliser la recherche de perception. Chaque type d'observable a une requête de recherche différente pour récupérer les observations. Nous lancerions une recherche différente pour chaque type d'observable. La recherche de plusieurs observables pour une recherche d'observation n'est pas possible dans FireEye, car elle effectuerait une opération ET sur les observables et le résultat pourrait être inexact.

Remarque : Pour la recherche d'observations, seules cinq recherches actives peuvent être présentes à la fois. Les observations restantes seront mises en file d'attente et commenceront après la fin de l'une des observations en cours.

Si vous souhaitez créer un profil de recherche de perceptions, suivez les étapes ci-dessous pour en créer un :

Procédure

1. Accédez à la **Intégrations** > **Configuration de la recherche de perceptions**.
2. Cliquer sur **Nouveau**.
3. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom du profil d'aptitude.
Est une recherche enregistrée	Exécutera une recherche enregistrée, par exemple, le champ Nom doit correspondre au nom de la recherche enregistrée.
Source de recherche de perceptions	Définit la source configurée pour l'intégration.
Rechercher	Ajoutez une chaîne de recherche native pour former une requête.
Actif	La requête s'exécutera uniquement si elle est active.
Type d'observable	Définit le type de catégorie de l'observable.
Nombre maximum d'observables par recherche	Le nombre d'observables avant que la requête de recherche ne soit fractionnée

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	en plusieurs requêtes. Définissez cette valeur sur 1 pour cette intégration.
Paramètres de la recherche de perceptions	Utilisez les paramètres de recherche de perceptions pour définir des requêtes plus complexes qui incluent la logique et d'autres opérateurs pris en charge par le magasin de journaux spécifié.

4. Cliquer sur **Soumettre** pour terminer la configuration.

Invoquer la recherche de perception à partir d'un incident de sécurité

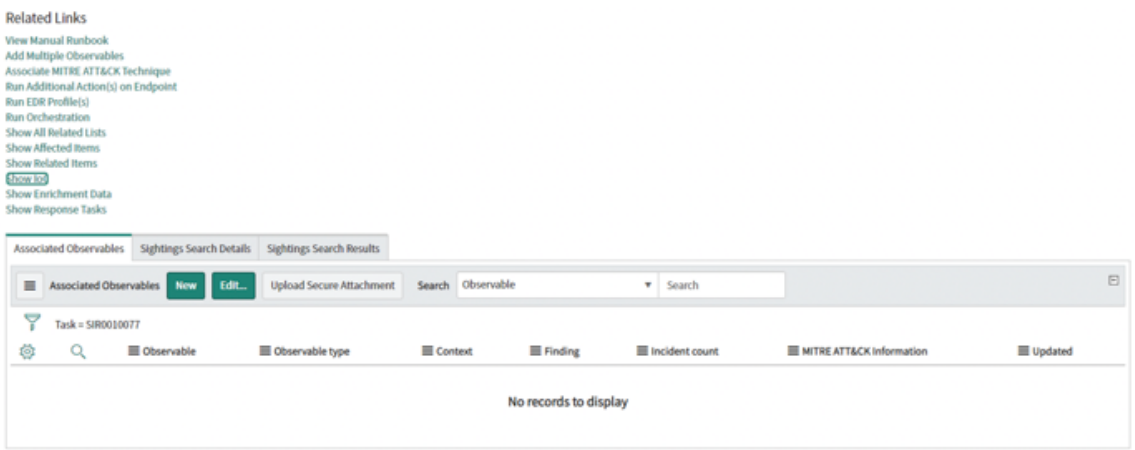
Invoquer la recherche de perceptions à partir d'un incident de sécurité SIR en suivant la procédure ci-dessous.

Avant de commencer

Rôle requis : administrateur Now Platform (sn_si.admin)

Procédure

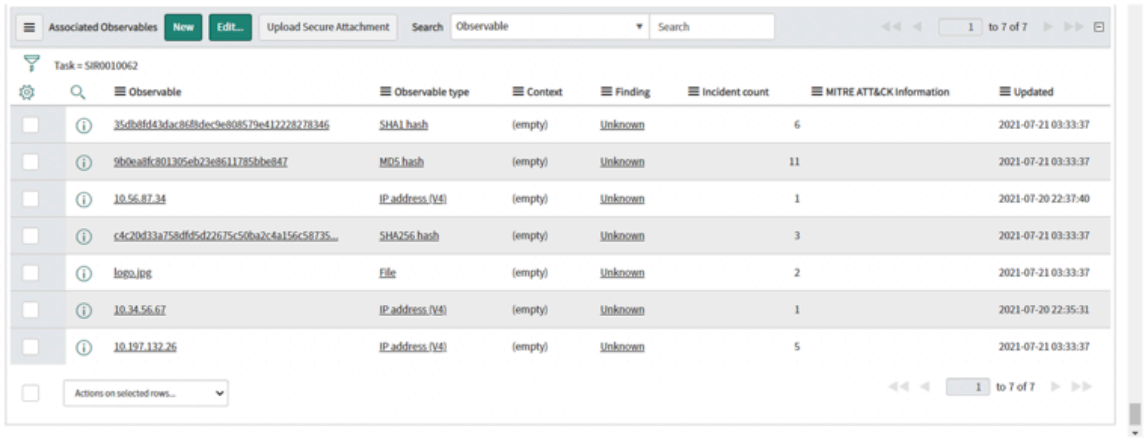
1. Accédez aux incidents de sécurité.
2. Ouvrez n'importe quel SIR existant ou créez-en un nouveau.
3. Cliquez sur Afficher IoC dans les liens connexes.
4. Cliquer sur **Observables associés** listes connexes.



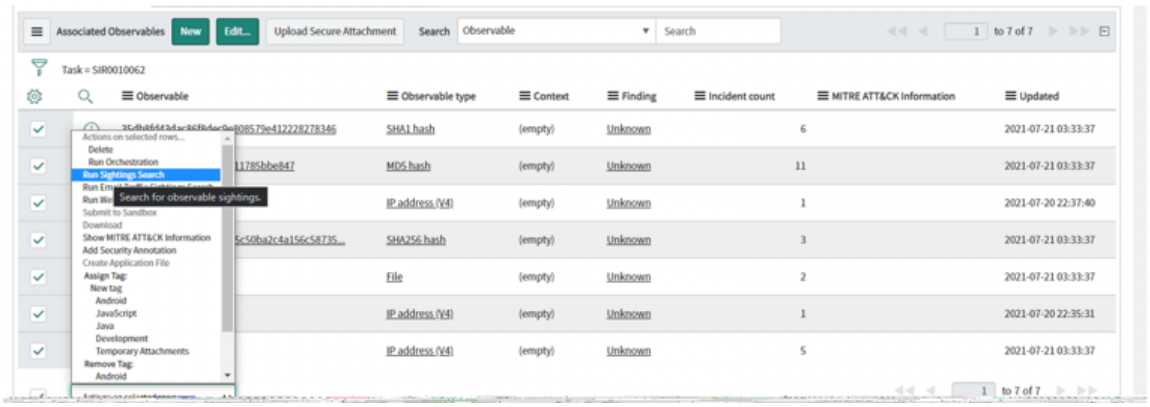
5. Ajoutez des observables existants ou créez un nouvel observable.

Traduction automatique

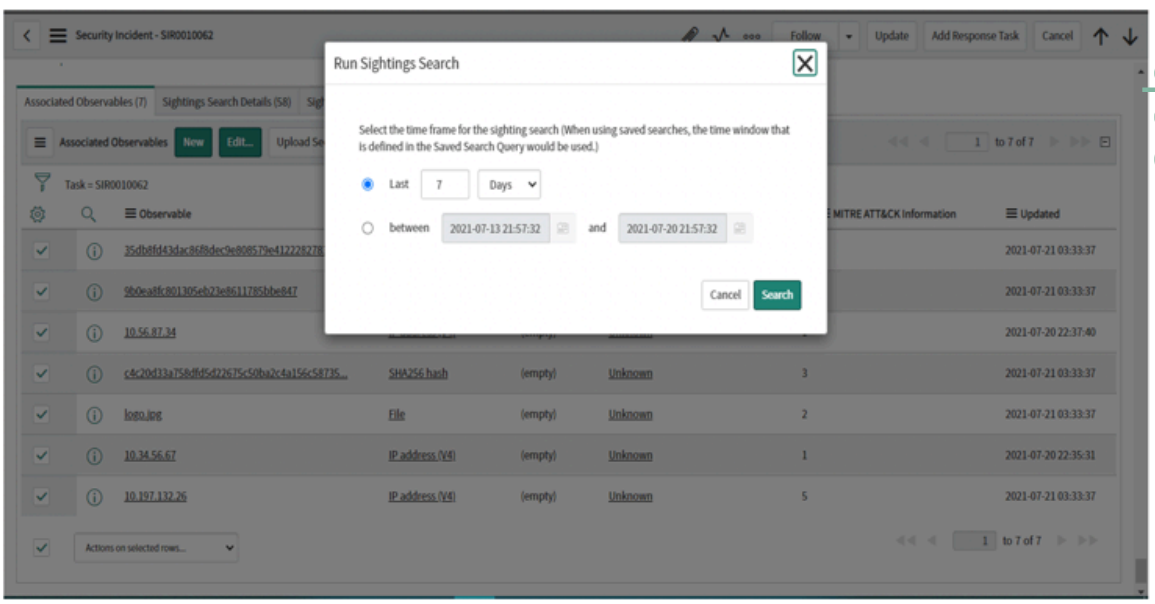
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Sélectionner les observables et, dans Actions sur les lignes sélectionnées, cliquer sur **Exécuter la recherche de perception**.



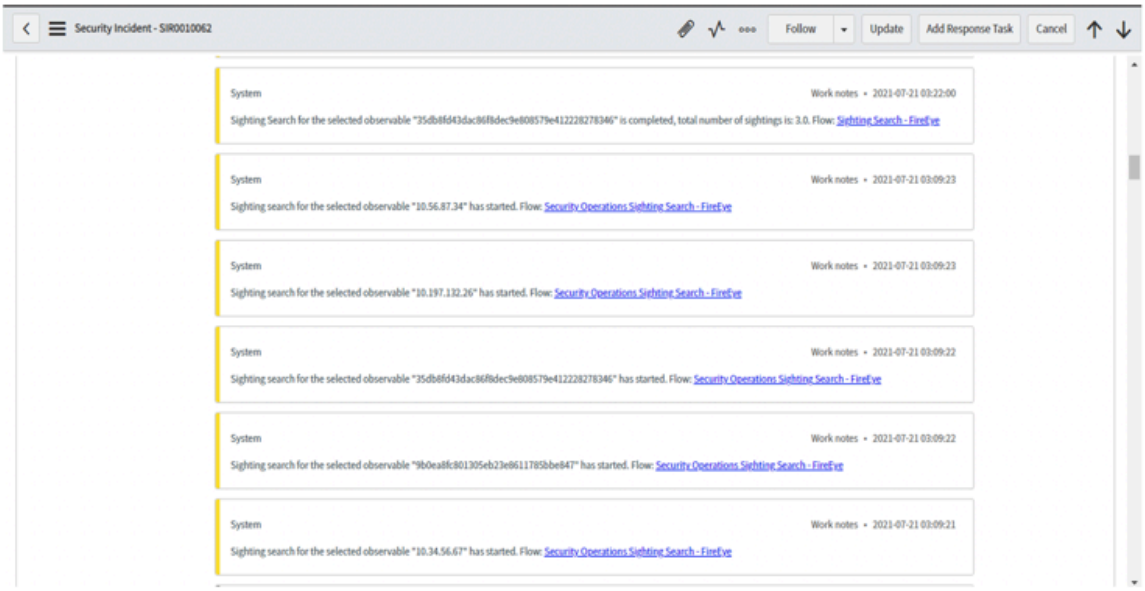
7. Ignorez les entrées de la boîte de dialogue suivante qui demande des données horaires. Les valeurs par défaut sont renseignées. Toutefois, la recherche est effectuée en temps réel et les valeurs de temps sont ignorées pour cette intégration.



8. Vérifiez l'état dans les notes de travail.

Traduction automatique

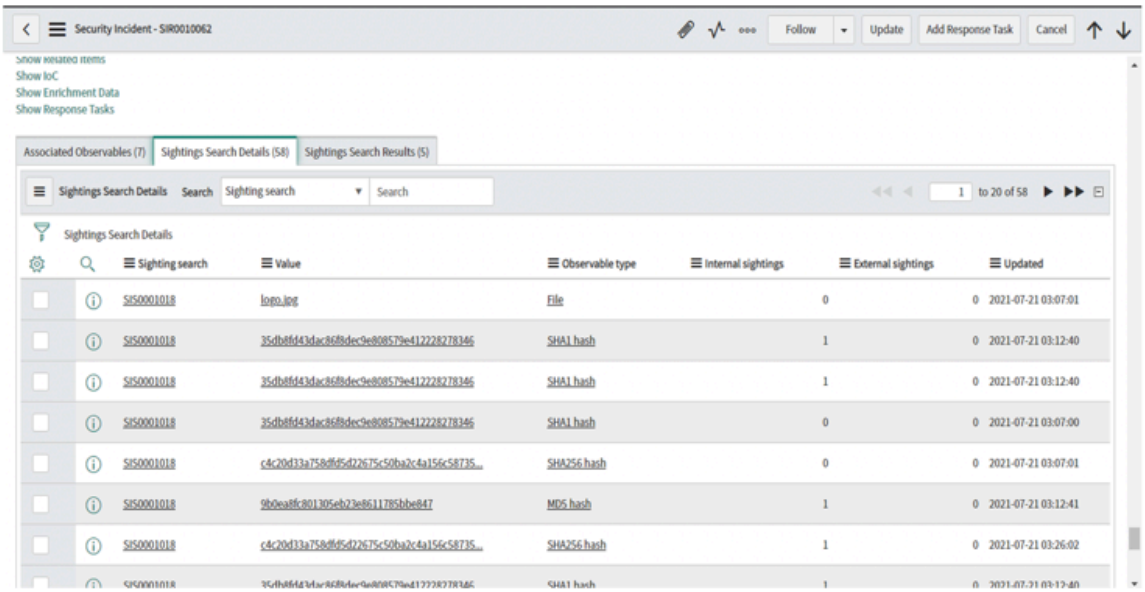
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

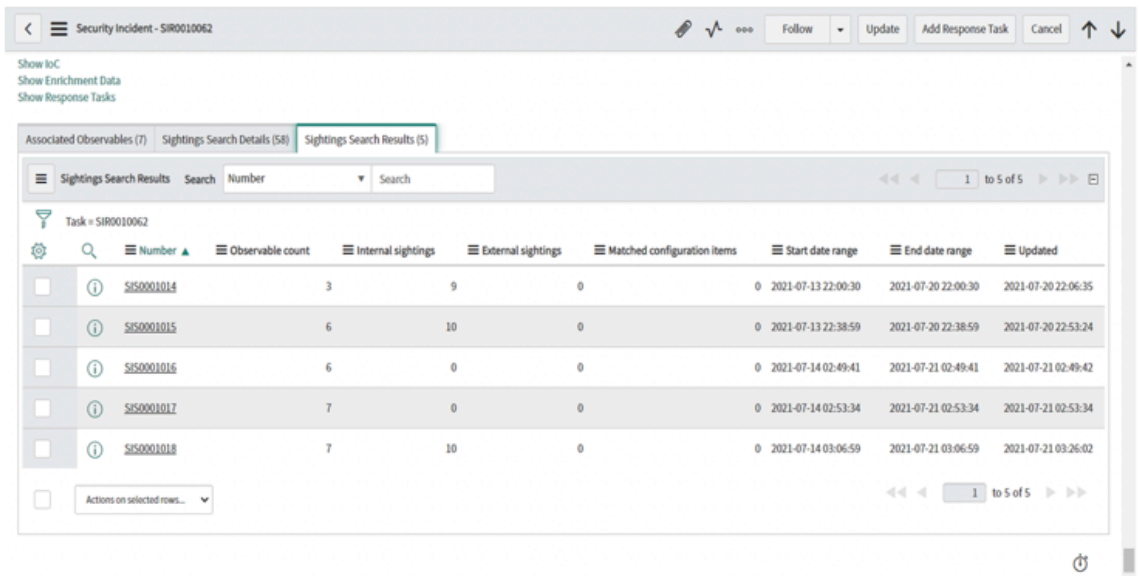


9. À la fin de la recherche, vérifiez les résultats et les détails dans les listes connexes.
10. Cliquez sur **Détails de la recherche de perception** pour plus de détails et **Résultats de recherche de perceptions** Onglet des résultats de la recherche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





Traduction automatique

Have I been pwned? intégration

L'intégration Opérations de sécurité Have I been pwned? vous permet de soumettre des recherches sur les noms de domaine et les adresses e-mail pour déterminer si les données personnelles des utilisateurs ont été compromises par des violations de données.

Explorer Intégrations de Réponse aux incidents de sécurité	**Configurer** • Configuration de l'intégration de Security Operations Have I been pwned? • Activer l'intégration Security Operations Have I been pwned?
Utiliser	**Développer**

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Effectuer des recherches sur les observables Recherche de menace : Have I been pwned? flux	• ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide • Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service et assistance client	

Configuration de l'intégration de Security Operations Have I been pwned?

Have I been pwned? est une ressource gratuite utilisée pour évaluer si une personne a pu être mise en danger en raison de la compromission ou de la violation de données de son compte en ligne. Il s'intègre facilement à Opérations de sécurité.

Avant de pouvoir utiliser l'intégration Have I been pwned? , vous devez activer le module d'extension. Si nécessaire, vous pouvez également mettre à jour votre certification X509 SSL.

Les Réponse aux incidents de sécuritémodules d'extension , Renseignements sur les menaces, et Opérations de sécurité Have I been pwned? sont requis pour implémenter l'intégration Opérations de sécurité Have I been pwned? .

Recherche de menace : Have I been pwned? flux

Le flux Recherche Have I been pwned? de menace - effectue une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par , les observables sont analysés à Have I been pwned?la recherche de programmes malveillants et les résultats sont renvoyés.

Rôle requis : sn_si_admin

Ce flux est déclenché lorsque Security Operations Integration - Aptitude Recherche de menace vous effectuez une recherche de menace sur un ou plusieurs observables et que l'implémentation Have I been pwned? est sélectionnée. Pour plus d'informations, consultez Effectuer des recherches sur les observables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ai-je été pwned flow



Pour en savoir plus sur les activités utilisées par ce flux, reportez-vous à Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Activer l'intégration Security Operations Have I been pwned?

La fonctionnalité de configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration Opérations de sécurité Have I been pwned? . Avant de pouvoir utiliser l'intégration Have I been pwned? , vous devez la télécharger à ServiceNow Storepartir du fichier .

Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être installé et activé avant de pouvoir utiliser l'intégration Opérations de sécurité Have I been pwned? .

Rôle requis : sn_si_admin

Procédure

Téléchargez l'intégration à partir de ServiceNow Store.
Cette intégration prend en charge une API ouverte et ne nécessite pas de configuration supplémentaire. Have I been pwned? peut maintenant être sélectionné pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Mettre à jour votre certificat X.509

Si vous avez besoin d'une connexion SSL pour l'intégration, il peut arriver que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou qu'il ait expiré. Cette tâche est facultative.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Procurez-vous le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.

   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
   Par exemple : `https://<3rdparty>/`.

   b. Cliquez sur l'icône de cadenas dans la ligne d'adresse.

   c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .

   d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .

   e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.

   f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
   Il doit commencer par `-----BEGIN CERTIFICATE` ----- et se terminer par `-----END CERTIFICATE`-----.

2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Ajoutez le certificat à l'enregistrement du fournisseur d'identité.
   a. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
   b. Sélectionnez le fournisseur d'identité par défaut actif pour lequel vous avez créé le nouveau certificat.
   c. Faites défiler vers le bas jusqu'à la liste connexe **des certificats X.509** , puis cliquez sur **Modifier**.
   d. Déplacez le certificat nouvellement créé vers la colonne **Sélectionné** .
6. Cliquez sur **Enregistrer**.
   Les autres champs de l'enregistrement sont générés automatiquement.

> **Remarque :** Si vous avez un certificat qui a expiré, vous devez le supprimer. Pour plus d'informations sur la suppression du certificat expiré, reportez-vous à KB0691439 Remplacement d'un certificat SAML arrivant à expiration .

HPE Security ArcSight ESM - Intégration de l'analyseur d'e-mails

L'intégration de l'analyseur d'e-mails HPE Security ArcSight ESM est prise en charge à l'aide d'un analyseur d'e-mails qui utilise les notifications par e-mail d'ESM pour créer des incidents de sécurité.

Configurer HPE Security ArcSight ESM : intégration de l'analyseur d'e-mails

L'intégration de l'analyseur d'e-mails de HPE Security ArcSight ESM utilise les notifications par e-mail d'ESM pour diriger les workflows d'enrichissement et de réponse.

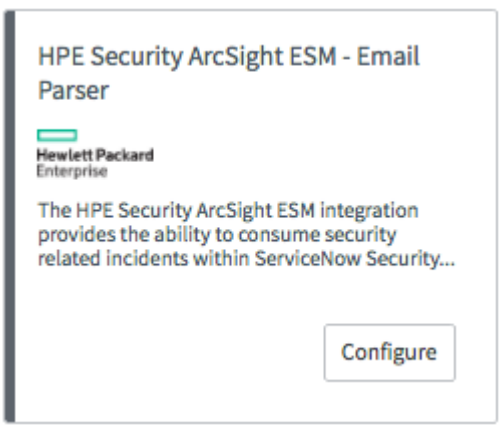
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si_admin

Pourquoi et quand exécuter cette tâche
Un modèle d'analyseur d'e-mails HPE Security ArcSight ESM est fourni pour être utilisé pour l'intégration. Il doit être configuré et activé avant que l'intégration n'ait lieu. La mise à jour de l'analyseur l'active.

Procédure
1. Accédez à la **Tout** > **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.



2. Dans la carte de l'analyseur d'e-mails HPE Security ArcSight ESM, cliquez sur **Configurer**.
3. Dans la boîte **de dialogue HPE Security ArcSight ESM - Email Parser Configuration (Configuration de l'analyseur d'e-mails**), cliquez sur le lien **Configurer l'analyseur d'e-mails** .
4. Cliquez sur le lien **ArcSight ESM** pour modifier les paramètres dans l'analyseur d'e-mail de modèle fourni.
   Renseignez au minimum le champ `L'e-mail provient de` . Pour créer votre propre analyseur d'e-mails, reportez-vous à la section Créer des analyseurs d'e-mails dans Security Operations.
5. Cochez la case **Actif** .
6. Cliquez sur **Mettre à jour** dans le formulaire **Analyseur d'e-mail** .
   L'analyseur d'e-mail est actif. Vous n'avez pas besoin de revenir aux **configurations d'intégration**.

HPE ArcSight Logger - Intégration de l'enrichissement des incidents

L'intégration HPE ArcSight Logger d'enrichissement d'incident recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer	Configurer
Intégrations de Réponse aux incidents de sécurité	• Commencez avec l'intégration de l'enrichissement HPE ArcSight Logger des incidents • Créer des enregistrements de configuration de recherche d'observations

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser

- Exécuter une recherche d'observations
- Security Operations Integration - Workflow de recherche de perceptions
- Opérations de sécurité : workflow de recherche de perceptions Arcsight Logger
- Afficher les détails de la recherche d'observations
- Afficher les résultats de recherche d'observations

Développer

- ServiceNow Opérations de sécurité Directives de développement de l'intégration
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté des opérations de sécurité
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Commencez avec l'intégration de l'enrichissement HPE ArcSight Logger des incidents

HPE ArcSight Logger diffuse des données en temps réel et les catégorise dans des journaux spécifiques et s'intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l'intégration HPE ArcSight Logger d'enrichissement d'incident, vous devez la télécharger à partir de et ajouter l'URL de l'API ServiceNow Store et les informations d'identification de connexion.

Avant de commencer

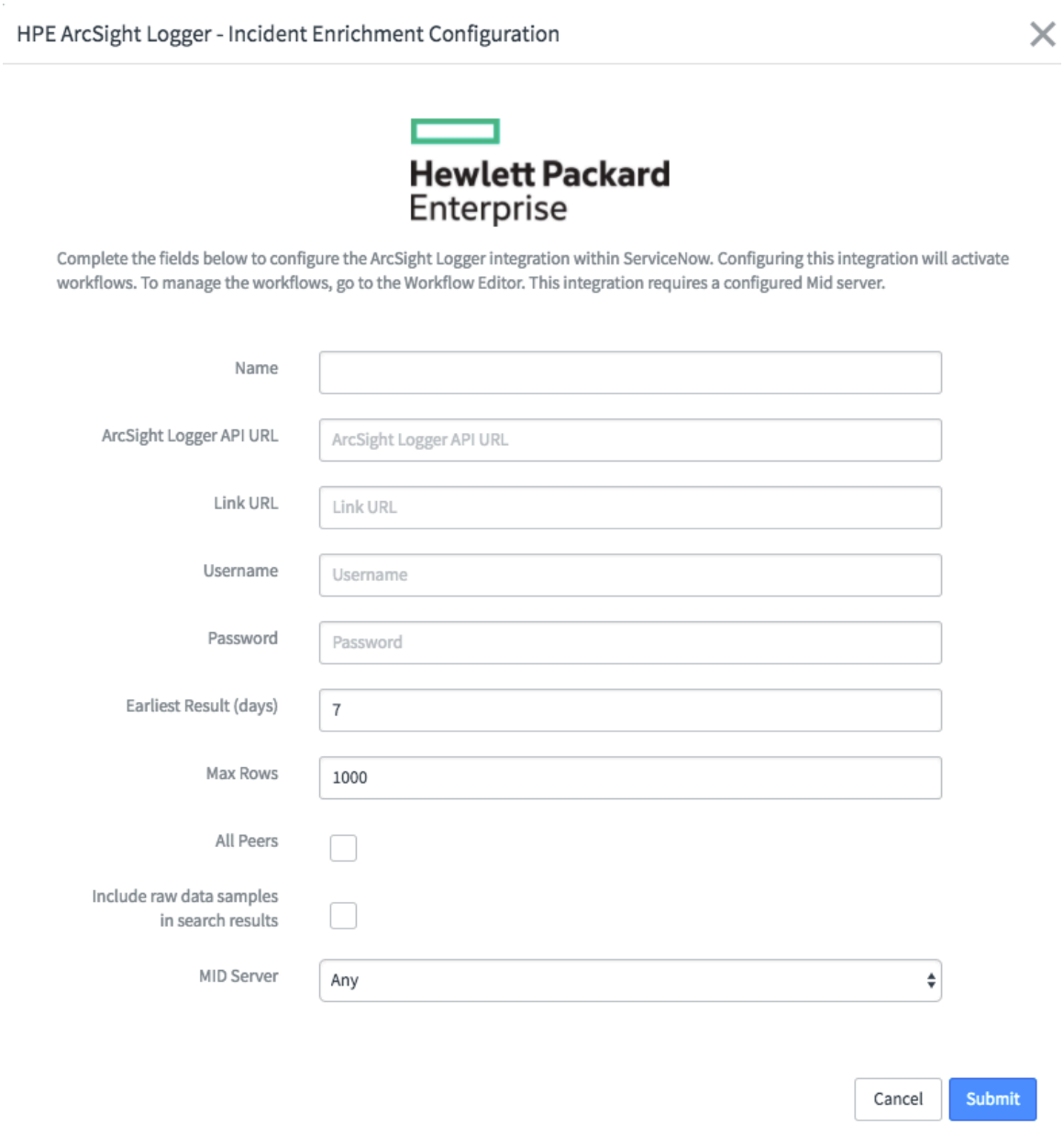
Rôle requis : sn_si_admin

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Sur la carte Enrichissement d'incident HPE ArcSight Logger , cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

4. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
URL de base de l'API ArcSight Logger	URL de base que vous avez acquise à partir du site HPE Security ArcSight Logger.
URL de lien	[Facultatif] URL du lien qui établit un lien vers une instance de HPE Security ArcSight Logger, lorsqu'elle est disponible.
Nom d'utilisateur	Votre nom d'utilisateur Intel HPE ArcSight Logger .
Mot de passe	Votre mot de passe Intel HPE ArcSight Logger .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tous les pairs	La valeur par défaut n'est pas cochée et ne recherche que l'enregistreur local auquel vous êtes connecté. Lorsqu'elle est cochée, elle recherche tous les enregistreurs connectés les uns aux autres.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend du paramètre que vous définissez sur le **nombre de lignes de la propriété de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	Sélectionnez **N'importe lequel** pour utiliser n'importe quel Serveur MID actif ou sélectionnez un nom de Serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

5. Cliquez sur **Envoyer**.
   La carte de configuration de l'intégration s'affiche.
6. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
7. Pour revenir à la liste initiale des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Hybrid Analysis intégration

L'application Hybrid Analysis fait partie d'une communauté en ligne ouverte dans laquelle les utilisateurs analysent les fichiers et les URL à la recherche de menaces. Vous partagez les résultats et utilisez les recherches de la communauté pour des réponses plus efficaces aux incidents. Lorsqu'elles sont intégrées au Now Platform Opérations de sécurité produit, les renseignements sur les menaces partagés vous fournissent des informations supplémentaires sur la gravité d'observables spécifiques.

L'intégration Hybrid Analysis effectue des recherches de menaces sur les observables suivants :

- Hachages de fichiers
- Adresses IP
- URL

Le flux recherche les nouveaux observables à mesure qu'ils arrivent dans les incidents de sécurité. Si les observables sont d'un type reconnu par l'intégration de l'API, les observables sont évalués. Les observables jugés malveillants sont étiquetés.

Installer et configurer Hybrid Analysis

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration pour que l'application s'intègre Hybrid Analysis correctement à Now Platform Opérations de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform AND Réponse aux incidents de sécurité .	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur (admin) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration et vérifie les résultats attendus. Ce rôle a également accès au Opérations de sécurité module et attribue le rôle sn_si.analyst.
Procurez-vous une clé API.	Visitez le site Web d'Hybrid Analysis pour plus d'informations sur les clés API et pour créer un compte : site Web d'Hybrid Analysis . La configuration nécessite que vous saisissiez les clés API.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Pour la version Madrid et les versions ultérieures de la famille, le module d'extension com.snc.si_dep est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications. Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour garantir une installation fluide : **1.** Cadre de travail de Security Integration **2.** Security Support Common **3.** Orchestration de support de sécurité **4.** Réponse aux incidents de sécurité Pour en savoir plus sur la configuration de votre Now Platform instance pour l'intégration, consultez et .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : administrateur

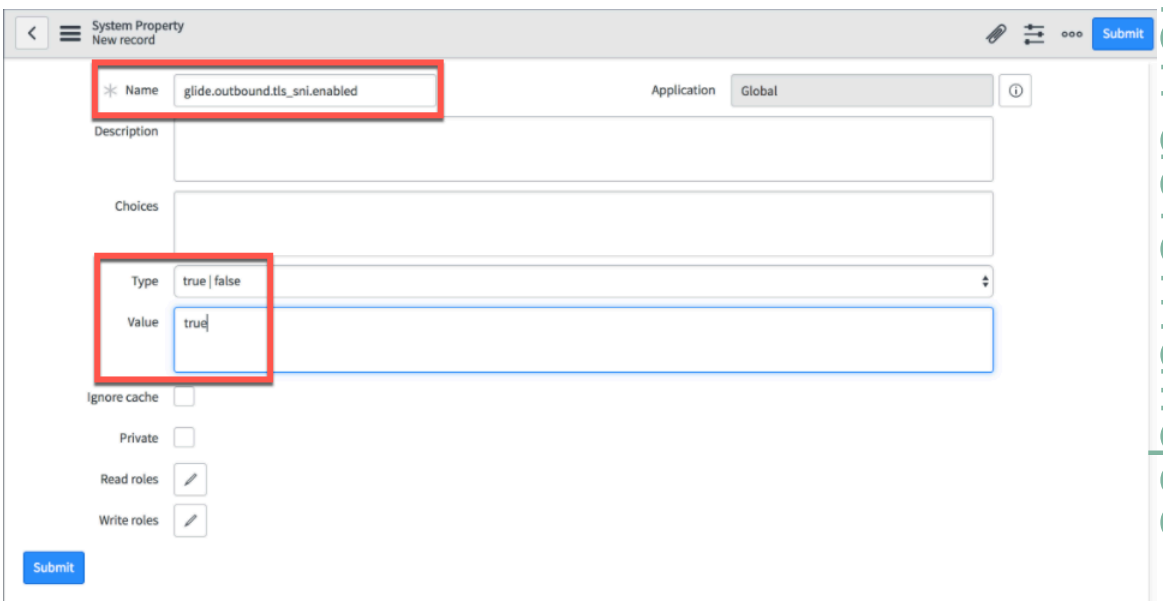
Pourquoi et quand exécuter cette tâche

Procédez comme suit pour mettre à jour les propriétés système et installer et configurer l'intégration.

Procédure

1. Dans le filtre de navigation, saisissez `sys_properties.list`, puis appuyez sur la touche **Entrée**.
   La liste **des propriétés système** s'affiche.
2. Cliquez sur **Nouveau**.
   Un nouvel enregistrement s'affiche.
3. Renseignez les champs ou sélectionnez les valeurs répertoriées dans la table suivante et cliquez sur **Soumettre**.

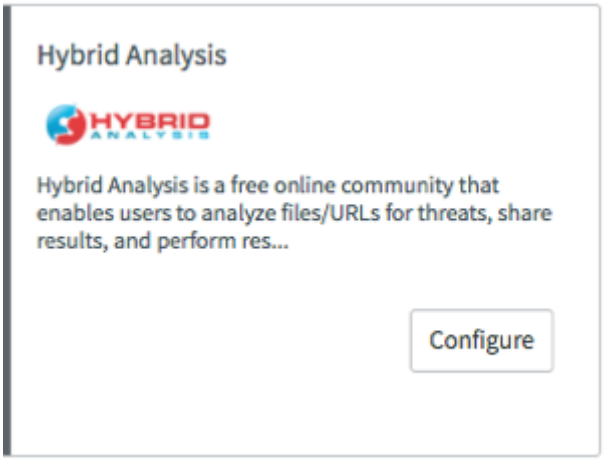
Nom de champ	Valeur
Nom	`glide.outbound.tls_sni.enabled`
Type	Sélectionner **vrai I faux**
Valeur	`true`



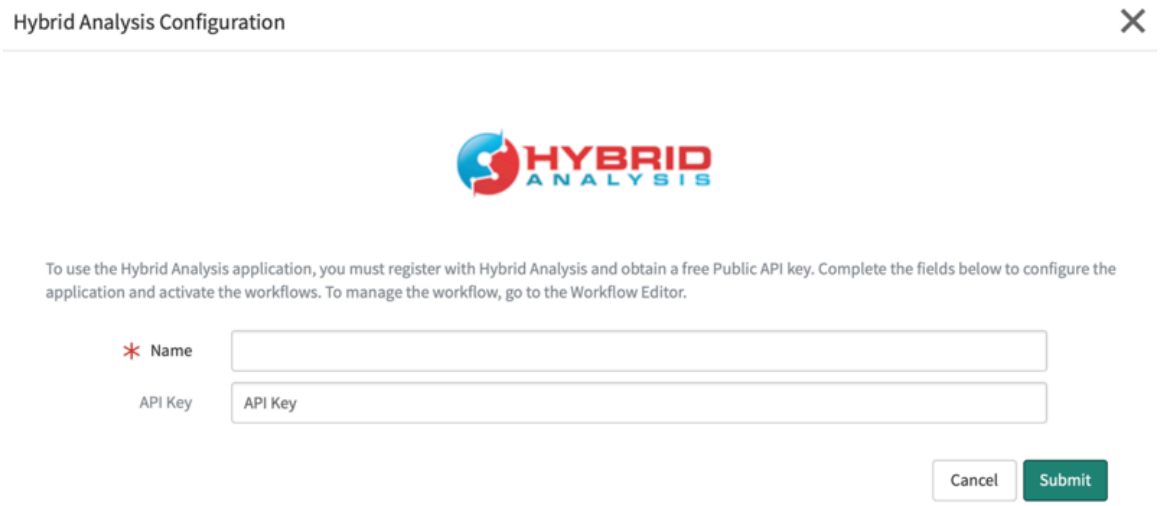
4. Si vous n'avez pas installé l'application pour l'intégration, consultez et suivez les étapes pour l'installer.
5. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la Hybrid Analysis tuile.
6. Cliquez sur **Configurer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Dans la boîte de dialogue **Configuration de l'analyse hybride** , entrez la clé API que vous avez obtenue à partir du Hybrid Analysis site Web et cliquez sur **Envoyer**.



8. Vérifiez que la configuration est correcte.
La configuration est terminée avec succès, sauf si un message d'erreur s'affiche.

Trouble?

Si un message d'erreur s'affiche lors de la configuration, la clé API n'est Hybrid Analysis peut-être pas valide.

Vérifier les résultats attendus pour Hybrid Analysis

Les observables sont générés automatiquement par un incident de sécurité et analysés par l'application. Localisez les résultats de la recherche sur l'incident de sécurité pour vérifier que la recherche de menaces a été exécutée avec succès. Affichez également les données brutes et exécutez des recherches de menaces sur les observables enfants.

Avant de commencer

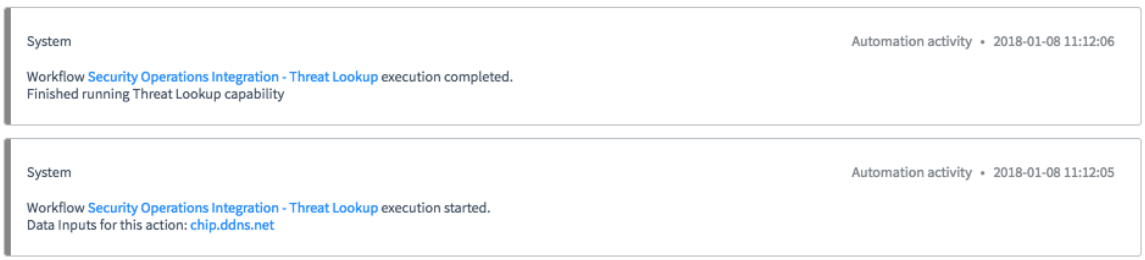
Rôle requis : sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez l'enregistrement d'incident de sécurité avec lequel vous travaillez et vérifiez que la recherche a été exécutée avec succès.

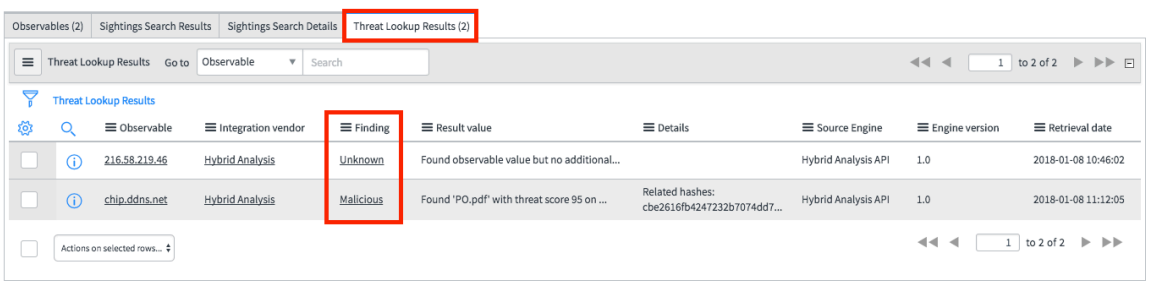


   Une fois l'application configurée, le flux se lance automatiquement lors de la création de l'incident. L'état d'exécution et d'achèvement de la recherche est ensuite affiché dans les notes de travail de l'incident de sécurité.

2. Examinez les notes de travail pour plus d'informations sur la façon de procéder si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.

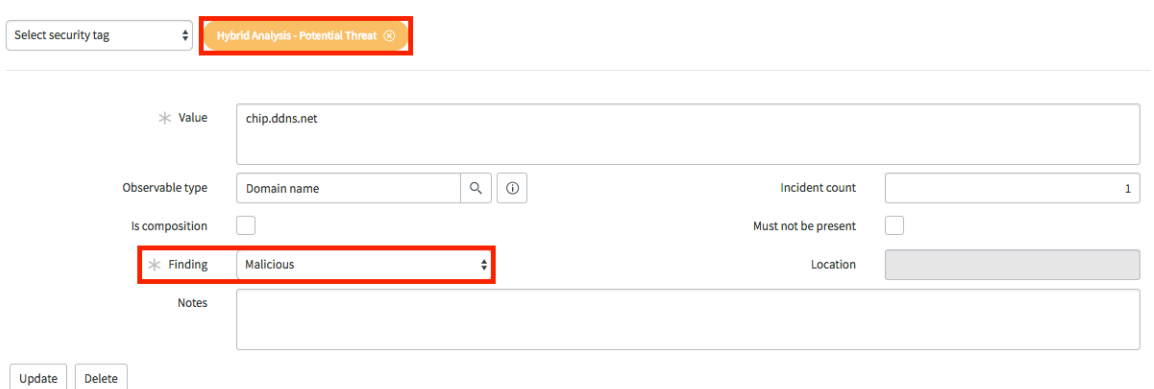
3. Naviguez jusqu'au bas de l'enregistrement d'incident de sécurité et cliquez sur le lien connexe **Afficher toutes les listes connexes** pour afficher les résultats.

   Remarque : Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres du système. Dans le coin supérieur droit de la bannière, cliquez sur l'icône d'engrenage Paramètres. Dans la boîte de dialogue **Paramètres du système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que les **champs Formulaires à onglets** et **Avec formulaire** sont sélectionnés.



   L'onglet Résultats de la recherche de menace affiche les résultats de la recherche au bas de l'enregistrement d'incident de sécurité. Notez que la colonne **Résultat** affiche `Inconnu` pour les enregistrements qui n'ont pas été déterminés comme malveillants. Pour les résultats correspondant à malveillants, la colonne **Résultat** affiche `malveillant`.

4. Dans la colonne **Observable** , cliquez sur un observable pour ouvrir l'enregistrement.



Traduction automatique

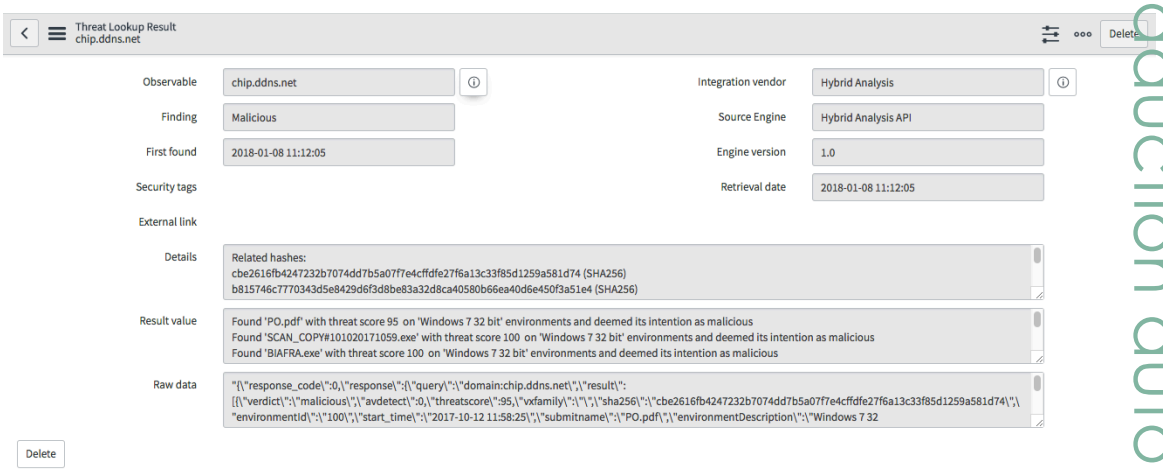
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour les recherches correspondant à malveillant, le champ **Résultat** affiche `malveillant` et l'observable est étiqueté avec la source qui l'a trouvé malveillant, dans ce Renseignements sur les menaces cas, l'intégration Hybrid Analysis .

5. Facultatif : Suivez les étapes pour afficher les données brutes, afficher une liste des observables enfants et exécuter une recherche de menace sur les observables enfants sélectionnés.

   a. Revenez à l'incident de sécurité et, dans l'onglet **Résultats de la recherche de menace** , cliquez sur l'icône d'informations bleue en regard d'un observable.

   b. Dans la fenêtre qui s'affiche, cliquez sur **Ouvrir l'enregistrement** pour afficher les données.
   À partir de tous les observables visibles dans les données brutes affichées à partir de la recherche, l'intégration Hybrid Analysis crée également des observables enfants ou connexes.



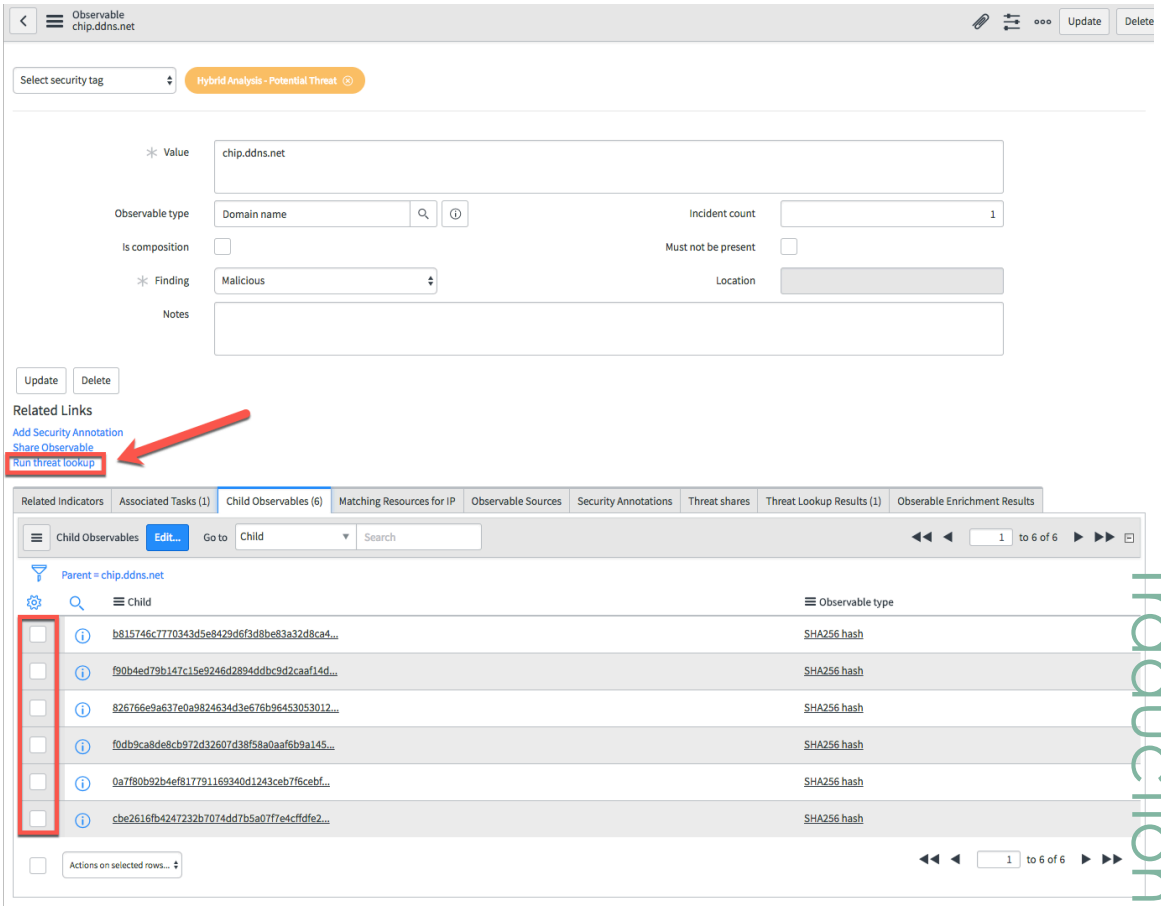
   Le lien créé par l'API, les données brutes et d'autres informations s'affichent.

   c. Revenez à l'incident de sécurité et cliquez sur le lien connexe **Afficher IoC** .
   Les observables enfants sont affichés dans l'onglet **Observables enfants** de l'incident de sécurité, car la recherche a trouvé un lien existant entre ces observables associés et l'observable initialement soumis.

   d. Cliquez sur le champ en regard d'un observable dans la colonne **Enfant** pour le sélectionner, puis sur le lien connexe **Exécuter la recherche de menace** pour effectuer une recherche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



e. Dans la boîte de dialogue qui s'affiche, vérifiez que l'intégration Hybrid Analysis est sélectionnée et cliquez sur **Soumettre**.

f. Dans les notes de travail, vérifiez que la recherche a été exécutée avec succès et, dans l'onglet Résultats de la **recherche de menace** de l'incident de sécurité, localisez les résultats de la recherche pour les observables enfants.

Trouble?
Si vous ne voyez pas de résultats sous l'onglet **Résultats de la recherche de menace** , vérifiez que l'observable est d'un type pris en charge pour la recherche par l'intégration.

(Facultatif) Joindre manuellement un observable pour Hybrid Analysis

Vous pouvez joindre manuellement des observables lorsque vous souhaitez effectuer des recherches de menaces sur des observables qui ne sont pas joints à un incident de sécurité sur le déclencheur d'événement initial. Vous pouvez également effectuer cette tâche lorsque vous souhaitez plus d'informations sur un observable associé.

Avant de commencer

Vérifiez que l'observable est d'un type pris en charge par l'intégration. L'intégration effectue des recherches sur les types d'observables suivants :

- Hachages de fichiers
- Adresses IP
- URL

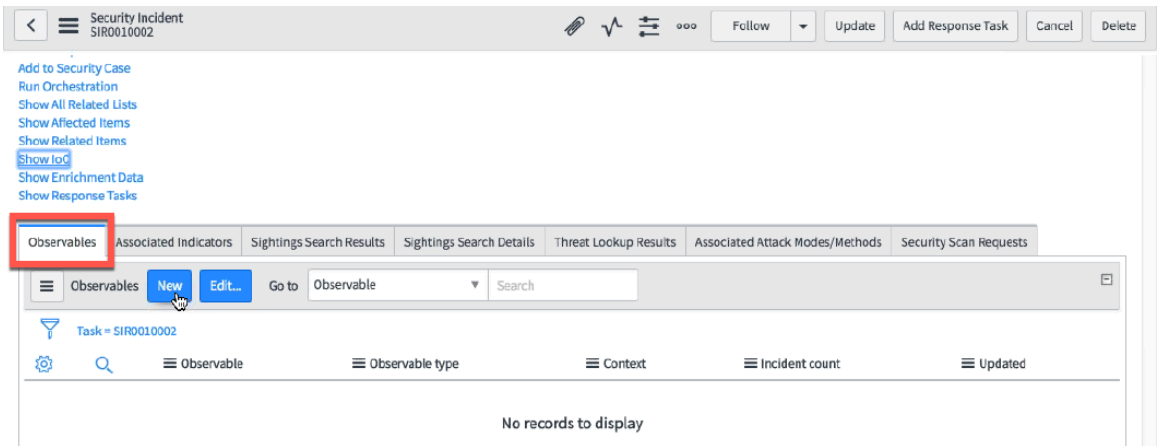
Rôle requis : sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

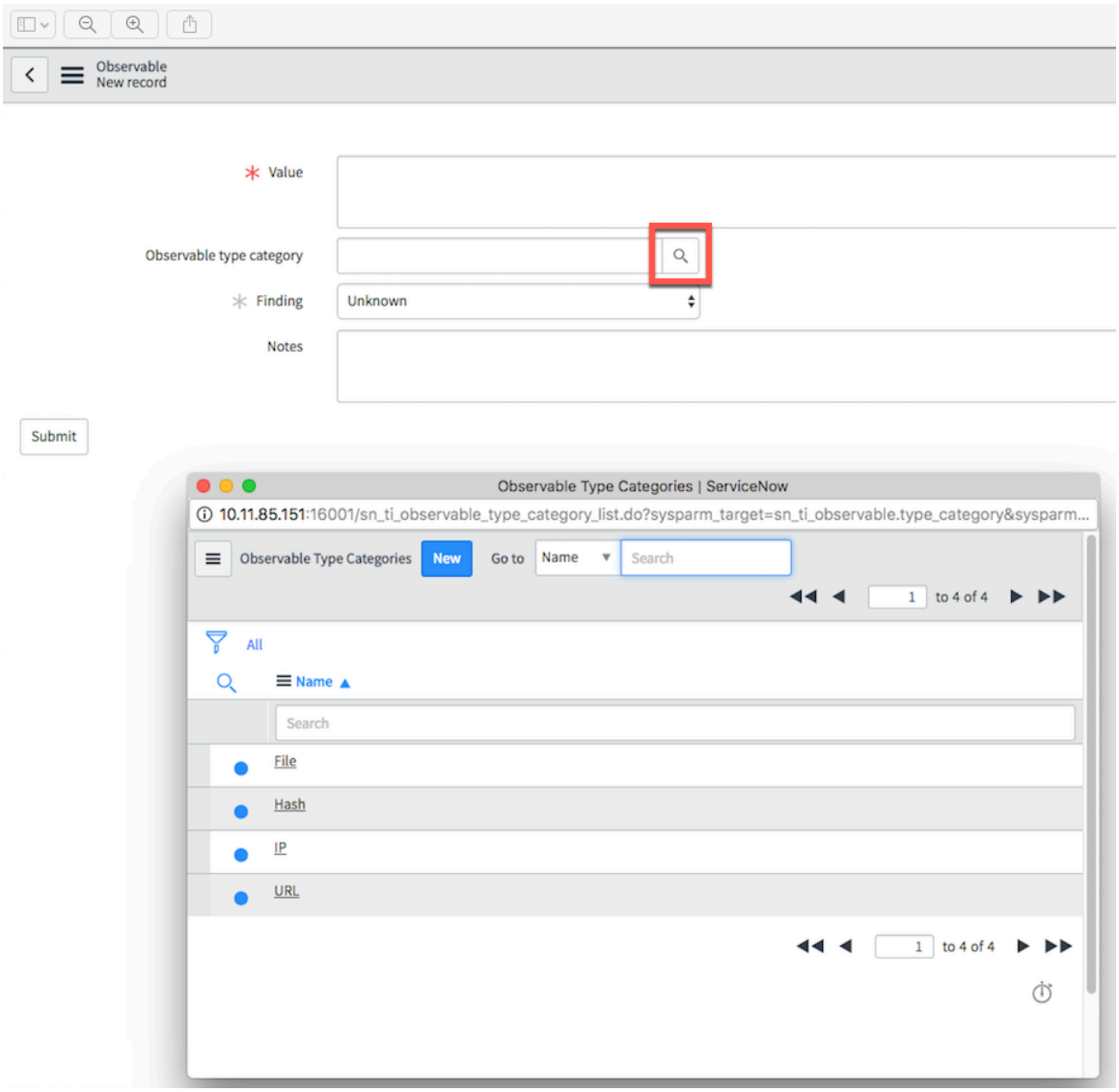
1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents** et ouvrez un incident de sécurité auquel vous souhaitez joindre l'observable.
2. Sur l'incident de sécurité ouvert, cliquez sur le lien **Afficher IoC**dans **Liens connexes**.



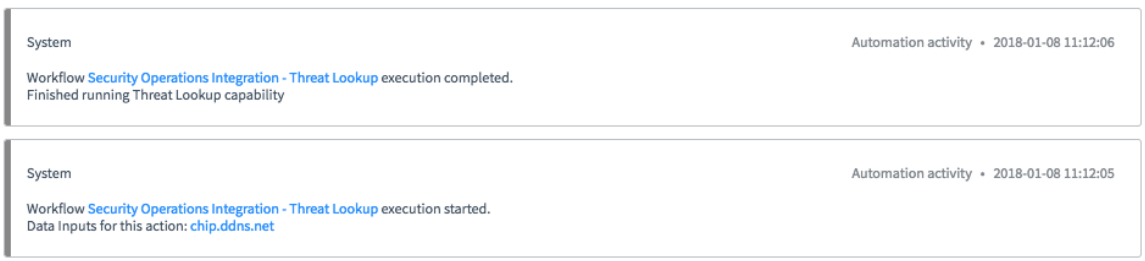
3. Dans l'onglet **Observables** , cliquez sur **Nouveau**.
   Le formulaire Observable s'affiche.
4. Dans le champ **Valeur** , entrez un observable (hachage de fichier, adresses IP ou URL).
5. Cliquez sur l'icône de recherche puis, dans la boîte de dialogue **Catégories de types d'observables** , cliquez sur le type d'observable souhaité dans la liste pour remplir le champ.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



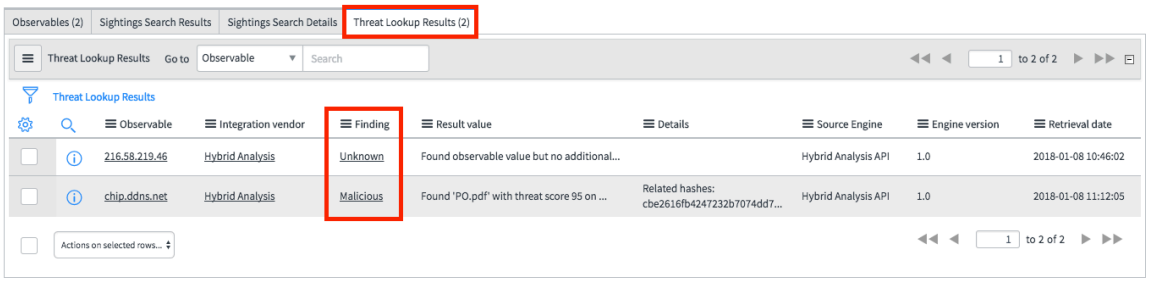
6. Cliquez sur **Envoyer**.
   Le flux lance et vérifie le nouvel observable. L'état d'exécution et d'achèvement est affiché dans la section Notes de travail de l'enregistrement d'incident de sécurité.
7. Accédez à votre incident de sécurité et passez en revue les notes de travail.



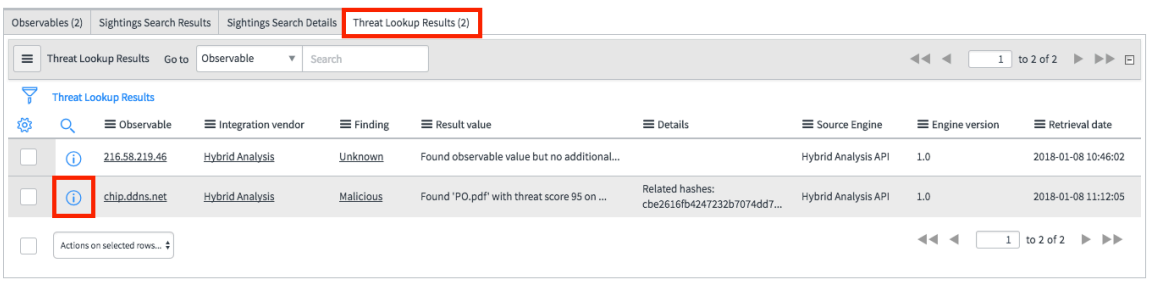
8. Au bas de l'enregistrement, cliquez sur le lien connexe **Afficher toutes les listes connexes** .
9. Cliquez sur l'onglet **Résultats de la recherche de menaces** pour afficher les résultats.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Dans la colonne **Observable** , cliquez sur l'icône d'information bleue en regard d'un observable donné pour plus d'informations et de données brutes.



11. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement** pour afficher les données brutes et plus de détails.
Vous pouvez également joindre un observable existant à l'enregistrement d'incident de sécurité.

12. Facultatif : Avec l'onglet **Observables** sélectionné, cliquez sur **Modifier**.

13. Facultatif : Dans le formulaire **Modifier les membres** qui s'affiche, déplacez un observable existant de **Collection** vers **Liste des observables** et cliquez sur **Enregistrer**.
Vous êtes renvoyé à l'incident de sécurité.

14. Dans la colonne située tout à gauche, sélectionnez les observables sur lesquels vous souhaitez exécuter la recherche et, dans la liste de choix **Actions sur les lignes sélectionnées...** , sélectionnez **Exécuter la recherche de menace**.
Un message s'affiche en haut de l'enregistrement indiquant que la demande est en cours de traitement. Vérifiez que la recherche a été exécutée avec succès.

Trouble?
Consultez les notes de travail pour plus d'informations et pour savoir comment procéder si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.

IBM QRadar Offense Ingestion Intégration

L'intégration IBM QRadar Offense Ingestion vous permet d'extraire IBM QRadar automatiquement les infractions et de les convertir en incidents de sécurité, et d'activer les actions de réponse automatisées.

Cette intégration prend en charge les éléments suivants :

- Détection des infractions qui sont candidates à des incidents de IBM QRadar sécurité.
- Récupération des événements récents ou des flux associés à une infraction.
- Suivez périodiquement les principales mises à jour des infractions.
- Mappage des champs d'infraction, d'événement et de flux aux champs d'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vue préliminaire des champs mappés.
- Configurez des ingestions planifiées des infractions pour créer des incidents de sécurité périodiquement.
- Clôturer les infractions lorsque les incidents de sécurité sont clos.

Installez et configurez l'application ServiceNow pour l'intégration d'ingestion d'infractions IBM QRadar

Avant d'exécuter l'intégration sur votre Now Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre Réponse aux incidents de sécurité correctement aux produits et Opérations de sécurité sur votre Now Platform instance.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si vous n'avez pas installé l'application IBM QRadar à partir de ServiceNow Store pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la IBM QRadar tuile.
3. Pour configurer l'application, cliquez sur **Nouveau**.
4. Si un bouton **Configurer** s'affiche sur une mosaïque, cliquez dessus pour modifier une configuration existante.
5. Renseignez les champs de la boîte **de dialogue Configuration des ingestions d'infractions** qui s'affiche.

Champ	Description
Nom	Nom de la console ou de l'instance IBM QRadarIBM QRadar utilisée pour l'intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge.
URL de base de l'API IBM QRadar	URL d'hôte pour votre IBM QRadar instance. **Remarque :** Vous n'avez besoin d'entrer que l'URL et le numéro de port ici. Par exemple, https://ibm-qradar.com:8443. Si le numéro de port est 443, il n'est pas nécessaire de le saisir explicitement.
URL du tableau de bord IBM QRadar	L'URL du tableau de bord ou de la IBM QRadar console. Cette URL est utilisée pour construire automatiquement les liens hypertexte pour les infractions dans le IBM QRadar tableau de bord.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Entrez uniquement l'URL de l'hôte, par exemple https://qradar.com. N'incluez pas le .jsp dans l'URL, par exemple, https://qradar.com/console/qradar/jsp/QRadar.jsp format n'est pas valide. **Remarque :** Si l'URL du tableau de bord n'est pas disponible, saisissez l'URL de base de l'API IBM QRadar ici.
IBM QRadar Version de l'API	Les versions 10 et supérieures sont prises en charge.
IBM QRadar Jeton de service autorisé d'API (sur site)	Le IBM QRadar jeton de service autorisé est utilisé pour l'authentification. Le jeton de service autorisé doit avoir un rôle d'utilisateur **administrateur** et un profil de sécurité **administrateur** . Pour générer le jeton de service autorisé, procédez comme suit : ◦ Dans la IBM QRadar console, accédez à l'onglet **Admin** et cliquez sur **Services autorisés**. ◦ S'il existe un jeton de service autorisé valide, vérifiez la date d'expiration et utilisez ce jeton. Si un jeton de service autorisé n'est pas disponible, procédez comme suit : ◦ Dans le IBM QRadar, accédez à l'onglet **Admin** et cliquez sur **Service autorisé**. ◦ Cliquez sur **Ajouter un service autorisé** et créez un jeton avec le rôle d'utilisateur **Administrateur** et le profil de sécurité **Administrateur** . Assurez-vous de spécifier une date d'expiration pour une longue période de validité.
IBM QRadar Jeton de service autorisé de l'API (pour QRoC)	Si vous utilisez IBM QRadar on Cloud (QRoC), utilisez l'application en libre-service pour générer le jeton de service autorisé avec le rôle d'utilisateur administrateur et le profil de sécurité administrateur pour l'authentification.
Déploiement sur site	La valeur par défaut est désactivée. Si cette option est activée, vous devez spécifier un nom d'application MID. Si vous utilisez IBM QRadar on Cloud (QRoC), vérifiez que la case n'est pas cochée.

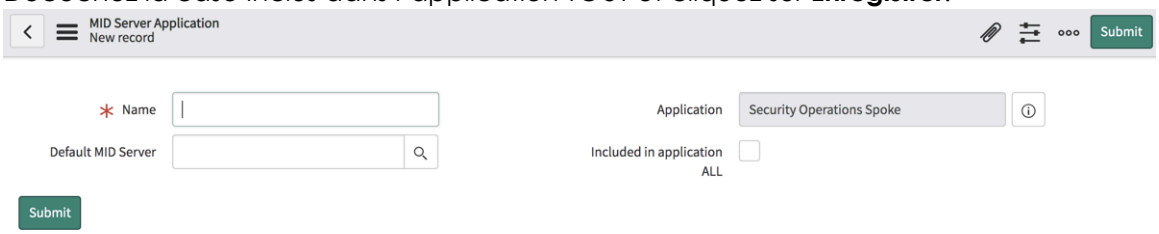
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom de l'application MID	Spécifiez une application de Serveur MID configurée dans votre environnement. Si aucune application de Serveur MID n'est configurée, vous devez créer une nouvelle application de Serveur MID pour cette intégration. **Remarque :** L'application Serveur MID ne peut être configurée que par les utilisateurs disposant du rôle d'administrateur système.

Pour créer une application de Serveur MID, procédez comme suit :

- Accédez à la **Serveur MID** > **Applications** et cliquez sur **Nouveau**.
- Entrez un nom pour l'application de Serveur MID et sélectionnez un serveur MID à utiliser par défaut.
- Décochez la case Inclus dans l'application TOUT et cliquez sur **Enregistrer**.

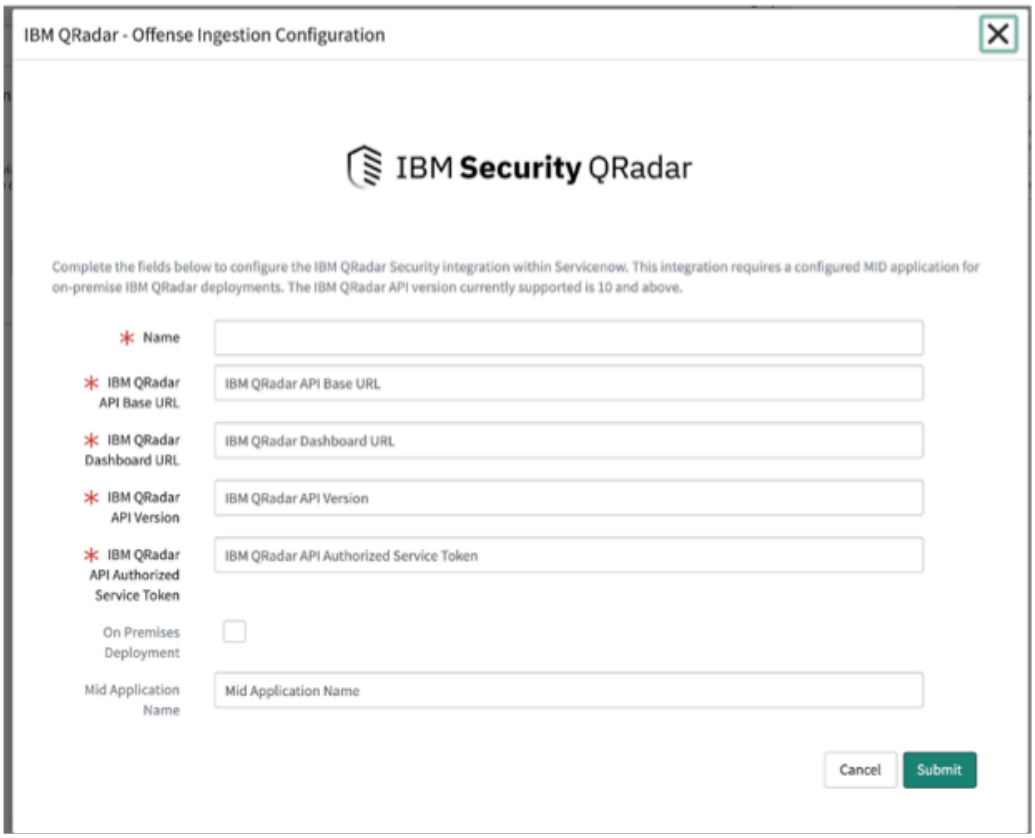


- Cliquez sur **Modifier**. Sur la page **Modifier les membres** , sélectionnez tous les serveurs MID disponibles, déplacez-les vers la liste des serveurs MID et cliquez sur **Enregistrer**. En fonction de la disponibilité, l'un des MID Servers configurés avec l'application MID Server sera utilisé.

6. Entrez les détails de la configuration et spécifiez l'application de Serveur MID que vous avez créée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La source que vous configurez sur le formulaire **de configuration de l'ingestion d'ingestion d'infractions IBM QRadar** peut être réutilisée pour plusieurs Now Platform profils, à condition que chaque profil ingère des infractions.

7. Cliquez sur **Envoyer**.
   Une fois validée et soumise, chaque IBM QRadar configuration de serveur est enregistrée sous forme de vignette sur la page Intégrations de sécurité. Si vos vignettes de configuration enregistrées ne s'affichent pas sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste de choix Afficher les configurations, cliquez sur **Oui**.

> **Remarque :** Si vous rencontrez des problèmes avec la fonctionnalité de segmentation de domaine, contactez IBM QRadar le support client pour obtenir de l'aideIBM QRadar.

Que faire ensuite

Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer le profil.

Configurer votre Now Platform® instance pour l'intégration de l'ingestion d'infractions IBM QRadar

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform® instance avant d'installer l'application à partir du ServiceNow Store.

Avant de commencer

Rôle requis : sn_si.admin

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application pour garantir une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform® et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre Now Platform® instance. • Un utilisateur disposant du rôle administrateur Now Platform® (admin) installe l'application à partir de et ServiceNow Store affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Un utilisateur disposant du rôle sn_si.admin supervise les tâches suivantes dans :Now Platform® ◦ Nomme, crée et modifie les profils d'infraction. ◦ Sélectionne et mappe IBM QRadar les champs de données d'infraction aux champs d'incident de sécurité. ◦ Prévisualise l'exactitude des détails de l'incident de sécurité avant de finaliser la configuration. ◦ Planifie l'ingestion d'infractions en cours. ◦ Active les mises à jour d'infraction lorsqu'un incident SIR est créé et fermé. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Les utilisateurs avec l'sn_si.analyst travaillent avec des incidents de sécurité. Pour plus d'informations sur les rôles et l'affectation de rôles aux utilisateurs, consultez Rôles sur le site web de la documentation produit ServiceNow .
Vérifiez que vous utilisez les versions suivantes : • IBM QRadar version 7.3.2 ou ultérieure. • IBM QRadar Version d'API 10 ou ultérieure. Les versions antérieures ne sont pas prises en charge.	Si vous avez accès à la IBM QRadar console, vous avez accès à l'API requise pour cette intégration. Aucune autre configuration spéciale n'est requise pour l'API.
Vérifiez que vous avez installé et configuré une application de Serveur MID.	Application de Serveur MID configurée. Un serveur MID dans votre Now Platform® instance est requis pour se connecter au IBM QRadar service si le IBM QRadar serveur est déployé au sein de votre réseau d'entreprise. Consultez le site web de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	la documentation produit ServiceNow pour plus d'informations sur les MID Servers. Si vous utilisez le IBM QRadar service Cloud, un Serveur MID n'est pas nécessaire.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Ingestion d'événements et d'alertes pour Security Operations : Cette application nécessite : ◦ com.glide.hub.integration.runtime => l'exécution du Centre d'intégration ServiceNow ◦ com.glide.hub.action_step.rest => Étape d'action du Centre d'intégration ServiceNow : REST **Remarque :** Les composants du concentrateur d'intégration sont installés en même temps que le module d'extension d'ingestion d'événements et d'alertes. Si ceux-ci ne sont pas installés, contactez le support client pour obtenir de l'aide. Pour plus d'informations sur l'installation des Opérations de sécurité applications principales, consultez et .

Que faire ensuite

Vous avez correctement configuré votre Now Platform® instance pour l'intégration. L'étape suivante consiste à installer l'application IBM QRadar à partir de ServiceNow Store pour l'intégration.

Créer un profil pour IBM QRadar l'intégration de l'ingestion d'infractions

En tant qu'utilisateur disposant du rôle sn_si.admin, vous créez un profil d'infraction dans votre Now Platform instance et déterminez quelles infractions créent des incidents de sécurité. SIRAvant Now Platform Réponse aux incidents de sécurité que () les incidents de sécurité ne soient créés à partir d'infractions, les valeurs de champ à partir d'infractions sont affichées sur la mise en page d'un Now Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera créé.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Du point de vue de l'intégration, à l'aide des API disponibles, IBM QRadar les infractions sont automatiquement ingérées dans l'environnement Opérations de sécurité de votre Now Platform instance en fonction du type de profil défini. Les workflows d'intégration ingèrent différents types d'infractions telles que les tentatives d'accès non autorisé et les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

logiciels malveillants, par exemple. Ces infractions sont ingérées en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance. Toutes les infractions sont initialement ingérées pour un type d'infraction configuré dans un profil. Les infractions ingérées peuvent ensuite être filtrées davantage pour spécifier quelles infractions créent des incidents de sécurité. Par exemple, vous pouvez préférer des filtres qui créent des incidents de sécurité uniquement pour les infractions identifiées comme à haut risque. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir d'infractions ingérées, les valeurs de champ individuelles des infractions sont mappées aux champs correspondants sur une mise en page de l'incident de sécurité pour un aperçu.

Les noms des profils d'infraction dans votre Now Platform instance doivent être uniques. Vous pouvez créer plusieurs configurations pour plusieurs sources et vous pouvez également créer plusieurs profils pour une seule source.

Créer des profils pour ingérer IBM QRadar les infractions

Vous pouvez configurer un profil pour ingérer les infractions.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Pour créer un profil pour une infraction dans votre Now Platform instance, accédez à **Intégration d'IBM QRadar** > **Profil IBM QRadar**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs.

   Le tableau ci-dessous un exemple de formulaire rempli.

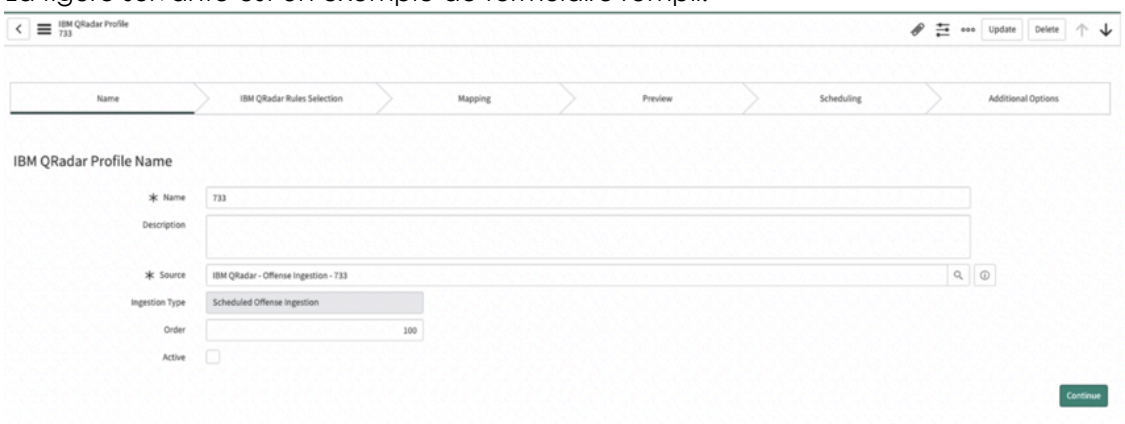
Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre Now Platform instance doivent être uniques.
Actif	La case n'est pas cochée par défaut. Si cette option est désactivée, le profil n'est pas actif et l'ingestion n'a pas lieu. **Remarque :** Vous devez remplir toutes les sections du profil avant de l'activer.
Source	Le IBM QRadar serveur que vous avez configuré pour ingérer les infractions. Si vous avez configuré plusieurs IBM QRadar serveurs, sélectionnez le serveur approprié pour les types d'infractions qui seront ingérés pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Le workflow du profil dont le numéro est le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

La figure suivante est un exemple de formulaire rempli.



Que faire ensuite

L'étape suivante consiste à sélectionner les infractions à ingérer.

Sélectionner IBM QRadar des règles

En fonction de la IBM QRadar source, sélectionnez une ou plusieurs IBM QRadar règles pour le profil.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Consultez les règles disponibles IBM QRadar dans votre instance Now Platform afin de connaître les règles actives IBM QRadar pour lesquelles vous souhaitez ingérer et créer des incidents de sécurité.

Dans IBM QRadar, vous pouvez identifier les règles en fonction de leur origine en tant que règles système, remplacement et utilisateur. Par défaut, l'origine d'une règle est liée à une règle système. Lorsque vous modifiez une règle système dans IBM QRadar, son origine est définie comme Remplacement.

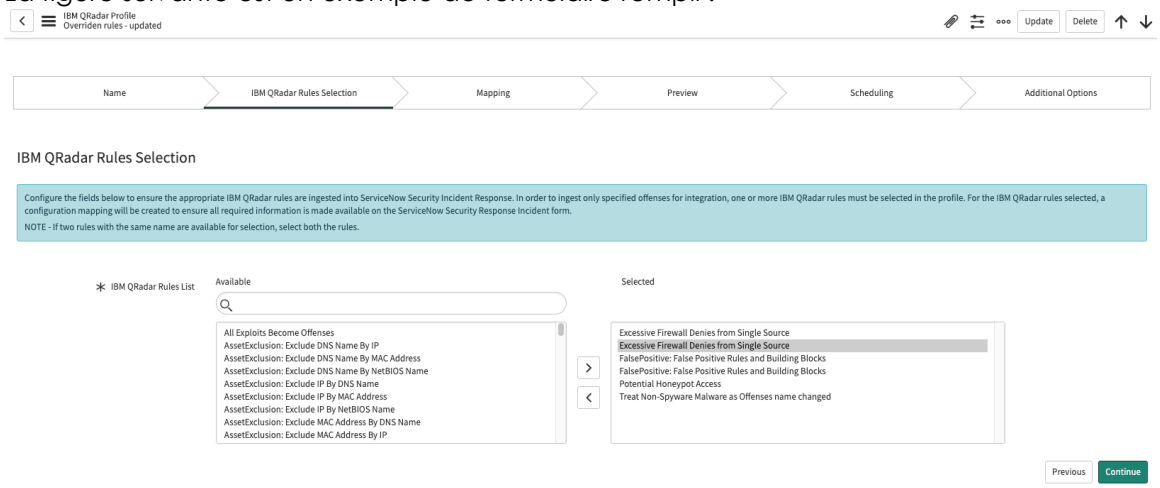
Cliquez sur la liste dans le IBM QRadar champ Liste de règles. La liste des règles actives IBM QRadar présentes dans la console s'affiche IBM QRadar . Sélectionnez une ou plusieurs règles dans la liste et déplacez-les vers la colonne **Sélectionné** . Les infractions déclenchées par une ou plusieurs des IBM QRadar règles sélectionnées sont ingérées dans ce profil.

Règles portant le même nom : dans l'instance, une liste de règles actives ou activées s'affiche Now Platform . Si vous modifiez une règle système active ou activée dans IBM QRadar, une nouvelle règle de remplacement est créée. Il en résulte que deux règles portant le même nom sont affichées dans le Now Platformfichier . Lorsque ce scénario se produit, sélectionnez à la fois les règles à ingérer et à créer des incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La figure suivante est un exemple de formulaire rempli :



Cliquez sur **Continuer** pour passer à l'étape suivante dans l'assistant.

Mappage des champs d'infraction pour l'intégration IBM QRadar

Une fois que vous avez sélectionné les règles, l'étape suivante consiste à mapper les champs d'infraction, d'événement ou de flux aux champs du formulaire d'incident de sécurité.

Vue d'ensemble

Pour l'étape de mappage, vous devez d'abord ingérer des exemples d'infractions pour une ou plusieurs règles sélectionnées IBM QRadar . Ensuite, vous devez vous assurer que toutes les données pertinentes du champ d'infraction sont mappées à l'endroit approprié sur le SIR formulaire d'incident, puis visualiser l'incident SIR dans la section d'aperçu.

Le mappage des exemples de champs d'infraction implique les éléments suivants :

- Extraction et remplissage des exemples de données : reportez-vous à la section Ingérer les exemples IBM QRadar d'infractions.
- Mappage des champs d'infraction à l'incident de sécurité : reportez-vous à la section Mappage IBM QRadar des champs d'infraction aux champs de réponse aux incidents de sécurité.

Ingérer les exemples IBM QRadar d'infractions

Vous pouvez ingérer des exemples d'infractions pour une ou plusieurs règles sélectionnées IBM QRadar .

Avant de commencer

Rôle requis : sn_si.admin

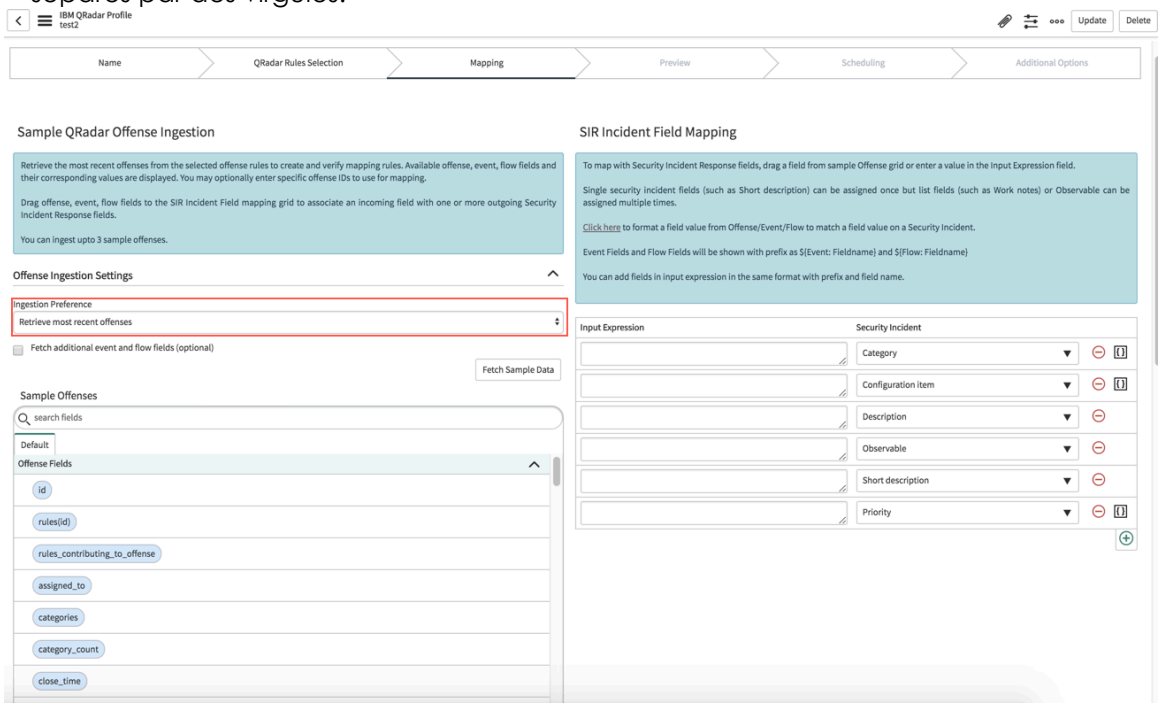
Procédure

1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Vous pouvez soit extraire les trois exemples d'infractions les plus récents, soit fournir les ID d'infraction uniques pour les infractions spécifiques que vous souhaitez utiliser pour votre expérience de mappage.
   Dans la liste de choix **Préférences d'ingestion** , sélectionnez l'une des options suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Récupérer les infractions les plus récentes : les trois infractions les plus récentes pour les règles sélectionnées sont récupérées.
- Sélectionner les infractions en fonction de l'ID d'infractions : spécifiez l'ID d'infraction pour les infractions à récupérer. Vous pouvez spécifier un maximum de 3 ID d'infractions séparés par des virgules.



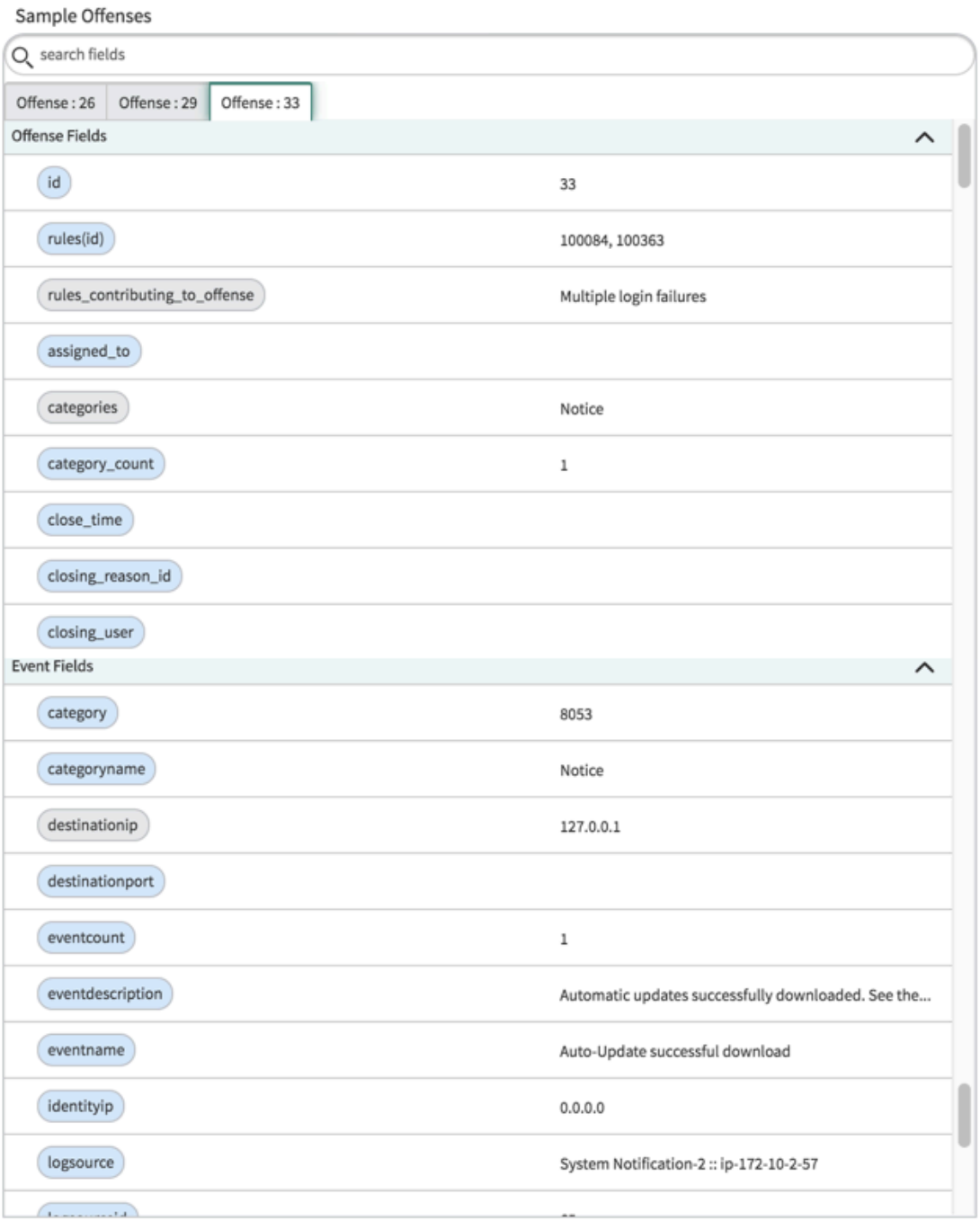
3. Cliquez sur **Extraire les données d'exemple** pour extraire les derniers exemples de données d'infraction de la IBM QRadar console pour les règles d'infraction sélectionnées.

   Les champs et les résultats des valeurs d'infraction sont affichés sous forme d'onglets individuels. Une infraction peut être déclenchée par trois types de règles :

   - Événement : dans cette règle, les journaux d'événements sont vérifiés et si les critères spécifiés sont remplis, une infraction est créée.
   - Flux : les données et le trafic réseau sont vérifiés et si certaines conditions sont remplies, une infraction est créée.
   - Commun : dans ce cas, vous pouvez spécifier des conditions pour les événements ou les flux si l'une ou l'autre ou les deux conditions sont remplies, une infraction est créée.

   L'extraction d'échantillons d'infractions peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran. En fonction de la ou des règles qui ont déclenché l'infraction, les champs d'événement ou de flux sont renseignés, comme illustré dans la figure ci-dessous :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Remarque : Les champs d'événement ou de flux affichés appartiennent au premier événement ou champ de flux qui a déclenché l'infraction en fonction de la règle d'événement ou de flux correspondante.

4. Les champs d'infraction personnalisés suivants sont créés pour cette intégration. Des champs d'infractions standard en plus de ces champs personnalisés sont disponibles pour le mappage.
   - rules_contributing_to_offense : IBM QRadar règles qui ont contribué à l'infraction d'après l'ID de règle.
   - users : noms d'utilisateur pour l'infraction

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

◦ remote_destination_ip : adresses IP de destination distantes pour l'infraction.

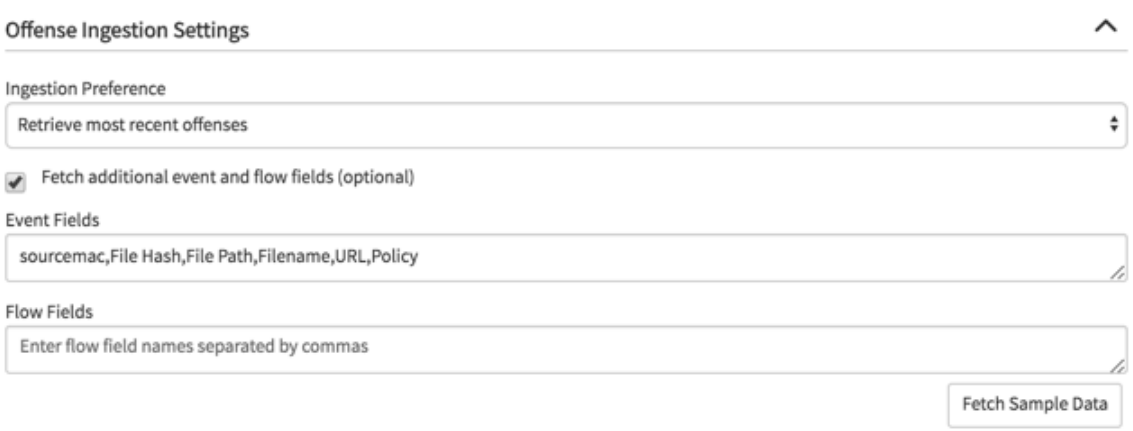
En fonction des ID de destination locaux pour l'infraction, les champs d'adresse de destination locale personnalisée suivants sont disponibles :

- local_destination_address (domain_id)
- local_destination_address (event_flow_count)
- local_destination_address (first_event_flow_seen)
- local_destination_address (ID)
- local_destination_address (last_event_flow_seen)
- local_destination_address (local_destination_address_ids)
- local_destination_address (magnitude)
- local_destination_address (réseau)
- local_destination_address (offense_ids)
- local_destination_address (local_destination_ip)

◦ Les adresses sources suivantes sont disponibles en fonction des ID sources de l'infraction :

- source_addresses (domain_id)
- source_addresses (event_flow_count)
- source_addresses (first_event_flow_seen)
- source_addresses (ID)
- source_addresses (last_event_flow_seen)
- source_addresses (source_address_ids)
- source_addresses (magnitude)
- source_addresses (réseau)
- source_addresses (offense_ids)
- source_addresses (source_ip)

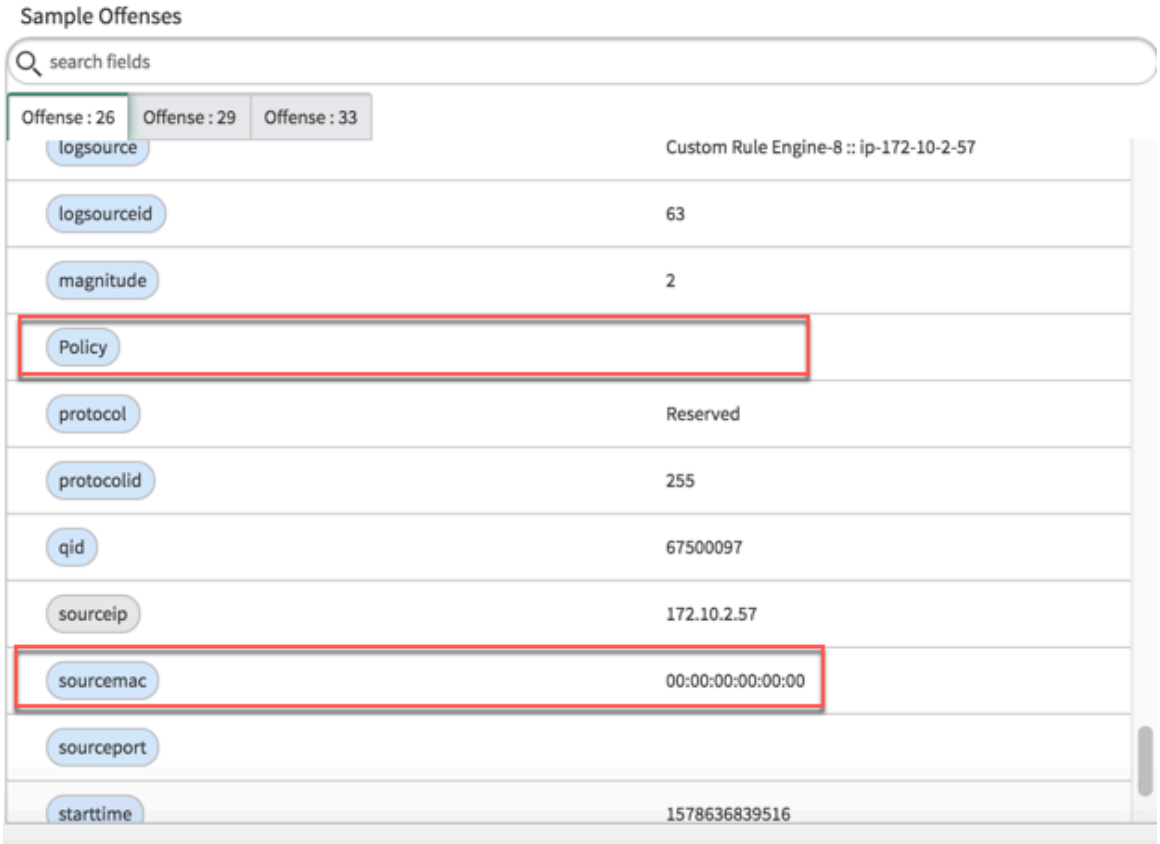
Cochez la case **Extraire des champs d'événements et de flux supplémentaires (facultatif).** Vous pouvez extraire des échantillons de données d'événement et de flux à partir de n'importe quel champ de flux et d'événement personnalisé actif et valide. Spécifiez les champs personnalisés séparés par des virgules, comme indiqué ci-dessous :



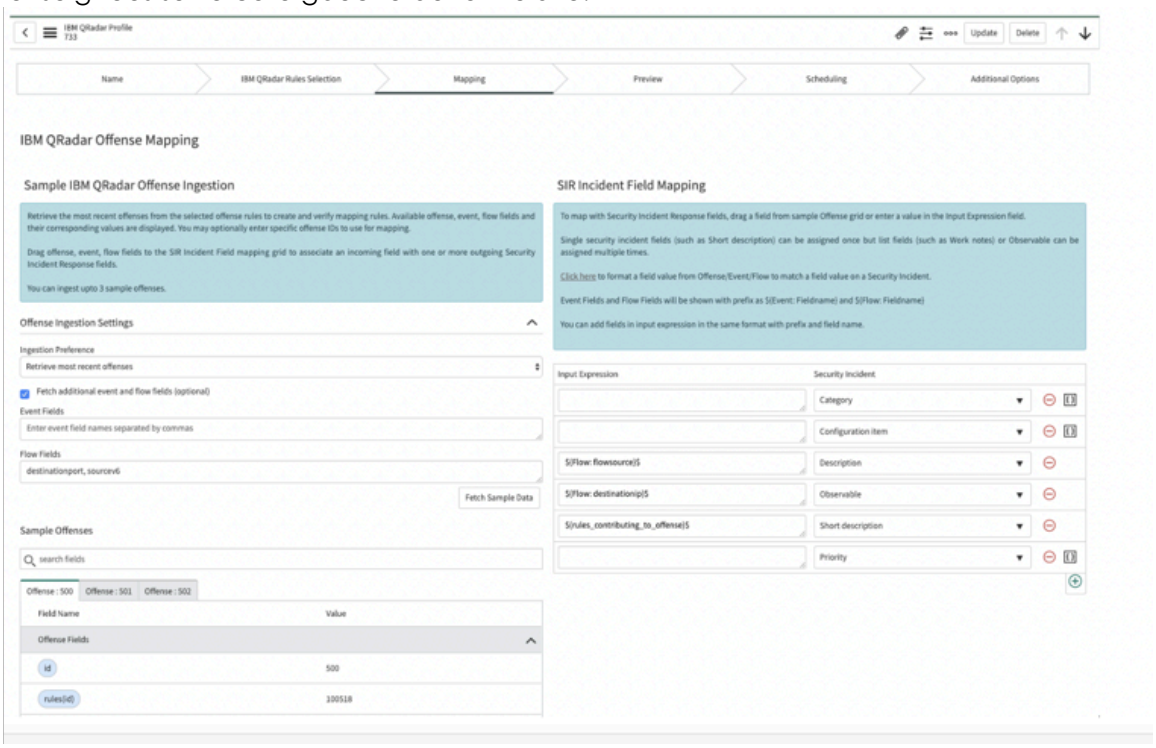
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cliquez sur **Extraire des exemples de données**. Les champs d'événement ou de flux spécifiés ainsi que leurs valeurs (le cas échéant) sont ajoutés à la section Événement ou Flux, comme indiqué ci-dessous :



Une fois les exemples de données extraits, les valeurs correspondantes de ces champs sont renseignées sur le côté gauche du formulaire.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Une fois que vous avez extrait les données d'échantillon, l'étape suivante consiste à mapper les champs d'infraction à l'incident de sécurité.

Mappage IBM QRadar des champs d'infraction aux champs de réponse aux incidents de sécurité

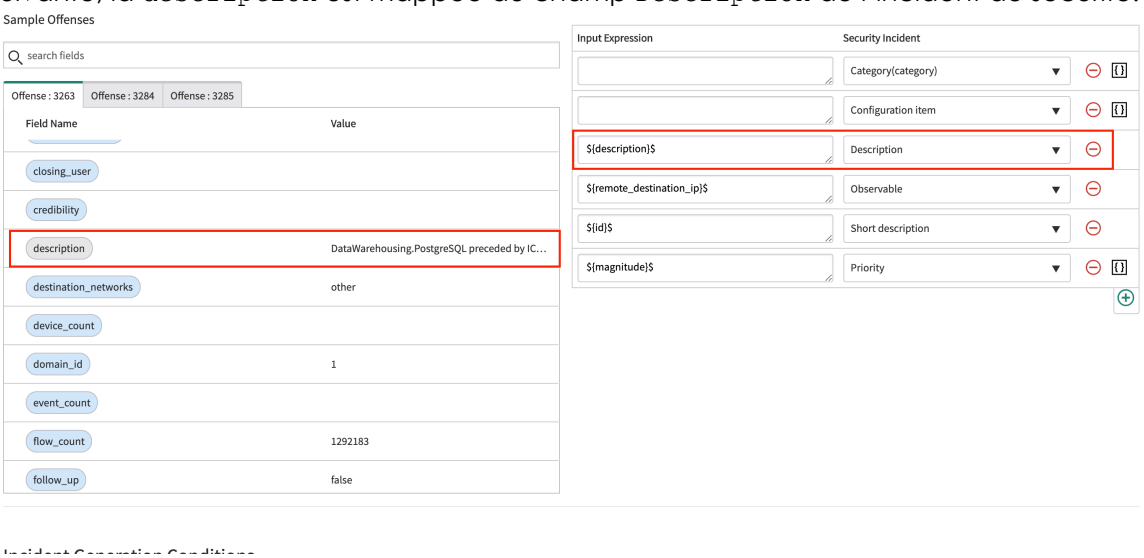
Mappez les champs d'infraction, d'événement et de flux individuels aux champs d'un Now Platform SIR incident de sécurité.

Mappage du champ d'attaque

En tant qu'utilisateur disposant du rôle sn_si.admin, utilisez les champs de la section Exemples d'infractions sur la gauche et mappez-les aux champs d'incident de sécurité dans la colonne Mappage de champ d'incident SIR. Modifiez la configuration du mappage en faisant glisser les champs d'infraction, d'événement ou de flux depuis le côté gauche et en les déposant dans la ServiceNow SIR section de mappage des incidents située à droite. Le mappage sur la droite associe le champ d'infraction entrant à un champ d'incident de sécurité sortant.

1. Une fois que vous avez extrait les exemples de données, l'étape suivante consiste à mapper les champs d'infraction, d'événement ou de flux à l'incident de sécurité. Pour mapper une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez longuement sur un nom de champ bleu sur le côté gauche du formulaire.
2. Faites glisser le nom du champ, par exemple `Description` et déposez-le sur un champ de la colonne Expression d'entrée en regard d'un nom de champ dans la colonne Incident de sécurité.

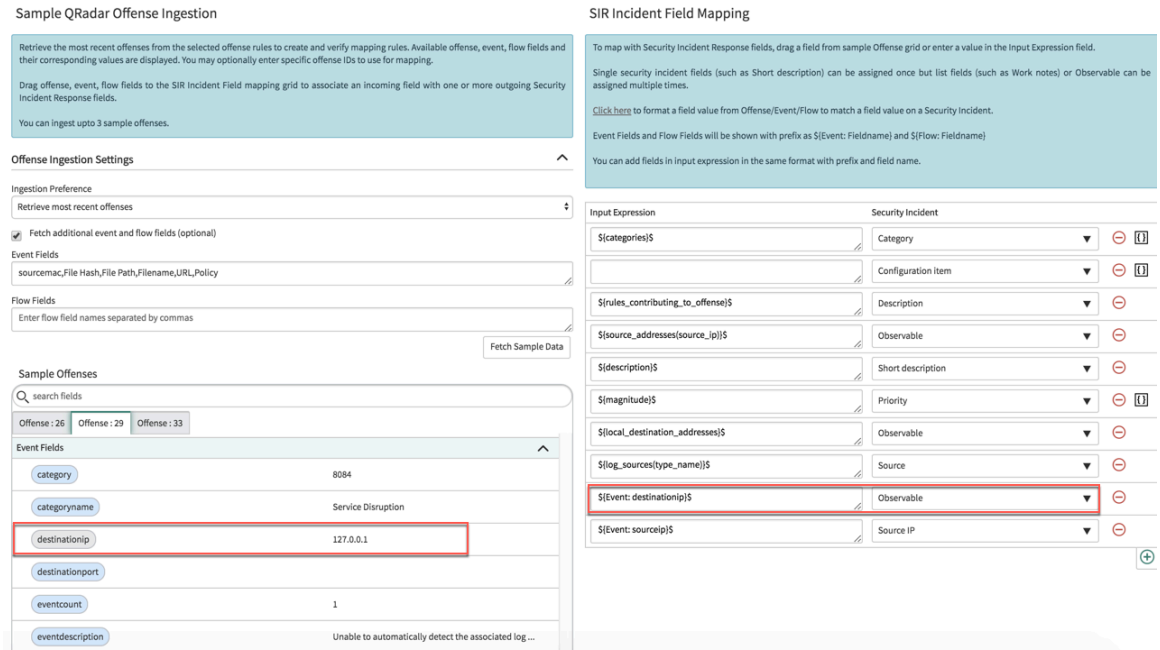
   La valeur du champ est affichée dans la colonne Expression d'entrée. Dans l'image suivante, la `description` est mappée au champ `Description` de l'incident de sécurité.



Remarque : Si vous saisissez manuellement le nom du champ d'événement ou de flux dans la section expression d'entrée, vous devez ajouter un préfixe en tant que *${Event :eventfield}$* ou *${Flow :flowfield}$* avant le nom du champ en cours de mappage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



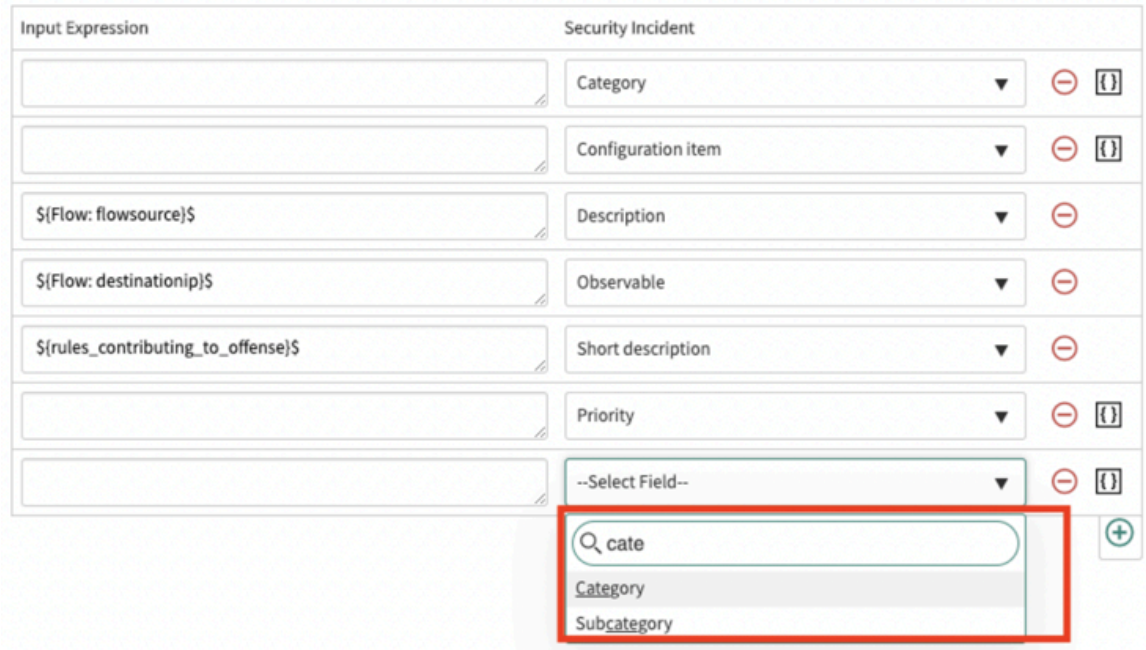
Pour vous assurer qu'aucun champ d'infraction, d'événement ou de flux n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par couleur. Le codage couleur des champs d'infraction vous aide à suivre les valeurs d'infraction que vous avez déjà mappées, car elles sont grisées tandis que tous les champs non mappés restants apparaissent en bleu. Cela vous aide à mieux visualiser quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si des informations d'infraction importantes restantes restent non mappées.

Les champs bleu clair sur la gauche indiquent qu'un champ d'infraction n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ d'infraction, d'événement ou de flux entrant à plusieurs champs sur un incident de sécurité. Un champ gris indique qu'un champ a été sélectionné et mappé à un champ sur l'incident de sécurité. Ce code couleur vous aide à suivre le mappage.

3. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit :
   a. À droite du formulaire, dans la section Mappage de champs d'incidents SIR, en bas de la grille, cliquez sur l'icône plus (+). Un nouveau champ s'affiche.
   b. Dans la colonne Incident de sécurité, développez la liste de choix qui s'affiche, puis sélectionnez un champ.

      Dans la liste de choix développée pour le nouveau champ, certains champs sont grisés. Dans la figure suivante, la catégorie a un arrière-plan gris, car elle a été mappée dans l'incident de sécurité. À l'instar du code couleur pour les champs d'infraction sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident SIR déjà mappés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Étant donné que plusieurs observables peuvent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité dispose d'une liste de choix dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affiché dans la liste de choix, le champ n'est pas renseigné sur l'incident de sécurité.

c. Vous pouvez également saisir une valeur dans le champ Rechercher pour la nouvelle ligne.

d. Sur le côté gauche du formulaire, sélectionnez le champ d'infraction et faites-le glisser pour le déposer dans un champ d'incident de sécurité approprié à droite.

4. Supprimez des champs à l'aide de l'icône - en regard du nom du champ dans la section de mappage de champs d'incident SIR.

5. Poursuivez le mappage en ajoutant ou en supprimant des valeurs de champ au mappage.

Champs d'infraction à valeurs multiples

- Les champs d'incident de sécurité tels que les champs **Catégorie** et **Utilisateur** (par exemple, Utilisateur affecté, Affecté à) disponibles avec le produit de base ne prennent pas en charge plusieurs valeurs.
- Les champs suivants IBM QRadar prennent en charge plusieurs valeurs :
  - *Catégories*
  - *destination_networks*
  - *source_address_ids*
  - *local_destination_address_ids*

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- *remote_destination_ips*
- *rules_contributing_to_offense*
- *utilisateurs*

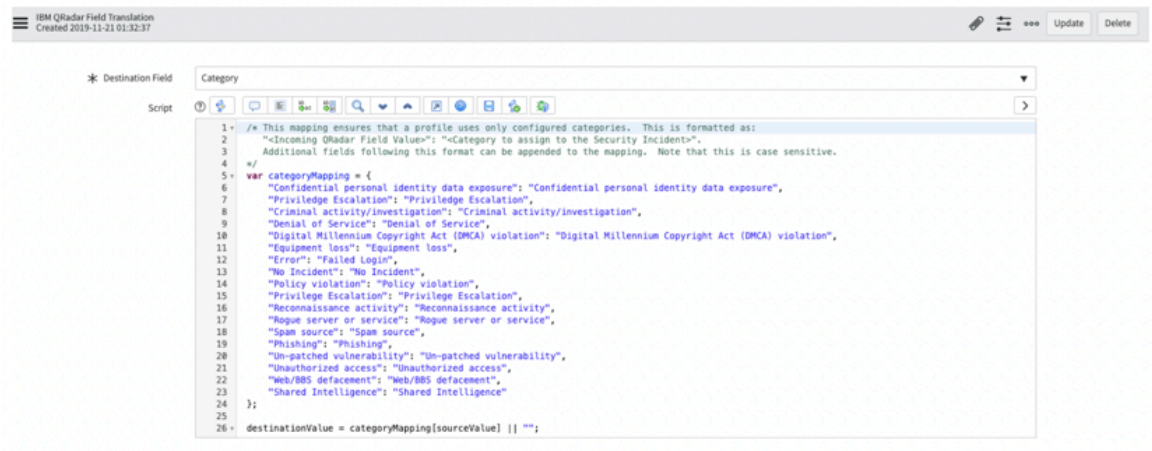
Si vous devez mapper les champs ci-dessus à des Réponse aux incidents de sécurité champs autres que les champs de type CI et Observable, vous devez créer de nouveaux Réponse aux incidents de sécurité champs de type **Liste** et les utiliser pour le mappage.

Remarque : Par défaut, seuls les champs de type **liste** de non-référence sont pris en charge.

Formater la traduction du champ

Dans certains cas, les valeurs de champ d'infraction dans IBM QRadar peuvent ne pas se traduire directement dans les champs de l'incident de sécurité SIR. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez mettre en forme des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident de sécurité SIR à l'aide de la fonctionnalité Formater la traduction de champ.

Pour utiliser l'éditeur de script, cliquez sur {{}}. L'éditeur de script s'affiche.



Entrez les changements apportés au script et cliquez sur **Mettre à jour** pour enregistrer les changements et revenir à la page Mappage.

Conditions de génération d'incidents

Une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de spécifier quelles infractions doivent créer des incidents de sécurité par rapport à celles qui doivent être filtrées (par exemple, les infractions de faible priorité). Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir les critères supplémentaires qu'une infraction entrante doit satisfaire pour créer un incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Faites défiler l'écran jusqu'à la section **Conditions de génération d'incidents** du formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

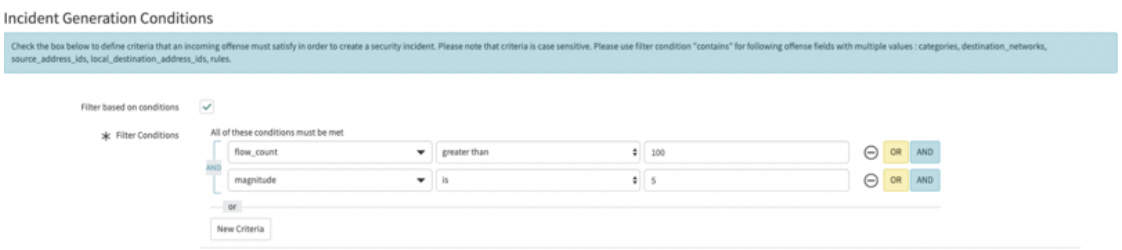
   Le Créateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

   Les options des listes de choix pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Exemple d'ingestion d'infractions QRadar pour les infractions que vous avez ingérées. Ces champs sont dynamiques et changent en fonction des infractions que vous ingérez. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'infraction IBM QRadar . Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférez peut-être revenir à votre IBM QRadar console et examiner vos infractions pour les mots-clés.

   Remarque : Les champs *Catégories*, *destination_networks*, *source_address_ids*, *local_destination_address_ids*, *remote_destination_ips*, *rules_contributing_to_offense* et *Infractions d'utilisateurs* peuvent comporter plusieurs valeurs (car les valeurs sont stockées dans des tableaux). Étant donné que la condition de filtre ne peut récupérer que des chaînes, vous devez utiliser la condition de filtre *contient* pour ces champs afin de vous assurer que les données sont filtrées correctement.

2. À l'aide des listes de choix et des champs du générateur de conditions, définissez des filtres pour la première ligne.
3. Pour ajouter d'autres conditions, à droite des champs, cliquez sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. (Facultatif) Dans la deuxième ligne, définissez une deuxième condition de filtre.

   L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création des incidents de sécurité.



   Vous avez défini les conditions de génération d'incident de sorte que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

   Ce type de filtrage des conditions de génération d'incident vous aide à affiner les infractions et à limiter le nombre d'incidents de sécurité inutiles que vous créez sans modifier la règle ou les filtres sous-jacents dans IBM QRadar. Si des critères de filtrage

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

supplémentaires sont définis, seules les infractions qui correspondent à tous les critères sont mappées aux incidents.

Remarque : Si l'un des noms de champs d'infraction comporte des caractères spéciaux tels que des guillemets («), des traits d'union ('), des traits de soulignement (-) ou des esperluettes (@), ces caractères peuvent devoir être remplacés à des fins de filtrage, mais un suffixe numérique est ajouté pour différencier les champs avec des noms d'infraction en double. Par exemple, si le premier champ d'infraction est `alerts.alert` et que le champ deuxième champ d'infraction est `alerts@alerts`, ces champs ne peuvent pas être identifiés de manière unique, car les caractères de texte standard restants sont les mêmes. Dans ce cas, un suffixe est ajouté au champ de la deuxième infraction et le champ est renommé `en alerts@alert(1)` lorsqu'il est affiché dans la liste Conditions de filtre.

Critères d'agrégation des infractions pour traiter les infractions similaires et empêcher les incidents en double

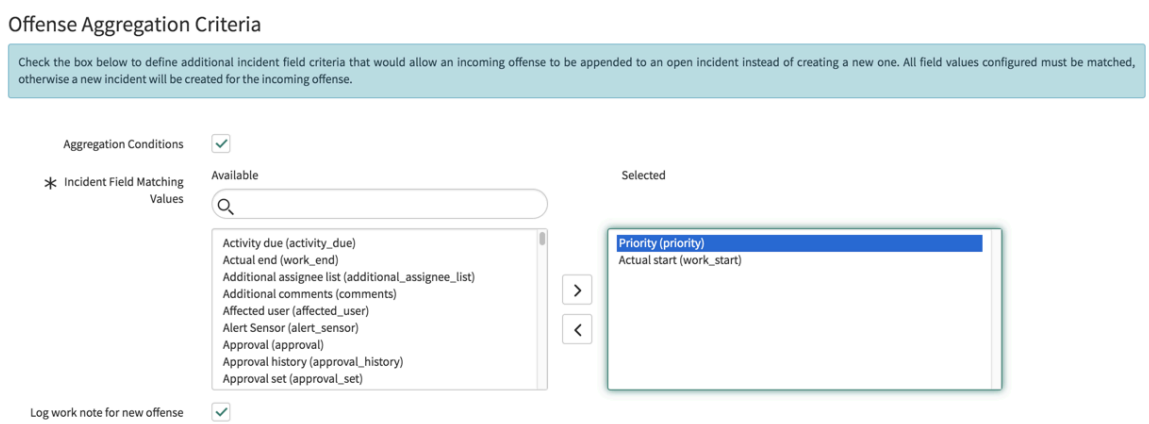
Définissez des critères d'agrégation des infractions supplémentaires qui regroupent une infraction entrante en un incident de sécurité SIR existant au lieu de créer des incidents similaires et potentiellement dupliqués. En utilisant des critères de valeur de correspondance de champ pour chaque profil, cette capacité d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données d'infraction connexes sur un seul incident de sécurité. Pour définir les critères, procédez comme suit :

1. Faites défiler l'écran jusqu'à la section Critères d'agrégation des infractions du formulaire et cochez la case Conditions **d'agrégation** pour activer cette option.

   Les colonnes Incident Field Matching Values (Valeurs correspondantes du champ d'incident) s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés dans l'incident SIR de sécurité.

2. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre Now Platform et déplacez-les vers la liste Sélectionné.

   Toutes les valeurs de champ que vous sélectionnez doivent correspondre pour ajouter cette alerte entrante à un incident de sécurité existant. Cela inclut les champs, tels que les observables et les éléments de configuration, qui peuvent avoir plusieurs valeurs de champ d'infraction mappées. Toutes les valeurs doivent correspondre. Si seul un sous-ensemble de valeurs est mis en correspondance, les conditions d'agrégation d'infractions ne seront pas remplies et un nouvel incident de sécurité sera créé. Voir la capture d'écran ci-dessous pour le mappage de champs à valeurs multiples.



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si une nouvelle infraction correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation à l'étape de mappage, la nouvelle infraction est automatiquement ajoutée à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur les incidents de sécurité, vous pouvez afficher toutes les infractions agrégées ajoutées dans une liste connexe d'un incident de sécurité. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi ces infractions sont regroupées en incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de l'enregistrement sous Liens connexes et cliquez sur le lien **Afficher toutes les listes connexes** .

3. (Facultatif) Pour consigner une note de travail pour une nouvelle infraction récemment ajoutée à l'incident de sécurité, cochez la case pour activer cette option. La note de travail consigne qu'une nouvelle infraction a été ajoutée, ainsi qu'un lien vers les détails de l'infraction et tous les autres détails qui ont pu être ajoutés au champ Note de travail dans votre section de mappage.

   Vous avez mappé avec succès les valeurs d'une IBM QRadar infraction aux champs d'un incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage de génération d'incidents. Vous avez également ajouté des infractions aux incidents de sécurité existants lorsque les valeurs de champ d'infraction correspondent aux critères d'agrégation configurés.

4. Cliquez sur **Continuer** pour poursuivre la configuration du profil. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité

Prévisualiser l'incident de sécurité pour l'intégration IBM QRadar

Une fois que vous avez terminé l'étape de mappage, prévisualisez les valeurs que vous avez mappées dans un SIR incident de sécurité. Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs d'infraction que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

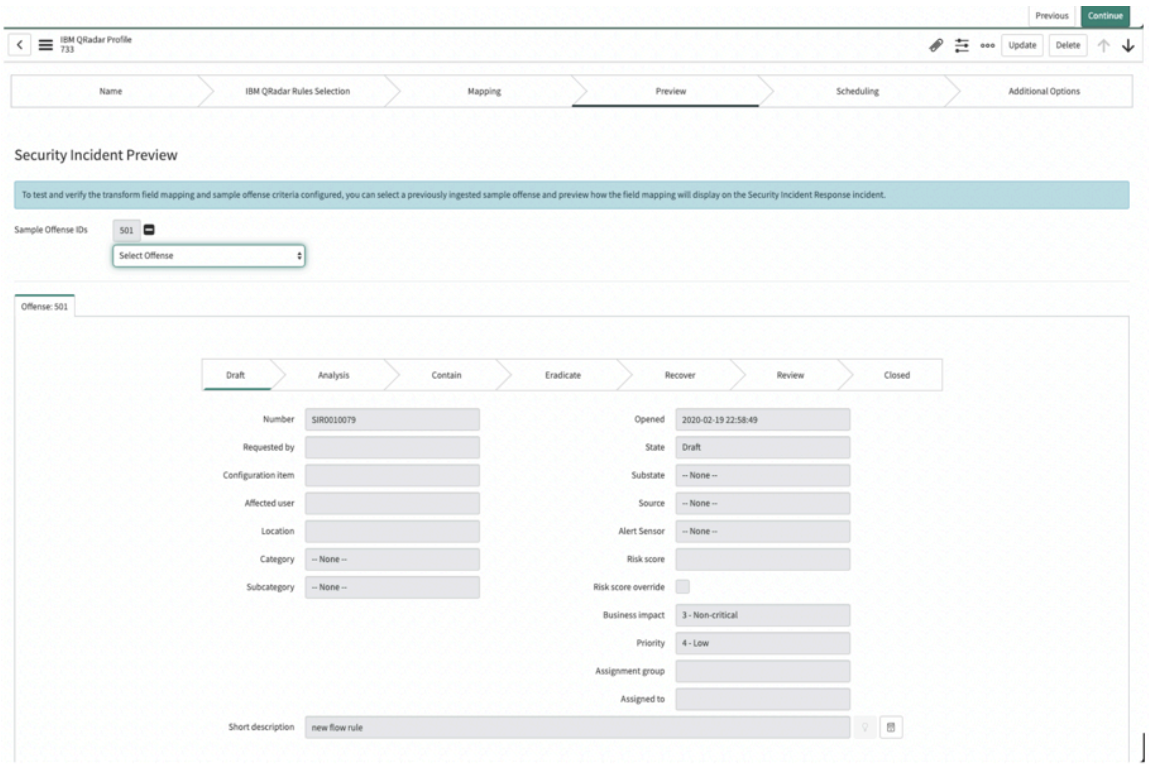
Pourquoi et quand exécuter cette tâche

En tant qu'utilisateur disposant du rôle sn_si.admin, prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs contenant des erreurs ou pour renseigner les données manquantes. Si l'aperçu n'est pas terminé, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de SIR sécurité ne sont pas enregistrés en tant qu'incidents réels dans le Réponse aux incidents de sécurité produit.

Procédure

1. Si l'aperçu de l'incident de sécurité n'est pas affiché, cliquez sur **Aperçu** dans la barre de progression.
2. Dans la liste de choix Exemples d'ID d'infraction, sélectionnez un élément.
   L'incident de sécurité s'affiche. Il s'agit d'une vue en lecture seule et un enregistrement de cet incident de sécurité n'est pas enregistré.
3. Passez en revue le mappage des champs des valeurs d'infraction sur l'incident de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'image précédente est un exemple d'aperçu avec une erreur de mappage des échantillons qui ont été ingérés.

4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

Que faire ensuite
Si aucun message d'erreur n'est affiché et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à définir le calendrier.

Définir le calendrier de l'intégration IBM QRadar

Vous pouvez définir le calendrier de l'ingestion de l'infraction. Au cours de cette étape, vous pouvez vérifier les paramètres par défaut pour la récupération des infractions ou modifier la planification selon vos besoins. Cette étape vous permet également de récupérer les infractions historiques à l'aide d'une plage de dates.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez choisir d'ingérer des infractions historiques au cours de l'étape de planification. Vous choisissez également la fréquence à laquelle vous allez interroger les nouvelles infractions futures et les infractions mises à jour qui correspondent à la configuration du profil.

En tant qu'utilisateur disposant du rôle sn_si.admin, vous configurez ces intervalles d'interrogation pour chaque profil. Les performances de l'intégration de l'ingestion IBM QRadar d'infractions peuvent être impactées par les différents intervalles d'interrogation. Lors de la planification, vous préférerez peut-être trouver un équilibre entre la réduction de la surcharge d'interrogation sur le serveur et le IBM QRadar désir d'être averti dès que possible

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

lorsqu'une infraction est créée ou mise à jour. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférerez peut-être modifier ce paramètre à une minute si nécessaire.

Extraction des infractions nouvelles et mises à jour

Lorsque le calendrier d'interrogation est défini, la tâche planifiée extrait les infractions nouvelles et mises à jour qui ont été extraites précédemment mais qui ne répondaient pas aux critères de filtrage des incidents. Vous avez ainsi la possibilité de créer des incidents en fonction de critères qui peuvent ne pas être présents lors de la création d'une infraction, mais qui deviennent disponibles après une mise à jour, par exemple pendant la phase d'enquête. Une fois qu'un incident est créé pour une infraction spécifique, ses mises à jour ultérieures sont ignorées, car il est prévu que l'infraction soit maintenant traitée comme un incident de sécurité actif ServiceNow . Toutefois, toutes les autres infractions qui ont déjà été ingérées, mais qui ne répondent pas aux critères de génération d'incidents, continueront d'être extraites et vérifiées par rapport aux critères de génération d'incidents jusqu'à ce qu'elles fassent partie d'un incident actif.

Procédure

1. Si la page Planification de la barre de progression n'est pas affichée, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les infractions sont extraites de la IBM QRadar console.

Option	Description
Champ d'ingestion de l'infraction en cours sélectionné	Attaque en cours En fonction du paramètre par défaut, l'instance Now Platform extrait du serveur pour les IBM QRadar infractions nouvelles et mises à jour toutes les cinq minutes. Les incidents de sécurité sont créés si des infractions sont détectées et si les critères de filtrage de génération d'incidents sont respectés. Pour équilibrer les frais généraux d'interrogation d'ingestion afin d'obtenir les données les plus récentes, le paramètre par défaut est de cinq minutes. Toutefois, cette valeur peut être modifiée jusqu'à une minute si nécessaire.
◦ Ingestion d'infractions en cours sélectionnée ◦ Définir le délai d'ingestion de l'infraction initiale	Délai d'ingestion initial Si vous souhaitez planifier l'ingestion initiale à une heure précise, procédez comme suit : ◦ Sélectionnez les champs Intégration de l'infraction en cours et Définir la durée d'ingestion de l'infraction initiale. ◦ Spécifiez le délai dans le champ Délai d'ingestion de l'infraction initiale d'entrée. L'ingestion initiale aura lieu à l'heure spécifiée ici. Les ingestions suivantes seront ba-

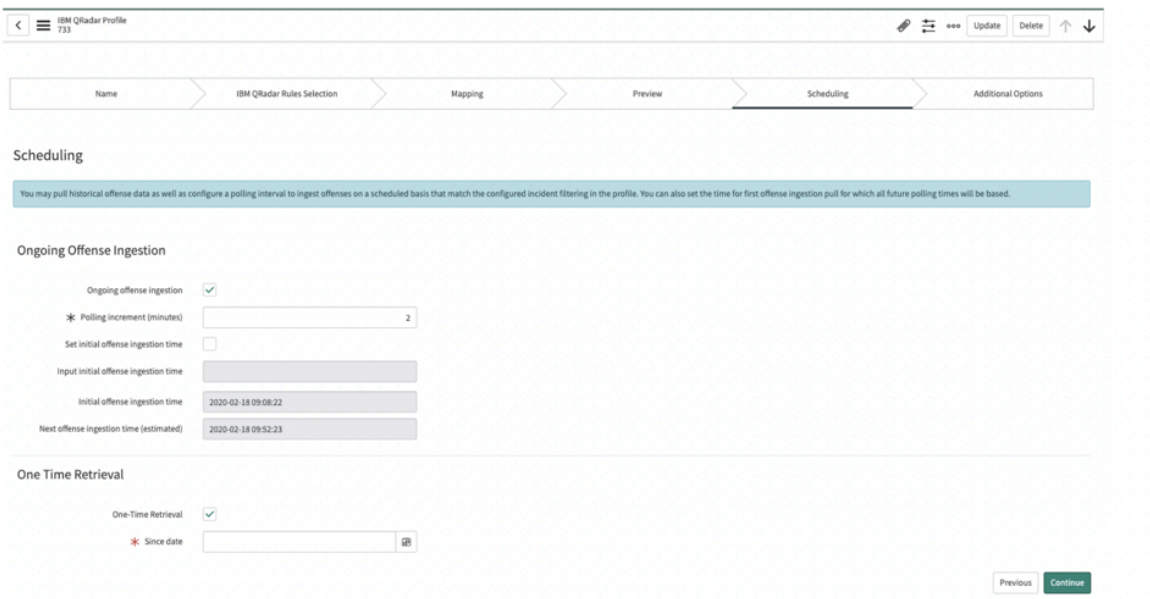
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	sées sur le calendrier défini dans le champ Incrémentation de l'interrogation (minutes). Par exemple, pour planifier un délai d'ingestion d'une infraction initiale, si vous avez un contrôle de sécurité quotidien IBM QRadar qui s'exécute une fois par jour à 4 h (heure locale), vous pouvez configurer le profil d'infraction correspondant dans votre Now Platform instance pour qu'il s'exécute à 4 h 05, heure locale, afin de capturer immédiatement la défaillance de sécurité et créer un incident de sécurité. Entrez `<date> 04 05 00` dans le champ Ingestion de l'infraction initiale. Dans le champ Incrémentation de l'interrogation (minutes), saisissez `<date> 1440` (24 heures) pour planifier l'ingestion de la prochaine infraction dans les 24 heures suivant l'ingestion de l'infraction initiale. Le temps d'ingestion de l'infraction initiale et le temps d'ingestion de l'infraction suivante sont affichés dans les champs. L'ingestion initiale aura lieu à 4h05. Les ingestions suivantes seront basées sur l'intervalle d'interrogation. Dans ce cas, étant donné que l'incrément d'interrogation est de 24 heures, la prochaine ingestion aura lieu le lendemain à 4h05.
Champ de récupération unique sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhaitez une transmission par pull unique pour ingérer des infractions historiques. Lorsque ce paramètre est configuré, un profil est utilisé une seule fois pour récupérer les infractions à partir d'événements historiques basés sur une plage de dates. À droite du champ Depuis date, cliquez sur l'icône Calendrier. Dans le calendrier qui s'affiche, sélectionnez la date à laquelle vous souhaitez commencer à extraire les infractions. À partir de la valeur Date de début, les infractions sont récupérées jusqu'à la date actuelle. Notez que vous pouvez remonter jusqu'à sept jours en arrière à partir de la date actuelle. Cette fonctionnalité n'est pas destinée à récupérer des quantités importantes d'infractions historiques à partir IBM QRadar de raisons d'archivage, mais plutôt une quantité minimale d'infractions en cours de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	traitement au moment de l'activation du profil. Une fois les infractions extraites, ce paramètre ne récupérera pas d'autres infractions pour ce profil à partir de la date actuelle. Ce paramètre remplit l'incident de sécurité avec toutes les infractions détectées pour la plage que vous saisissez.



3. Cliquez sur **Continuer** pour accéder à la page Options supplémentaires.

Automatiser les mises à jour et la fermeture des infractions en fonction de l'état de l'incident SIR

L'intégration IBM QRadar dispose d'une interface bidirectionnelle qui permet aux deux infractions de créer des incidents de sécurité, ainsi que la possibilité de mettre à jour les infractions une fois l'incident de sécurité créé et/ou fermé avec les détails pertinents de l'incident tels que le numéro d'incident de sécurité, le groupe d'affectation, l'URL de l'incident de sécurité, entre autres.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si la page Options supplémentaires de la barre de progression n'est pas affichée, sélectionnez **Options supplémentaires**.
2. Suivez les instructions ci-dessous pour terminer la configuration de mise à jour des infractions lors de la création de l'incident de sécurité.

Option ou champ	Description
Mettre à jour les infractions lors de la création de l'incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour le statut de l'infraction et ajouter des commentaires supplémentaires lors-

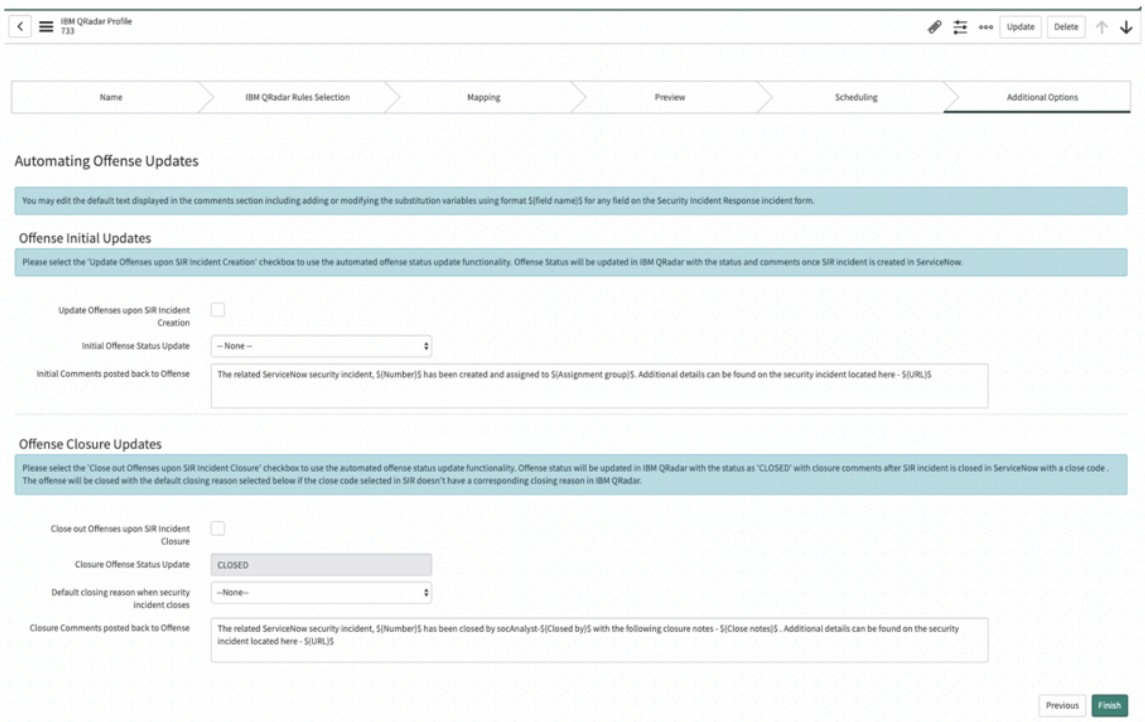
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	qu'un incident de sécurité est créé à partir de l'infraction. Cela peut se produire à la fois pour les infractions déclenchantes initiales qui créent l'incident de sécurité et pour les infractions agrégées.
Mise à jour du statut de l'infraction initiale	Vous pouvez sélectionner : ◦ Ouvert : le statut de l'infraction est défini sur **Ouvert** et un commentaire est ajouté indiquant qu'un incident de sécurité a été créé pour l'infraction. ◦ Masqué : le statut de l'infraction est défini sur **Masqué** et cette infraction est masquée dans le IBM QRadar tableau de bord.
Commentaires initiaux renvoyés à l'attaque	En fonction de l'étape que vous avez sélectionnée, les commentaires initiaux tels que définis dans la IBM QRadar console s'affichent ici.
Fermer les infractions lors de la fermeture de l'incident SIR	Sélectionnez cette option si vous souhaitez utiliser l'option de fermeture automatisée des infractions. Lorsque l'incident de sécurité est fermé avec ServiceNow un code de fermeture pertinent, l'état de l'infraction est mis à jour dans IBM QRadar**Fermé** avec des commentaires de fermeture. **Remarque :** Le code de fermeture spécifié pour l'incident de sécurité doit correspondre au motif de fermeture spécifié dans le IBM QRadar tableau de bord. L'infraction n'est IBM QRadar clôturée que si un motif de fermeture correspondant est trouvé. Si aucun motif correspondant n'est trouvé, l'infraction est fermée avec un code de fermeture par défaut.
Commentaires de fermeture renvoyés à l'infraction	Les commentaires de fermeture tels que définis dans le IBM QRadar tableau de bord sont affichés ici.
Motif de fermeture par défaut lors de la fermeture de l'incident de sécurité	Le motif par défaut à utiliser lorsqu'un incident de sécurité est fermé, Lorsqu'un incident de sécurité est fermé, un code de fermeture (ou le motif de la fermeture) est spécifié dans l'enregistrement d'incident de sécurité. Si le code de fermeture ne correspond pas au motif de fermeture spécifié dans le IBM QRadar tableau de bord et que vous tentez de fermer l'incident de sécurité, un message d'erreur s'affiche. Dans de tels cas, le motif de fermeture par défaut spéci-

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	fié ici est utilisé lors de la fermeture de l'incident de sécurité.



3. Cliquez sur **Terminer** pour terminer la configuration et déplacer le profil vers l'état **En attente** .
   Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Activez ce profil pour extraire les infractions de la IBM QRadar console en fonction de votre planification.

IBM QRadar Paramètres de configuration d'intégration

Utilisez cette option pour modifier les propriétés système par défaut de l'intégration d'ingestion IBM QRadar .

Pour modifier les propriétés système, connectez-vous en tant qu'utilisateur ayant le rôle *sn_si.admin* et accédez à **Intégration d'IBM QRadar** > **Paramètres d'intégration d'IBM QRadar**.

Paramètres d'intégration d'IBM QRadar

Nom de la propriété	Description
Appliquer une limite au nombre d'incidents de sécurité qui peuvent être créés dans la période de 24 heures. sn_sec_qradar.max_si_par_jour	Spécifie le nombre maximal d'incidents de sécurité qui peuvent être créés en 24 heures. • Type : nombre entier • Valeur par défaut : 1 000
Appliquez une limite au nombre d'infractions qui peuvent être regroupées en un seul incident.	Limite de l'agrégation des infractions pour un incident de sécurité. Par exemple, s'il y a 102 infractions, les 100 premières infractions

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres d'intégration d'IBM QRadar (suite)

Nom de la propriété	Description
sn_sec_qradar.max_aggregation_per_si	sont agrégées aux incident_1 de sécurité et les 2 autres aux incident_2 de sécurité. • Type : nombre entier • Valeur par défaut : 100
Cette propriété définit la période d'AQL pour extraire les événements/flux récents pour une infraction particulière. sn_sec_qradar.on_demand_recent_days_limit	Spécifie le nombre de jours nécessaires pour extraire les événements ou flux récents pour une infraction particulière. • Type : nombre entier • Valeur par défaut : 7
Cette propriété limite le nombre d'événements récents récupérés pour une infraction particulière. sn_sec_qradar.on_demand_event_limit	Spécifie le nombre d'événements récupérés pour une infraction. Les événements les plus récents sont récupérés en premier en fonction de l'horodatage de l'événement. • Type : nombre entier • Valeur par défaut : 100
Cette propriété limite le nombre de flux récents récupérés pour une infraction particulière. sn_sec_qradar.on_demand_flow_limit	Spécifie le nombre de flux récupérés pour une infraction. Les flux les plus récents sont récupérés en premier sur la base de l'horodatage du flux. • Type : nombre entier • Valeur par défaut : 100
Cette propriété définit la valeur de délai d'expiration (secondes) pour l'AQL qui extrait les flux/événements récents pour une infraction particulière. sn_sec_qradar.on_demand_timeout	• Type : nombre entier • Valeur par défaut : 300
ID de recherche Délai d'expiration (secondes) des enregistrements en file d'attente pour l'interrogation des AQL d'une infraction. sn_sec_qradar.sid_ttl	Délai d'attente de l'AQL pour une infraction dans la file d'attente avant de créer un incident de sécurité. Par exemple, s'il y a 90 infractions, les 50 premières infractions sont traitées pour les données AQL dans le premier lot, et les 40 infractions restantes dans le lot suivant dans le même intervalle d'interrogation. • Type : nombre entier • Valeur par défaut : 300
Seuil permettant de contrôler le nombre de recherches qui peuvent être exécutées IBM QRadar en même temps et qui est déclenché par l'intégration planifiée	Spécifie le nombre d'infractions que vous pouvez extraire en un seul lot dans un intervalle d'interrogation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres d'intégration d'IBM QRadar (suite)

Nom de la propriété	Description
job.sn_sec_qradar.records_threshold_in_que_for_agl	• Type : nombre entier • Valeur par défaut : 50
Il s'agit du nombre de jours pour le nettoyage des tables d'intégration. sn_sec_qradar.queue_item_expire	Les tables d'intégration sont les suivantes : • sn_sec_qradar_events : événements IBM QRadar • sn_sec_qradar_flows : flux IBM QRadar • sn_sec_qradar_offense_updates - Mises à jour de l'infraction IBM QRadar • sn_sec_qradar_offense_to_task : infraction IBM QRadar à la tâche • Type : nombre entier • Valeur par défaut : 30
Limite d'infractions par exécution de tâche planifiée par profil, soit en récupération ponctuelle, soit en ingestion continue. sn_sec_qradar.max_offense_limit_per_run	Spécifie le nombre d'infractions que vous récupérez dans Now Platform en une seule récupération. • Type : nombre entier • Valeur par défaut : 1 000
Définissez cette propriété pour activer la fonctionnalité Mises à jour des infractions. sn_sec_qradar.get_offense_updates	**Remarque :** L'activation de ce paramètre peut entraîner un retard dans la création d'un incident de sécurité. • Type : true | false • Valeur par défaut : faux

Tous les paramètres d'intégration modifiés seront appliqués lors du prochain intervalle d'interrogation, tel que défini dans le profil.

Facultatif : copier un IBM QRadar profil

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils pour gagner du temps.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

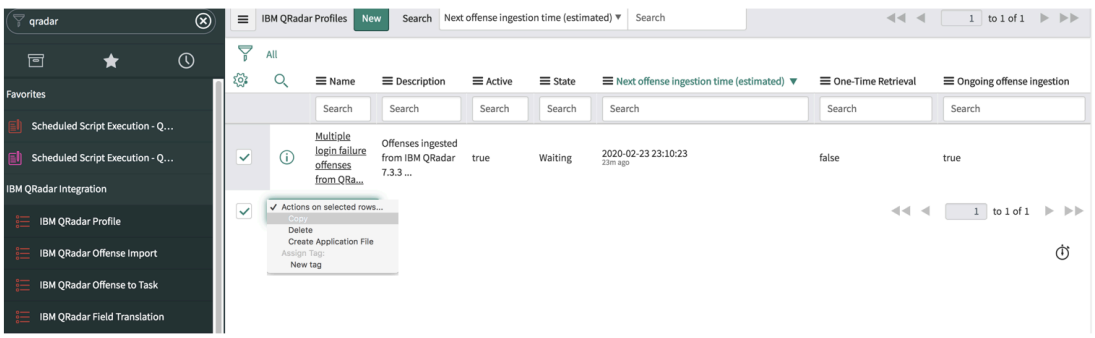
En tant qu'utilisateur disposant du rôle sn_si.admin, si vous copiez un profil, le nom du profil est d'abord modifié pour éviter les profils en double. En outre, le profil copié est désactivé (faux) afin qu'il ne soit pas activé accidentellement avant la fin de la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

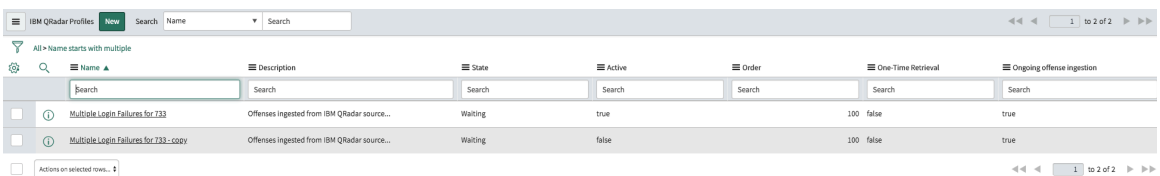
Procédure

1. Accédez à la **Tout** > **Intégration d'IBM QRadar** > **Profil IBM QRadar**.
2. Dans la liste IBM QRadar Profiles qui s'affiche, sélectionnez un profil que vous souhaitez copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier**.



Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (`vrai`), la copie est désactivée à ce stade (`faux`). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.

Remarque : Si vous sélectionnez une source différente pour le profil, vous devez sélectionner de nouvelles règles (Sélectionner IBM QRadar des règles) pour le profil. Mais si vous utilisez la même source et sélectionnez de nouvelles règles, les exemples d'infractions seront effacés.



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. Notez que l'état de la colonne **Actif** est défini sur faux, car le profil doit être activé.

Que faire ensuite

Vous êtes invité à activer le nouveau profil une fois que vous avez terminé les étapes de configuration.

Séparation de domaine et IBM QRadar intégration d'infractions

L'ingestion d'infractions prend en charge IBM QRadar Séparation de domaine. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : basique

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de service de l'application.
- L'application prend en charge Séparation de domaine lors de l'exécution. Séparation de domaine inclut la séparation à partir de l'interface utilisateur, des clés de cache, du reporting, des déploiements et des agrégations.
- Le propriétaire de l'instance doit configurer l'application de sorte qu'elle fonctionne sur plusieurs locataires.

Exemple de cas d'utilisation : lorsqu'un fournisseur de service (SP) utilise la messagerie instantanée pour répondre au message d'un locataire-client, le client doit pouvoir afficher la réponse du SP.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

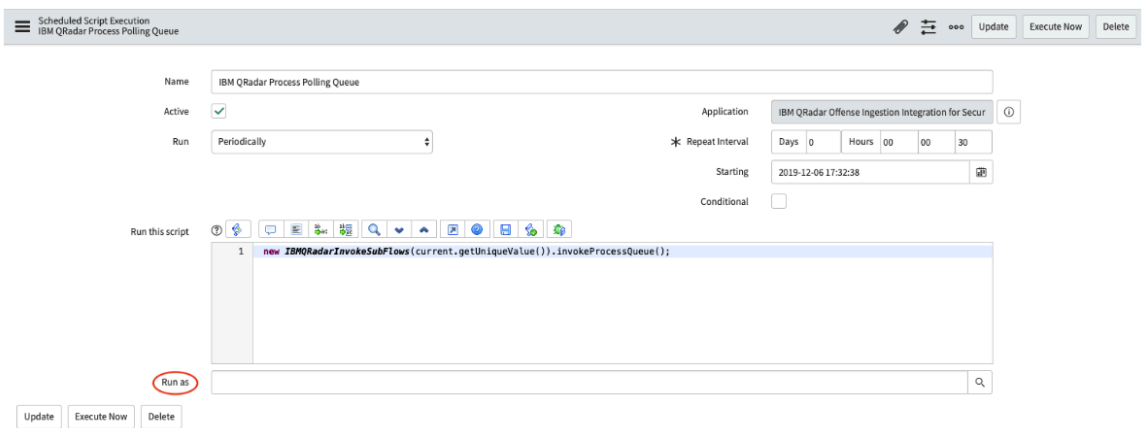
Comment fonctionne Séparation de domaine dans IBM QRadar Offense Ingestion

Procédez comme suit pour réaliser Séparation de domaine :

- Créez un utilisateur avec le rôle *sn_si.admin* dans le domaine correspondant.

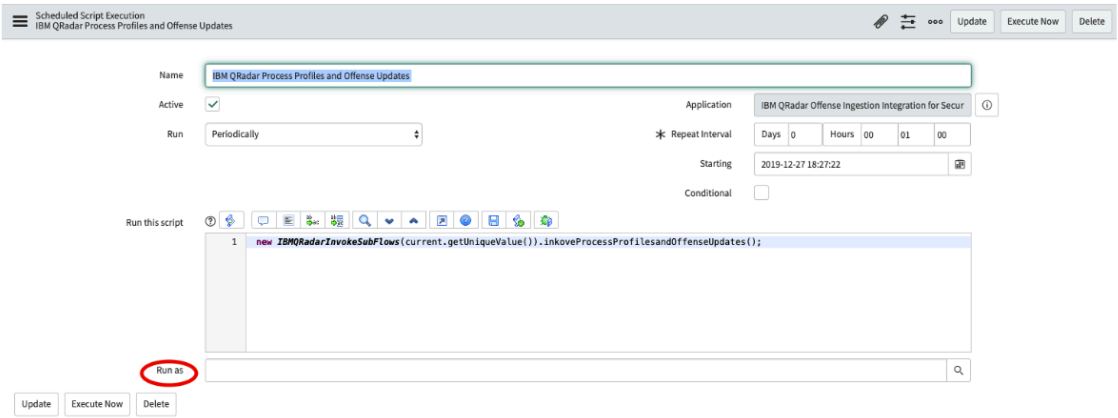
> **Remarque :** Lorsque vous créez le profil, utilisez le sélecteur de domaine pour sélectionner le domaine spécifique. Ne créez pas l'utilisateur dans le domaine parent et ne modifiez pas ultérieurement le domaine du profil. Vous devez avoir un utilisateur spécifique pour chaque domaine pour votre profil avec le rôle *sn_si.admin*. Utilisez cet utilisateur pour créer ou modifier les paramètres du profil.

- Désactivez les travaux planifiés existants.
- Répliquer la file d'attente d'interrogation de processus, les IBM QRadarIBM QRadar profils de processus et l'infraction Met à jour les travaux planifiés pour chaque domaine.
- Changez **l'option Exécuter en tant que de** l'utilisateur système à l'utilisateur disposant du rôle *sn_si.admin* dans le domaine respectif et exécutez la tâche planifiée.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Information associée

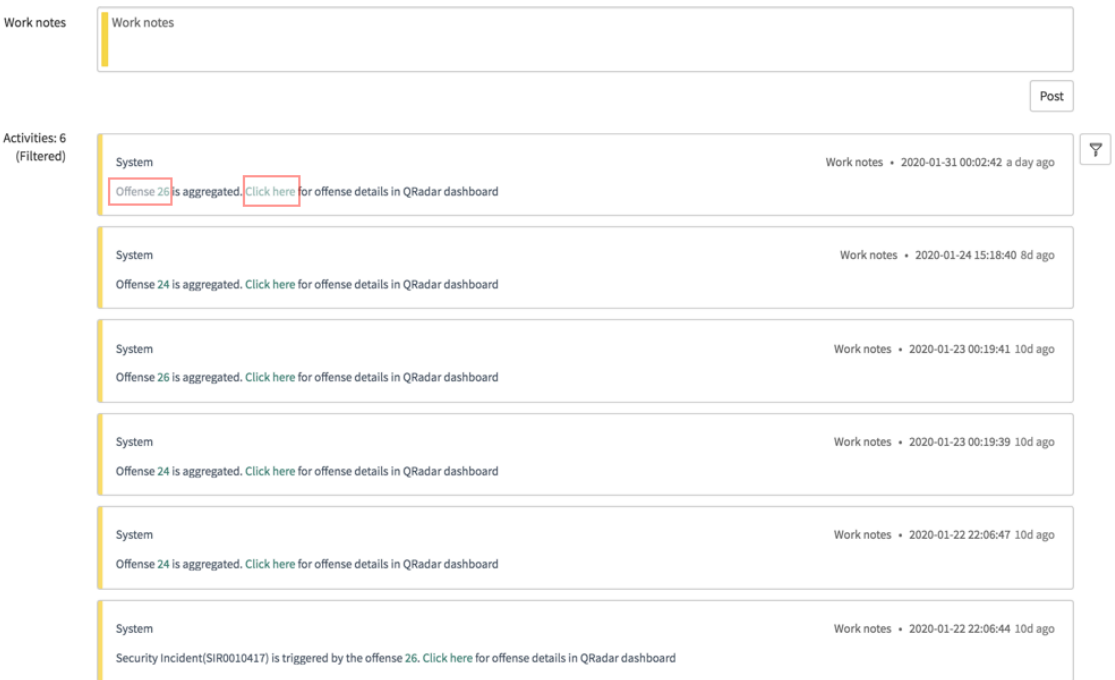
Séparation de domaine pour les fournisseurs de services

Formulaire Security Incident Response après l'ingestion de l'infraction

Une fois qu'une IBM QRadar infraction a été ingérée, un incident de sécurité est créé et les mises à jour correspondantes sont apportées à l'enregistrement d'incident de sécurité.

Notes de travail

Une note de travail est publiée avec les détails de l'infraction qui a déclenché l'incident de sécurité.

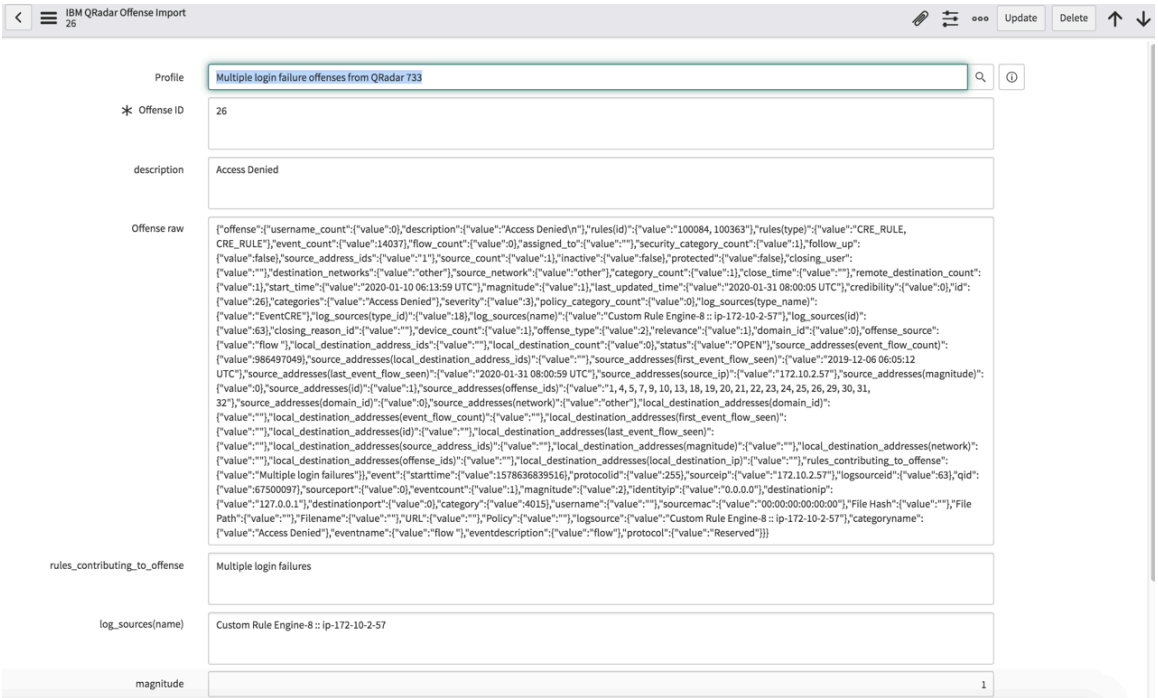


Cliquez sur le lien de l'infraction pour accéder à l'enregistrement de l'incident de sécurité interne. Le lien hypertexte **Cliquez ici** vous dirige vers le IBM QRadar tableau de bord où vous pouvez afficher les détails de l'infraction.

Si vous aviez sélectionné l'option **Consigner la note de travail pour la nouvelle infraction** dans les critères d'agrégation des infractions, comme décrit dans le , une note de Mappage IBM QRadar des champs d'infraction aux champs de réponse aux incidents de sécuritétravail est publiée lorsque l'infraction est regroupée.

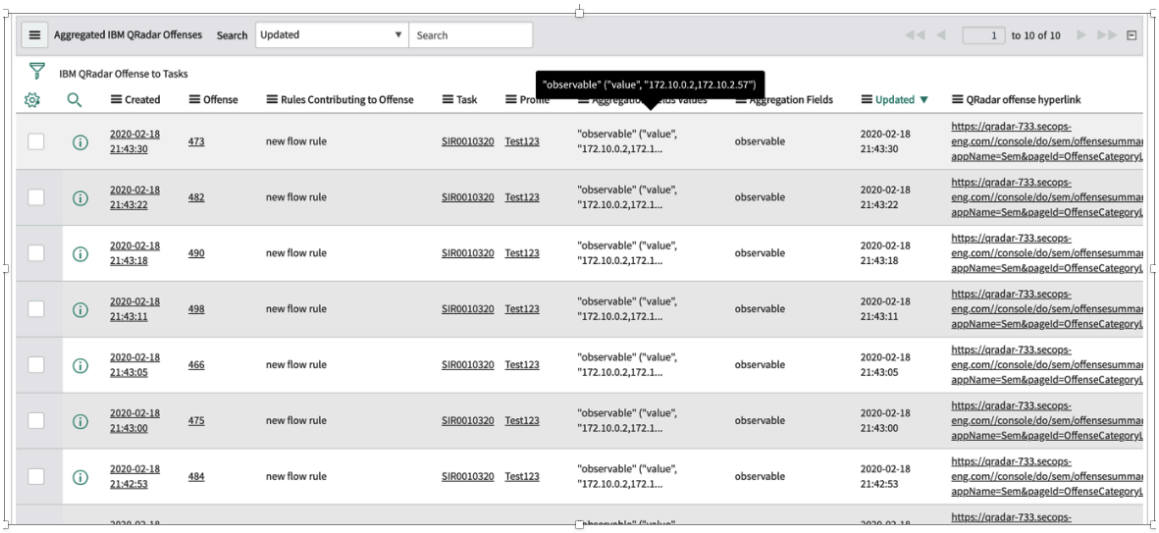
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Infractions agrégées

Cliquer sur **Listes connexes** > **Infractions IBM QRadar agrégées** pour afficher les infractions agrégées à l'incident de sécurité. Cliquez sur le lien hypertexte de l'infraction QRadar pour afficher l'infraction dans le IBM QRadar tableau de bord.

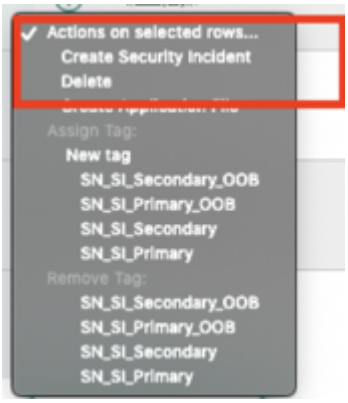


Créer un incident de sécurité : sélectionnez une infraction dans la liste, cliquez sur le menu **Actions** , puis sur **Créer un incident de sécurité**. Cette option crée un incident de sécurité pour l'infraction et cette infraction est désagrégée à partir de l'incident de sécurité parent.

Supprimer l'enregistrement des infractions : sélectionnez une infraction dans la liste, cliquez sur le menu **Actions** , puis sur **Supprimer**. Cette option supprime l'enregistrement de l'infraction.

Traduction automatique

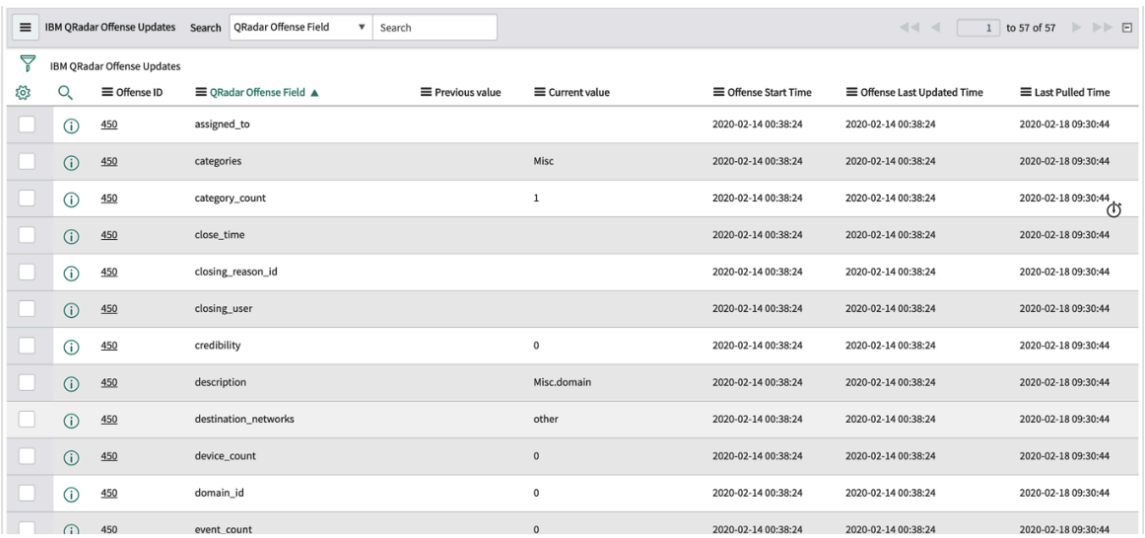
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Mises à jour de l'infraction IBM QRadar

Cela affiche les champs d'infraction standard et personnalisés et suit les changements apportés à l'infraction à chaque intervalle de sondage. Cela est utile car vous pouvez afficher les mises à jour des infractions directement sans avoir à naviguer dans le IBM QRadar tableau de bord. Tous les changements apportés aux valeurs sont affichés dans les champs Valeur précédente et Valeur actuelle.

Pour activer la fonctionnalité de mises à jour des infractions, accédez à **Intégration d'IBM QRadar** > **Paramètres d'intégration d'IBM QRadar** et activez **Définir cette propriété pour activer la fonctionnalité Mises à jour des infractions**. Par défaut, ce paramètre est désactivé.

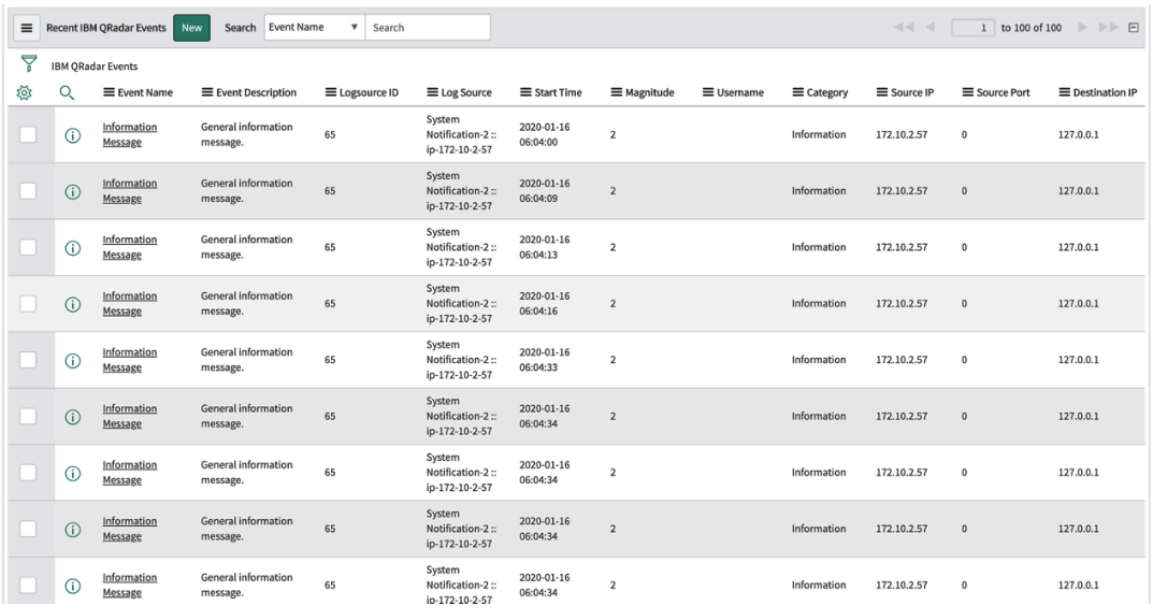


Offense ID	QRadar Offense Field	Previous value	Current value	Offense Start Time	Offense Last Updated Time	Last Pulled Time
450	assigned_to			2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	categories		Misc	2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	category_count		1	2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	close_time			2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	closing_reason_id			2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	closing_user			2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	credibility		0	2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	description		Misc.domain	2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	destination_networks		other	2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	device_count		0	2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	domain_id		0	2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44
450	event_count		0	2020-02-14 00:38:24	2020-02-14 00:38:24	2020-02-18 09:30:44

Événements IBM QRadar récents

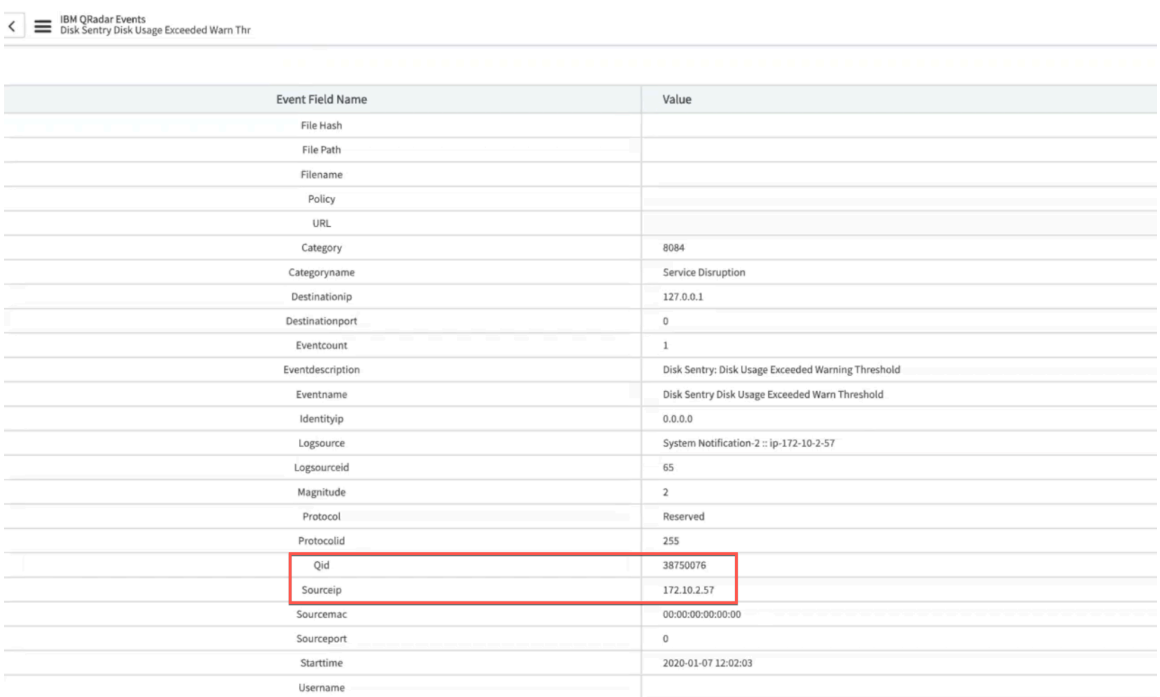
Cliquez sur l'option **Fetch Recent IBM QRadar Events (Extraire les événements IBM QRadar récents**) sous **Liens connexes** pour afficher les événements les plus récents IBM QRadar .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Par défaut, un nombre maximal de 100 événements est affiché. Vous pouvez modifier ce paramètre par défaut dans le IBM QRadar Paramètres de configuration d'intégrationfichier .

Remarque : L'image ci-dessus montre les champs d'événement standard associés à l'infraction. Si vous avez configuré et mappé des champs d'événements personnalisés (reportez-vous à la section Mappage IBM QRadar des champs d'infraction aux champs de réponse aux incidents de sécurité), vous pouvez les afficher dans la vue de liste en cliquant sur le lien Nom d'événement.

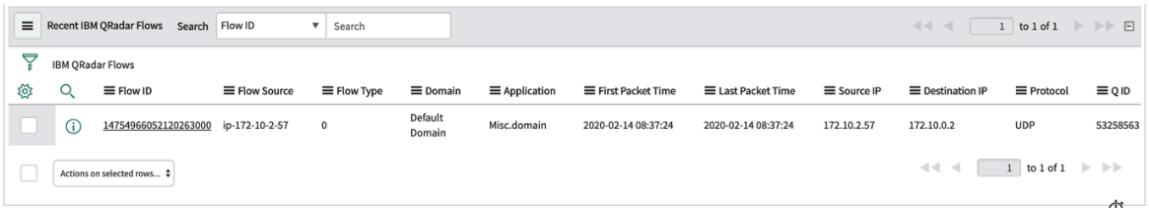


Flux IBM QRadar récents

À l'aide du concentrateur d'intégration et de Flow Designer, plusieurs flux, flux secondaires et actions sont disponibles avec l'intégration IBM QRadar . Lorsque vous cliquez sur l'option **Extraire les flux IBM QRadar récents** sous les liens connexes, les flux les plus récents sont récupérés. Pour afficher ces flux, cliquez sur **Flux IBM QRadar récents**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique



Par défaut, un nombre maximum de 100 flux est affiché. Vous pouvez modifier ce paramètre par défaut dans le IBM QRadar Paramètres de configuration d'intégrationfichier .

Remarque : L'image ci-dessus montre les champs de flux standard associés à l'infraction. Si vous avez configuré et mappé des champs de flux personnalisés (reportez-vous à la section Mappage IBM QRadar des champs d'infraction aux champs de réponse aux incidents de sécurité), vous pouvez les afficher dans la vue de liste en cliquant sur le lien ID de flux.

Utilisation de Flow Designer et d'Integration Hub avec l'intégration de l'ingestion d'infractions IBM QRadar

À l'aide des fonctionnalités de Concepteur de flux et de concentrateur d'intégration, plusieurs flux secondaires et actions ont été créés dans le cadre de l'intégration de l'ingestion IBM QRadar d'infraction.

Les flux secondaires suivants IBM QRadar sont disponibles :

- Validation de la connexion et des informations d'identification : cette option est utilisée dans la tuile de configuration pour valider l'hôte et les informations d'identification lors de la configuration initiale.
- Récupération des règles IBM QRadar : cette option est utilisée dans la section Règles de la configuration du profil pour récupérer toutes les règles actives dans IBM QRadar. Ce flux secondaire est déclenché de façon asynchrone.
- Fetch Sample Offences Data (Extraire des données d'échantillons d'infractions) à partir d'IBM QRadar : cette option est utilisée dans la section Mapping (Mappage) de la configuration du profil pour extraire des exemples de données. Ce flux secondaire est déclenché de façon asynchrone.
- Mises à jour de l'état des infractions IBM QRadar : elles sont déclenchées par une tâche planifiée toutes les minutes et mettent à jour l'infraction lors IBM QRadar de la création ou de la fermeture de l'incident de sécurité.
- Traiter les profils à partir d'une tâche planifiée et d'une file d'attente Infractions : cette option est déclenchée par une tâche planifiée toutes les minutes pour extraire les infractions par profil en fonction de l'intervalle d'interrogation. Cela extrait les infractions et les met en file d'attente vers la table de vote pour un traitement ultérieur.
- Traiter la file d'attente d'interrogation et l'interrogation par lots : ceci est déclenché par une tâche planifiée toutes les 30 secondes pour traiter la file d'attente de la table d'interrogation.
- Extraire les flux IBM QRadar récents : cette option est déclenchée à partir du lien du formulaire d'incident de sécurité pour obtenir les flux d'infraction les plus récents.
- Extraire les événements IBM QRadar récents : cette option est déclenchée à partir du lien du formulaire d'incident de sécurité pour obtenir les derniers événements d'infraction.

Pour afficher ces flux secondaires, connectez-vous en tant qu'utilisateur ayant le rôle *sn_si.admin* et accédez à **Concepteur de flux** > **Concepteur**. Cliquez sur le lien Nom de l'un des flux secondaires répertoriés ci-dessus pour afficher le flux secondaire en détail.

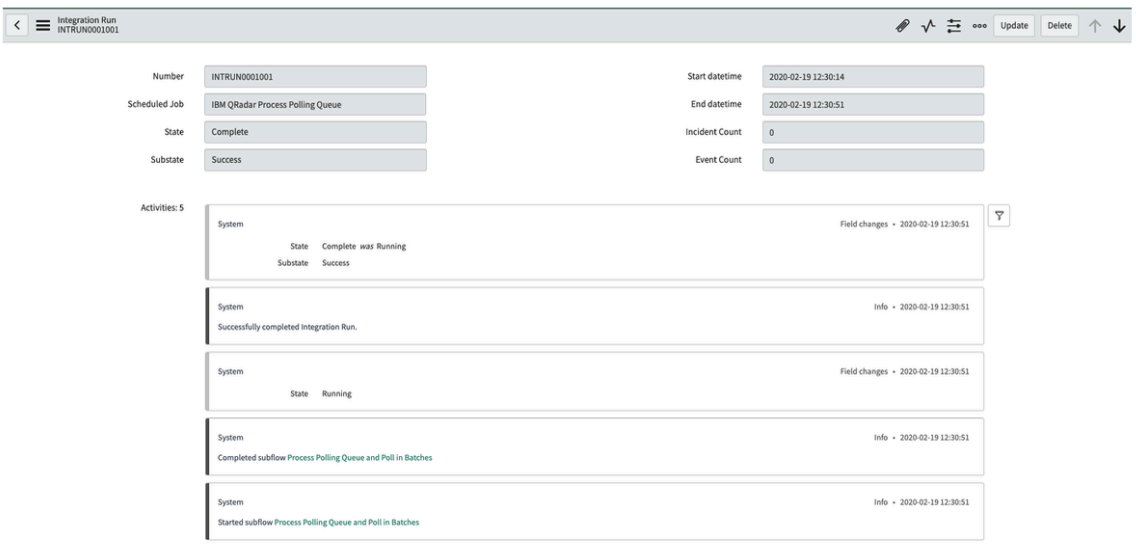
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résolution des problèmes liés à l'intégration IBM QRadar de l'ingestion d'infraction

Cette section couvre des conseils de dépannage importants et les questions fréquemment posées relatives à l'ingestion d'infractions IBM QRadar .

- Exécution de l'intégration : lorsqu'une tâche planifiée commence à s'exécuter, un enregistrement d'exécution de l'intégration avec les journaux, les erreurs et les avertissements s'affiche. Le nombre d'infractions extraites et le nombre d'incidents créés dans une exécution de tâche planifiée sont également affichés. Les utilisateurs disposant du rôle sn_si.analyst peuvent voir si l'extraction des erreurs/profils a échoué pendant l'exécution de l'intégration.

  Les notes de travail de l'exécution de l'intégration fournissent des liens vers les flux secondaires exécutés. Les utilisateurs disposant du rôle sn_si.analyst peuvent consulter la table `sn_event_ingestion_integration_run` pour détecter les erreurs survenues. Pour résoudre tout problème d'intégration, vous devez d'abord vérifier l'exécution de l'intégration. Les erreurs sont enregistrées sous forme de notes de travail dans les enregistrements d'exécution de l'intégration pour chaque exécution de tâche planifiée.



- Problèmes SSL : lors de la connexion à des instances cloud IBM QRadar , assurez-vous que l'instance dispose d'un certificat CA valide qui n'a pas expiré. Vous pouvez importer RSA ou vos propres certificats dans la plateforme et vous assurer que le nom commun du certificat correspond au nom d'hôte. Consultez https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 pour en savoir plus.
- Profil incomplet : lors de la configuration du profil, dans la section Options supplémentaires (Automatiser les mises à jour et la fermeture des infractions en fonction de l'état de l'incident SIR), vous devez cliquer sur le bouton **Terminer** pour vous assurer que le profil passe à l'état En attente, ce qui indique qu'il est en attente d'ingestion.
- Valider le profil : pour valider si l'intégration fonctionne correctement, vérifiez les états du profil, la date de la dernière opération Pull du profil, la table d'importation d'infraction, les enregistrements de la table d'infractions à la tâche.
- Configuration du serveur MID : si vous installez l'application IBM QRadar sur site, après avoir configuré le serveur MID, vous devez créer une application de serveur MID. Le nom de l'application du serveur MID doit être utilisé dans la vignette de configurations d'intégration au lieu du nom du serveur MID.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le délai d'expiration par défaut du service MID est de 30 secondes. Pour obtenir des instructions sur la désactivation du délai d'expiration, reportez-vous à la section <link>. Notez qu'il s'agit d'un changement à l'échelle du système qui peut avoir un impact sur d'autres intégrations.

- Mises à jour des infractions : si vous avez activé la propriété *sn_sec_qradar.get_offense_updates* et que vous remarquez un retard dans la création des incidents de sécurité, désactivez la propriété. N'activez pas cette propriété lorsque l'intervalle d'interrogation est faible et que la charge des infractions sur QRadar est élevée, car cela augmente la charge de la file d'attente.
- Données d'événement remote_ip, de flux ou d'utilisateurs manquantes dans un incident de sécurité : si vous observez que des données d'événement, de flux remote_ip ou d'utilisateurs sont manquantes dans un incident de sécurité, augmentez le délai d'expiration (en secondes) du paramètre *sn_sec_qradar.sid_ttl*. L'augmentation de la durée retarde la création de l'incident de sécurité jusqu'à ce que les AQL aient terminé l'analyse de chaque infraction.
- Délais d'expiration : si vous affichez des erreurs de délai d'expiration dans les journaux d'application, examinez et modifiez les actions suivantes du concepteur de flux :

Actions du concepteur de flux

Paramètres	Action
Extraire les exemples d'infractions `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 60000) ;`	Examinez et mettez à jour la durée en millisecondes.
Extraire les exemples d'infractions `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs) ;`	Ajoutez un paramètre pour *executeAction* et saisissez la durée en millisecondes.
Extraire les infractions pour les enregistrements de profil et de file d'attente dans la table d'interrogation `var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 180000) ;`	Examinez et mettez à jour la durée en millisecondes.
Couche pour le REST de test de la connexion `var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest', rest_inputs) ;`	Ajoutez un paramètre pour *executeAction* et saisissez la durée en millisecondes.
Couche pour REST de validation des informations d'identification d'API	Ajoutez un paramètre pour *executeAction* et saisissez la durée en millisecondes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres	Action
`var rest_outputs = sn_fd. FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs) ;`	
Étape REST pour les mises à jour IBM QRadar Offense `var résultat = sn_fd. FlowAPI.executeAction('sn_sec_qradar.' +restStep, entrées,60000) ;`	Examinez et mettez à jour la durée en millisecondes.

IBM QRadar : intégration de l'enrichissement d'incident

L'intégration IBM QRadar d'enrichissement d'incident recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

- Commencez avec l'intégration de l'enrichissement IBM QRadar des incidents
- Créer des enregistrements de configuration de recherche d'observations

Utiliser

- Exécuter une recherche d'observations
- Security Operations Integration - Workflow de recherche de perceptions
- Security Operations - Workflow de recherche de perceptions QRadar
- Afficher les détails de la recherche d'observations
- Afficher les résultats de recherche d'observations

Développer

- ServiceNow Opérations de sécurité Directives de développement de l'intégration
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté des opérations de sécurité
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Commencez avec l'intégration de l'enrichissement IBM QRadar des incidents

IBM QRadar est un produit SIEM (Enterprise Security Information and Events Management) qui s'intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l'intégration IBM

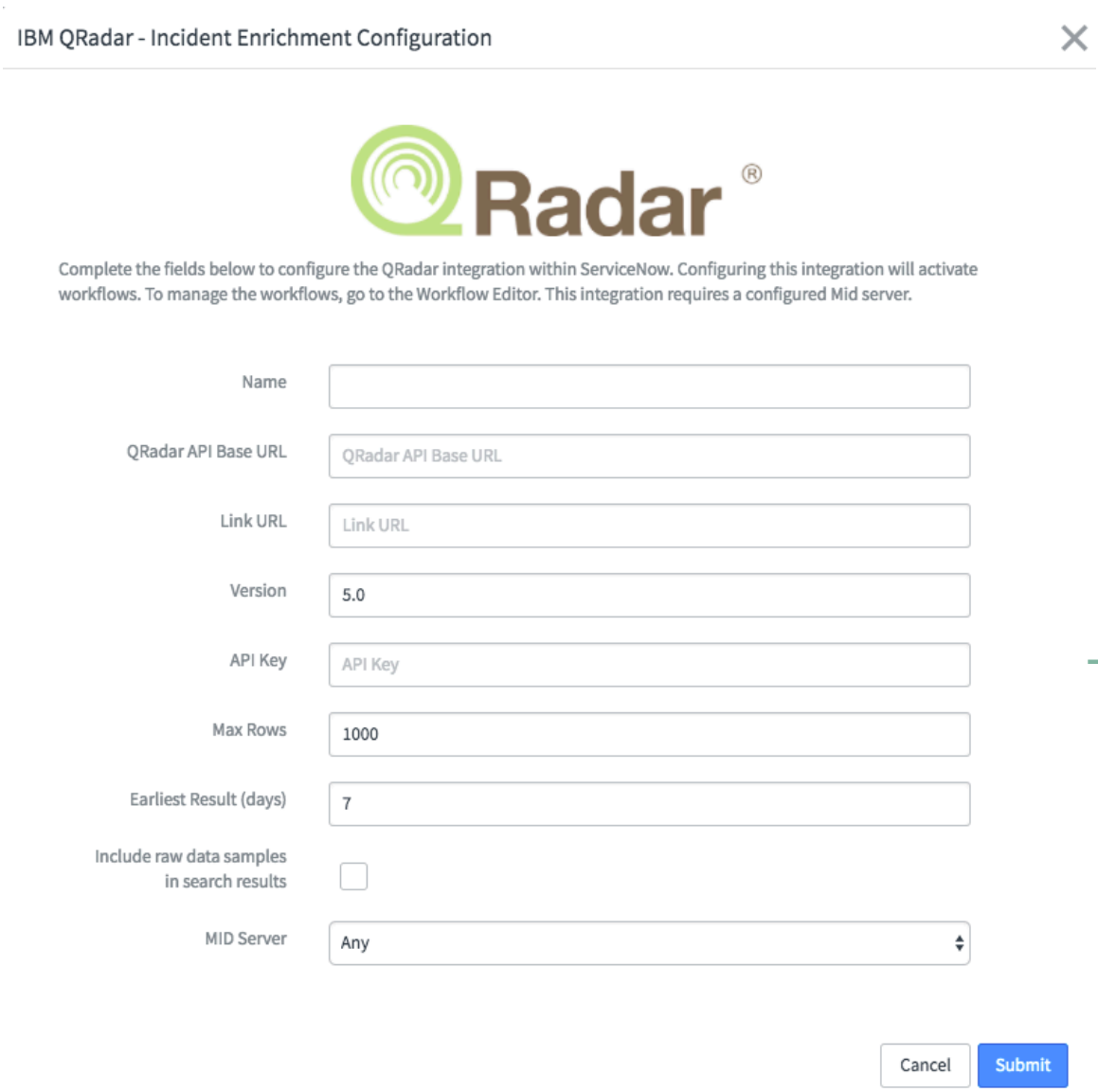
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

QRadar d'enrichissement d'incident, vous devez la télécharger à partir de et ajouter l'URL de base de l'API ServiceNow Store et la clé API appropriées.

Avant de commencer
Rôle requis : sn_si_admin

Procédure
1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à IBM QRadar l'URL de base API et à la clé API sous votre IBM QRadar profil, et obtenez-les.
3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Sur la carte Enrichissement d'incident IBM QRadar , cliquez sur **Nouveau**.



5. Renseignez les champs nécessaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom de cette configuration.
URL de Base de l'API QRadar	L'URL de base que vous avez acquise à partir du IBM QRadar site.
URL de lien	[Facultatif] L'URL du lien qui renvoie à une instance, lorsqu'elle IBM QRadar est disponible.
Version	La IBM QRadar version 5.0 est la version par défaut.
Clé API	La clé API que vous avez obtenue à partir du IBM QRadar site.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend du paramètre que vous définissez sur le **nombre de lignes de la propriété de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	Sélectionnez **N'importe lequel** pour utiliser n'importe quel Serveur MID actif ou sélectionnez un nom de Serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

6. Cliquez sur **Envoyer**.
   La carte de configuration de l'intégration s'affiche.
7. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
8. Pour revenir à la liste initiale des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

LogRhythm Vue d'ensemble

La flexibilité de mappage de cette intégration offre à l'analyste une visibilité sur les événements et les données d'alarme connexes qui peuvent être intégrées dans Now Platform les incidents de sécurité pour une enquête et une correction plus approfondies.

Les profils d'alarme sont créés dans votre Now Platform instance pour personnaliser la façon dont les différents LogRhythm champs d'alarme sont affichés sur un Now Platform incident de sécurité. Un mappage par défaut des champs d'alarme est fourni, qui peut être modifié pour répondre aux besoins spécifiques du client.

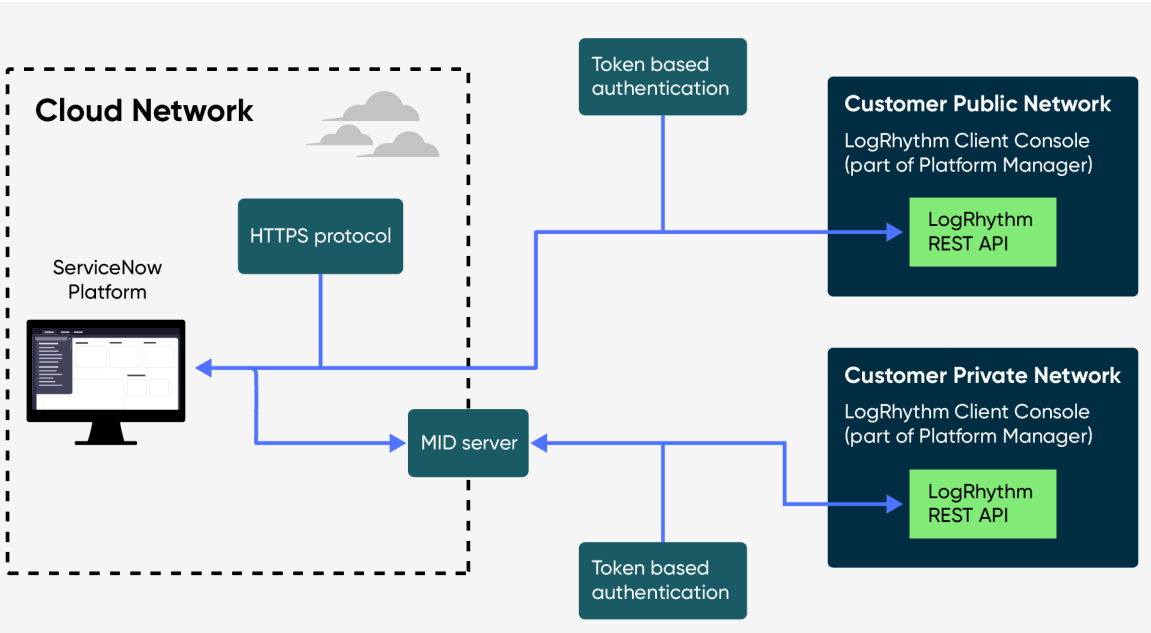
La figure suivante est un exemple d'environnement client. Lorsqu'un événement déclenche la création d'un incident de sécurité dans l'instance Now Platform® , une demande est envoyée à partir de votre Now Platform® instance pour extraire des alarmes de la console cliente, LogRhythm via un MID Server ou même sans celui-ci.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La clé API REST est utilisée par le pour s'authentifier Now Platform® auprès de la LogRhythm console cliente. Cette connexion permet à votre Now Platform instance d'extraire des alarmes individuelles LogRhythm en fonction des profils configurés.

L'API REST est utilisée pour recueillir les détails du message auxquels l'API REST n'a pas accédé.

Intégration de LogRhythm



Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

- Flexibilité de création de plusieurs profils d'alarme pour différents types d'alarmes tels que Hameçonnage et Programmes malveillants.
- Glisser-déposer le mappage des valeurs de champ d'alarme LogRhythm aux champs d'incident de sécurité associés SIR .
- Un aperçu de la mise en page de l'incident SIR de sécurité basée sur LogRhythm des échantillons d'alarmes.
- Ingérer les alarmes historiques, ainsi que les alarmes futures en cours à intervalles configurables.
- Fermeture automatisée de l'alarme lors SIR de la fermeture de LogRhythm l'incident. Une URL pour l'incident SIR ainsi qu'un ID d'incident sont fournis pour une référence facile.

Versions prises en charge de Now Platform

Cette intégration est compatible avec la version Quebec ou une version ultérieure du Now Platform®fichier .

Versions prises en charge de LogRhythm

Cette intégration est compatible avec LogRhythm la version 7.8 ou ultérieure. Les versions antérieures ne sont pas prises en charge en raison de limitations d'API.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les sujets suivants sont numérotés. Pour une installation fluide et pour vous aider à vérifier les résultats attendus, suivez les rubriques dans l'ordre dans lequel elles sont présentées.

Configurer l'API REST pour LogRhythm

Vous utilisez la clé API REST pour collecter des détails supplémentaires sur l'événement LogRhythm pour les champs d'alarme individuels. La clé API fournit des détails qui ne sont pas disponibles à l'aide de REST LogRhythm API.

Avant de commencer

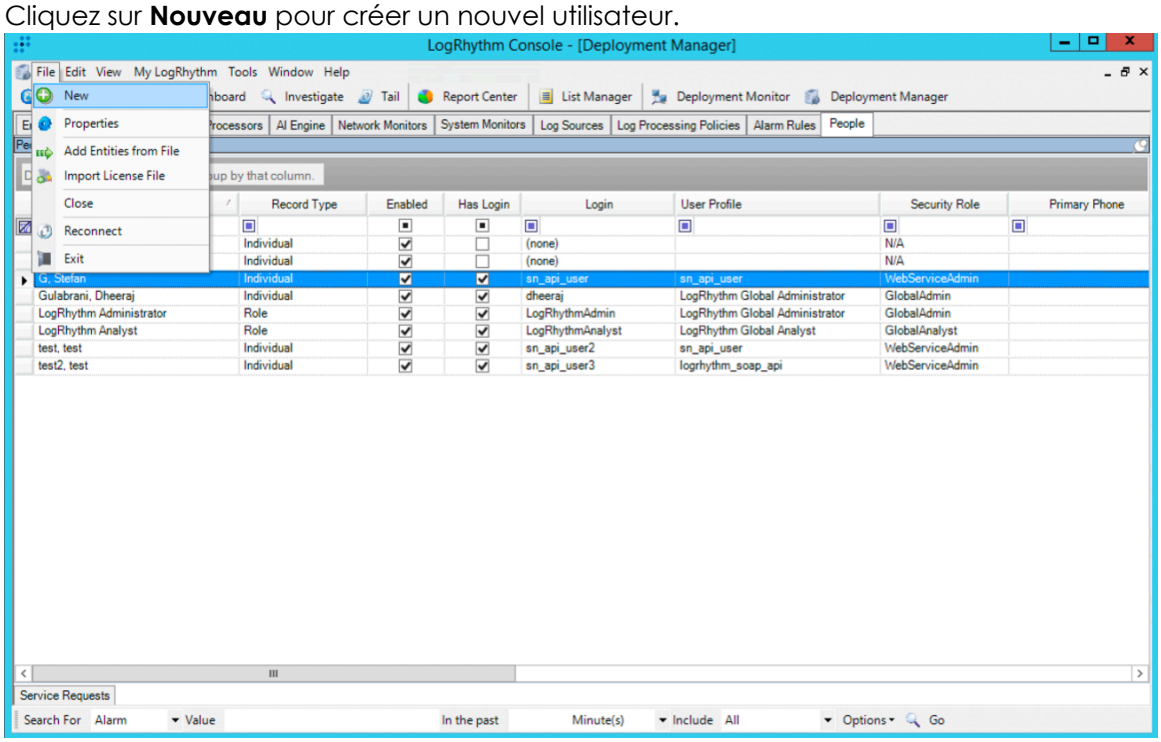
Rôle requis : LogRhythm Console client/Administrateur gestionnaire de la plateforme

Pourquoi et quand exécuter cette tâche

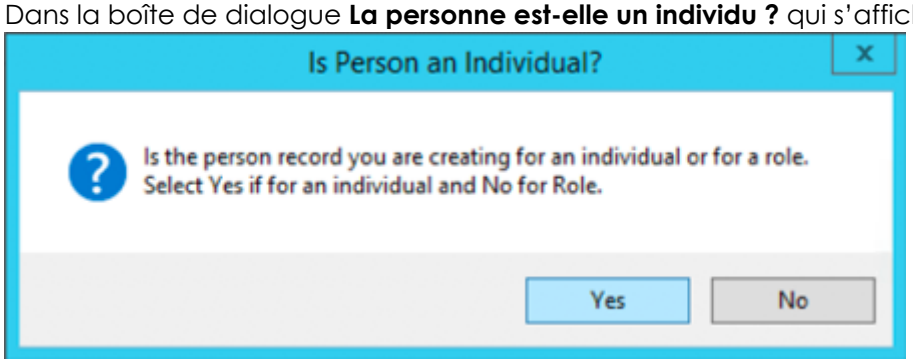
Cette tâche est exécutée sur la LogRhythm console cliente. Configurez l'API LogRhythm REST avant d'installer le module d'extension à partir du ServiceNow Store.

Procédure

1. Accédez à la LogRhythm console cliente et sélectionnez le menu **Fichier** .
2. Cliquez sur **Nouveau** pour créer un nouvel utilisateur.



3. Dans la boîte de dialogue **La personne est-elle un individu ?** qui s'affiche, cliquez sur **Oui**.

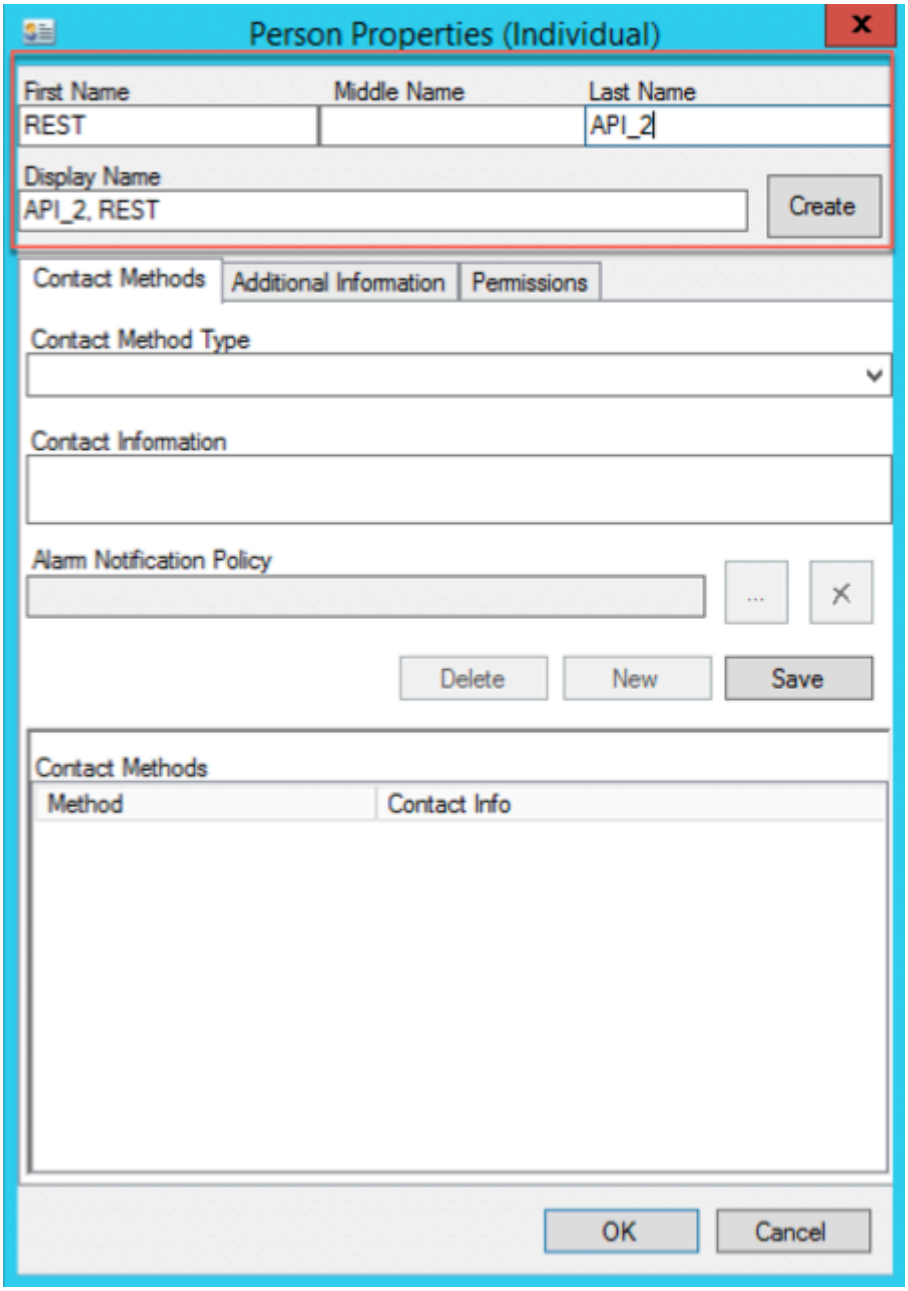


4. Dans la boîte de dialogue Propriétés de la personne qui s'affiche, renseignez les champs Nom.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

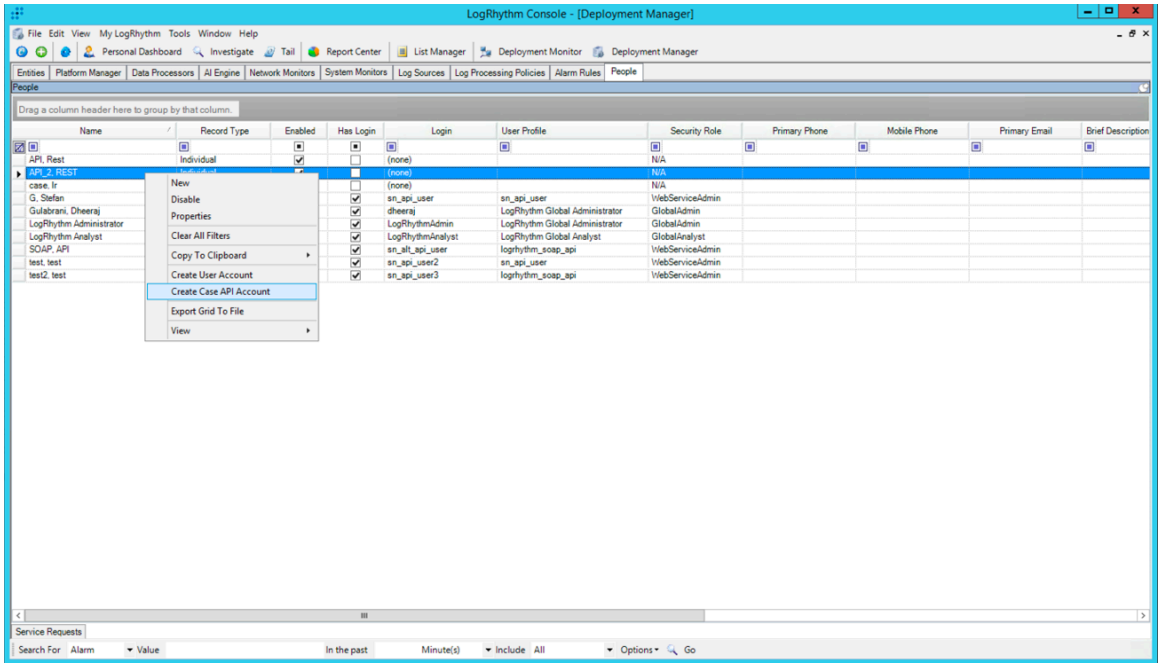
Utilisez un nom différent de celui que vous avez utilisé pour LogRhythm créer l'API REST, par exemple `REST API_2`.



5. Cliquez sur **OK**.
6. Cliquez avec le bouton droit de la souris sur la nouvelle liste dans la colonne Nom (**API_2_REST**) et, dans la liste de choix, sélectionnez **Créer un compte API de ticket**.

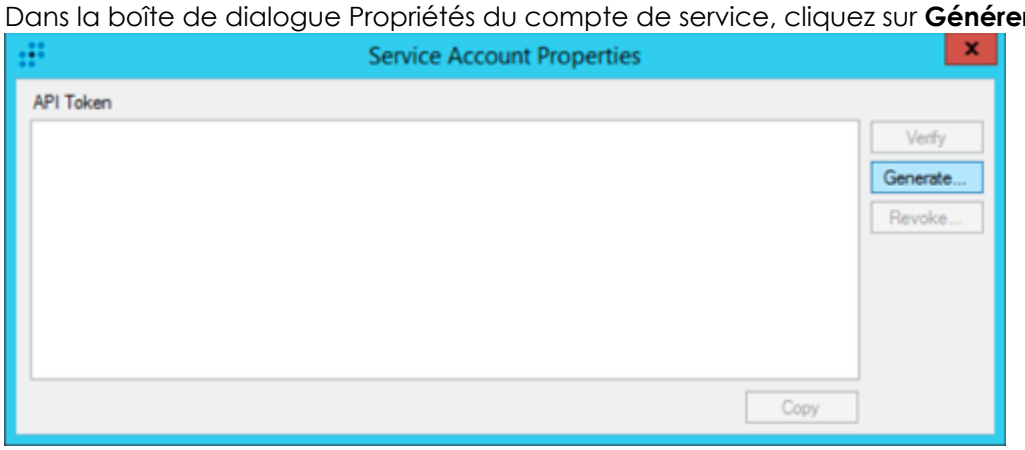
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

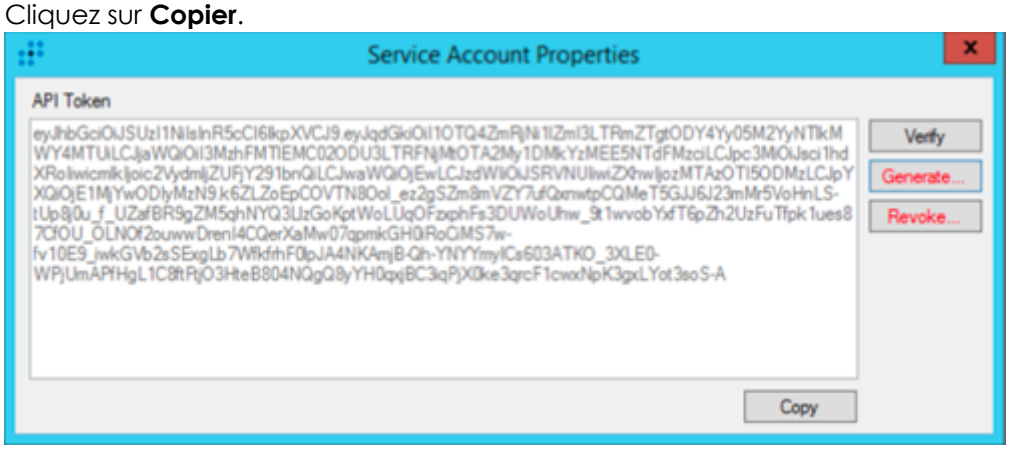


Remarque : L'API de ticket n'est pas utilisée, mais les informations d'identification du compte d'API de ticket et de l'API LogRhythm REST sont les mêmes.

7. Dans la boîte de dialogue Propriétés du compte de service, cliquez sur **Générer**.



8. Cliquez sur **Copier**.



Vous avez maintenant configuré l'API LogRhythm REST. Vous collez la chaîne que vous avez copiée à l'étape précédente dans votre Now Platform instance dans le champ Jeton d'API LogRhythm REST au cours des étapes de configuration répertoriées dans Installer le module d'extension et configurer LogRhythm.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Vous êtes maintenant prêt à Installer le module d'extension et configurer LogRhythm.

Installer le module d'extension et configurer LogRhythm

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que l'application s'intègre Opérations de sécuritéNow Platform®correctement au .

Avant de commencer

Rôle requis : administrateur

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides. La dernière LogRhythm version est 7.8 ou ultérieure.

Remarque : Vos profils d'alarme existants ne seront plus pris en charge sur la dernière LogRhythm version, vous devez donc créer de nouveaux profils d'alarme et effectuer les configurations requises.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform® et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (admin) installe le module d'extension de l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Le (sn_si.admin) supervise les tâches suivantes : ◦ Nomme, crée et modifie les profils d'alarme. ◦ Mappe et filtre les alarmes : identifie les alarmes spécifiques LogRhythm qui créent des incidents de sécurité et configure la façon dont ces champs d'alarme sont mappés à un Now Platform® incident de sécurité. ◦ Prévisualise l'exactitude des détails de l'incident de sécurité avant de finaliser la configuration. ◦ Ingère les alarmes historiques et planifie les alarmes extraites. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Ce rôle a également accès au Opérations de sécurité module. • L'analyste des incidents de sécurité (sn_si.analyst) répond aux incidents de sécurité créés en fonction des paramètres du profil d'alarme.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
Procurez-vous un nom d'utilisateur et un mot de passe d'API et vérifiez que vous utilisez la LogRhythm version LogRhythm 7.8 ou une version ultérieure.	Visitez le site Web du produit pour plus d'informations sur les clés API et pour créer un compte : site Web de LogRhythm Enterprise . Les comptes utilisateur, les informations d'identification et les certificats doivent être configurés correctement avant l'installation de l'application. L'intégration nécessite la LogRhythm version 7.8 ou ultérieure et les LogRhythm API REST. Consultez Configurer l'API REST pour LogRhythm.
Vérifiez que vous avez installé et configuré un serveur MID.	Un serveur MID est requis dans votre Now Platform environnement. Consultez le site web de la documentation du produit ServiceNow pour plus d'informations sur l'installation et la configuration des serveurs MID.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Pour la version Rome et les versions ultérieures de la famille, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Orchestration de support de sécurité Pour en savoir plus sur la configuration de votre Now Platform instance pour l'intégration, consultez et .

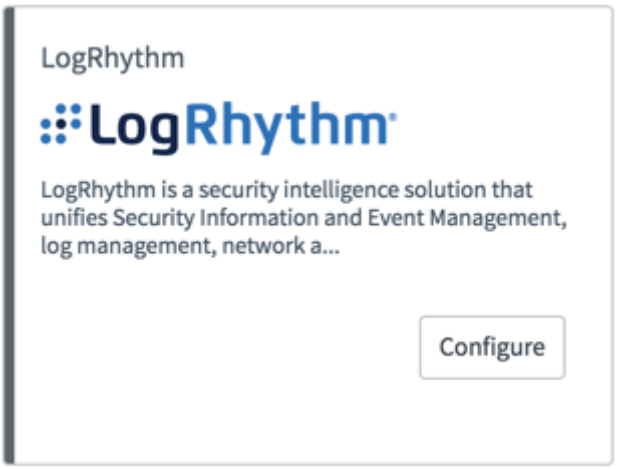
Important : Si vous rencontrez des problèmes de connectivité à la LogRhythm console cliente, reportez-vous à la Vérifier la connectivité pour LogRhythmsection .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si vous n'avez pas installé l'application pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la LogRhythm tuile.
3. Cliquez sur **Configurer**.



4. Cliquez sur le lien **Nouvelle configuration** .



5. Renseignez les champs suivants du formulaire :

Configuration LogRhythm

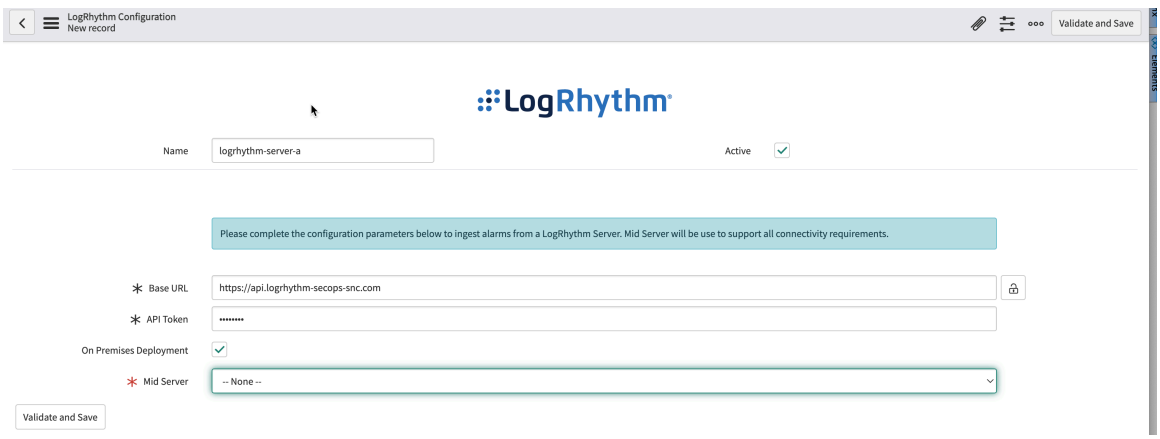
Champ	Description
Nom	LogRhythm Nom du serveur, par exemple, `logrhythm-server-a`.
URL de base	URL de base hébergeant l'API LogRhythm REST. Le MID Server permet d'accéder au réseau où la console cliente LogRhythm est hébergée. Cette URL est l'endroit où le LogRhythm serveur est hébergé dans ce réseau. Cliquez sur l'icône de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	verrou à l'extrémité droite pour modifier le champ et saisissez le texte d'une URL, par exemple `https://logrhythm.secops-eng.com:8501/`.
Jeton d'API	Saisissez le jeton associé à votre API REST que vous avez créée sur la LogRhythm console cliente.
Déploiement sur site	Option permettant de sélectionner s'il s'agit d'un LogRhythm déploiement sur site.
Serveur MID	Serveur MID spécifique configuré dans votre environnement. Seuls les MID Server actifs qui ont été validés sont disponibles dans cette liste de choix.

La figure suivante est un exemple de formulaire rempli.



6. Cliquez sur **Valider et enregistrer**.
   Une fois la validation terminée, un message s'affiche et la LogRhythm page Configurations est rechargée. L'étape suivante consiste à créer un profil d'alarme.

Que faire ensuite
Une fois que vous avez terminé la validation avec succès, l'étape suivante consiste à Création d'un profil d'alarme pour LogRhythm.

Création d'un profil d'alarme pour LogRhythm

Dans un profil d'alarme que vous créez et nommez, vous spécifiez les alarmes que vous souhaitez extraire de la LogRhythm console cliente. Vous définissez également la manière dont ils sont mappés aux champs d'un Now Platform incident de sécurité.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
En fonction du profil d'alarme configuré, un profil d'alarme peut ingérer tous les types d'alarmes prêtes à l'emploi, mais vous pouvez utiliser des critères de filtre pour ingérer des types d'alarmes spécifiques. Grâce à cette Now Platform intégration, toutes les règles d'alarme configurées ou spécifiques en fonction du profil créé sont ingérées. Les règles d'alarme, telles que les alarmes de niveau de risque élevé, peuvent alors être filtrées pour spécifier quelles alarmes doivent créer des incidents de sécurité. Avant que les incidents de

Traduction automatique

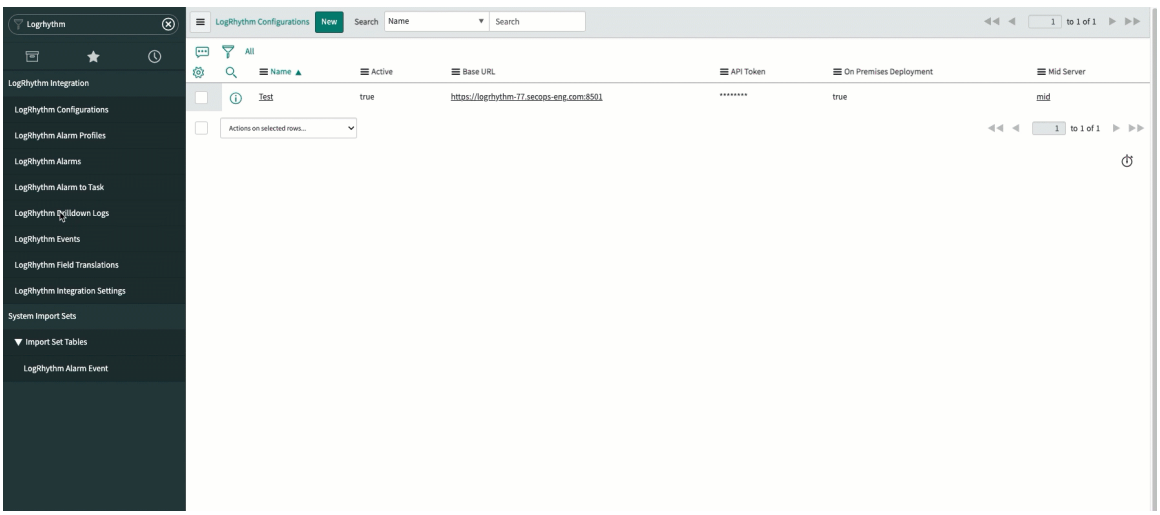
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sécurité ne soient créés, les valeurs de champ individuelles des alarmes filtrées sont mappées aux champs correspondants de l'incident Now Platform de sécurité. Cette configuration s'effectue via un profil d'alarme au sein de votre Now Platform instance.

Procédure

1. Accédez à la **Tout** > **Intégration de LogRhythm**.
2. Sélectionnez le module **Profils d'alarme LogRhythm pour** afficher la liste **des profils d'alarme** .

Profil de l'alarme



3. Pour créer un profil d'alarme, cliquez sur **Nouveau**.
   Un nouveau formulaire de profil d'alarme s'affiche. En haut de la page, dans la barre de progression, **le nom** est sélectionné. Cette barre permet de suivre votre progression au cours de la configuration.
4. Renseignez les champs du formulaire.

Profil de l'alarme

Champ	Description
Nom	Nom du profil de l'alarme. Ce nom vous aide à identifier les types d'alarmes tels que Accès non autorisé (VPN), Programme malveillant ou Hameçonnage.
Description brève	Texte court pour plus d'informations sur le profil d'alarme, qui peut inclure le type d'alarmes ou une catégorie d'alarme. Un exemple de description : Toutes les alarmes associées à des tentatives d'accès non autorisées à Powershell et Sudo.
Source	Serveur source dans la liste de choix. La liste se compose des LogRhythm configurations que vous avez déjà configurées, par exemple, `logrhythm-server-a`. Consultez Installer le module d'extension et configurer LogRhythm.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ordre	Priorité du profil de l'alarme. Ce champ indique l'ordre dans lequel les profils d'alarme sont exécutés lorsque deux profils d'alarme ou plus partagent les conditions de déclenchement.
Actif	Par défaut, cette option n'est pas sélectionnée. Une fois que vous avez terminé toutes les étapes de configuration du profil d'alarme et cliqué sur **Terminer**, vous êtes invité à cocher cette case pour activer le profil d'alarme. Lorsque le profil d'alarme est actif, il extrait automatiquement les alarmes de la LogRhythm console cliente.

5. Cliquez sur **Continuer** pour enregistrer vos données et accéder au formulaire de mappage.

   Si la validation est réussie, la page se recharge et le formulaire **de mappage** s'affiche. Vous ne pouvez pas procéder à la configuration tant que vous n'avez pas validé votre connexion et vos informations d'identification.

Information associée

Mapper LogRhythm les alarmes à l'incident de sécurité

Mapper LogRhythm les alarmes à l'incident de sécurité

Après avoir sélectionné la LogRhythm source que vous souhaitez ingérer, vous devez mapper les champs d'alarme individuels LogRhythm aux champs d'incident Now Platform de sécurité.

Le mappage des alarmes comprend les tâches suivantes :

- Cartographier LogRhythm les alarmes. Pour cette tâche, vous répertoriez et ingérez (extractions) des échantillons d'alarmes à l'aide des ID d'alarme ou des alarmes les plus récentes de la LogRhythm console cliente.
- Les champs d'alarme d'échantillon sont classés en trois groupes :
  - Champs d'alarme : les champs d'alarme disponibles et leurs valeurs correspondantes sont affichés.
  - Champs d'événement : les champs d'événement disponibles et leurs valeurs correspondantes sont affichés.
  - Champs DrillDownLog : les champs du journal d'exploration vers le bas qui sont disponibles et leurs valeurs correspondantes sont affichés.
- Chaque ID d'alarme que vous avez extrait s'affiche sous forme d'onglet. Dans les onglets ID d'alarme, vérifiez que tous les champs d'alarme critiques de la section Ingestion d'échantillons d'alarme à gauche du formulaire sont mappés à la section Mappage de champs d'incident SIR à droite du formulaire.
- Une fois que vous avez mappé les alarmes au champ Mappage de champ d'incident SIR , vous pouvez voir la catégorie d'alarme également affichée dans le champ expression d'entrée . Par exemple, `${Alarm : alarmid}$`.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous pouvez modifier la configuration en ajoutant ou en supprimant des champs sur l'incident de sécurité. Suivez les champs négligés ou dupliqués grâce au code couleur fourni.
- Vous pouvez filtrer les alarmes pour spécifier quelles alarmes sont ingérées dans l'application SIR. Vous pouvez filtrer les alarmes directement ou utiliser les catégories d'alarmes pour approfondir votre recherche en fonction des alarmes, des événements ou des journaux de détail.
- Utilisez l'éditeur de script si vous souhaitez formater les valeurs des champs Priorité et Catégorie de l'incident de sécurité.

L'étape suivante consiste à Mapper LogRhythm les champs d'alarme aux champs d'incident de sécurité.

Information associée

Mapper LogRhythm les champs d'alarme aux champs d'incident de sécurité

Utiliser l'éditeur de script pour formater LogRhythm les valeurs

Filtrer les alarmes pour LogRhythm

Mapper LogRhythm les champs d'alarme aux champs d'incident de sécurité

Vous mappez les champs d'alarme individuels aux champs d'incident de sécurité. Le mappage préconfiguré peut être modifié et le code couleur fourni pour les champs vous aide à surveiller les alarmes que vous avez déjà mappées. Cette étape vous permet de visualiser l'impact de vos modifications sur les champs de l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin
Si vous n'êtes pas familier avec les LogRhythm alarmes, accédez à la LogRhythm console du client et passez en revue quelques exemples d'ID d'alarme. Pour l'exemple suivant, LogRhythm les alarmes `9468` et `9474` ont été utilisées pour mapper les alarmes à l'incident de sécurité.

Pourquoi et quand exécuter cette tâche

À l'aide de ce formulaire, vous mappez les LogRhythm règles d'alarme de gauche aux champs d'incident de sécurité de droite.

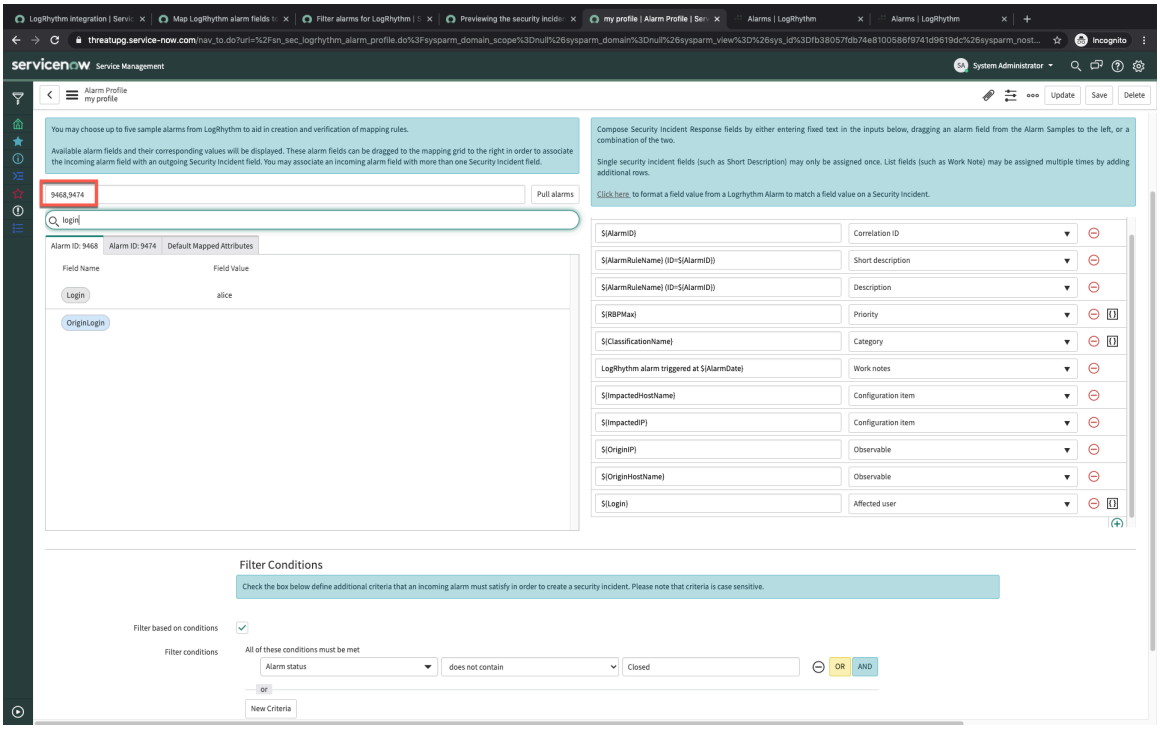
La figure suivante montre le mappage par défaut des alarmes qui est préconfiguré pour chaque profil d'alarme. Ce mappage par défaut peut être modifié et, avec ce formulaire, vous pouvez personnaliser les champs qui renseignent l'incident de sécurité. Une fois ce mappage terminé, vous pouvez voir comment l'ajout ou la suppression de champs d'alarme peut impacter les valeurs de champ sur l'incident de sécurité.

Sur le côté gauche de ce formulaire, dans la figure suivante, les règles d'alarme LogRhythm sont décrites. Les valeurs de ces règles d'alarme sont mappées aux champs d'incident de sécurité sur le côté droit du formulaire.

Procédure

1. Après avoir créé un profil d'alarme pour LogRhythm, cliquez sur **Mappage** dans la barre de progression.
2. Dans le champ **Alarm Sample Ingestion** , entrez jusqu'à cinq ID d'alarme d'échantillon LogRhythm séparés par des virgules (`9468,9474`).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. À côté du champ d'alarme, cliquez sur **Extraire les alarmes**.

L'extraction des échantillons d'alarmes peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran.

Une fois que les ID d'alarme d'échantillon sont soumis et extraits avec succès du serveur, les champs d'alarme LogRhythm et leurs valeurs correspondantes sont affichés dans des onglets.

Remarque : Une fois qu'un ID d'alarme est extrait avec succès, le Now Platform peut renvoyer le message suivant : `Les nouveaux champs suivants seront disponibles pour le filtrage sous peu. Veuillez recharger ce profil dans quelques minutes si le filtrage basé sur ces champs est requis. itemspacketsin, itemspacketsout`.

Ce message se produit lorsque l'alarme unique qui a été extraite contient des noms de champs qui n'ont pas été traités auparavant par le Now Platform. Ces champs sont disponibles pour le mappage. Toutefois, si ce message s'affiche, rechargez le formulaire afin que ces champs soient affichés et disponibles dans les listes de choix de filtres du générateur de conditions lorsque vous êtes prêt à définir les conditions de filtrage.

L'ingestion de ces échantillons d'alarmes dans la configuration du profil d'alarme vous aide à empêcher le mappage des champs d'alarme à l'incident de sécurité qui ne contiennent aucune valeur. Il aligne également les champs d'alarme avec les valeurs sur les champs appropriés dans l'incident de sécurité. Cette étape permet de s'assurer que tous les champs d'alarme critiques sont mappés et qu'aucune valeur de champ n'est manquante dans l'incident de sécurité.

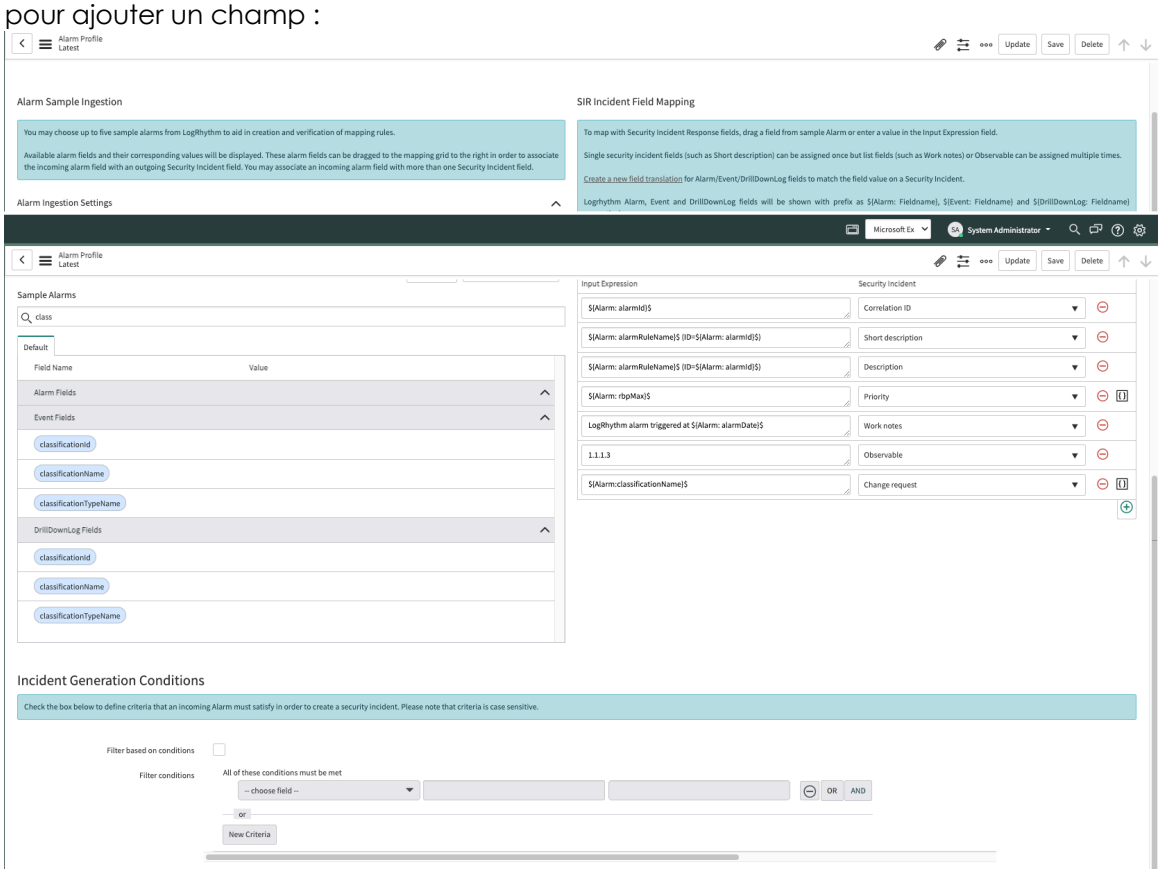
Pour vous assurer qu'aucune alarme n'est négligée ou dupliquée dans le processus de mappage, les champs d'alarme sont codés par couleur. Un champ d'alarme bleu clair (`Compte`, `AlarmRuleID`, `AlarmStatus`, etc.) indique qu'un champ n'est pas encore sélectionné pour être mappé à un incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un champ gris (`AlarmDate`, `AlarmID` et `AlarmRuleName`) indique qu'un champ a déjà été sélectionné et a été mappé à un champ sur l'incident de sécurité. Ce code couleur vous aide à suivre le mappage, car dans certains cas, un champ d'alarme peut être mappé à plusieurs champs sur un incident de sécurité. Par exemple, les champs `Observables` et `Note de travail` peuvent avoir plusieurs valeurs.

4. Pour effacer les données d'alarme d'échantillon, cliquez sur **Effacer les données d'alarme d'échantillon**.
5. Pour modifier la configuration par défaut sur l'incident de sécurité, procédez comme suit pour ajouter un champ :



   a. En bas à droite du formulaire, cliquez sur l'icône plus.
   Un nouveau champ s'affiche.

   b. Dans la colonne Incident de sécurité, sélectionnez un champ disponible dans la liste de choix.

   Dans la liste de choix développée, certains champs sont ombrés. Par exemple, la `catégorie` a un arrière-plan gris, ce qui indique qu'elle a été mappée dans l'incident de sécurité. À l'instar du code couleur pour LogRhythm les champs d'alarme, ce code couleur pour les champs d'incident de sécurité garantit que les valeurs des champs d'alarme ne sont pas mappées par inadvertance au même champ d'incident de sécurité.

   Dans l'illustration ci-dessus, la règle de l'alarme `${Alarm :classificationName}$` est déjà mappée au champ `Catégorie` dans l'incident de sécurité de ce profil.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ Observable peut être mappé à plusieurs champs sur le même incident de sécurité afin que plusieurs observables puissent être affichés. De même, les champs `Élément de configuration` et `Notes de travail` peuvent être mappés pour afficher plusieurs valeurs.

Du côté de l'ingestion d'échantillon d'alarme du formulaire, le bleu indique qu'un champ de règle d'alarme n'a pas été mappé. Le gris indique qu'il a été mappé. Dans la liste de choix du côté du formulaire Mappage de champ d'incident SIR, le blanc indique qu'un champ n'a pas été mappé. Le gris indique qu'un champ a été mappé. Utilisez ce code couleur pour vous aider à suivre le mappage de vos champs.

Dans l'illustration ci-dessus, `Utilisateur affecté` a été sélectionné dans la liste de choix comme un nouveau champ sur l'incident de sécurité.

c. Dans la section Ingestion d'échantillons d'alarme sur le côté gauche du formulaire, cliquez avec le bouton gauche de la souris pour sélectionner l'ID d'alarme souhaité dans le champ expression d'entrée.

Dans l'illustration ci-dessus, `Login (Connexion )` a été sélectionné.

d. Faites-le glisser vers le champ vide et relâchez-le.
Dans la colonne de gauche, dans la section Mappage de champs d'incidents SIR, la nouvelle valeur du champ `Utilisateur affecté` s'affiche. Dans ce cas, la valeur `de connexion` de l'alarme LogRhythm s'affiche dans le champ `Utilisateur affecté` de l'incident de sécurité.

6. Vous pouvez également saisir manuellement une valeur pour les champs de la colonne Expression d'entrée : placez votre curseur dans le champ d'expression d'entrée et saisissez la valeur d'alarme souhaitée.

Par exemple, dans l'illustration ci-dessus, un autre champ a été ajouté (`Groupe d'affectation`) au formulaire d'incident de sécurité et `l'affectation d'incident de sécurité` a été saisie manuellement dans le champ.

7. Continuez à modifier le mappage préconfiguré au besoin.
Si vous avez besoin de convertir des valeurs de champs d'alarme en valeurs prises en charge par les champs de l'incident de sécurité, vous pouvez utiliser l'éditeur de LogRhythm script. Consultez Utiliser l'éditeur de script pour formater LogRhythm les valeurs.

Que faire ensuite
Une fois que vous avez terminé le mappage des champs, l'étape suivante consiste à Filtrer les alarmes pour LogRhythm.

Filtrer les alarmes pour LogRhythm

Définir des critères de filtrage pour les alarmes une fois que vous avez mappé les champs vous aide à déterminer quelles alarmes doivent être ingérées dans l'application SIR. Le filtrage des alarmes vous aide à réduire considérablement le nombre d'alarmes que vous ingérez lorsque le profil d'alarme est activé.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Utilisez les conditions de filtrage au bas du formulaire de mappage pour filtrer des alarmes spécifiques ou limiter l'ingestion aux seules alarmes qui répondent à certains critères au

Traduction automatique

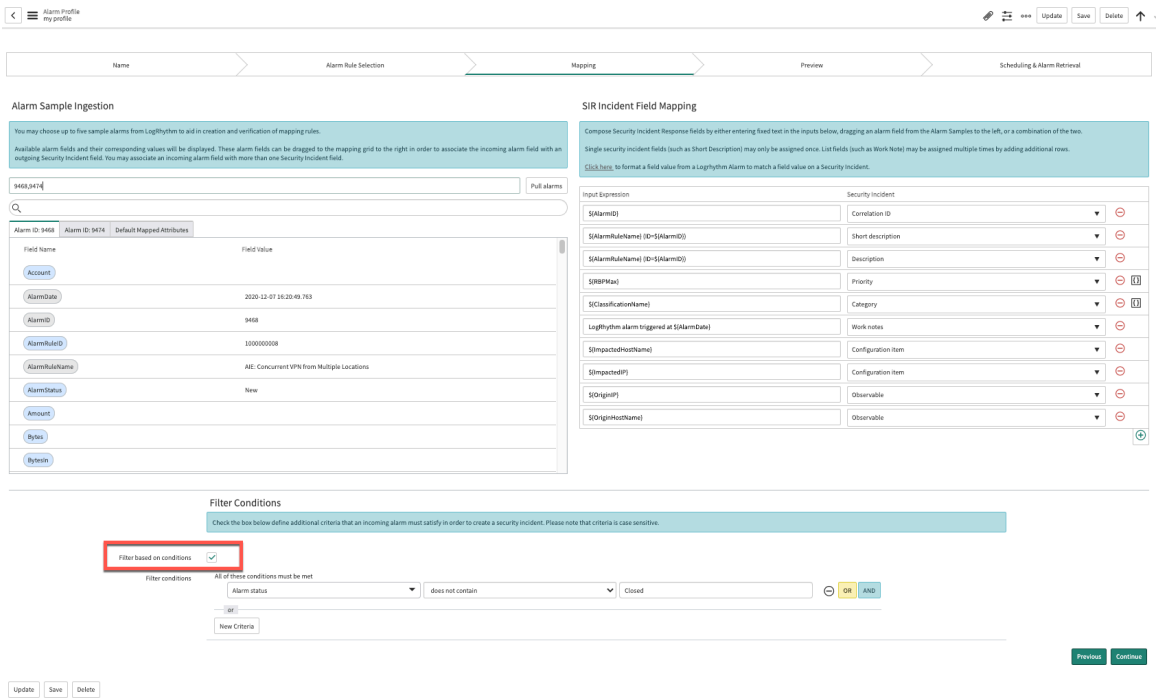
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

niveau du champ. Le filtrage réduit considérablement le nombre d'alarmes que vous ingérez une fois que le profil d'alarme est activé. Utilisez le filtrage pour ingérer une quantité gérable d'alarmes que le personnel de votre centre des opérations de sécurité (SOC) peut prendre en charge.

Remarque : L'exemple suivant montre un paramètre de filtre par défaut dans lequel `l'état de l'alarme ne contient pas fermé` est le paramètre par défaut. Ce filtre n'extrait que les alarmes actives, et ce paramètre réduit le nombre d'alarmes extraites. Les étapes suivantes illustrent comment ajouter un autre filtre utile qui inclut uniquement les alarmes avec les valeurs de gravité ou de priorité les plus élevées.

Procédure

1. Pour modifier les critères de filtrage, cochez la case **Filtre basé sur les conditions** .

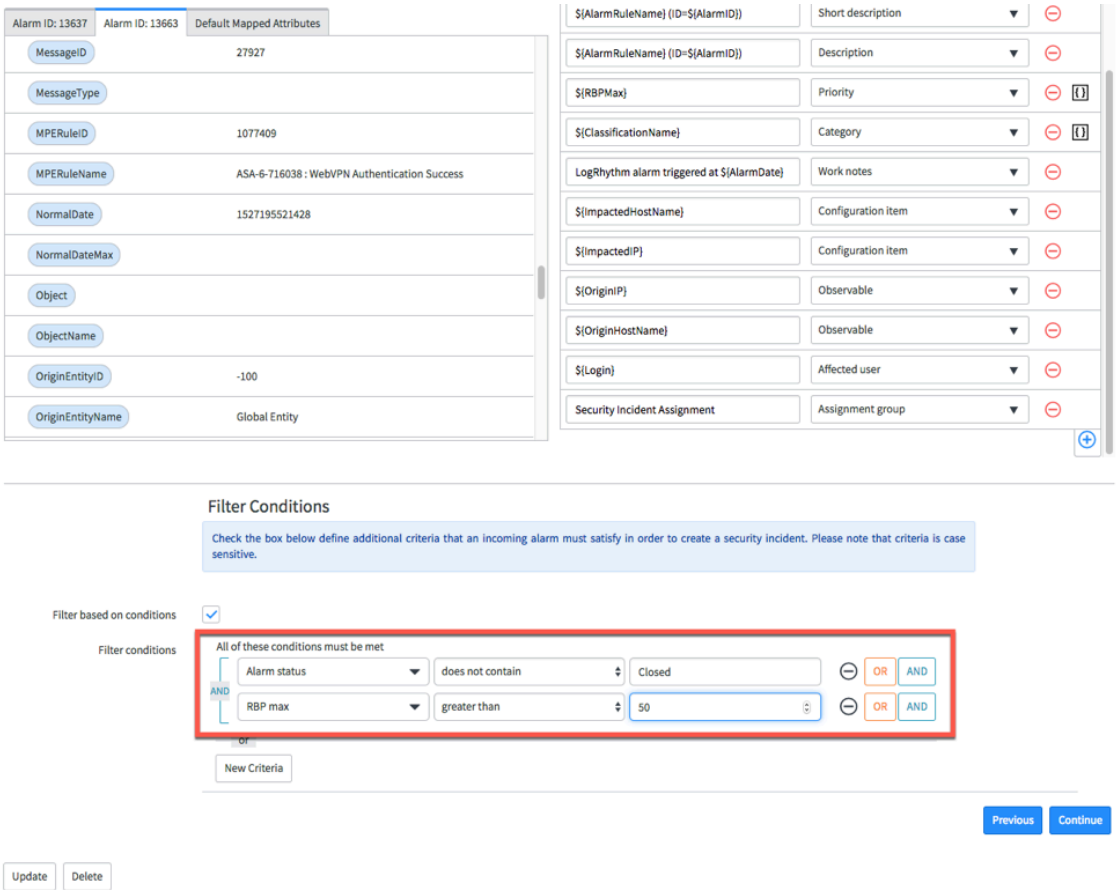


2. À droite du champ **Conditions de filtre** , cliquez sur **OU** ou **ET**.
3. Dans la nouvelle ligne qui s'affiche, sélectionnez les conditions de filtrage dans les listes de choix.

   L'image suivante montre un filtre supplémentaire ajouté aux critères dans lesquels la priorité basée sur le risque (`RBP max`) est supérieure à `50`. Avec ce paramètre de filtre, seules LogRhythm les alarmes dont la valeur de priorité basée sur le risque est supérieure à 50 sont déclenchées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Après avoir vérifié que tous les champs d'alarme critiques LogRhythm sont mappés à l'incident de sécurité et que vous avez défini des critères de filtrage pour limiter l'ingestion Now Platform d'alarmes, choisissez-en un pour poursuivre la configuration.

Option	Description
Continuer ou prévisualiser	Le formulaire d'aperçu de l'incident de sécurité avec votre configuration de mappage s'affiche. **L'aperçu** est sélectionné dans la barre de progression. L'étape suivante consiste à afficher l'incident de sécurité avec vos alarmes mappées.
Mettre à jour	Enregistrez vos données et revenez à la liste **Profils d'alarme** .
Précédent	L'enregistrement du profil d'alarme s'affiche.
Supprimer	Supprimez ce profil d'alarme et la liste **des profils d'alarme** s'affiche.

Que faire ensuite

L'étape suivante consiste à prévisualiser vos champs mappés sur l'incident de sécurité. Consultez Aperçu de l'incident de sécurité avec les valeurs d'alarme mappées LogRhythm.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçu de l'incident de sécurité avec les valeurs d'alarme mappées LogRhythm

Une fois que vous avez terminé l'étape de mappage, prévisualisez les valeurs que vous avez mappées aux champs de l'incident de sécurité. Cette étape de prévisualisation vous permet de vérifier que vous avez mappé tous les champs d'alarme critiques LogRhythm que vous souhaitez afficher sur l'incident de sécurité.

Rôle requis : sn_si.admin.

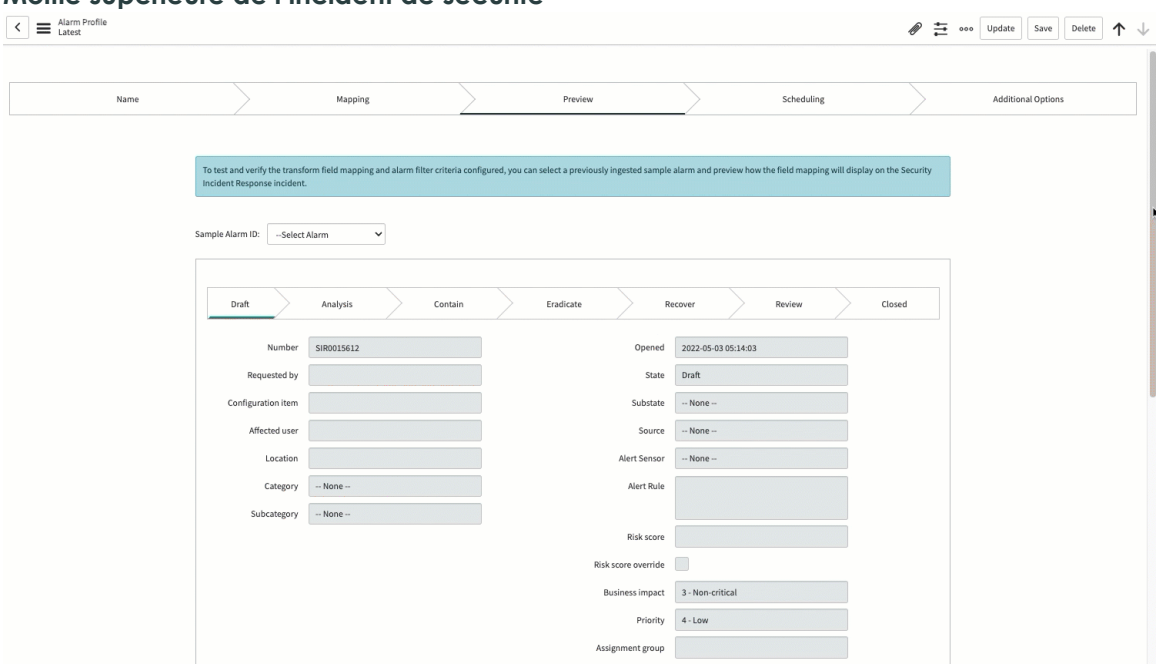
Incident de sécurité

Si l'aperçu de l'incident de sécurité n'est pas affiché, cliquez sur **Aperçu** dans la barre de progression.

Les deux figures suivantes présentent un exemple de l'aperçu de l'ensemble Now Platform de l'incident de sécurité. Cet exemple d'aperçu de l'incident de sécurité est renseigné avec les champs d'alarme mappés à partir de l'alarme LogRhythm`d'échantillon 13663`.

La figure suivante indique que les champs `Élément de configuration`, `Utilisateur affecté`, `Priorité`, `Groupe d'affectation` et `Description brève` de l'incident de sécurité sont renseignés.

Moitié supérieure de l'incident de sécurité



Dans la moitié inférieure du formulaire d'incident de sécurité, le champ `Description` est renseigné. Sous la section Éléments connexes, les champs `Élément de configuration`, `Observable` et `Note de travail` sont renseignés avec des valeurs. Si plusieurs valeurs sont mappées pour ces champs, chaque valeur s'affiche sur l'incident de sécurité, car chacun de ces champs peut accepter plus d'une valeur.

Conditions d'erreur dans l'aperçu

Les messages d'avertissement suivants peuvent s'afficher lors de la prévisualisation de l'incident de sécurité. Si un échantillon d'alarme ne répond pas aux critères de filtrage, l'incident de sécurité complet n'est pas renseigné.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur d'entrée introuvable

Si l'ID d'alarme est inclus dans les conditions de filtrage, un message d'avertissement peut toujours être affiché si des valeurs d'entrée spécifiques ne sont pas trouvées pour certains champs mappés. Pour les besoins de l'exemple suivant, dans l'aperçu de l'enregistrement, supposons qu'il n'y a aucune valeur dans le champ `Affecté à` , bien qu'il ait été mappé.

Pour ce type de message, vérifiez que la valeur d'entrée est correcte dans l'enregistrement de mappage. Dans ce cas, la personne figurant dans le champ `Affecté à` dans l'incident de sécurité est incorrecte dans l'instance Now Platform . Lorsque cette alarme est ingérée et qu'elle crée un incident de sécurité avec cette condition, les champs avec cette valeur d'entrée (`Abel Tuter`) sont laissés vides dans l'incident de sécurité.

Les autres messages en bleu sont informatifs et indiquent que ces champs n'ont aucune valeur à afficher dans l'aperçu. Cet aperçu permet à l'administrateur d'incident de sécurité qui configure le profil d'alarme de vérifier que ces champs ne doivent avoir aucune valeur lors de l'étape de création initiale, car dans certains cas, les champs d'incident de sécurité peuvent être renseignés automatiquement ultérieurement. D'autres erreurs de mappage sont également affichées.

Une fois que vous êtes satisfait du mappage et de l'aperçu de l'incident de sécurité, choisissez-en un pour poursuivre la configuration.

Option	Description
Cliquez sur **Continuer** ou **Planification** dans la barre de progression.	Passez au formulaire **Planification et récupération d'alarme** . **La planification et la récupération des alarmes** sont sélectionnées dans la barre de progression. L'étape suivante consiste à planifier la récupération de l'alarme.
Cliquez sur **Précédent**.	Revenez au profil d'alarme et continuez le mappage.
Entrez un autre ID d'alarme dans la liste de choix **d'ID d'échantillon d'alarme** en haut du formulaire d'aperçu.	La liste de choix **d'ID d'échantillon d'alarme s'affiche** pour chaque ID d'alarme que vous avez saisi. Vous pouvez sélectionner jusqu'à cinq alarmes. Cette option vous permet de prévisualiser un autre LogRhythm ID d'alarme sur un incident de sécurité.

Une fois que vous avez prévisualisé l'incident de sécurité et que vous êtes satisfait des résultats, l'étape suivante consiste à Programmer et récupérer LogRhythm des alarmes.

Programmer et récupérer LogRhythm des alarmes

Après avoir prévisualisé l'incident de sécurité avec les LogRhythm alarmes que vous avez sélectionnées et mappées, vous êtes prêt à planifier la récupération de l'alarme. Une fois que vous avez terminé cette étape, le profil d'alarme est prêt à être activé.

Avant de commencer

Rôle requis : sn_si.admin

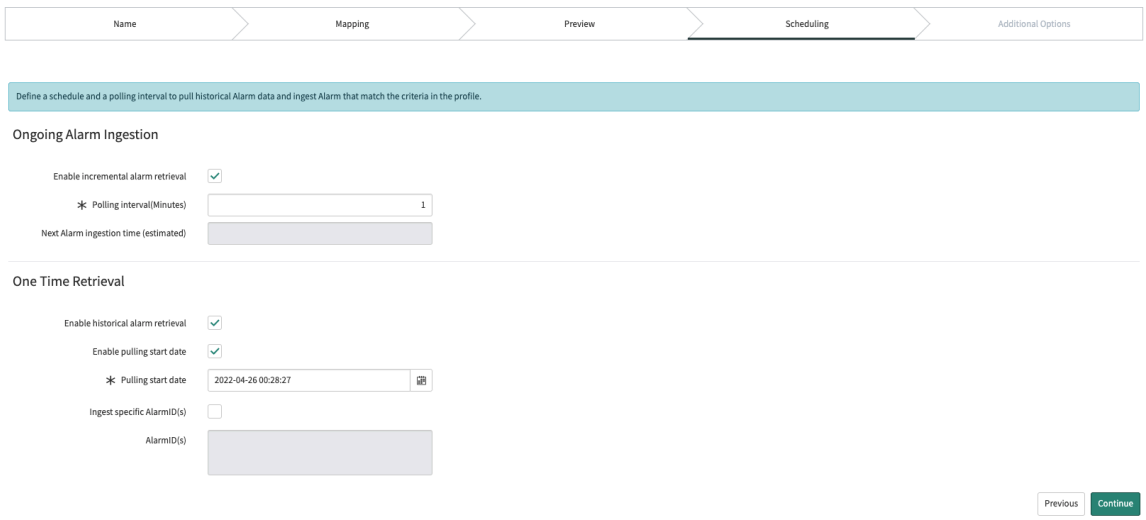
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

La planification vous permet de modifier la planification et les types d'alarmes sélectionnés pour la récupération. Vous filtrez les alarmes que vous ingérez en fonction d'une plage de dates ou d'ID d'alarme spécifiques. Cette étape vous permet de déterminer si vous souhaitez ingérer des alarmes historiques et à quelle fréquence vous interrogez les alarmes futures qui correspondent à la configuration du profil d'alarme.

Procédure

1. Cliquez sur l'étape Planification dans la barre **de** progression.



2. Choisissez parmi les options suivantes pour configurer votre récupération d'alarme.

Option	Description
Activer la récupération d'alarme de pas	Cette valeur est sélectionnée par défaut. Sélectionnez cette option pour récupérer les alarmes incrémentielles.
Intervalle d'interrogation (en minutes)	L'instance Now Platform extrait de la console cliente pour les LogRhythm nouvelles alarmes toutes les minutes. Si des alarmes mappées sont trouvées et que les critères de filtrage sont respectés, des incidents de sécurité sont créés. Ce paramètre peut être modifié, cependant, le paramètre par défaut équilibre l'ingestion d'alarme par rapport à la charge du serveur et récupère les données les plus récentes.
Temps d'ingestion de la prochaine alerte (estimation)	Affiche la date de la prochaine ingestion planifiée pour le profil d'alarme actuel. Il ne s'agit que d'une estimation.
Activer la récupération d'alarme historique	La valeur par défaut est effacée. Aucune donnée historique n'est extraite. Si cette option est sélectionnée, les champs suivants sont affichés. Choisissez-en un pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

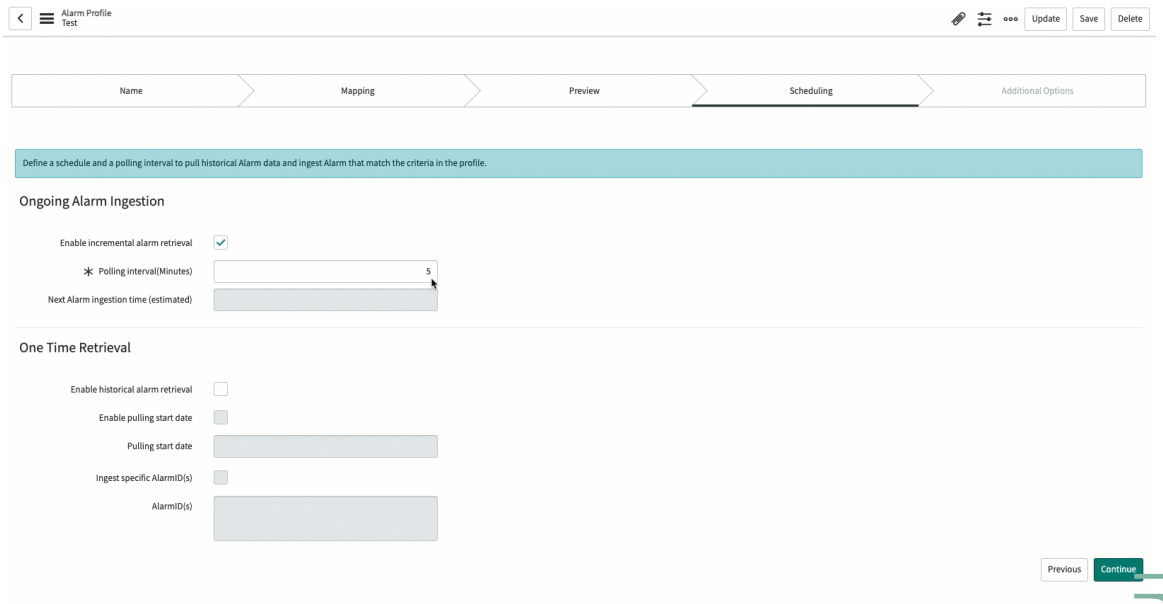
Option	Description
	configurer la récupération soit par date, soit par ID d'alarme. Activer la date de début de l'extraction La valeur par défaut est effacée. Sélectionnez cette option pour activer la date d'extraction. Date de début de déclenchement La valeur par défaut est effacée. Sélectionnez cette option pour définir la date de début de déclenchement. Cliquez sur l'icône Calendrier pour entrer une date et une heure. Les alarmes sont extraites à partir de la date et de l'heure que vous entrez jusqu'à la date actuelle. Ingérer une alarme spécifique ID d'alarme La valeur par défaut est effacée. Sélectionnez cette option pour ingérer des ID d'alarme spécifiques. AlarmID(s) Entrez des ID d'alarme spécifiques. Vous extrayez les alarmes spécifiées et vous pouvez entrer plusieurs ID d'alarme séparés par des virgules. **Remarque :** Une fois qu'une extraction unique et historique d'alarmes est terminée, cette case n'est plus cochée. Vous devrez cocher à nouveau cette case avant d'exécuter une autre extraction ponctuelle d'alarmes historiques.

3. Pour modifier la récupération d'alarme historique, procédez comme suit pour entrer une date de récupération d'alarme ou un ID d'alarme spécifique.

   a. Sélectionnez **Activer la date de début d'extraction**, puis sélectionnez **Date de début d'extraction**.

   b. Dans le champ **Date de début d'extraction** , cliquez sur le calendrier qui s'affiche, sélectionnez la date suivie de la coche verte pour enregistrer votre entrée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La date s'affiche.

c. Vous pouvez également sélectionner l'option **Ingérer un ou plusieurs ID d'alarme spécifiques** et, dans le champ **AlarmID(s),** saisir les ID d'alarme spécifiques pour les données historiques afin de récupérer des ID d'alarme spécifiques.

Vous pouvez saisir jusqu'à cinq alarmes séparées par des virgules.

d. Cliquez sur **Mettre à jour**.

4. Choisissez l'une des options suivantes pour continuer à modifier ou terminer la configuration.

Option	Description
Mettre à jour	Enregistrez vos données et restez sur le formulaire.
Options supplémentaires (dans la barre de progression)	Pour accéder à l'étape Options supplémentaires.
Précédent	Revenir à l'étape d'aperçu.
Supprimer	Supprimez ce profil d'alarme et la liste des profils d'alarme s'affiche.

Que faire ensuite

Une fois que vous avez configuré les détails de l'ingestion d'alarme continue et de la récupération ponctuelle, l'étape suivante consiste à .Options supplémentaires pour LogRhythm les alarmes

Options supplémentaires pour LogRhythm les alarmes

L'intégration LogRhythm d'entreprise vous offre la possibilité de mettre à jour ou de fermer automatiquement les LogRhythm alarmes en fonction des incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Lorsque vous activez l'option de mise à jour initiale de l'alarme, les alarmes sont automatiquement mises à jour dans les commentaires LogRhythm avec les mises à jour initiales de l'alarme. De même, lorsque vous activez l'option Mises à jour de fermeture d'alarme, les alarmes sont automatiquement fermées dans LogRhythm avec le code de fermeture SIR et les commentaires de fermeture.

L'ID LogRhythm d'alarme est lié à l'ID Now Platform d'incident de sécurité tout au long du cycle de vie de l'incident. Cette corrélation permet la fermeture simultanée et automatisée d'un incident de sécurité ou d'une alarme. Lorsque l'enregistrement d'incident de Réponse aux incidents de sécurité sécurité (SIR) est fermé, un commentaire est publié dans l'alarme sur la LogRhythm console Web. Ce commentaire indique que l'alarme a été fermée en fonction de la clôture de l'incident Now Platform de sécurité. Le numéro de l'incident et une URL qui renvoie à l'incident de sécurité pour référence sont également inclus dans la section des commentaires de l'alarme LogRhythm .

Procédure

1. Cliquez sur l'étape **Options supplémentaires** dans la barre de progression.
2. Pour utiliser la mise à jour automatisée d'alarme pour la création d'incidents SIR, choisissez parmi les options suivantes pour configurer votre récupération d'alarme.

Option	Description
Mettre à jour les alarmes LogRhythm lors de la création de l'incident SIR	La valeur par défaut est effacée. Sélectionnez cette option pour mettre à jour automatiquement les LogRhythm alarmes lorsque l'incident SIR est créé.
Commentaires initiaux envoyés à l'alarme LogRhythm	Indique les commentaires initiaux qui sont publiés pour l'alarme LogRhythm . Modifiez le texte par défaut qui s'affiche dans la section des commentaires en ajoutant ou en modifiant les variables de substitution en utilisant le format ${nom de champ}$ pour n'importe quel champ sur le formulaire d'incident SIR. Par exemple, `l'incident de sécurité ServiceNow associé, ${Number}$ a été créé et affecté à ${Assignment group}$. Des détails supplémentaires sur l'incident de sécurité peuvent être trouvés ici : ${URL}$.`

3. Pour utiliser la mise à jour automatisée d'alarme pour la fermeture de l'incident SIR, choisissez parmi les options suivantes pour configurer votre récupération d'alarme.

Option	Description
Fermer les alarmes LogRhythm lors de la fermeture de l'incident SIR	La valeur par défaut est effacée. Sélectionnez cette option pour fermer automatiquement les LogRhythm alarmes lorsque l'incident SIR est fermé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Commentaires de fermeture envoyés à l'alarme LogRhythm	Indique les commentaires de fermeture qui sont publiés pour l'alarme LogRhythm . Modifiez le texte par défaut qui s'affiche dans la section des commentaires en ajoutant ou en modifiant les variables de substitution en utilisant le format ${nom de champ}$ pour n'importe quel champ sur le formulaire d'incident SIR. Par exemple, `l'incident de sécurité ServiceNow associé, ${Number}$, a été fermé par SOC Analyst-${Closed by}$ avec les notes de fermeture suivantes : ${Close notes}$. Des détails supplémentaires sur l'incident de sécurité peuvent être trouvés ici : ${URL}$.`

4. Cliquez sur **Terminer** pour enregistrer le profil de l'alarme.

Trouble?
Si vous ne voyez pas de notes indiquant que l'alarme s'est correctement fermée lors de l'incident de sécurité, consultez les notes de travail pour plus d'informations sur la procédure à suivre pour résoudre le problème. Vérifiez également la connexion de votre serveur. Si vous confirmez que l'incident Now Platform de sécurité a été fermé et que le serveur n'a pas expiré, vous devrez peut-être fermer manuellement l'alarme sur la LogRhythm console Web.

Configurations supplémentaires pour l'intégration LogRhythm

Utilisez les paramètres d'intégration LogRhythm pour modifier le système prédéfini et les propriétés de dépannage en fonction de vos besoins.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Intégration de LogRhythm** > **Paramètres d'Intégration de LogRhythm**.
2. Configurez les propriétés système selon vos besoins.
3. Renseignez les champs du formulaire.

LogRhythm Propriétés système d'intégration

Champ	Description
Cela appliquera le filtre avant que les données ne soient enregistrées dans les tables ServiceNow.	Option permettant de déterminer si vous souhaitez appliquer le filtre avant que les données ne soient stockées dans les tables ServiceNow. Par défaut, cette valeur est définie sur Oui.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Un incident de sécurité maximal peut être créé en une journée	Option permettant de définir le nombre maximal d'incidents de sécurité qui peuvent être créés en une journée. Par défaut, la valeur est définie sur 2 000.
LogRhythm L'ingestion périodique peut être 1000+ alarmes, d'où l'utilisation de la pagination pour ingérer les alarmes. Limite par page autorisée pour extraire le nombre d'alarmes par page.	Option permettant de définir le nombre maximal d'alarmes à récupérer dans une seule page. Par défaut, cette valeur est définie sur 100.
Supprimez les enregistrements de table « Source à tâche » plus anciens que le nombre de jours spécifié.	Option permettant de supprimer les enregistrements de la table Source vers tâche lorsque le nombre spécifié de jours a été rompu. Par défaut, cette valeur est définie sur 30.

4. Configurez les propriétés de dépannage en fonction de vos besoins.
5. Renseignez les champs du formulaire.

Propriétés de dépannage de LogRhythm Integration

Champ	Description
Déboguer l'ingestion planifiée : active les journaux système de niveau débogage pour l'ingestion effectuée par la tâche planifiée. Cela consignera la totalité des messages/exceptions générés par l'ingestion planifiée lors de l'extraction des alarmes/Drilldownlogs/événements de .LogRhythm	Option permettant d'activer les journaux système de niveau débogage pour l'ingestion effectuée par la tâche planifiée. Par défaut, cette valeur est définie sur Non.
Déboguer la carte de transformation : active les journaux système de niveau débogage pour la carte de transformation. Cette action consignera tous les messages générés par les cartes de transformation lors de la création d'un incident de sécurité à partir de l'importation d'alarme. Cela a également activé l'action d'interface utilisateur sur la table d'importation d'alarme pour réexécuter la carte de transformation.	Option permettant d'activer les journaux système de niveau débogage pour la carte de transformation. Par défaut, cette valeur est définie sur Non.
Déboguer l'ingestion d'échantillons dans le profil d'alarme : active les journaux système de niveau débogage pour l'ingestion d'échantillons. Cela consignera tous les messages générés lorsque des échantillons seront ingérés.	Option permettant d'activer les journaux système de niveau débogage pour l'ingestion d'échantillons. Par défaut, cette valeur est définie sur Non.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Aperçu du débogage dans le profil d'alarme : active les journaux système de niveau débogage pour l'aperçu du profil d'alarme. Cela consignera tous les messages générés pendant que l'aperçu est affiché pour l'alarme d'échantillon.	Option permettant d'activer les journaux système de niveau de débogage pour l'aperçu du profil d'alarme. Par défaut, cette valeur est définie sur Non.
Déboguer les appels REST sortants : l'activation de cette propriété permettra la journalisation du niveau de débogage dans la table Journaux système pour tous les appels REST (demande et réponse) qui se déroulent avec ou sans serveur MID à partir de LogRhythm.	Option permettant d'activer la journalisation du niveau de débogage dans la table Journaux système pour tous les appels REST avec ou sans serveur MID à partir de LogRhythm. Par défaut, cette valeur est définie sur Non.

6. Cliquez sur **Enregistrer**.

Utiliser l'éditeur de script pour formater LogRhythm les valeurs

En plus des champs directement mappés à partir des valeurs d'alarme extraites et des valeurs d'alarme que vous saisissez manuellement, vous pouvez utiliser l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage, qui est facultative.

Avant de commencer

Rôle requis : sn_si.admin

L'éditeur de script modifie les valeurs d'une LogRhythm alarme afin que les valeurs mappées aux champs `Priorité` et `Catégorie` de l'incident de sécurité soient prises en charge.

Pourquoi et quand exécuter cette tâche

Dans certains cas, si LogRhythm les valeurs d'alarme sont mappées aux champs `Priorité` et `Catégorie` de l'incident de sécurité, vous pouvez modifier les valeurs mappées. Si vous souhaitez convertir la valeur d'une LogRhythm alarme en une valeur prise en charge par les champs `Priorité` ou `Catégorie` de l'incident de sécurité, utilisez l'éditeur de script.

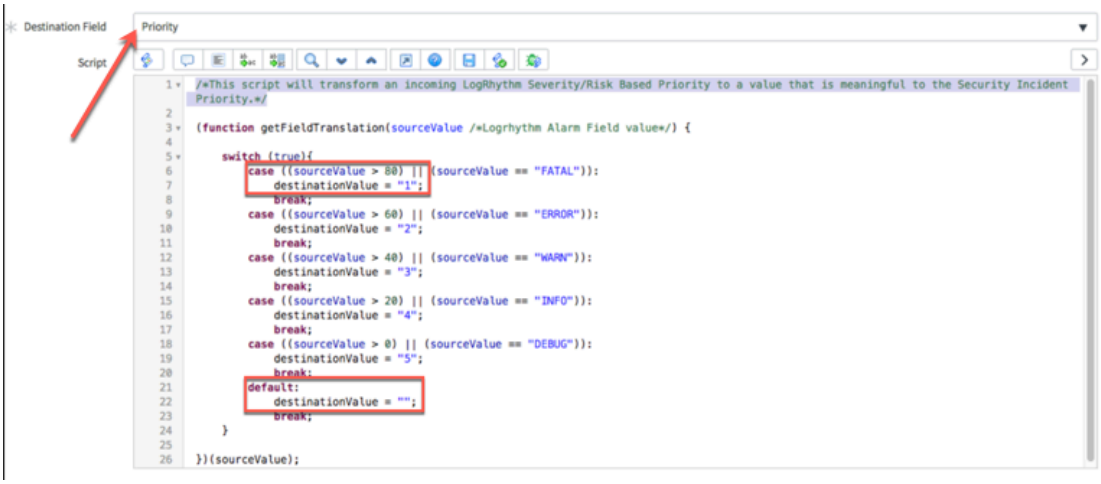
Procédure

1. Une fois le formulaire de mappage affiché, cliquez sur l'icône de crochet `[{}]` pour ouvrir l'éditeur de script dans la section Mappage de champ d'incident SIR.

   Les valeurs par défaut sont incluses pour les champs `Priorité` et `Catégorie` de l'incident de sécurité. Vous pouvez modifier ces valeurs.

   Pour cet exemple, dans l'éditeur ouvert, vérifiez que la **priorité** est affichée dans la liste de choix **Champ de destination** , comme illustré dans la figure suivante. Notez que ce champ est la priorité de l'incident de sécurité, et non la priorité basée sur le LogRhythm risque.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



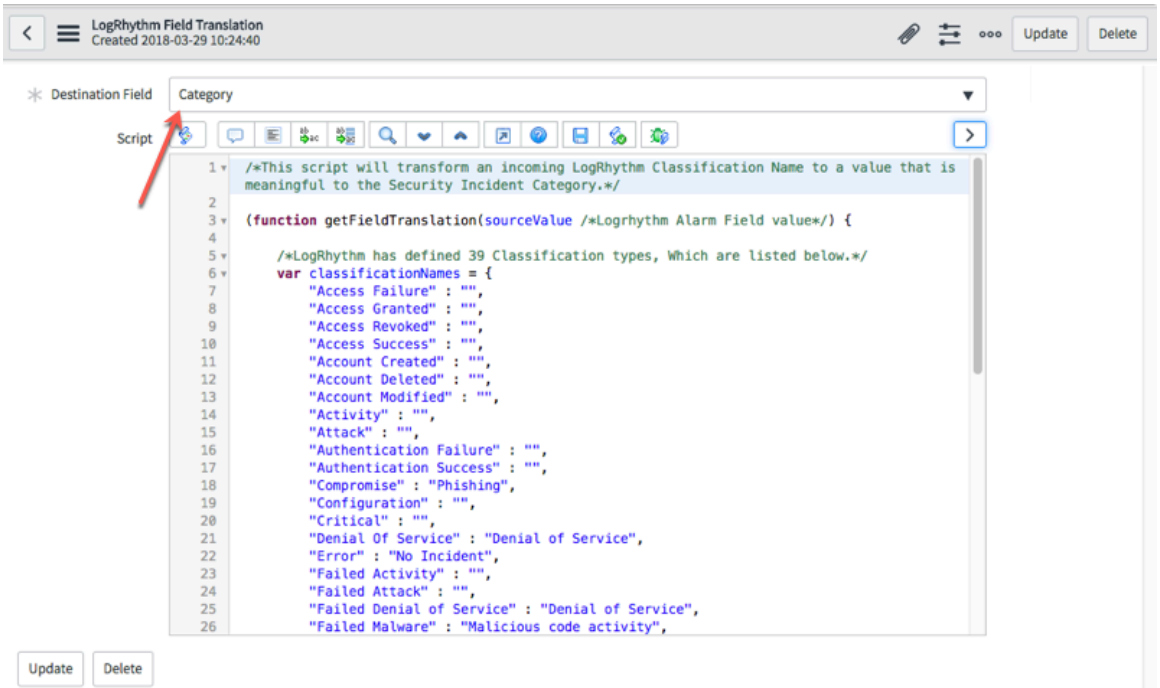
Dans certains cas, un include de script peut être approprié pour le champ `Priorité` . Pour une LogRhythm alarme, par exemple, un score de priorité basé sur le risque se voit attribuer une valeur comprise entre 0 et 100. Toutefois, dans le Now Platform, le champ de priorité d'un incident de sécurité prend en charge des valeurs comprises entre 1 et 5. Comme illustré dans la figure précédente, un script include convertit les valeurs de champ d'alarme LogRhythm en valeurs appropriées prises en charge par le champ sur l'incident de sécurité dans le Now Platform.

Dans cet exemple pour le champ `Priorité` , si la valeur de l'alarme LogRhythm est supérieure ou égale à `80` , `1` s'affiche dans le champ Incident de sécurité (`Priorité`). Cette valeur se traduit par une priorité `critique` dans l'incident de sécurité. S'il n'y a pas de valeur pour l'alarme, le champ de l'incident de sécurité est défini sur null.

2. Saisissez toutes les modifications, puis cliquez sur **Mettre à jour** pour enregistrer vos modifications.
   La LogRhythm table Traductions de champ s'affiche.
3. Fermez la table pour revenir au formulaire de mappage.

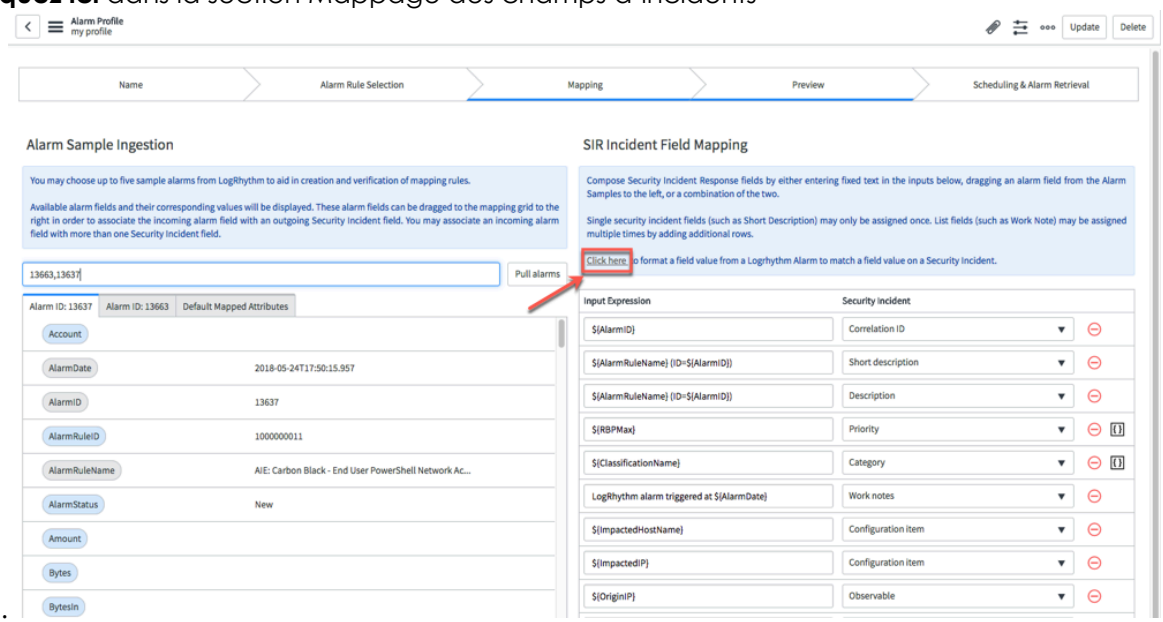
   La figure suivante montre l'éditeur de script dont la `catégorie` est sélectionnée dans la liste de choix Champ de destination.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Si vous souhaitez ajouter un nouveau champ à la liste Traductions de champs, procédez comme suit pour ajouter un nouvel enregistrement.

a. Une fois le formulaire de mappage affiché, cliquez sur le lien **Cliquez ici** dans la section Mappage des champs d'incidents SIR.

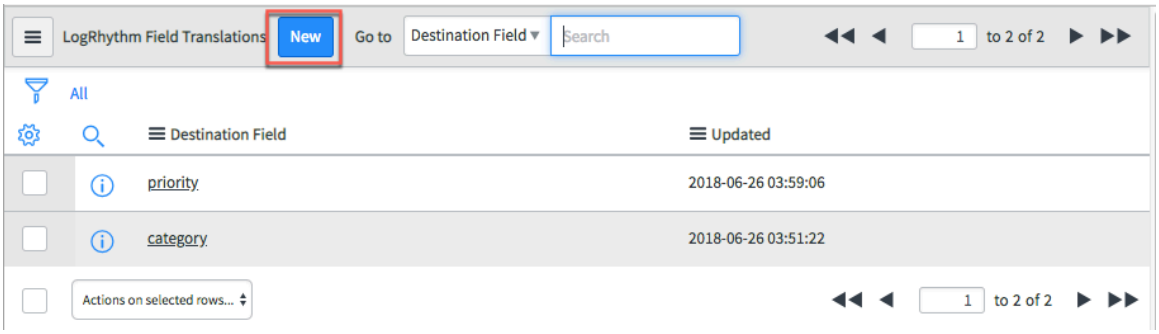


La LogRhythm liste Traduction de champ avec les champs de destination de `priorité` et de `catégorie` s'affiche.

b. Cliquez sur Nouveau.

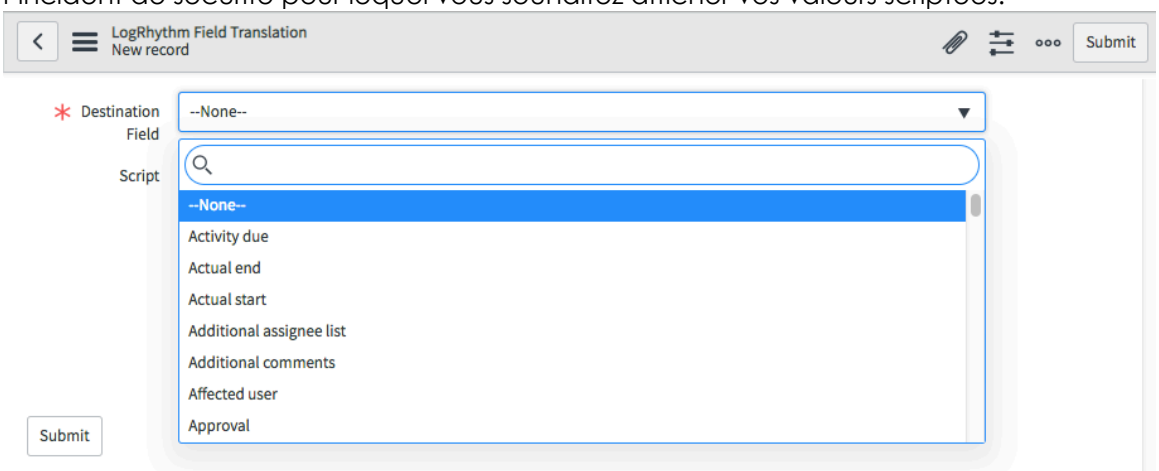
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Un nouvel enregistrement s'affiche.

c. Dans la liste de choix Champs de destination, sélectionnez un champ de destination sur l'incident de sécurité pour lequel vous souhaitez afficher vos valeurs scriptées.



d. Cliquez sur **Envoyer**.
L'éditeur de script s'affiche.

e. Saisissez toutes les modifications dans l'éditeur, puis cliquez sur **Soumettre** pour enregistrer vos modifications.
La LogRhythm table Traductions de champ avec votre nouvel enregistrement s'affiche.

5. Fermez la table pour revenir au formulaire de mappage.

Copier un profil d'alarme pour LogRhythm

Copiez un profil existant et ses paramètres associés au lieu de créer un nouveau profil d'alarme. Si vous créez plusieurs profils d'alarme pour différents types d'alarmes et que vous souhaitez réutiliser les paramètres d'un profil existant, vous pouvez copier des profils d'alarme pour gagner du temps. Ce processus est facultatif.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Si vous copiez un profil, le nom du profil est d'abord modifié pour éviter les doublons. En outre, le profil copié est défini sur inactif afin qu'il ne soit pas activé accidentellement avant la finalisation de la configuration.

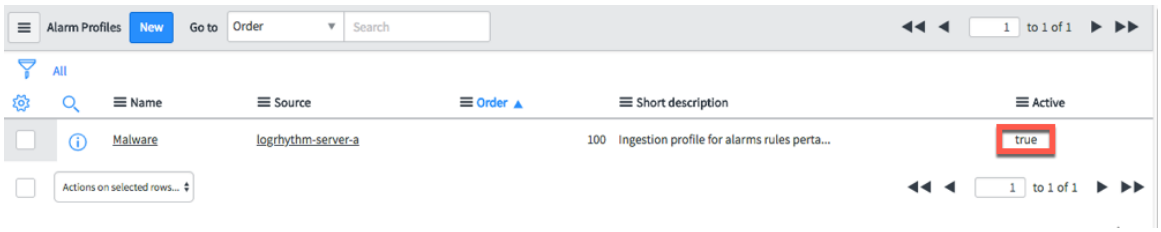
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

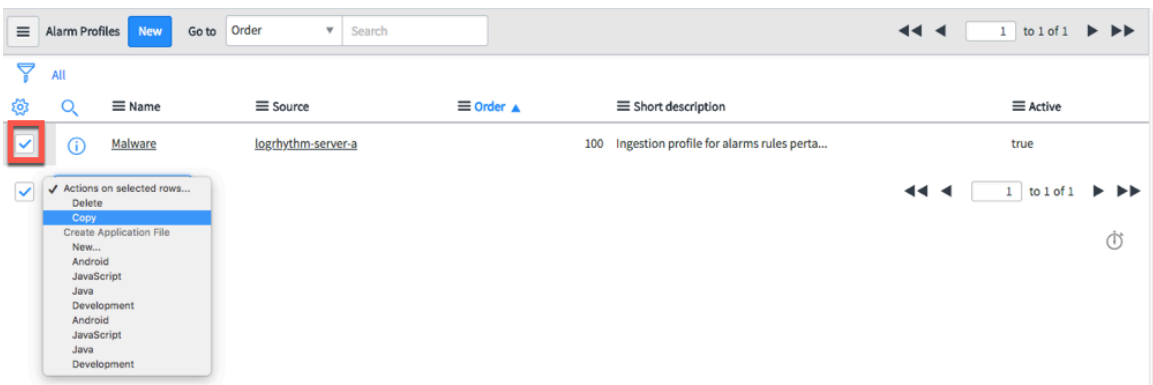
Procédure

1. Accédez à la **Tout** > **Intégration de LogRhythm** > **Profils d'alarme LogRhythm**.

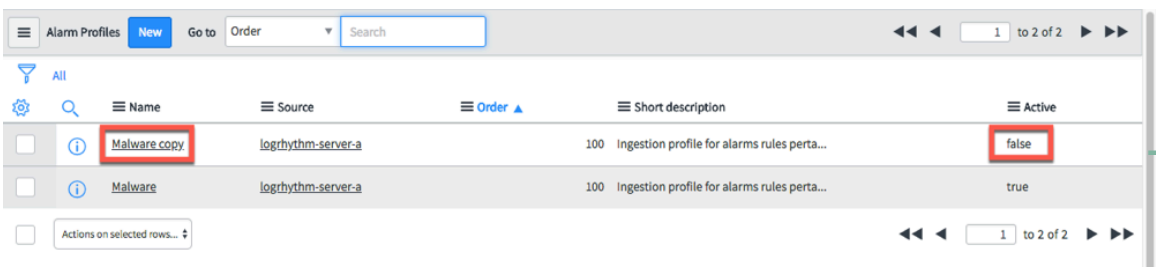
   Dans la liste qui s'affiche, notez que la colonne `Actif` indique si le profil est actif (`vrai`).



2. Dans le champ situé à gauche de la colonne **Nom** , sélectionnez le nom de l'enregistrement.
3. Dans la liste de choix **Actions sur les lignes sélectionnées** , sélectionnez **Copier**.



   Dans la liste **Profils d'alarme** , la copie et le profil d'origine sont affichés. Bien que l'enregistrement d'origine soit actif, la copie est inactive à ce stade (`faux`). Après l'avoir configuré, vous activez ce profil copié.



   Vous pouvez modifier les valeurs du profil copié et le renommer afin que les règles d'alarme que vous tirez s'appliquent au nouveau profil. Vous êtes invité à activer le nouveau profil une fois les étapes de configuration terminées.

Désactiver la fermeture automatisée de l'alarme pour LogRhythm

Désactivez l'aptitude de fermeture d'alarme automatisée si vous ne souhaitez plus afficher les informations de fermeture de l'incident de sécurité sur la LogRhythm console Web. Une fois désactivé, les alarmes ne Now Platform se ferment plus dans la LogRhythm console Web. Ce processus est facultatif.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

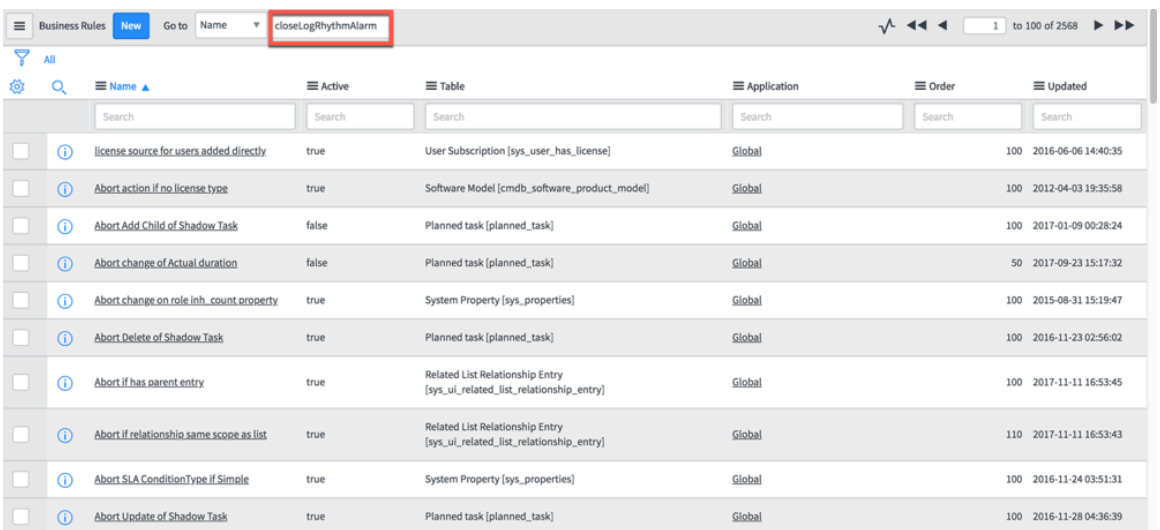
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Une fois désactivé, les notes d'état et autres informations de fermeture de l'incident de sécurité ne sont plus affichées sur la LogRhythm console Web.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Règles métier** et sélectionnez le module **Règles métier** .
2. S'il n'est pas affiché dans la liste **Règles métier** , saisissez **LogRhythm Close Alarm On SI Closure** dans le champ de recherche et appuyez sur **Entrée**.



3. Dans la colonne **Nom** , cliquez sur le lien **LogRhythm Close Alarm On SI Closure** pour ouvrir l'enregistrement.
4. Dans l'enregistrement qui s'affiche, décochez la case **Actif** .
5. Cliquez sur **Mettre à jour**.
   La fonctionnalité de fermeture automatisée de l'alarme est maintenant désactivée.

Afficher les LogRhythm événements d'exploration vers le bas

Affichez les événements bruts ou de base connexes pour une LogRhythm alarme dans l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

En tant qu'analyste de sécurité, vous pouvez afficher les événements bruts ou de base connexes d'une LogRhythm alarme sans avoir à revenir à la LogRhythm console. Pour ce faire, accédez à une liste connexe qui contient tous les événements détaillés sur l'incident SIR .

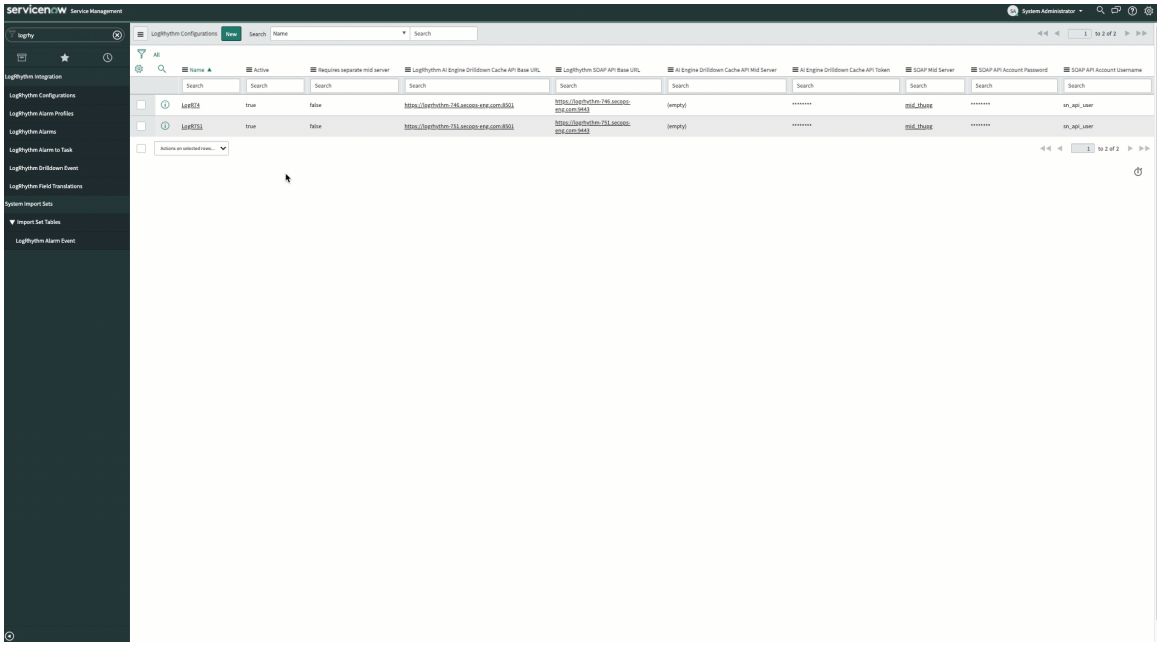
Procédure

Accédez à la **Tout** > **Intégration de LogRhythm** > **Événements d'analyse LogRhythm**.

L'illustration suivante montre comment accéder au module **LogRhythm Drilldown Events** , trier la liste des événements par **groupe par ID d'alarme** et cliquer sur l'incident de sécurité associé. Dans l'incident de sécurité, vous pouvez trouver l'onglet **Événements d'exploration LogRhythm** dans les liens connexes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Dépanner l'intégration de LogRhythm

Résolvez les problèmes de connectivité et d'ingestion d'alarme.

Consultez les rubriques suivantes pour le dépannage :

- Vérifier la connectivité pour LogRhythm
- Exécution du script et journal système pour LogRhythm

Vérifier la connectivité pour LogRhythm

Vérifiez votre connexion à la LogRhythm console cliente en envoyant des demandes curl pour tester l'API LogRhythm REST. Le processus de vérification est facultatif.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Pour vérifier que la connexion à la LogRhythm console cliente fonctionne correctement après avoir configuré les LogRhythm API REST, envoyez deux requêtes curl à partir de l'ordinateur hébergeant le serveur MID que vous avez configuré dans Installer le module d'extension et configurer LogRhythm.

L'API LogRhythm REST utilise WSSE pour l'authentification, ce qui nécessite un scripting externe pour fonctionner avec Curl et Postman.

L'API LogRhythm REST utilise un jeton pour l'authentification, de sorte que vous puissiez effectuer l'appel de validation réel que l'intégration utilise. Le « 0 » à la fin de l'URL est un LogRhythm ID d'alarme. L'API LogRhythm REST avec une configuration par défaut nécessite le port 8501. Ce numéro de port doit être inclus dans l'URL que vous prévoyez d'utiliser pour le test.

Procédure

Mettez à jour l'URL **<url REST LogRhythm>** et le jeton **<jeton d'API>** dans la demande curl suivante et envoyez-la pour valider l'API LogRhythm REST : `curl -k -i -v --trace-time -o /dev/null -H « Content-Type : text/json » -H « Authorization : Bearer`

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

`<api token> » « https://<cache Drilldown URL>/lr-drilldown-cache-api/drilldown/0 »`
Pour une connexion réussie à l'API LogRhythm REST, vous devez recevoir un message HTTP 404, mais le corps de réponse contient `l'ID d'alarme : 0 introuvable`.

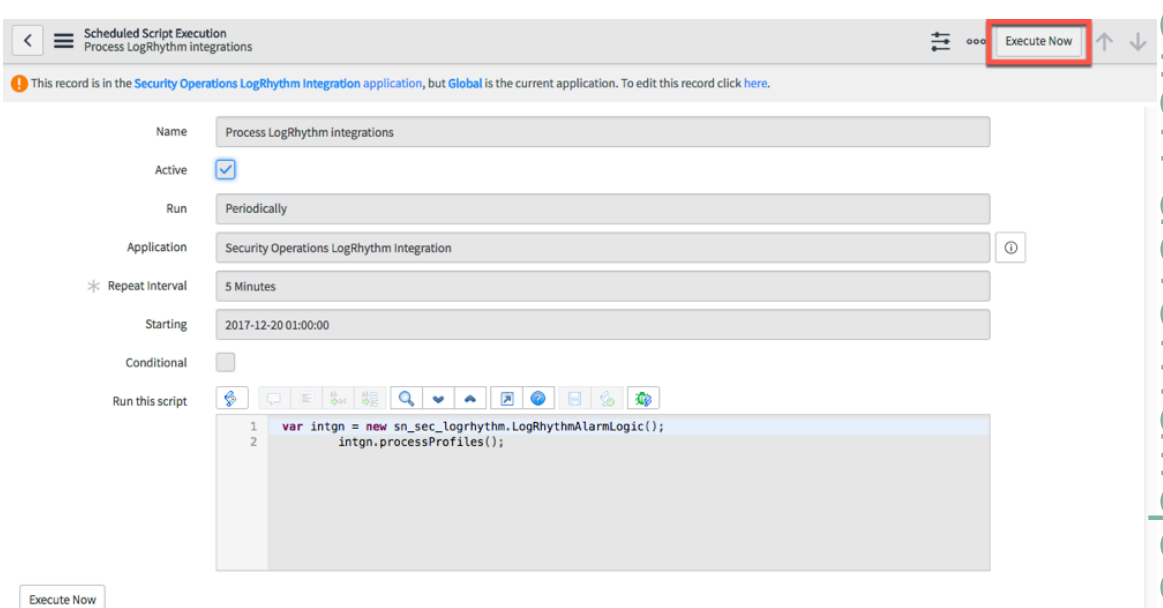
Exécution du script et journal système pour LogRhythm

Si vous résolvez un problème d'ingestion d'alarme, vous pouvez remplacer l'intervalle d'interrogation par défaut de cinq minutes pour afficher les résultats immédiatement. Dans ce scénario, appelez manuellement l'exécution du script pour exécuter l'interrogation. Cette exécution est facultative.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Tâche planifiée** > **Travaux planifiés** et sélectionnez le module **Travaux planifiés** .
2. Cliquez sur l'enregistrement de tâche Intégrations de processus LogRhythm .
3. Dans l'enregistrement Exécution de script planifiée qui s'affiche, cliquez sur **Exécuter maintenant**.



Si vous avez besoin d'aide supplémentaire pour le dépannage, vous pouvez accéder au journal système des LogRhythm requêtes.

4. Pour d'autres problèmes de dépannage généraux, procédez comme suit pour accéder aux journaux système.

   a. Accédez à la **Journal système** > **Tout** et sélectionnez **Tout**.

   b. Définissez le filtre (`Aller à`) sur **Source** et saisissez `sn_sec_logrhythm`.

   c. Appuyez sur **Entrée**.
   Tous les messages générés par l'intégration sont affichés dans cette table. Les messages répertoriés peuvent fournir un aperçu des processus en cours d'exécution de l'intégration et peuvent vous aider à résoudre des problèmes supplémentaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

McAfee ePO intégration

L'aptitude McAfee ePO de détection et de réponse des points de terminaison d'intégration (EDR) qui aide les analystes du centre des opérations de sécurité (SOC) à identifier les cybermenaces et à réparer les dommages causés par les fichiers malveillants.

Vue d'ensemble

Deux ensembles d'options McAfee ePO sont utilisés dans cette intégration : les options qui appellent des actions, telles que l'isolement d'un hôte et le lancement d'une analyse de programme malveillant, et les options qui exécutent des requêtes pour collecter les détails du système et les événements de menace. Les deux types d'options, les actions et les requêtes, sont invoqués à partir de votre Now Platform® instance. Vous pouvez regrouper ces options afin qu'elles s'exécutent automatiquement lorsqu'un type spécifique d'événement de sécurité se produit, ou vous pouvez les invoquer manuellement à partir d'un Now Platform® incident de sécurité.

Les options suivantes McAfee ePO sont disponibles pour cette intégration.

Obtenir les détails du système

Rassemblez les détails système, y compris les détails du système d'exploitation.

Lancer l'analyse anti-programme malveillant

En fonction de la configuration et de la planification de l'analyse, lancez une analyse d'un point de terminaison impacté.

Isoler/Ne pas isoler l'hôte

Supprimez un système de l'accès réseau pour enquête et restaurez l'accès au réseau.

Répertorier les événements de menace

Recueillez l'état de conformité et les événements de menace les plus récents.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes.

- Prend en charge le déclenchement automatisé de requêtes basées sur les conditions de McAfee ePO l'incident.
- Prend en charge le lancement McAfee ePO manuel d'options à partir d'incidents de Now Platform® Réponse aux incidents de sécurité sécurité (SIR) qui effectuent des actions à la demande.
- La possibilité de créer plusieurs profils pour déclencher différents types et McAfee ePONow Platform® Opérations de sécurité options. Ces profils collectent des informations sur les événements de menace ou effectuent des actions en fonction des conditions de catégories d'incidents spécifiques telles que les programmes malveillants.
- Validez la configuration de votre profil avec un aperçu des résultats sur SIR les McAfee ePO incidents de sécurité.
- Si le balisage est activé, les balises de sécurité identifient quelles McAfee ePO options sont initialement lancées par un workflow et quand les requêtes ou actions sont terminées avec succès.
- Une piste d'audit complète des requêtes et des actions est publiée dans les notes de McAfee ePO travail sur SIR les incidents de sécurité, et les Now Platform® commandes du sont consignées dans la McAfee ePO console.
- Prend en charge plusieurs McAfee ePO consoles.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Modules d'extension

Le module d'extension com.snc.si_dep est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications.

Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour garantir une installation fluide :

1. Cadre de travail de Security Integration
2. Security Support Common
3. Orchestration de support de sécurité
4. Réponse aux incidents de sécurité
5. Espace de travail Réponse aux incidents de sécurité

Pour en savoir plus sur la configuration de votre Now Platform instance pour l'intégration, reportez-vous à la section Configurer votre Now Platform instance pour l'intégration McAfee ePO.

Le ServiceNow module d'extension

Le module d'extension d'extension ServiceNow Security Operations pour McAfee ePO# est requis pour cette intégration. Vous installez ce ServiceNow module d'extension dans votre McAfee ePO console. Pour plus d'informations, consultez Configurer votre Now Platform instance pour l'intégration McAfee ePO.

Serveur MID

Cette intégration nécessite l'installation et la McAfee ePO configuration d'un serveur MID Server dans votre Now Platform® instance pour vous connecter au serveur (console). Consultez le site web de la documentation produit ServiceNow pour plus d'informations sur les MID Servers.

Versions prises en charge de McAfee

L'intégration prend en charge les versions 5.9.1 et 5.10 de McAfee ePO. Il prend en charge McAfee Agent : MA 5.5.1.388 Pour plus d'informations sur les produits McAfee et ePolicy Orchestrator, reportez-vous au site Web des produits McAfee .

L'intégration prend en charge la version 10.5 du produit McAfee Endpoint Security Threat Prevention. Si vous n'utilisez pas la version 10.5, consultez votre McAfee ePO administrateur pour savoir si votre version peut prendre en charge les analyses à la demande via des actions de balises.

McAfee ePO Les balises de sécurité sont utilisées dans cette intégration. Vous devez créer ces balises dans votre McAfee ePO console. Pour plus d'informations sur ces balises, reportez-vous à la section Configurer votre McAfee ePO console pour qu'elle s'intègre à Réponse aux incidents de sécurité (SIR).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Références

Référence	Identificateur de document	Titre de document
1	Site Web des produits McAfee	Site Web des produits McAfee
2	Documentation produit McAfee Business pour ePolicy Orchestrator Cloud	Documentation produit McAfee
3	ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Pour obtenir une liste de vérification permettant de suivre la progression de la configuration, de l'installation et de la vérification des résultats de l'intégration, reportez-vous à la section Liste de vérification pour l'intégration McAfee ePO.

Pour une installation fluide de l'application et pour vous aider à vérifier les résultats attendus, suivez les rubriques dans l'ordre où elles sont présentées.

Information associée

Architecture d'intégration pour McAfee ePO

Architecture d'intégration pour McAfee ePO

La rubrique suivante donne une vue d'ensemble de l'architecture système et répertorie les principales fonctionnalités de l'intégration. Cette section fournit également des informations sur les étapes de configuration que vous devez effectuer dans votre Now Platform instance et dans la console McAfee ePolicy Orchestrator (McAfee ePO) avant d'installer l'application à partir du ServiceNow Store.

Termes clés pour l'intégration McAfee ePO

Les termes suivants sont utilisés dans la documentation d'installation et de configuration de l'intégration.

Now Platform

Un produit d'entreprise ServiceNow ll Now Platform s'agit de la base sur laquelle les composants individuels, tels que Réponse aux incidents de sécurité (SIR), IT Service Management (ITSM) et d'autres produits sont construits.

Réponse aux incidents de sécurité (SIR)

Application Now Platform qui suit la progression des incidents de sécurité, depuis la détection et l'analyse initiale, en passant par le confinement, l'éradication et la récupération, jusqu'à l'examen final et la fermeture post-incident.

Module d'extension

Les modules d'extension sont des composants logiciels qui fournissent des fonctions et des fonctionnalités spécifiques au sein de votre Now Platform instance. Pour en savoir plus sur l'installation et la configuration des modules d'extension d'intégration, reportez-vous à la section Installer l'application et configurer un serveur pour l'intégration McAfee ePO.

ePolicy Orchestrator (McAfee ePO)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Console utilisateur dans laquelle vous gérez les services, les produits et les paramètres McAfee.

Module d'extension McAfee

Ce ServiceNow module d'extension est requis pour cette intégration. Ce module d'extension réside sur votre McAfee ePO console et connecte votre McAfee ePO console à votre Now Platform instance.

Option

Activité automatique lancée à partir de votre Now Platform instance qui est exécutée dans la McAfee ePO console pour effectuer des requêtes d'enrichissement et effectuer des actions sur vos actifs.

Profil

Paramètres des McAfee ePO options que vous configurez pour spécifier quand et dans quelles conditions, les capacités effectuent des requêtes d'enrichissement et effectuent des actions sur vos actifs.

Utiliser un MID Server

Application qui facilite la communication et le mouvement de données entre le et des Now Platform applications, sources de données et services externes.

ServiceNow Administrateur (admin)

Un utilisateur disposant de ce rôle télécharge et installe les SIR modules d'extension and McAfee ePO sur votre Now Platform instance. Un utilisateur ayant ce rôle affecte également le rôle d'administrateur d'incident de sécurité si nécessaire.

ServiceNow Administrateur d'incident de sécurité (sn_si.admin)

Un utilisateur disposant de ce rôle effectue la configuration de l'intégration McAfee ePO avec le Réponse aux incidents de sécurité produit (SIR) dans votre Now Platform instance selon les besoins. Un utilisateur ayant ce rôle affecte également le rôle d'analyste d'incident de sécurité si besoin.

ServiceNow Analyste des incidents de sécurité (sn_si.analyst)

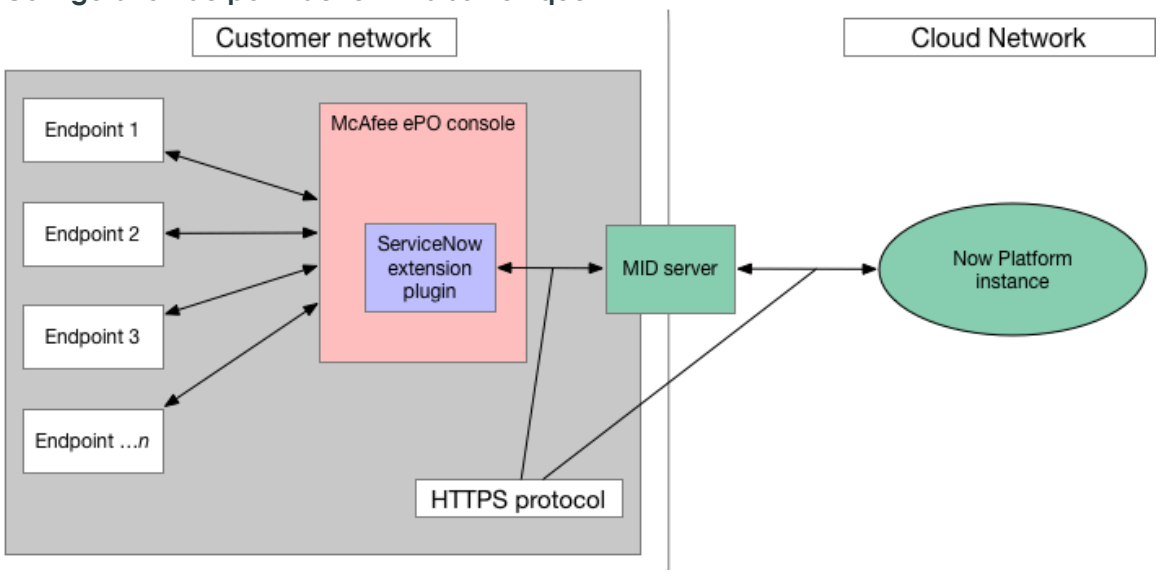
Un utilisateur disposant de ce rôle interagit avec les incidents de sécurité dans le produit SIR et les analyse.

Connexion au système et flux de données

La figure suivante est un exemple d'environnement client. Un Now Platform MID Server est nécessaire pour que votre Now Platform instance puisse se connecter à un McAfee ePO serveur (console) via un module d'extension ServiceNow d'extension. Une fois connecté, vous appelez les options de votre Now Platform pour lancer des analyses de logiciels malveillants, isoler les ordinateurs hôtes et les restaurer sur votre réseau, récupérer les résultats de la dernière analyse et collecter des détails système sur vos actifs. Lorsque ces options renvoient des résultats à partir de vos actifs qui correspondent à vos critères de recherche, les données sont extraites via le MID Server vers votre Now Platform instance. Les données sont affichées sur les listes connexes d'un Now Platform Réponse aux incidents de sécurité incident de sécurité (SIR). La figure suivante illustre le flux de données pour un groupe de points de terminaison gérés par une McAfee ePO console.

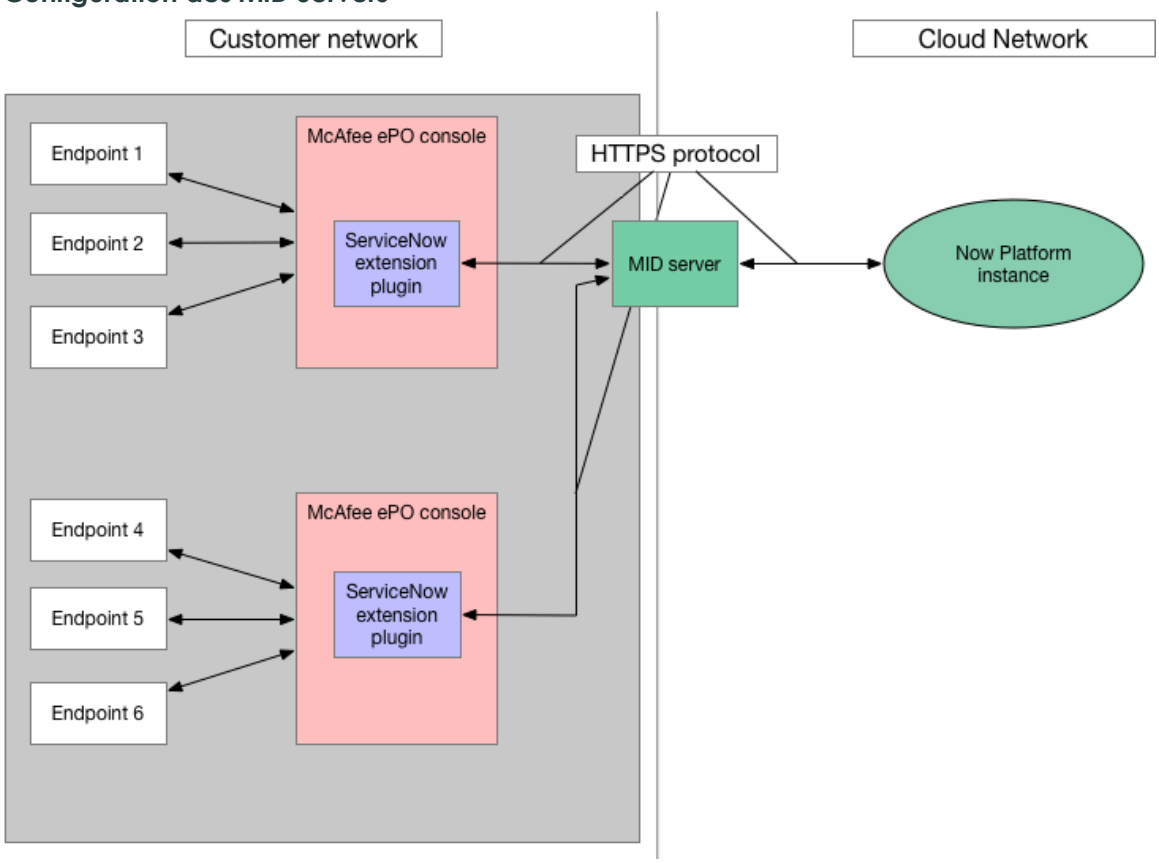
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de point de terminaison unique



Comme le montre la figure suivante, cette intégration peut prendre en charge plusieurs McAfee ePO consoles. Vous pouvez avoir un groupe de points de terminaison gérés par une McAfee ePO console et un autre groupe de points de terminaison géré par une autre McAfee ePO console. Les données de plusieurs McAfee ePO consoles sont extraites via un seul MID Server. Toutefois, vous pouvez également préférer configurer plusieurs MID Server si votre organisation l'exige.

Configuration des MID Servers



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflows pour l'intégration McAfee ePO

Cette intégration inclut les workflows suivants. Ces workflows sont préconfigurés et conçus spécifiquement pour cette intégration. Vous pouvez modifier ces workflows pour répondre aux besoins de votre organisation selon vos besoins. Pour plus d'informations générales sur les workflows et l'utilisation de l'éditeur de workflow, consultez Premiers pas avec les workflows .

- Intégration McAfee ePO pour Security Operations : obtenir les détails de l'hôte
- Intégration McAfee ePO pour Security Operations - Lancer l'analyse des programmes malveillants
- Intégration McAfee ePO pour Security Operations : isoler l'hôte
- Intégration McAfee ePO pour Security Operations : liste des événements de menace
- Intégration McAfee ePO pour Security Operations : supprimer l'isolement

Connexion à des systèmes externes

L'intégration nécessite que le MID Server communique avec la McAfee ePO console via le protocole HTTPS.

Liste de vérification pour l'intégration McAfee ePO

Utilisez cette liste de vérification pour vous guider dans toutes les tâches de l'intégration. La liste de vérification suivante comprend les tâches de configuration et d'installation, ainsi que des exemples de cas d'utilisation incluant les résultats attendus pour l'intégration.

Avant de commencer

Rôle requis : les rôles sont répertoriés pour chaque étape.

Pourquoi et quand exécuter cette tâche

Suivez la progression de l'installation, de l'installation et de la configuration de l'intégration à l'aide de la table suivante. Terminez toutes les tâches d'une étape avant de passer à l'étape suivante. Chaque ligne du tableau répertorie les tâches et identifie les rôles requis pour effectuer les tâches. Les rubriques numérotées du guide d'installation et de configuration sont également référencées.

Procédure

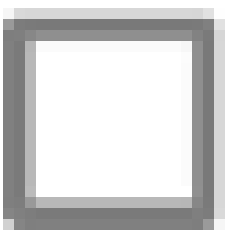
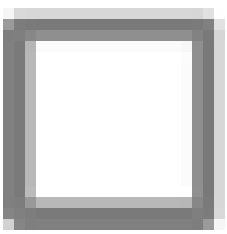
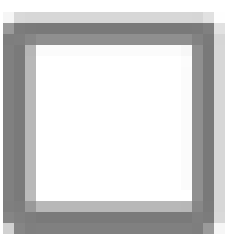
Suivez les étapes du tableau dans l'ordre dans lequel elles sont présentées.

Liste de vérification

Élément	Description
☐	En tant qu'utilisateur disposant du Now Platform® rôle administrateur, configurez votre Now Platform® instance. **a.** Affecter Now Platform® et Réponse aux incidents de sécurité les rôles. **b.** Vérifiez que tous les ServiceNow Réponse aux incidents de sécurité modules d'extension prenant en charge l'intégration et les autres modules d'extension sont installés et activés pour votre version du Now Platformfichier .

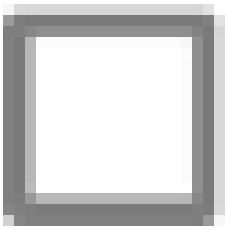
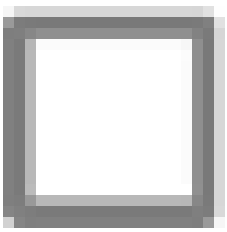
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	c. Installez et configurez un MID Server dans votre Now Platform® instance. **d.** Créez un groupe d'approbation si vous souhaitez traiter les demandes soumises par l'analyste des incidents de sécurité pour l'opération Isoler l'hôte et lancer des actions d'analyse des programmes malveillants. Pour plus d'informations, consultez Configurer votre Now Platform instance pour l'intégration McAfee ePO.
	En tant qu'administrateur McAfee ePO , configurez votre McAfee ePO console. **a.** Vérifiez que vous utilisez la version 5.9 de McAfee ePO. **b.** Installez le module d'extension ServiceNow dans votre McAfee ePO console. **c.** Vérifiez que vous avez créé des balises de sécurité dans votre McAfee ePO console pour l'opération Isoler l'hôte et lancez des actions d'analyse anti-programme malveillant. Pour plus d'informations, consultez Configurer votre McAfee ePO console pour qu'elle s'intègre à Réponse aux incidents de sécurité (SIR). Pour plus d'informations et pour obtenir le fichier du module d'extension dans votre Now Platform instance, accédez à **Base de connaissances** > **Articles** > **Tout** et, dans le champ Rechercher, saisissez `ServiceNow Security Operations Extension for McAfee ePO`.
	En tant qu'utilisateur disposant du Now Platform rôle administrateur, installez l'application McAfee ePO à partir du ServiceNow Store, configurez un serveur et connectez-vous à la McAfee ePO console. Pour plus d'informations, consultez Installer l'application et configurer un serveur pour l'intégration McAfee ePO.
	En tant qu'utilisateur ayant le rôle d'administrateur d'incident Now Platform de sécurité, modifiez les noms de balises de sécurité dans votre Now Platform® instance afin qu'ils correspondent aux noms de balises que vous avez créés dans votre McAfee ePO console. Pour plus d'informations, consultez Modifier les balises de sécurité dans le Now Platform pour l'intégration McAfee ePO.
	En tant qu'utilisateur ayant le rôle d'administrateur d'incident de sécurité, créez un profil pour McAfee ePO les options. Pour en savoir plus sur les profils, reportez-vous à la section McAfee ePO Profils d'aptitude d'intégration. Pour connaître les étapes de création d'un profil, reportez-vous à la section Créer un profil d'aptitude pour l'intégration McAfee ePO.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	En tant qu'utilisateur ayant le rôle d'administrateur d'incident de sécurité, configurez un profil et testez les incidents de sécurité. **a.** Passez en revue les informations sur les conditions et paramètres de déclenchement. **b.** Configurez un profil. **c.** Testez et prévisualisez les incidents de sécurité. **d.** Recherchez les résultats de recherche et d'autres détails sur les listes connexes de l'incident de sécurité. **e.** Créez et configurez différents types de profils et testez les incidents de sécurité pour chaque type. Pour en savoir plus sur les conditions de déclenchement et les autres champs CI, reportez-vous à la section Définir des conditions de déclenchement avec un champ d'élément de configuration (CI) pour un McAfee ePO profil. Pour connaître les étapes nécessaires à la configuration d'un profil, tester et prévisualiser les incidents de sécurité et des exemples de types de profils, consultez les exemples ci-dessous Configuration des profils pour l'intégration McAfee ePO.
	En tant qu'utilisateur ayant le rôle d'analyste Now Platform des incidents de sécurité, soumettez des demandes supplémentaires pour les analyses de programme malveillant et la liste des événements de menace. Pour plus d'informations, voir Déclencher McAfee ePO manuellement un profil à partir d'un incident de sécurité Dans le Now Platform, en tant qu'utilisateur disposant d'un rôle d'approbation ou en tant que membre d'un groupe d'approbation, approuvez les demandes d'isolement de l'hôte et de suppression de l'isolement. Pour en savoir plus sur le traitement des demandes d'approbation, reportez-vous Créer un groupe d'approbationà .

Vous avez terminé avec succès les étapes d'installation, installé et configuré l'application, et vérifié les résultats attendus pour l'intégration.

Configurer votre Now Platform® instance pour l'intégration McAfee ePO

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform® instance avant d'installer l'application pour l'intégration McAfee ePO .

Configurez les exigences

Rôle requis : Now Platform administrateur (admin). Passez en revue les informations suivantes avant votre Now Platform® instance pour l'intégration McAfee ePO .

Le tableau suivant répertorie les exigences de configuration pour l'application. Vérifiez que vous avez effectué ces tâches avant d'installer l'application pour l'intégration à partir du ServiceNow Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la tâche	Description
Vérifiez que vous avez affecté les rôles requis Now Platform® et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis : • Un utilisateur ayant le rôle d'administrateur système (admin) pour installer l'application. • Un utilisateur ayant le rôle d'administrateur d'incident de sécurité (sn_si.admin) configure l'application et crée, active et supprime des profils. • Un utilisateur ayant le rôle d'analyste des incidents de sécurité (sn_si.analyst) travaille sur les incidents de sécurité. Les tâches incluent le lancement manuel de profils à partir d'incidents de sécurité. Si l'option d'approbation est sélectionnée dans un profil au cours de l'étape de configuration, les utilisateurs disposant de ce rôle soumettent également des demandes d'isolement des hôtes et de retour sur le réseau.
Vérifiez que vous utilisez la version 5.9 de McAfee ePO.	L'intégration prend en charge la version 10.4.3 de McAfee ePolicy Orchestrator.
Vérifiez que vous avez installé le module d'extension ServiceNow dans votre McAfee ePO console.	Installez le module d'extension ServiceNow dans votre McAfee ePO console. Pour plus d'informations et pour obtenir le fichier de module d'extension, dans votre Now Platform instance, accédez à **Base de connaissances** > **Articles** > **Tout** et, dans le champ Rechercher, saisissez ServiceNow Security Operations Extension for McAfee ePO .
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Le module d'extension Security Incident Response Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la tâche	Description
	1. Réponse aux incidents de sécurité **2.** Espace de travail Réponse aux incidents de sécurité **3.** Cadre de travail de Security Integration **4.** Security Support Common **5.** Orchestration de support de sécurité Pour plus d'informations sur l'installation des applications principales de Security Operations, consultez et .
Vérifiez que vous avez installé et configuré un serveur MID.	Un Serveur MID installé et configuré est requis dans votre Now Platform® instance. Consultez le site web de la documentation produit ServiceNow pour plus d'informations sur les MID Servers.
Si vous souhaitez activer le processus d'approbation des profils, vérifiez que vous avez créé un groupe d'approbation pour traiter les demandes.	Un processus d'approbation facultatif est disponible pour isoler les machines hôtes et les restaurer sur le réseau. Si cette option est activée, une approbation préalable est requise avant que les machines hôtes ne soient isolées et restaurées sur votre réseau. Si votre organisation souhaite un niveau de contrôle supplémentaire sur ces actions, activez l'option **Exiger l'approbation** pendant l'étape de configuration d'un profil. Par défaut, l'autorité d'approbation est affectée à l'administrateur d'incident Now Platform® de sécurité (sn_si.admin). Cette autorité peut être réaffectée à un groupe d'approbation. Au sein du groupe, tout membre a la permission d'approuver ou de rejeter des demandes. Vous sélectionnez un groupe d'approbation actif au cours de l'étape de configuration de la configuration de votre profil. Pour plus d'informations, consultez Créer un groupe d'approbation.

Configurer votre McAfee ePO console pour qu'elle s'intègre à Réponse aux incidents de sécurité (SIR)

La section suivante répertorie les étapes de configuration que vous devez effectuer dans votre McAfee ePO console avant d'installer l'application à partir du ServiceNow Store pour l'intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : McAfee ePO administrateur

En tant qu'utilisateur disposant de l'autorisation McAfee ePO administrateur, vérifiez que vous avez installé le module d'extension `Servicenow.zip` dans votre McAfee ePO console. Ce module d'extension est requis pour l'intégration. Pour obtenir des informations supplémentaires et pour obtenir le module d'extension, dans votre Now Platform instance, accédez à **Base de connaissances** > **Articles** > **Tout**. Dans le champ Rechercher, saisissez ServiceNow Security Operations Extension for McAfee ePO.

Pourquoi et quand exécuter cette tâche
Le ServiceNow module d'extension connecte votre Now Platform instance à votre McAfee ePO console. Cette connexion vous permet de référencer les balises de sécurité que vous créez dans votre McAfee ePO console pour Isoler l'hôte et de lancer des actions d'analyse anti-programme malveillant vers les profils d'aptitude de votre Now Platform instance.

Les balises de sécurité de votre McAfee ePO console doivent correspondre aux balises de sécurité des enregistrements d'aptitude de votre Now Platform instance.

Les étapes suivantes vous montrent comment installer le module d'extension d'extension, créer une balise de sécurité dans votre McAfee ePO console et affecter une action à la balise. Pour plus d'informations sur les balises de sécurité de la McAfee ePO console, consultez le site Web de la documentation produit McAfee .

Remarque : Les figures de la section suivante proviennent de la McAfee ePO console.

Procédure
1. Si vous n'avez pas installé le module d'extension ServiceNow sur votre McAfee ePO console, procédez comme suit pour l'installer.

   a. Connectez-vous à votre console à l'aide McAfee ePO de votre nom d'utilisateur et de votre mot de passe McAfee.

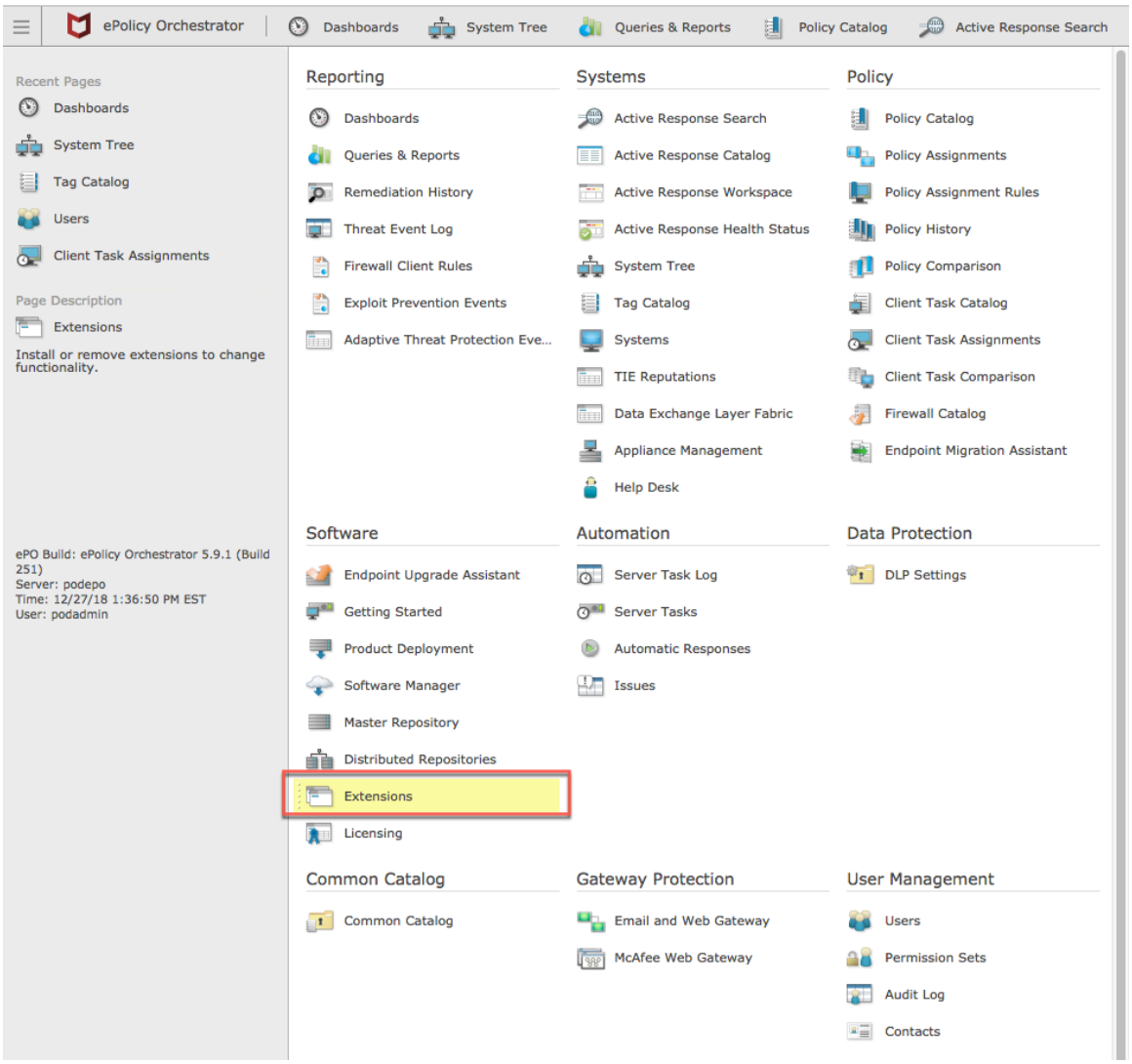


2. Si la page illustrée dans la figure suivante n'est pas affichée, en haut à gauche de la bannière de la page d'accueil, cliquez sur l'icône de menu pour l'afficher.

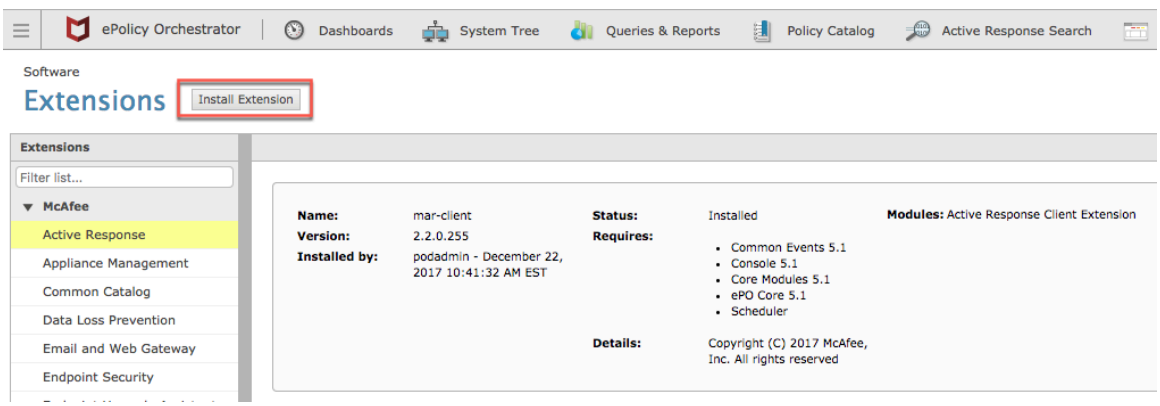
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans la section Logiciel, cliquez sur le lien **Extensions** .



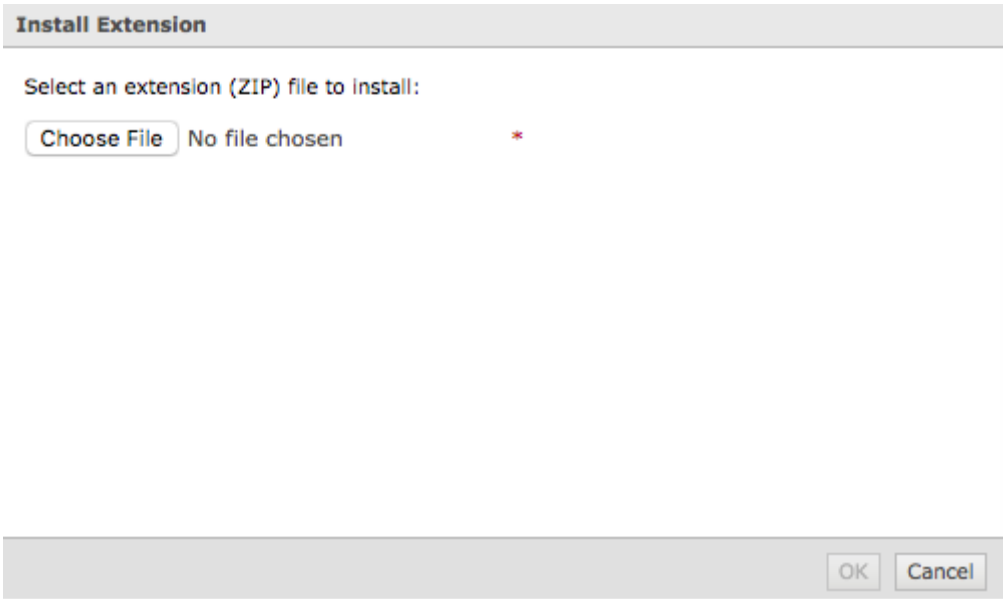
4. Sur la page Extensions qui s'affiche, cliquez sur **Installer l'extension**.



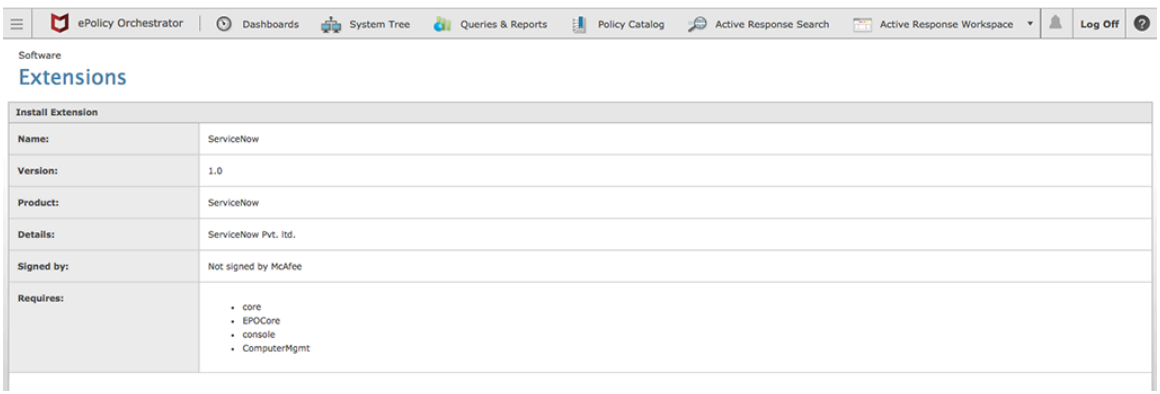
5. Dans la boîte de dialogue Installer l'extension, cliquez sur **Choisir un fichier**, accédez au fichier `Servicenow.zip` sur votre système, puis cliquez sur **OK** pour le télécharger.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois le téléchargement terminé, la page Extensions logicielles s'affiche avec le module d'extension ServiceNow Extension répertorié.



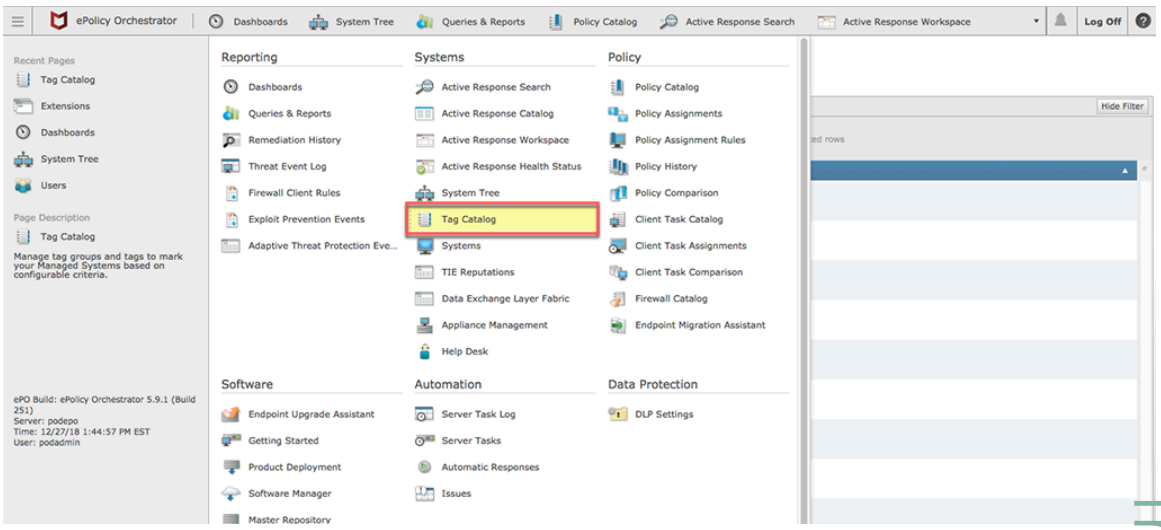
Vous avez correctement installé l'extension de module d'extension ServiceNow sur votre McAfee ePO console.

6. Si vous n'avez pas créé de balises de sécurité dans McAfee ePO la console pour les actions Lancer l'analyse anti-programme malveillant et Isoler l'hôte, procédez comme suit.

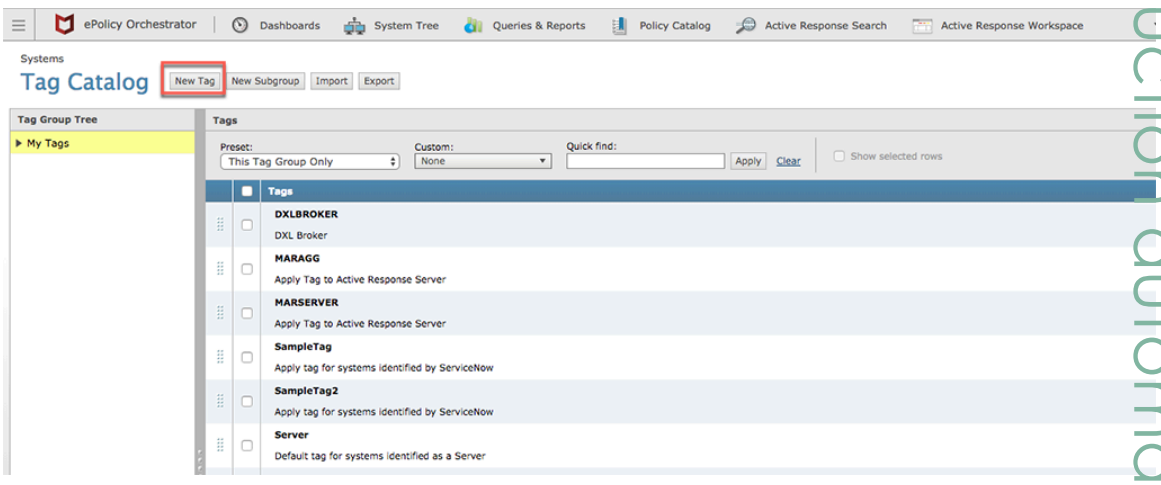
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la page d'accueil et cliquez sur le lien **Catalogue de balises** .

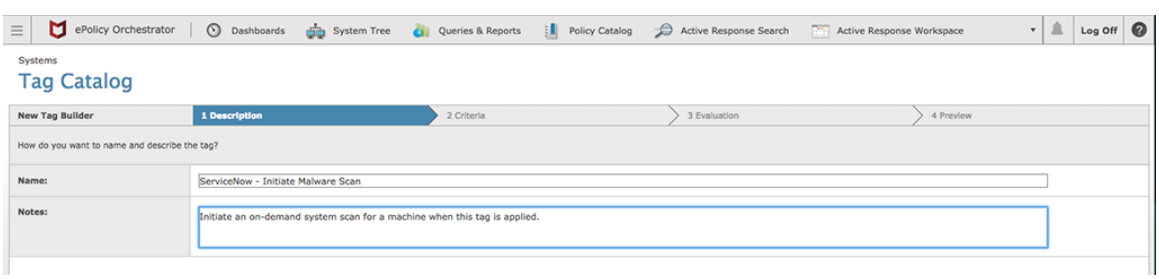


b. Sur la page Catalogue de balises qui s'affiche, cliquez sur **Nouvelle balise**.



c. L'étape Description étant sélectionnée dans la barre de progression qui s'affiche, saisissez un nom et une description pour la balise.

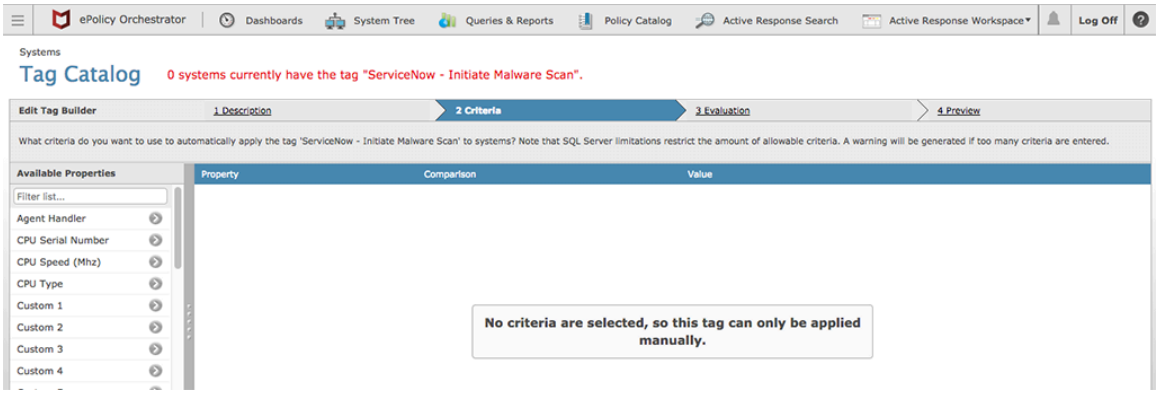
Dans cet exemple, une balise avec un nom et une description pour l'aptitude Lancer l'analyse anti-programme malveillant s'affiche. Ce nom de balise correspond et est référencé dans votre Now Platform instance.



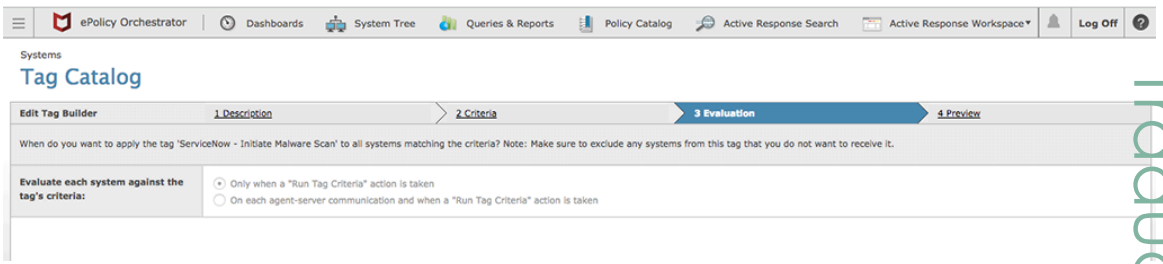
d. Pour passer à l'étape Critères, cliquez sur **Critères** dans la barre de progression.
Les messages qui s'affichent indiquent qu'aucune action n'est actuellement affectée à cette balise, et que la balise ne peut être appliquée que manuellement.

Traduction automatique

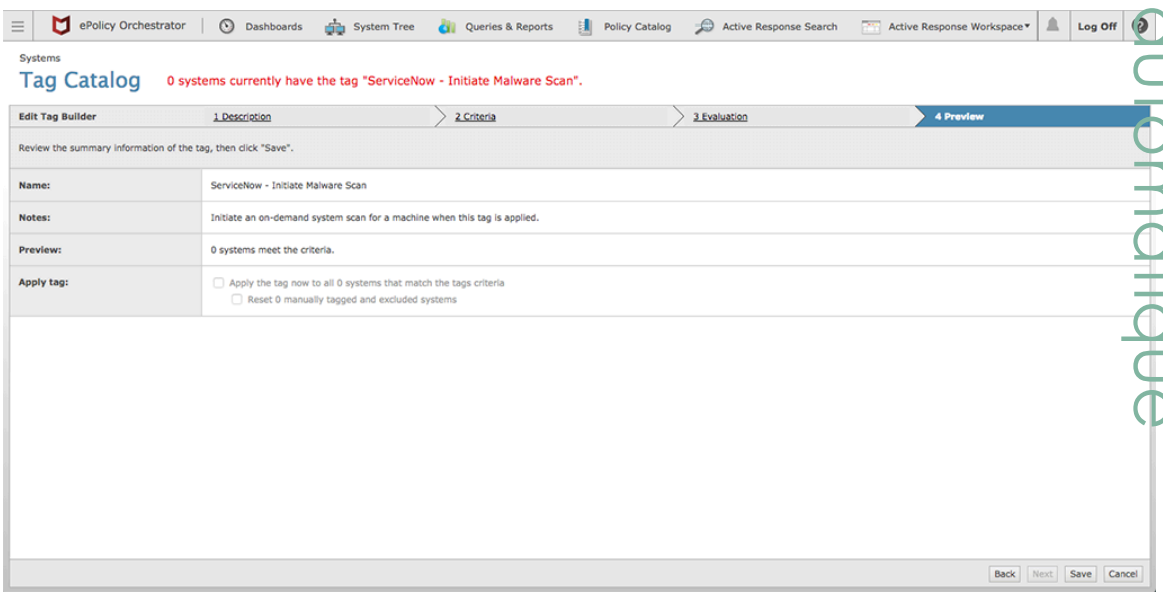
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



e. Cliquez sur **Évaluation** dans la barre de progression pour continuer.



f. Avec la page Catalogue de balises de l'étape d'évaluation affichée, laissez les paramètres de cette page dans leurs valeurs par défaut et, dans la barre de progression, cliquez sur **Aperçu**.

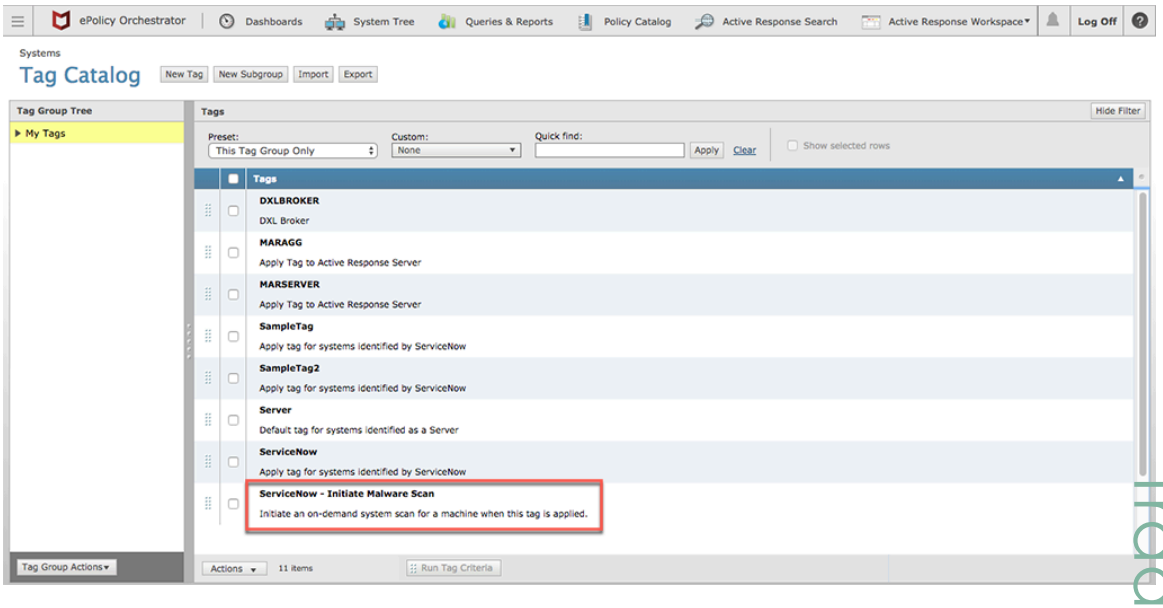


g. Avec la page Aperçu affichée, en bas à droite de la page, cliquez sur **Enregistrer** pour enregistrer l'enregistrement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La nouvelle balise est affichée dans le catalogue de balises, comme illustré dans la figure suivante.

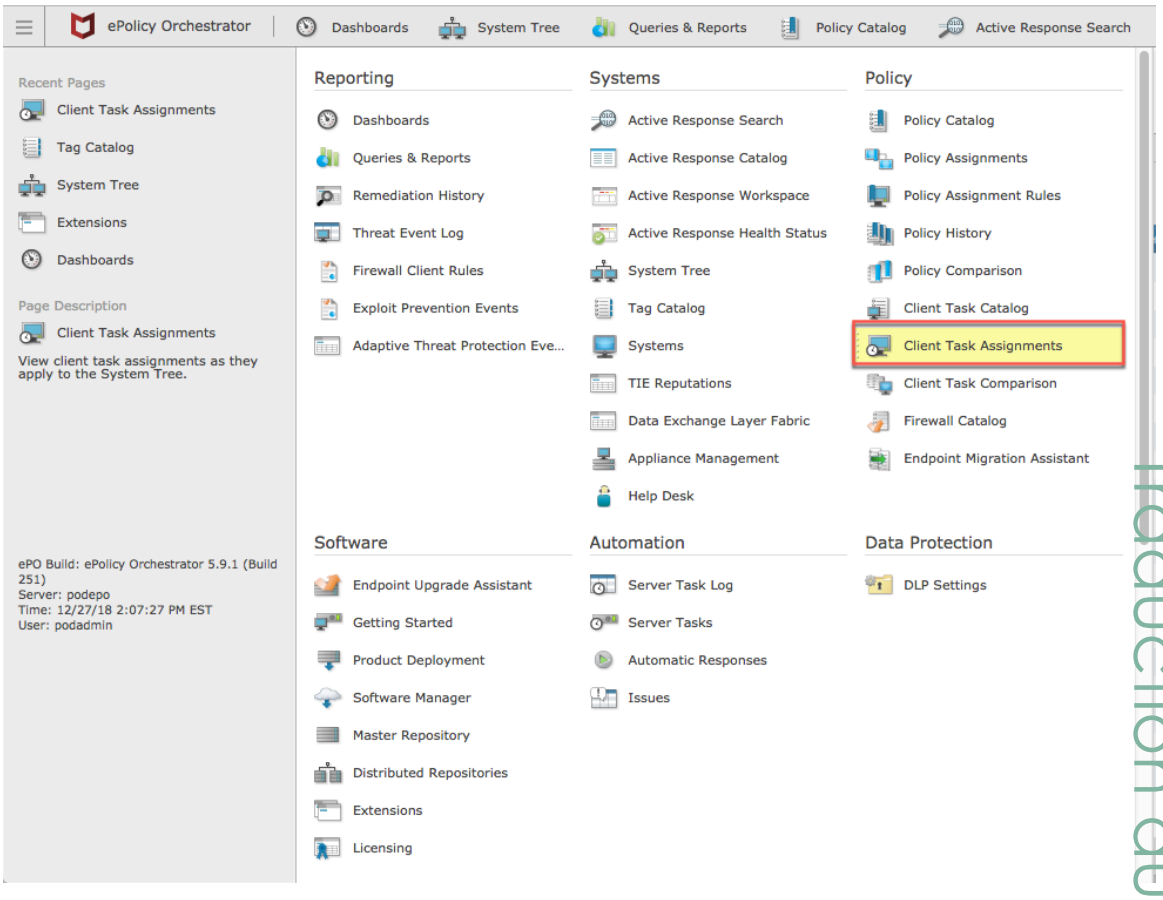


7. Créez une balise de sécurité pour l'action d'isolement de l'hôte en répétant les étapes précédentes.
   Une fois que vous avez créé les deux balises, vous êtes prêt à affecter des actions aux nouvelles balises.
8. Pour ajouter une action à votre nouvelle balise, procédez comme suit.

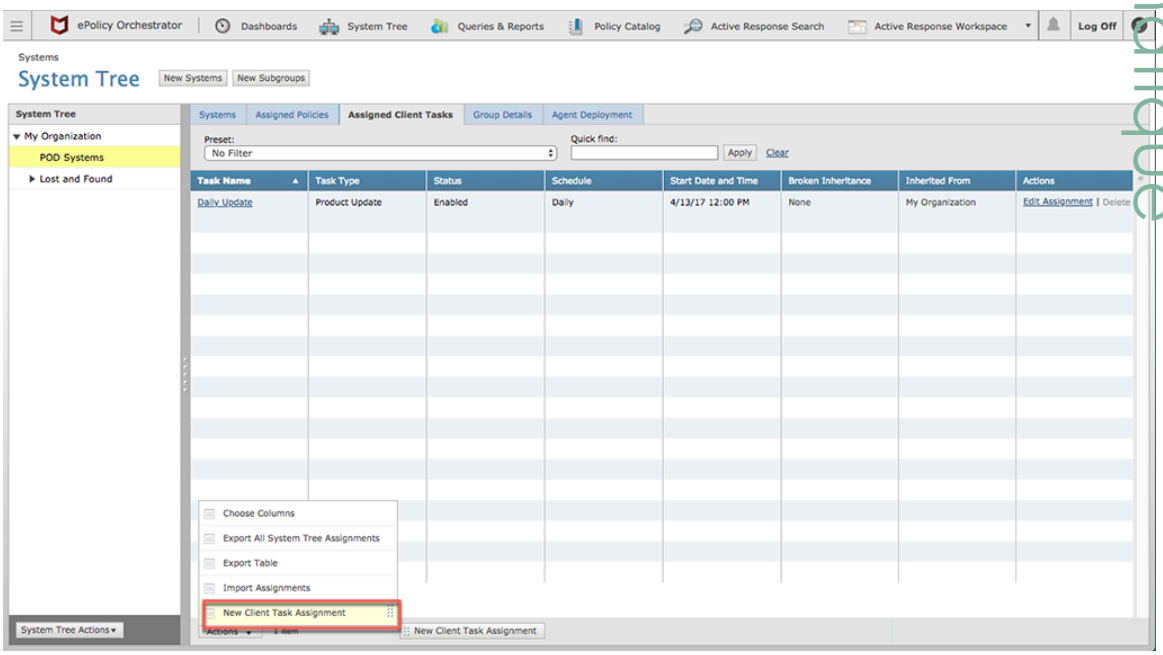
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la page d'accueil et, dans la section Politique, cliquez sur le lien **Affectations de tâches client** .



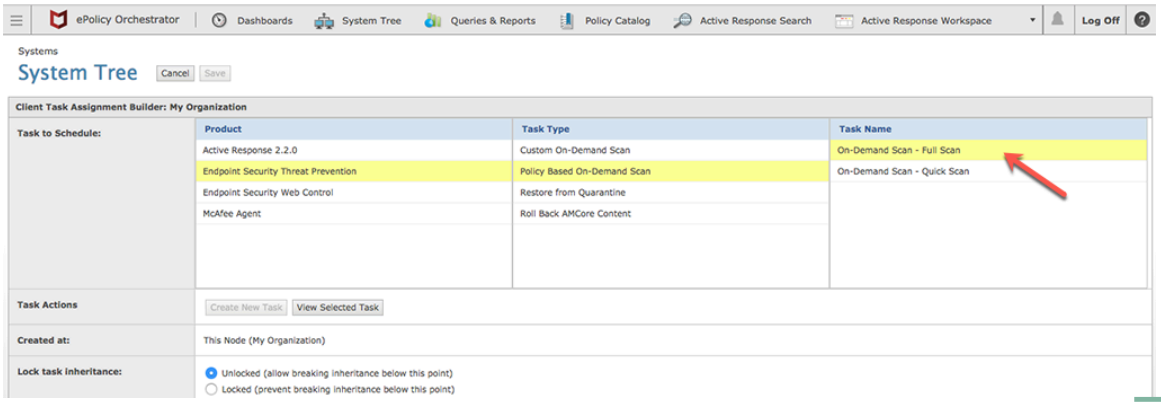
b. Dans la page de l'arborescence des systèmes qui s'affiche, en bas de la page, développez le menu **Actions** et sélectionnez **Nouvelle affectation de tâche client**.



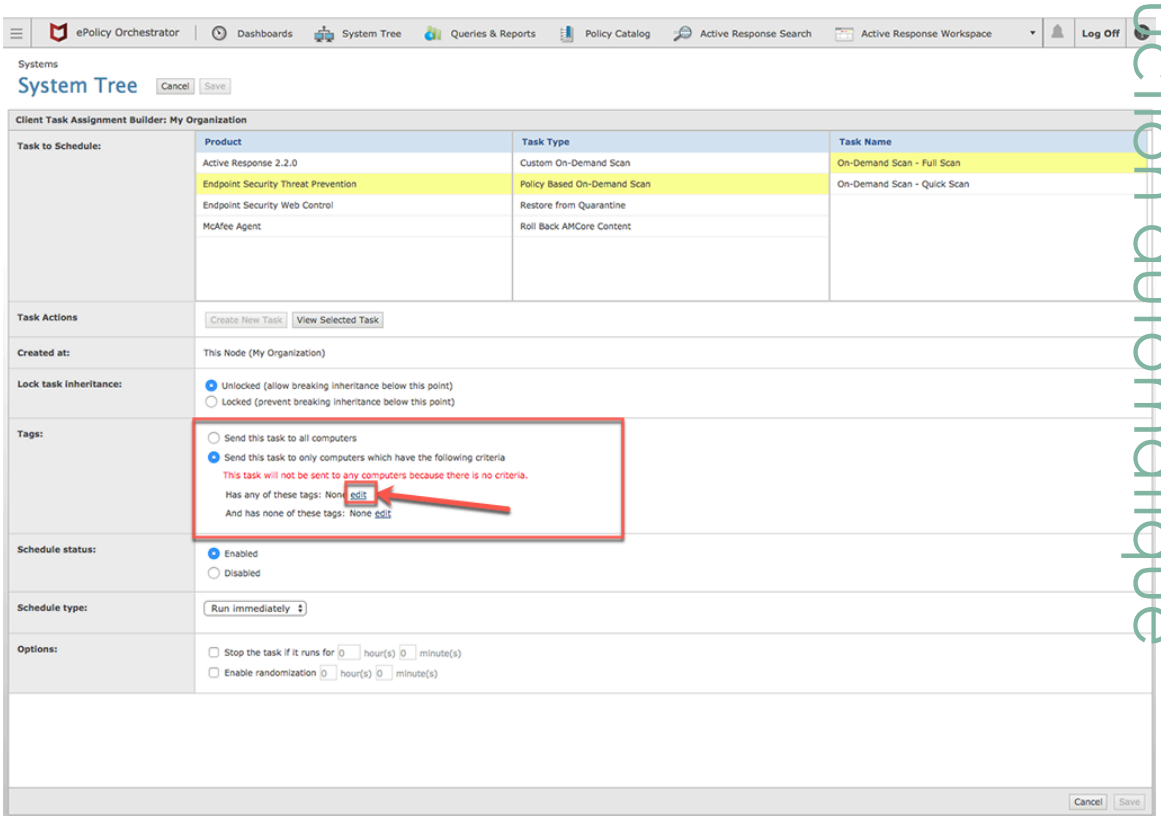
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Sur la page qui s'affiche, accédez à **Prévention des menaces pour la sécurité des points de terminaison** > **Analyse à la demande basée sur une politique** > **Analyse à la demande : analyse complète** en sélectionnant le chemin comme illustré dans la figure suivante.



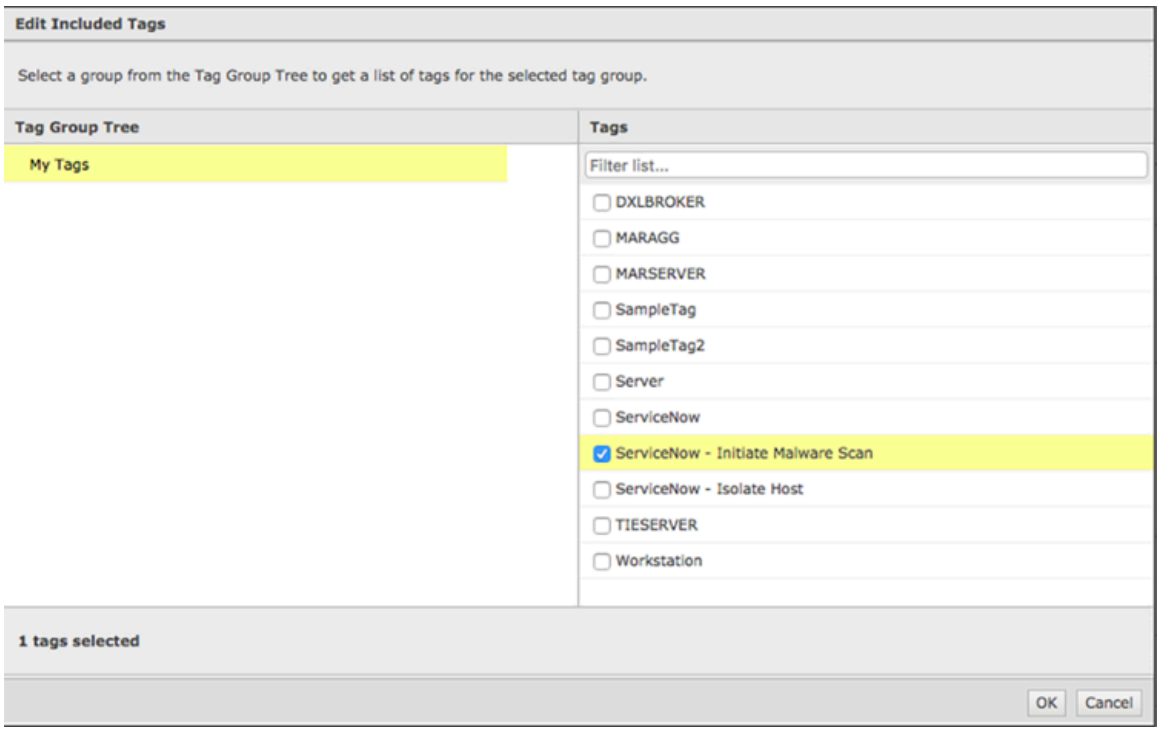
d. Dans la section Balises, sous la case d'option et à côté `de A l'une de ces balises :`, cliquez sur le lien **de modification** pour modifier les critères de la balise.



e. Dans la boîte de dialogue qui s'affiche, sélectionnez la balise Lancer l'analyse ServiceNow anti-programme malveillant que vous avez créée lors des étapes précédentes, puis cliquez sur **OK**.

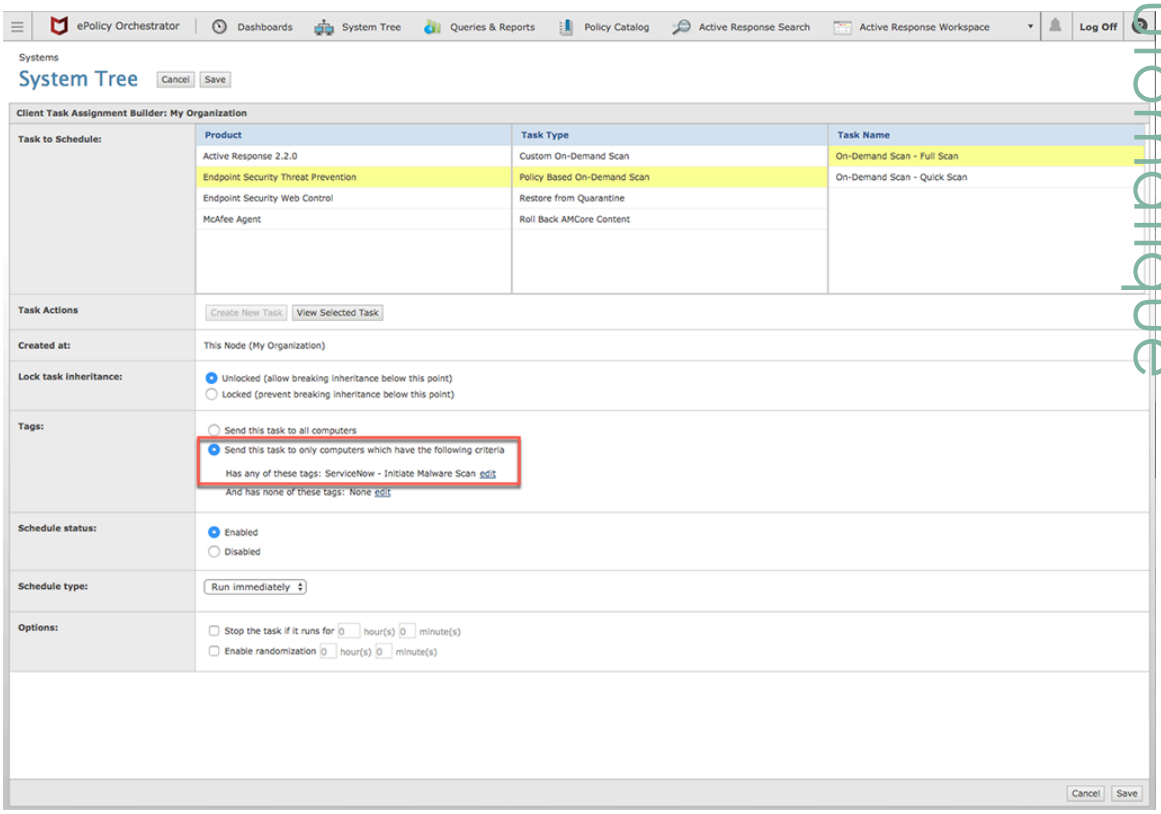
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La balise Lancer l'analyse anti-programme malveillant ServiceNow que vous avez créée est affectée à l'action Analyse à la demande.

f. Cliquez sur **OK**.
Dans la section Balises, sous la case d'option et à côté `de A l'une de ces balises :, la balise Lancer l'analyse anti-programme` malveillant s'affiche.

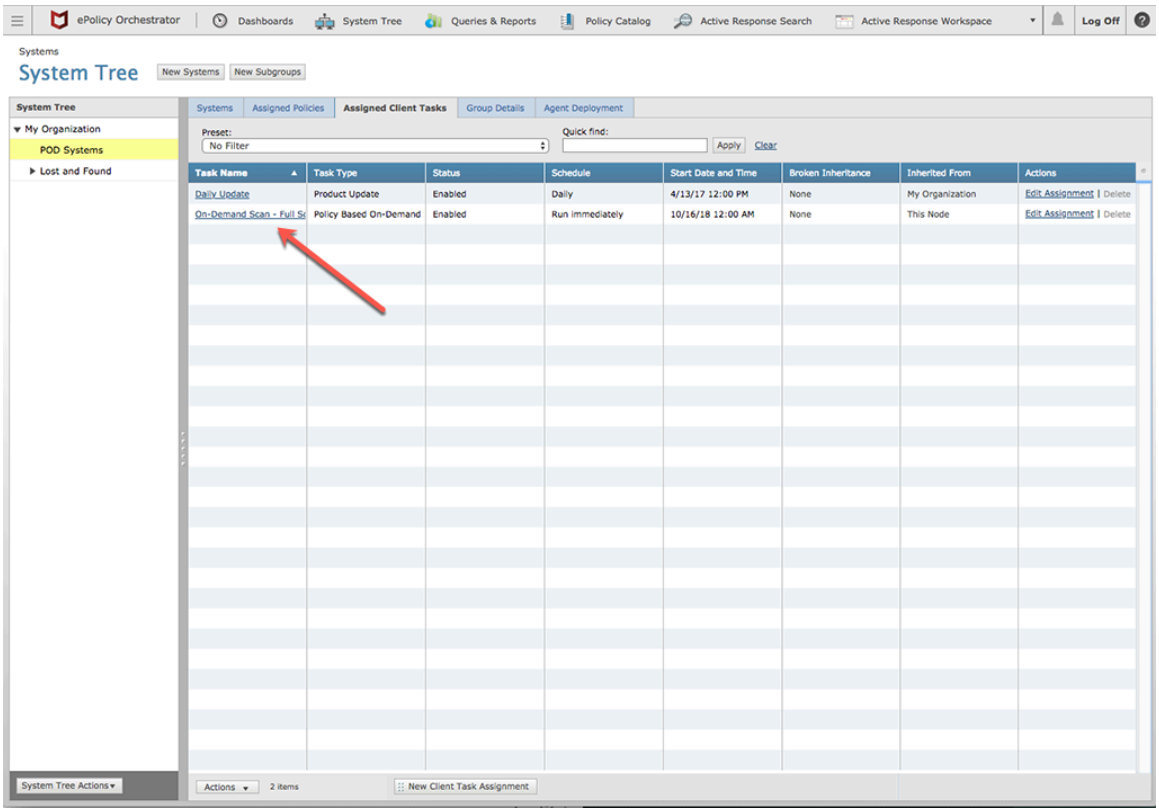


g. Cliquez sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sur la page de l'arborescence des systèmes, la tâche s'affiche dans la liste Tâches du client affecté (onglet).



h. Si vous n'avez pas affecté d'action à l'action Isoler l'hôte, répétez les étapes précédentes pour l'affecter.

Vous avez correctement installé le module d'extension de l'extension, créé des balises de sécurité et affecté des tâches à vos balises. Vous avez terminé la configuration de l'intégration dans votre McAfee ePO console. L'étape suivante consiste à configurer un serveur dans votre Now Platform instance.

Installer l'application et configurer un serveur pour l'intégration McAfee ePO

Avant d'appeler les workflows pour l'intégration, installez et configurez l'application McAfee ePO à partir de ServiceNow Store sur votre Now Platform instance. La configuration est requise pour se connecter à la McAfee ePO console.

Avant de commencer

Rôle requis : Now Platform administrateur (admin)

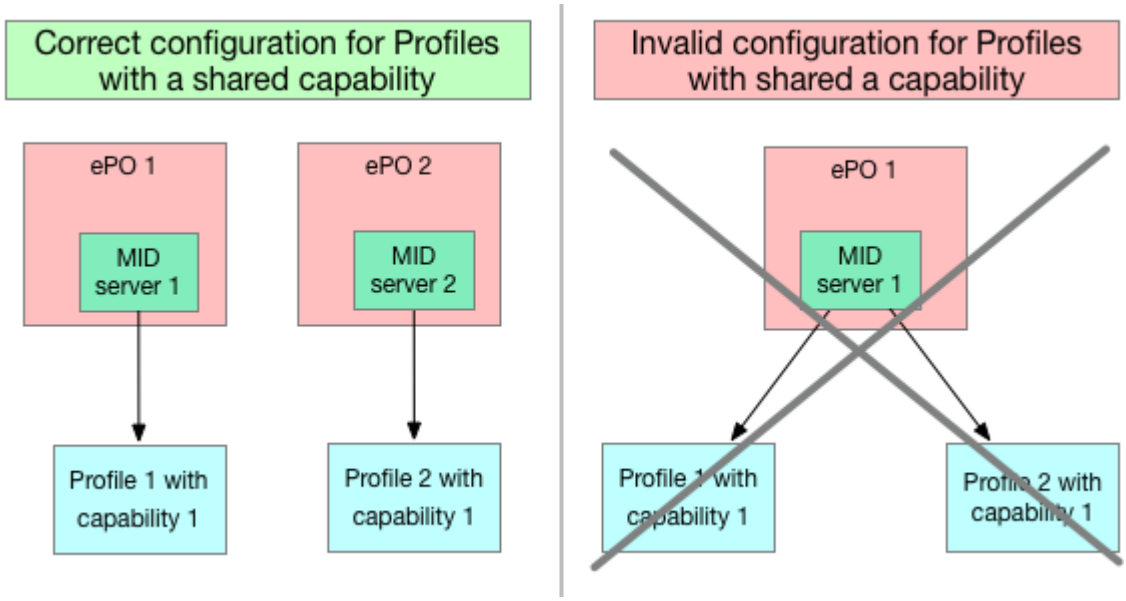
Pourquoi et quand exécuter cette tâche

L'intégration prend en charge plusieurs serveurs. Cependant, pour éviter les conflits entre les profils qui partagent les mêmes conditions de déclenchement, vous ne pouvez pas partager une McAfee ePO aptitude avec plusieurs profils qui utilisent le même McAfee ePO serveur. Par exemple, comme le montre la figure suivante, vous pouvez avoir l'option 1 dans plusieurs profils, à condition que chaque McAfee ePO serveur soit mappé à un profil unique doté de l'option 1.

Traduction automatique

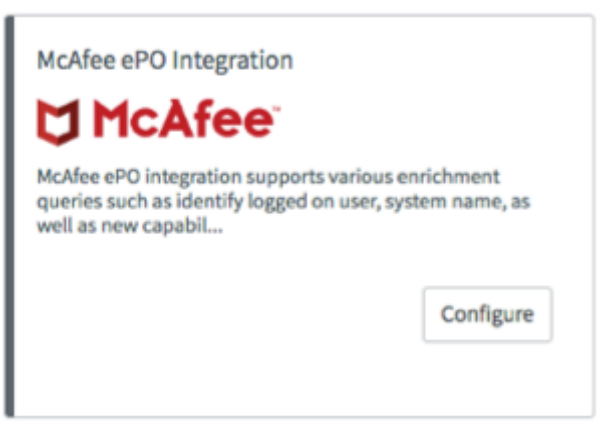
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Limitations de McAfee Shared Profile



Procédure

1. Téléchargez le McAfee ePO for à Opérations de sécurité partir de et ServiceNow Store installez-le.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette d'intégration McAfee ePOOpérations de sécurité , puis cliquez sur **Configurer**.



4. Renseignez les champs du formulaire.

Configuration de l'intégration de McAfee ePO

Champ	Description
Nom	Nom de l'intégration, par exemple `demo-1`.
Nom du serveur ePO	Nom du McAfee ePO serveur. Si vous utilisez un serveur, un exemple est `McAfee HQ` (McAfee Head Quarters). Ce nom est la façon dont le serveur et les informations d'identification associées sont reconnus.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si votre organisation a besoin d'une prise en charge de plusieurs serveurs, saisissez le nom de chaque serveur et répétez le processus.
URL REST API McAfee ePO	URL de base hébergeant l'API McAfee ePO REST. Entrez l'URL contenant le protocole https://, par exemple, `https ://corp.epo_server :8443`.
Nom d'utilisateur du compte API	Nom d'utilisateur de compte unique, par exemple `API ServiceNow`.
Mot de passe du compte API	Mot de passe unique pour le compte API.
Serveur MID	Sélectionnez le nom du Serveur MID que vous avez configuré lors de la configuration de votre Now Platform instance. Vous pouvez sélectionner un serveur MID spécifique dans la liste ou sélectionner **n'importe lequel** pour activer la sélection automatique d'un serveur MID valide dans la liste pour cette intégration. **Remarque :** ◦ Le serveur MID sélectionné pendant cette période de configuration s'applique à l'ensemble de cette intégration. ◦ Seuls les MID Servers actifs et validés sont affichés dans cette liste. Par défaut, cette valeur est définie sur **N'importe lequel**. Un exemple de nom est `secops_local_midserver`.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
   La liste des configurations de McAfee ePO s'affiche avec votre nouvel enregistrement de configuration. Vous avez terminé avec succès la configuration d'un McAfee ePO serveur.

   Remarque : Si votre organisation a besoin d'une prise en charge de plusieurs serveurs, répétez les étapes.

Modifier les balises de sécurité dans le Now Platform pour l'intégration McAfee ePO

Dans le cadre de la configuration de l'intégration, modifiez les noms de balises de sécurité que vous avez créés dans la McAfee ePO console de votre Now Platform instance. Modifiez les noms de balises dans votre Now Platform instance afin qu'ils correspondent aux noms des balises dans votre McAfee ePO console.

Avant de commencer

Rôle requis : Now Platform administrateur d'incident de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Les noms de balises de sécurité dans votre McAfee ePO console pour les actions Lancer l'analyse anti-programme malveillant et Isoler l'hôte doivent correspondre aux noms de balises de sécurité dans les enregistrements pour ces options de votre Now Platform instance.

Avant de créer un profil d'aptitude pour exécuter vos options, consultez la liste des options disponibles McAfee ePO et modifiez les balises de sécurité dans votre Now Platform instance afin qu'elles correspondent aux noms de balises de sécurité de votre McAfee ePO console.

Pour plus d'informations sur la création de noms de balises de sécurité dans votre McAfee ePO console, reportez-vous à la section Configurer votre McAfee ePO console pour qu'elle s'intègre à Réponse aux incidents de sécurité (SIR).

Traduction automatique

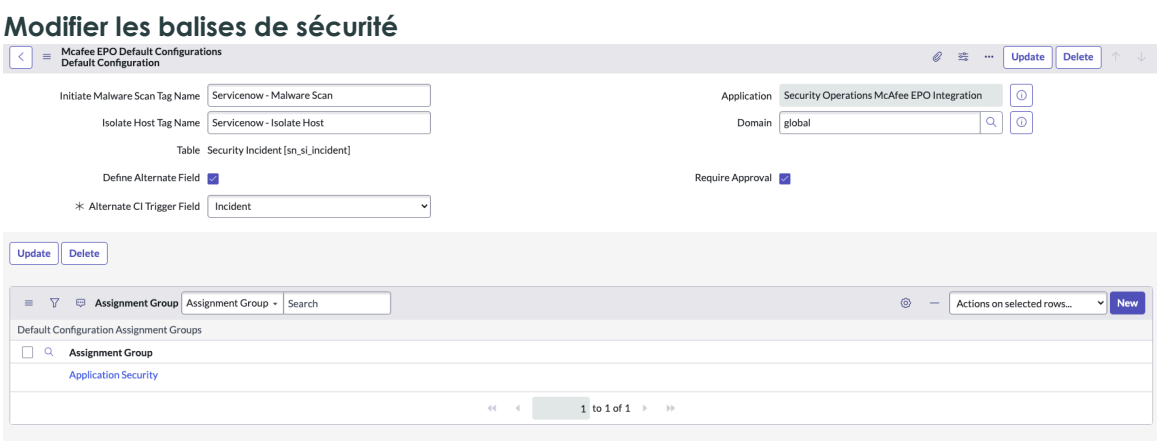
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Intégration de McAfee ePO** > **Paramètres par défaut**.
2. Pour modifier le nom de la balise de sécurité de l'intégration McAfee ePO , cliquez sur **Configuration par défaut**.

   Remarque : Assurez-vous d'effectuer cette configuration après avoir installé l'intégration McAfee ePO .

3. Dans le champ Nom de la balise Lancer l'analyse anti-programme malveillant, saisissez le nom de la balise de sécurité que vous avez créée dans votre McAfee ePO console pour l'action Lancer l'analyse.
   Par exemple, ServiceNow - Analyse des programmes malveillants
4. Dans le champ Nom de la balise Isoler l'hôte, saisissez le nom de la balise de sécurité que vous avez créée dans votre McAfee ePO console pour l'action Isoler l'hôte.
   Par exemple, ServiceNow - Isoler l'hôte
5. Si vous ne souhaitez pas utiliser le champ de déclencheur de CI lors de la création de l'incident, cochez la case **Définir un autre champ** .
   Lorsque cette option est activée, la liste de choix des champs de déclenchement CI alternatifs s'affiche.



6. Choisissez un autre champ dans la liste de choix pour vérifier vos critères de recherche de CI.
   Dans cet exemple, en tant qu'utilisateur disposant du rôle sn_si.admin, vous pensez que le champ CI ne sera pas renseigné sur l'incident de sécurité lors de sa création. Sinon, vous pensez que les informations CI pour un nom de domaine complet, un nom d'hôte ou une adresse IP seront renseignées dans le champ `CI identifié` de l'incident de sécurité et vous sélectionnez le champ CI identifié comme alternative. Le CI identifié est sélectionné pour cet exemple, mais vous pouvez utiliser n'importe quel champ de l'incident de sécurité pour l'autre CI.
7. Dans le champ Domaine, sélectionnez un domaine ou un groupe pour cette configuration à l'aide de l'option de recherche.
   Par exemple, global.
8. Dans le champ Exiger l'approbation, cochez la case **Exiger l'approbation** si vous utilisez les options Isoler l'hôte et Supprimer l'isolement.

   Remarque : Les options Lancer l'analyse anti-programme malveillant, Répertorier les événements de menace et Obtenir les détails du système n'ont pas besoin d'approbation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Cliquez sur **Mettre à jour**.
   Le nom de la balise ePO est mis à jour et affiché dans la liste Configurations par défaut de McAfee ePO. Le nom de la balise de sécurité de l'action d'analyse anti-programme malveillant dans votre Now Platform instance correspond au nom de l'analyse dans votre McAfee ePO console.

   Vous avez modifié avec succès les noms de la balise ePO pour l'analyse anti-programme malveillant et les options Isoler l'hôte dans votre Now Platform instance. L'étape suivante consiste à créer un profil pour vos options.

Information associée

Documentation produit McAfee

Créer un groupe d'approbation

Créez un groupe d'approbation pour l'intégration McAfee ePOOpérations de sécurité qui peut approuver les demandes d'isolement des ordinateurs hôtes et de restauration sur le réseau.

Avant de commencer
Vous ne pouvez pas réaffecter l'autorité d'approbation à un groupe, sauf si un groupe d'approbation est disponible dans votre instance.

Remarque : L'option d'approbations du module d'extension s'affiche Configuration des profils pour l'intégration McAfee ePO uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte.

Rôle requis : Now Platform® administrateur d'incident de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche
Les demandes d'approbation soumises par l'analyste des incidents de sécurité pour isoler les ordinateurs hôtes et supprimer l'isolement sont affectées par défaut à l'utilisateur disposant du rôle sn_si.admin. En tant qu'utilisateur disposant de ce rôle, vous pouvez réaffecter cette autorité d'approbation pendant l'étape de configuration d'un profil. Avant de pouvoir réaffecter l'autorité à un groupe d'approbation, un groupe d'approbation doit être disponible sur la liste `Groupes` de votre Now Platform instance.

Procédure
1. Accédez à la **Tout** > **Administration utilisateurs** > **Groupes**.
2. Dans la liste des groupes, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Groupe d'approbation

Champ	Description
Nom	Nom du groupe qui s'affiche lors de l'envoi d'une demande d'approbation ; par exemple, `Approbateurs McAfee Host Isolation`.
E-mail de groupe	Liste de distribution des e-mails de groupe ou adresse e-mail du point de contact, tel que le gestionnaire du groupe, `McAfeeapproval@servicenow`.com

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Responsable	Nom du gestionnaire de groupe. Cliquez sur l'icône de recherche pour afficher la liste.
Parent	(Facultatif) Autre groupe dont ce groupe est membre, si ce groupe a un parent.
Description	Informations supplémentaires sur ce groupe.
Inclut des membres	Option permettant d'inclure des membres à ce groupe.
Délégataire par défaut	Option permettant de choisir un utilisateur comme délégataire par défaut pour ce groupe. Utilisez l'option Rechercher pour ouvrir la liste des utilisateurs.
Rôles	Option permettant de sélectionner les rôles de ce groupe. Utilisez l'option Ajouter et supprimer pour ajouter et supprimer des rôles.
Type	Option permettant de choisir une catégorie pour ce groupe. Utilisez l'option Rechercher pour ouvrir la liste des types de groupes.
Fournisseurs	Option permettant de choisir un fournisseur pour ce groupe. Utilisez l'option Rechercher pour ouvrir la liste des fournisseurs.

4. Cliquez sur **Envoyer**.
   Le nouveau groupe s'affiche dans la liste Groupes.

   Ce groupe est disponible pour traiter les demandes lorsque vous activez l'option **Exiger une approbation** pendant la configuration de ce profil.

   Pour surveiller et traiter les demandes soumises par les utilisateurs disposant du rôle sn_si.analyst, chaque membre du groupe d'approbation accède à l'onglet **Mes approbations** dans le Now Platform.

McAfee ePO Profils d'aptitude d'intégration

En tant qu'utilisateur ayant le rôle d'administrateur d'incident de sécurité (sn_si.admin), vous créez des profils pour les McAfee ePO options de votre Now Platform® instance. Vous regroupez des requêtes ou des actions dans des profils et déterminez les McAfee ePO options que vous souhaitez exécuter lorsqu'un nouvel incident de sécurité est créé.

Profils d'aptitude

Vous créez des profils™ afin de regrouper McAfee ePO les options et configurer les paramètres de ces options à partir de votre Now Platform® instance. Vous pouvez créer plusieurs profils pour ces options, ce qui vous permet de déterminer quelles actions ou requêtes sont invoquées lorsqu'un Réponse aux incidents de sécurité incident (SIR) est créé. Pour répondre aux besoins de votre organisation, vous pouvez créer un profil unique qui exécute des requêtes pour les détails du système, lance des analyses de programmes malveillants et isole les ordinateurs hôtes, par exemple, ou vous pouvez créer plusieurs profils, chacun avec sa propre option.McAfee ePO

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types de profils et capacités requises McAfee ePO

Objectif primaire de votre profil	Configurez les exigences	Aptitudes de McAfee ePO requises pour ce type de profil
Collecter les détails du système	Aucun	**Obtenir les détails de l'hôte**
Isoler un hôte	Vérifiez auprès de votre McAfee ePO administrateur que vous avez créé les balises de sécurité pour l'action Isoler l'hôte dans votre McAfee ePO console. Pour plus d'informations, consultez Configurer votre McAfee ePO console pour qu'elle s'intègre à Réponse aux incidents de sécurité (SIR).	**Isoler l'hôte**
Analysez et recherchez les menaces sur votre hôte	Vérifiez auprès de votre McAfee ePO administrateur que vous avez créé les balises de sécurité pour l'action Lancer l'analyse anti-programme malveillant dans votre McAfee ePO console. Pour plus d'informations, consultez Configurer votre McAfee ePO console pour qu'elle s'intègre à Réponse aux incidents de sécurité (SIR).	**Lancer l'analyse anti-programme malveillant** **Remarque :** Dans le cadre de l'analyse anti-programme malveillant, l'option Répertorier les McAfee ePO événements de menace est invoquée automatiquement. Toutefois, vous n'êtes pas obligé d'ajouter l'option Répertorier les événements de menace au profil avec l'option Analyse anti-programme malveillant. Les résultats de l'analyse anti-programme malveillant sont affichés dans l'onglet Détails de l'événement de menace de l'incident de sécurité.
Supprimer l'isolement d'un hôte	Vérifiez auprès de votre McAfee ePO administrateur que vous avez créé les balises de sécurité pour l'action Isoler l'hôte dans votre McAfee ePO console. Pour plus d'informations,	**Supprimer l'isolement**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types de profils et capacités requises McAfee ePO (suite)

Objectif primaire de votre profil	Configurez les exigences	Aptitudes de McAfee ePO requises pour ce type de profil
	consultez Configurer votre McAfee ePO console pour qu'elle s'intègre à Réponse aux incidents de sécurité (SIR).	
Collecter des données d'enrichissement des menaces.	Aucun	**Répertorier les événements de menace**

Créer un profil d'aptitude pour l'intégration McAfee ePO

Créez un profil et sélectionnez les McAfee ePO options que vous souhaitez qu'il exécute.

Avant de commencer

Rôle requis : Now Platform® administrateur d'incident de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Pour cette étape de la configuration, vous allez créer un profil pour les McAfee ePO options. Lorsque vous créez des profils, tenez compte de l'intention du profil avant d'y ajouter McAfee ePO des options. Reportez-vous au tableau suivant lorsque vous créez des profils.

La table suivante répertorie les options que vous devez ajouter à un profil si vous souhaitez que le profil effectue certaines requêtes ou actions. Créez un profil unique qui exécute des requêtes pour obtenir des détails sur l'hôte, lance des analyses de programmes malveillants, supprime l'isolement et isole les machines hôtes, ou crée plusieurs profils, chacun avec sa propre option.

Procédure

1. Accédez à la **Intégration de McAfee ePO** > **Profils de fonctionnalités de McAfee ePO**. La liste des profils d'aptitude McAfee ePO s'affiche.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom du profil d'aptitude McAfee ePO . Ce nom vous permet d'identifier le type de profil et de le décrire. Un exemple de profil qui exécute des requêtes est Détails de l'hôte et de la menace. Ce nom est également le nom de la balise de sécurité de ce profil par défaut.
Description	Informations supplémentaires sur le profil qui décrivent plus en détail les activités du profil. Voici un exemple de description d'un profil qui exécute des requêtes : Enrichissement des menaces pour les détails du système et une liste d'événements de menace. Voici un exemple de description d'un

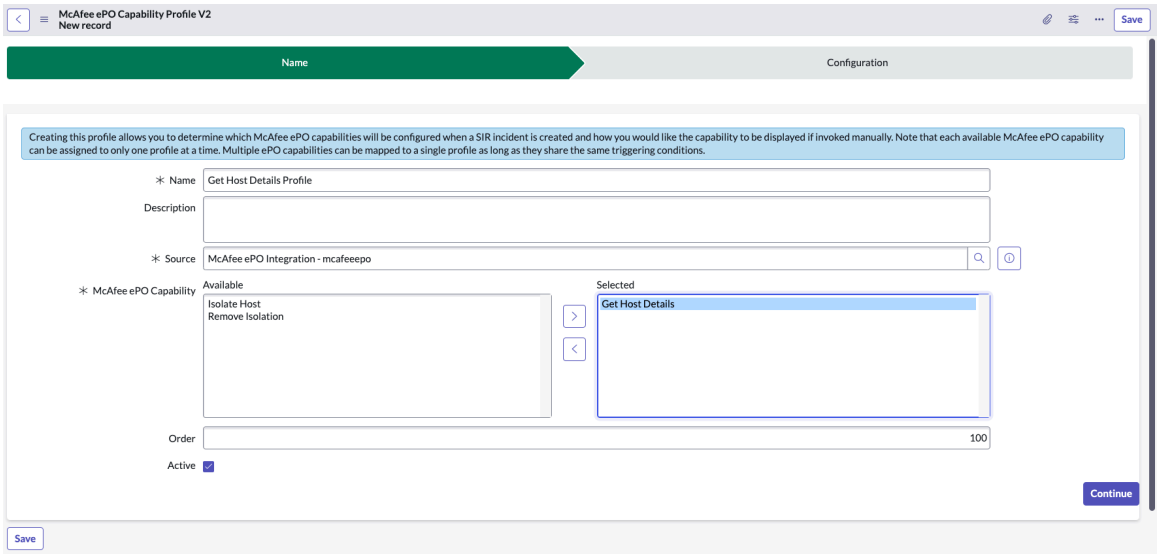
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	profil qui exécute des actions : Isoler l'ordinateur hôte.
Source	Nom du McAfee ePO serveur. Seuls les serveurs configurés sont disponibles dans la liste de choix.
Aptitude de McAfee ePO	Options du McAfee ePO profil. McAfee ePO prend en charge les fonctionnalités suivantes : ◦ Obtenir les détails de l'hôte ◦ Isoler le profil de l'hôte ◦ Lancer l'analyse anti-programme malveillant ◦ Supprimer l'isolement ◦ Répertorier les événements de menace Sélectionnez les options que vous souhaitez pour ce profil dans la colonne **Disponible** et déplacez-les vers la colonne **Sélectionné** . Vous ne pouvez pas ajouter Obtenir les détails de l'hôte, Lancer l'analyse anti-programme malveillant et Répertorier les événements de menace dans le même profil, ni Supprimer l'isolement et Isoler l'hôte sur le même profil.
Ordre	Priorité du workflow. La valeur par défaut est 100. La valeur de ce champ indique l'ordre dans lequel les workflows sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow dont le numéro est le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400.
Actif	La case est cochée par défaut pour indiquer que le profil est actif. Lorsque cette option est sélectionnée, le profil est actif et se déclenche automatiquement lorsqu'un incident de sécurité correspondant aux conditions de filtrage spécifiées lors de l'étape de configuration est créé. Lorsqu'il est inactif, le profil ne s'exécute pas et il n'est pas possible de l'appeler à partir d'une liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Pour enregistrer et valider le profil, cliquez sur **Continuer**.
   Si la validation est réussie, la page se recharge et le formulaire **de configuration** s'affiche.

Que faire ensuite

L'étape suivante consiste à configurer votre profil. Avant de configurer les paramètres du profil, il est préférable d'examiner les concepts de configuration des profils et des conditions de déclenchement. Voir Configurer votre McAfee ePO console pour qu'elle s'intègre à Réponse aux incidents de sécurité (SIR) et Définir des conditions de déclenchement avec un champ d'élément de configuration (CI) pour un McAfee ePO profil pour plus d'informations.

Définir des conditions de déclenchement avec un champ d'élément de configuration (CI) pour un McAfee ePO profil

Une fois que vous avez créé un profil et sélectionné les McAfee ePO options que vous souhaitez que le profil exécute, vous configurez les paramètres du profil afin qu'il ne s'exécute que lorsqu'un ensemble de conditions spécifiques est rempli.

Vous pouvez définir ces conditions de déclenchement afin que le profil s'exécute automatiquement en fonction des valeurs de champ par défaut qui correspondent à un Now Platform® Réponse aux incidents de sécurité incident de sécurité. Vous pouvez également configurer un profil afin qu'il recherche des correspondances sur des valeurs de champ que vous identifiez spécifiquement sur l'incident de sécurité.

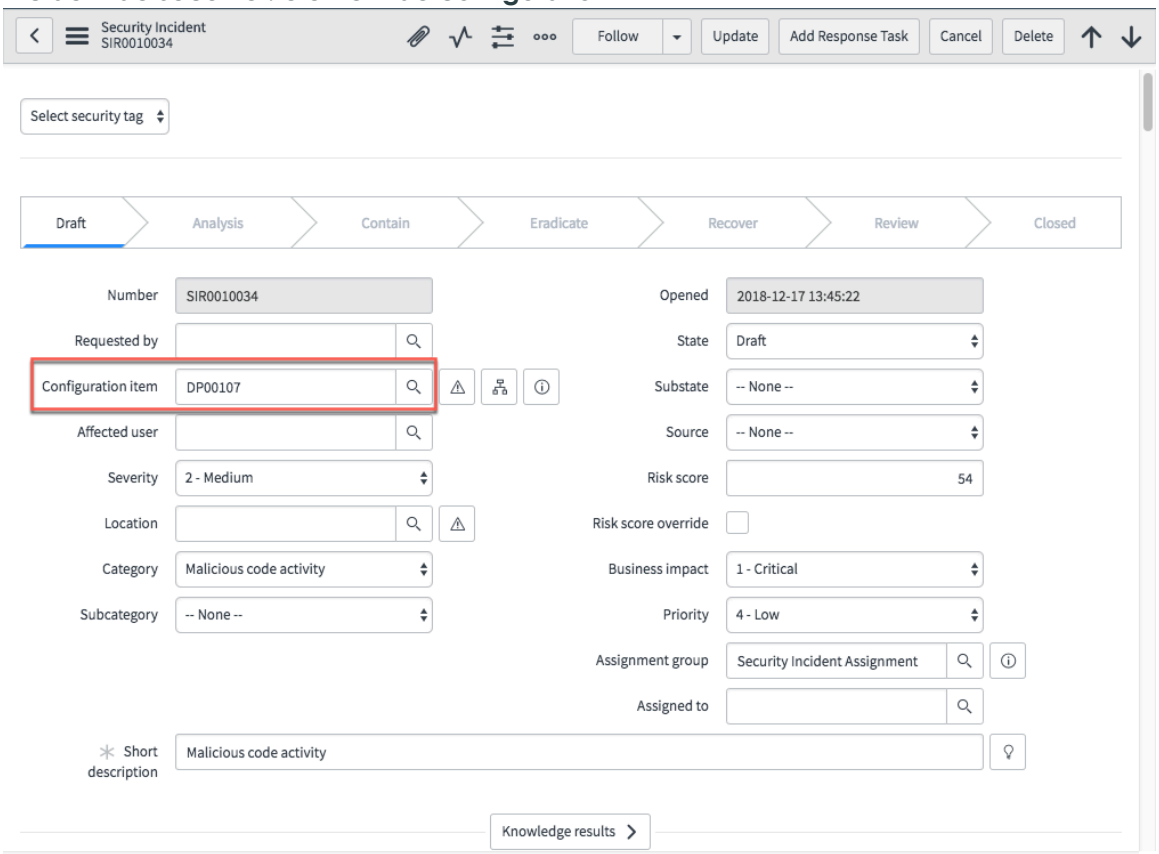
L'une des clés de la fonctionnalité de l'intégration et du fonctionnement d'un profil est le champ Élément de configuration (CI) de l'incident Now Platform® Réponse aux incidents de sécurité de sécurité (SIR). La valeur de ce champ est la valeur principale d'un incident de sécurité. Cette valeur est utilisée pour faire correspondre les ID de vos actifs avec les informations stockées dans la Now Platform® base de données. Lorsqu'un SIR incident de sécurité est créé par un événement de sécurité et qu'un profil est activé, vos actifs sont analysés à la recherche d'une valeur correspondante pour un nom de domaine complet (FQDN), un nom d'hôte ou une adresse IP en fonction de la valeur du champ Élément de configuration.

Dans l'idéal, une valeur correspondante est trouvée dans la base de données et les données peuvent être collectées à partir de la McAfee ePO console pour l'actif correspondant, extraites dans votre Now Platform® instance et affichées sur les listes connexes d'un incident de sécurité. La figure suivante est un exemple de champ Élément de configuration renseigné avec un nom d'hôte sur un SIR incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incident de sécurité : élément de configuration



Si le champ Élément de configuration (CI) n'est pas renseigné sur l'incident de sécurité, ou si une correspondance pour un nom de domaine complet, un nom d'hôte ou une adresse IP correspondant à la base de données est introuvable, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour afficher toutes les données d'enrichissement de CI correspondantes trouvées lors de l'analyse de vos actifs.

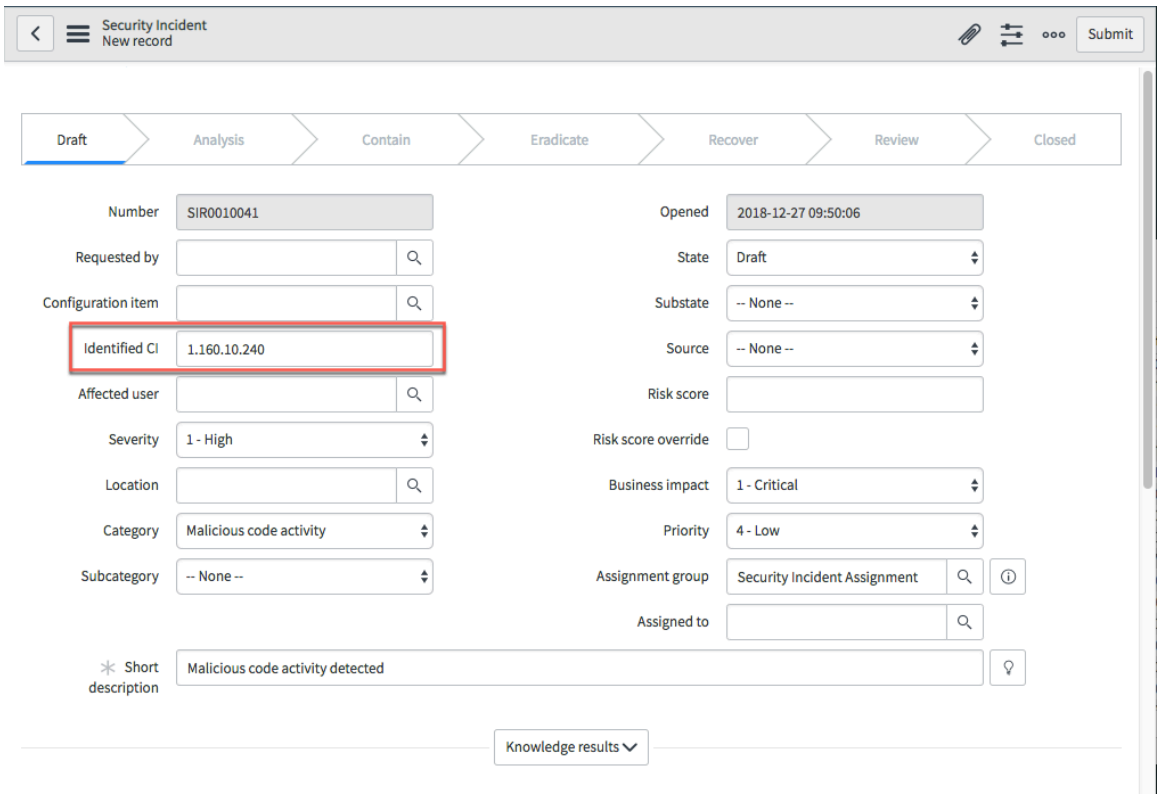
Au cours de l'étape de configuration de la configuration du profil, vous pouvez sélectionner un autre champ de déclenchement CI pour l'identification du point de terminaison afin de vous assurer que les données d'enrichissement de CI issues de la McAfee ePO recherche sont renseignées sur l'incident de sécurité associé. Vous pouvez sélectionner n'importe quel champ de l'incident de sécurité comme champ de déclenchement CI alternatif, y compris les champs personnalisés que vous créez. En sélectionnant ce champ CI alternatif comme copie de sauvegarde, vous vous assurez que vos profils s'exécutent même si le champ CI n'est pas renseigné pour l'incident de sécurité associé lors de la création de l'incident.

Par exemple, en tant qu'analyste du centre des opérations de sécurité (SOC), vous créez un champ personnalisé pour un incident de sécurité appelé « Adresse IP » dans mon incident de sécurité. Si vous pensez que la valeur de ce champ personnalisé ne s'affichera pas dans le champ Élément de configuration de l'incident de sécurité lors de la création de l'incident, vous pouvez configurer le profil afin qu'il recherche cette adresse IP. En cas de correspondance, l'adresse IP est affichée sur l'incident de sécurité dans le champ de votre choix. Dans la figure suivante, le champ `CI identifié` est sélectionné comme champ alternatif pour l'adresse IP pour cet exemple.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incident de sécurité : CI identifié

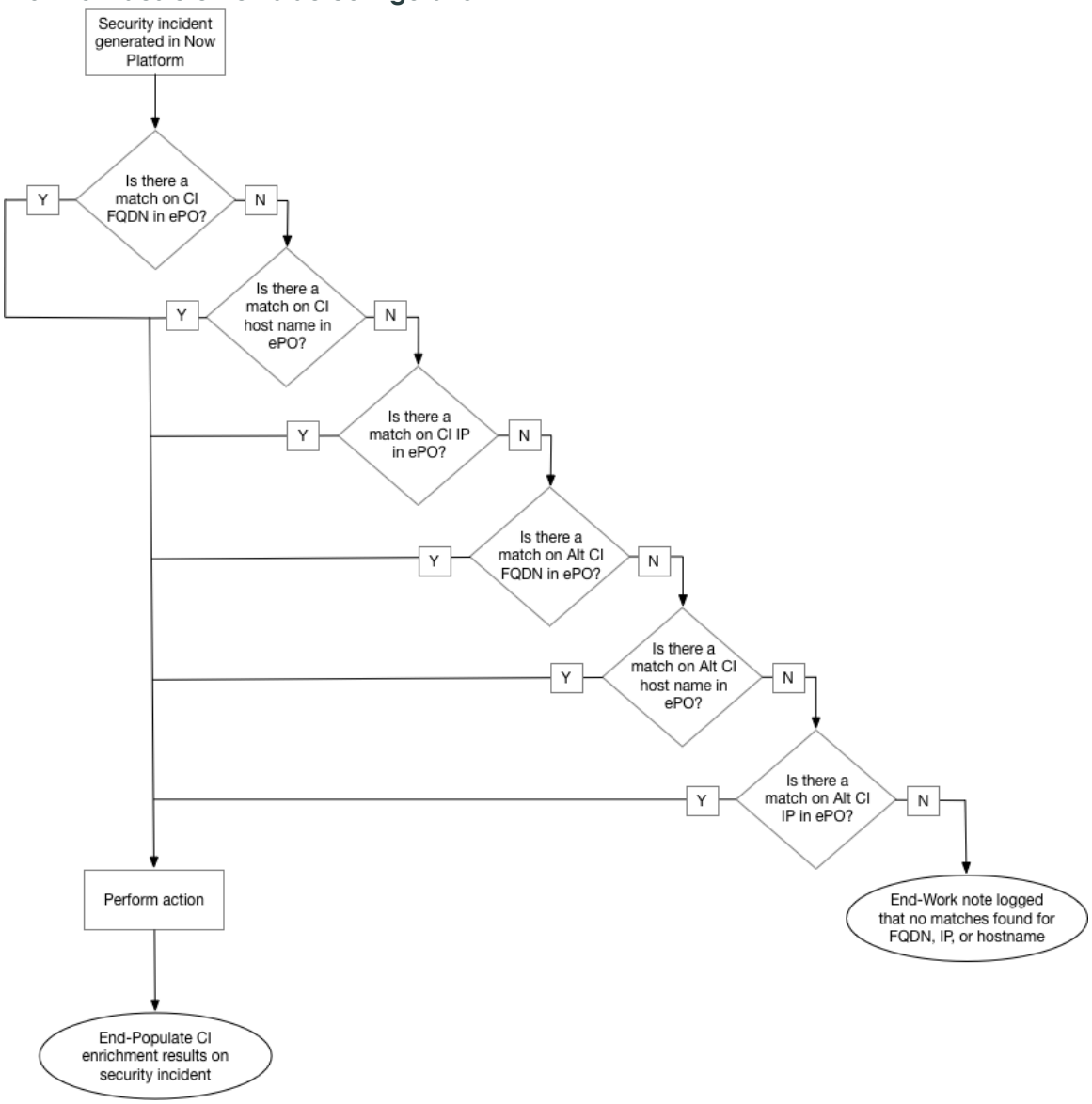


La figure suivante illustre comment la première recherche du workflow recherche des correspondances pour les éléments de configuration. Si le champ de déclenchement CI alternatif est activé, la deuxième recherche recherche les correspondances de valeurs alternatives.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow des éléments de configuration



Si les ID correspondants ne sont pas trouvés pour le champ CI ou l'autre champ CI, une note de travail est enregistrée et un message s'affiche sur l'incident de sécurité. Lorsqu'aucune correspondance n'est trouvée, aucune donnée d'enrichissement n'est renseignée sur les incidents de sécurité liés à l'événement.

Vous activez l'autre champ de déclenchement de CI et sélectionnez le champ dans lequel vous souhaitez afficher l'ID correspondant pendant l'étape de configuration d'un profil. Cette étape d'activation de l'autre champ CI est décrite ainsi que les autres exigences de configuration de profil de la section Configuration des profils pour l'intégration McAfee ePO.

Configuration des profils pour l'intégration McAfee ePO

Après avoir créé un profil et sélectionné les McAfee ePO options que vous souhaitez qu'il exécute, configurez les paramètres afin que le profil ne soit appelé que dans les conditions spécifiques que vous définissez.

Configuration d'un profil

Au cours de cette étape, vous configurez un profil d'aptitude afin qu'il ne s'exécute que lorsque les conditions que vous spécifiez sont remplies. Vous définissez les conditions des incidents de sécurité qui déclenchent automatiquement les McAfee ePO options que

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vous avez sélectionnées pour le profil. Vous pouvez également sélectionner un autre champ d'entrée pour le champ Élément de configuration (CI) et définir des conditions de filtrage afin que seuls les incidents de sécurité liés à votre événement déclencheur lancent automatiquement le profil. L'étape de configuration comprend les paramètres suivants sur le formulaire de configuration du profil.

Champ de déclenchement d'un autre élément de configuration (CI)

Si le champ Élément de configuration (CI) de l'incident de sécurité () n'est Now Platform® Réponse aux incidents de sécuritéSIRpas renseigné avec une valeur, ou si une correspondance est introuvable dans la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour afficher toute donnée d'enrichissement de CI correspondante trouvée lors de l'analyse de vos actifs. Pour plus d'informations sur les champs Élément de configuration et Autre élément de configuration dans un incident de sécurité, reportez-vous à la section Définir des conditions de déclenchement avec un champ d'élément de configuration (CI) pour un McAfee ePO profil.

Balises de sécurité

Pour vous aider à suivre l'état des ordinateurs hôtes isolés et le moment où des analyses de programmes malveillants sont lancées, une fonctionnalité de balisage facultative est disponible. Par défaut, cette option est désactivée dans le formulaire de configuration des profils. Si cette option est activée lors de l'étape de configuration, les noms des balises de sécurité sont affichés sur le formulaire de configuration. Il s'agit des noms des balises qui s'affichent dans les incidents de sécurité associés. Ces balises vous informent lorsqu'une action d'isolement de l'hôte est initiée avec succès et lorsqu'elle est approuvée. Une fois qu'un hôte est renvoyé avec succès au réseau, la balise de sécurité est automatiquement supprimée de l'incident de sécurité. Pour les analyses de programmes malveillants, une balise s'affiche sur l'incident de sécurité connexe lorsqu'une analyse est planifiée. Une fois l'analyse terminée, la balise planifiée est automatiquement remplacée par une balise qui indique que l'analyse est terminée avec succès.

Déclenchement automatique basé sur l'incident

Lorsque l'option Déclenchement automatique basé sur l'incident est activée, le créateur de conditions de filtre est disponible et vous devez définir des conditions de filtrage qui spécifient quand le profil s'exécute automatiquement. Les filtres courants sont Catégorie : activité de code malveillant™ et Impact sur l'entreprise est 1 - Critique™. Avec ces filtres, seuls les incidents de sécurité associés à un code malveillant et ayant un impact critique sur l'entreprise lancent le profil. L'utilisation de l'option Déclenchement automatique peut réduire le nombre d'incidents de sécurité qui invoquent automatiquement le profil.

Approbations

Si votre organisation souhaite un niveau de contrôle supplémentaire sur des actions telles que l'isolement des ordinateurs hôtes et le lancement d'analyses de programmes malveillants, vous pouvez activer l'option Exiger l'approbation pendant l'étape de configuration d'un profil.

Par exemple, si les fonctionnalités d'approbation et de balisage sont activées pour un profil, après qu'une demande d'isolement d'un ordinateur hôte ou de retour sur le réseau est soumise pour approbation, l'incident de sécurité associé est automatiquement balisé et l'action est initiée. Les demandes sont envoyées pour approbation à un utilisateur ayant le rôle sn_si.admin par défaut, mais cette approbation peut être réaffectée à une autre personne ou à un groupe d'approbation pour répondre aux besoins de votre organisation. Les approbateurs traitent les demandes dans **Mes approbations** au sein de leurs Now Platform® instances. Les balises de sécurité sont affichées sur les incidents de sécurité

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

associés. Toutes les activités du workflow sont également enregistrées dans des notes de travail pour créer une piste d'audit.

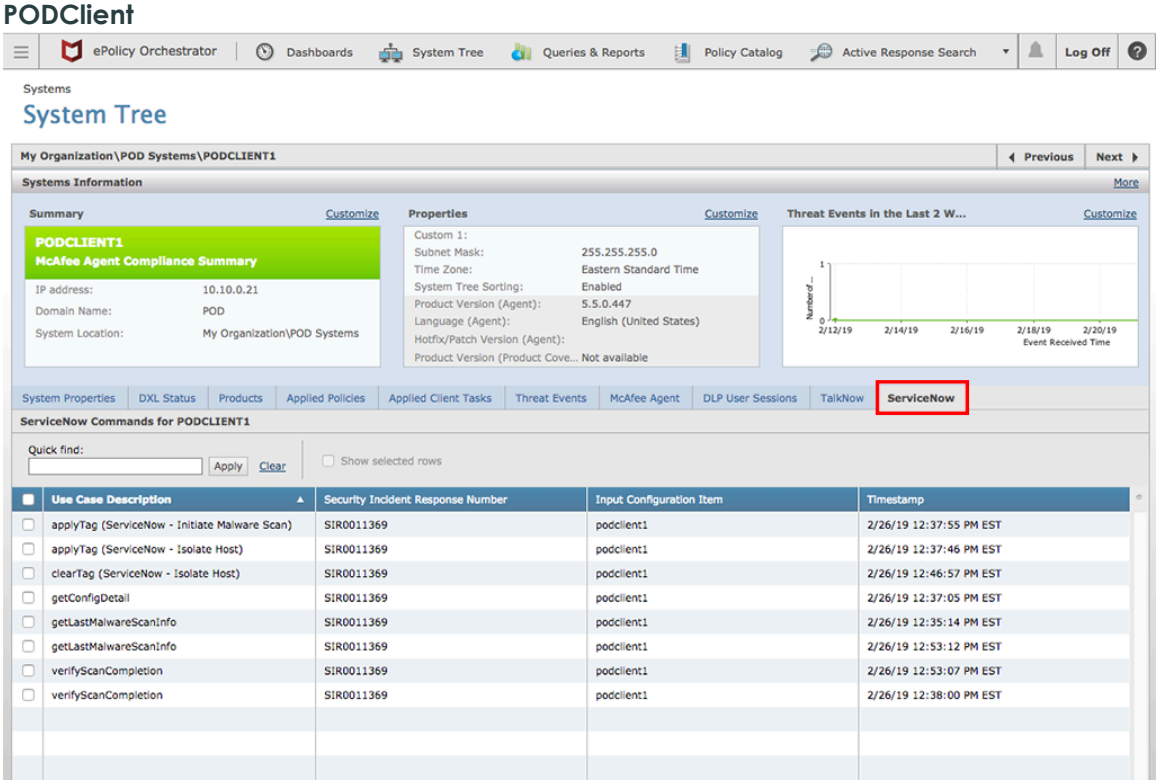
ServiceNow Journal d'audit dans la McAfee ePO console

Dans la version 5.10.0 de , un ServiceNow onglet s'affiche McAfee ePOavec un journal des commandes qui sont lancées à partir de votre Now Platform® instance. Une fois qu'une action ou une requête est appelée à partir d'un profil dans votre Now Platform® instance sur un ordinateur hôte (point de terminaison) dans la McAfee ePO console, un journal d'audit des ServiceNow commandes est créé dans la McAfee ePO console. Ce journal s'affiche dans l'arborescence système de la McAfee ePO console et vous aide à vérifier les heures des commandes envoyées à des points de terminaison spécifiques. Pour afficher les événements consignés ServiceNow sur des ordinateurs spécifiques dans une McAfee ePO console, procédez comme suit.

1. Accédez à l'arborescence du système dans votre McAfee ePO console et localisez l'onglet ServiceNow .
2. Cliquez sur l'onglet pour ouvrir une liste d'ordinateurs hôtes.
3. Dans la colonne Nom, cliquez sur un nom d'hôte pour ouvrir le journal d'audit.

L'image suivante montre un exemple de journal pour un hôte (`PODCLIENT1`).

PODClient



Les événements initiés à partir des profils de votre Now Platform® instance sont enregistrés et affichés dans le journal. Vérifiez en vérifiant l'état de l'ordinateur hôte que les événements répertoriés dans le journal sont effectués avec succès sur l'hôte.

Exemples de profils

Les rubriques suivantes comprennent des exemples sur la façon de configurer les profils et de tester les incidents de sécurité. Ces exemples incluent des McAfee ePO profils pour toutes les options disponibles pour cette intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les profils et les incidents de sécurité pour les requêtes d'enrichissement du système pour l'intégration McAfee ePO

Configurez les paramètres de votre profil afin que le profil se déclenche uniquement dans les conditions que vous définissez.

Avant de commencer

Rôle requis : Now Platform® administrateur d'incident de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Définissez les conditions qui déclenchent automatiquement les McAfee ePO options que vous avez sélectionnées pour le profil. Vous pouvez également sélectionner un autre champ d'entrée pour le champ Élément de configuration (CI). Dans cet autre champ, vous pouvez définir des conditions de filtrage afin que seuls les incidents de sécurité liés à votre événement déclencheur déclenchent automatiquement le profil.

Procédure

1. Si la page de configuration n'est pas affichée, cliquez sur **Configuration** dans la barre de progression.
2. Renseignez les champs du formulaire

Option	Description
Activer un champ de déclenchement CI alternatif	Champ de déclenchement d'autre élément de configuration (CI). La valeur par défaut est effacée. Lorsque cette case est décochée et que l'option de champ de déclenchement CI alternatif est désactivée, un autre champ CI n'est pas identifié. Si cette option est désactivée, une valeur pour le champ CI doit être renseignée sur un SIR incident de sécurité et la valeur du champ doit être reconnue par la McAfee ePO console avant que le profil ne collecte les données d'enrichissement. Cochez cette case si vous pensez que le champ CI ne sera pas renseigné lors de la création de l'incident, mais que les informations CI seront renseignées dans un autre champ de l'incident de sécurité. Lorsque cette option est activée, la liste de choix des champs de déclenchement CI alternatifs s'affiche. Choisissez un autre champ dans la liste de choix pour vérifier vos critères de recherche de CI. Pour plus d'informations sur les champs de déclenchement CI alternatifs, reportez-vous à la section Définir des conditions de déclenchement avec un champ d'élément de configuration (CI) pour un McAfee ePO profil.

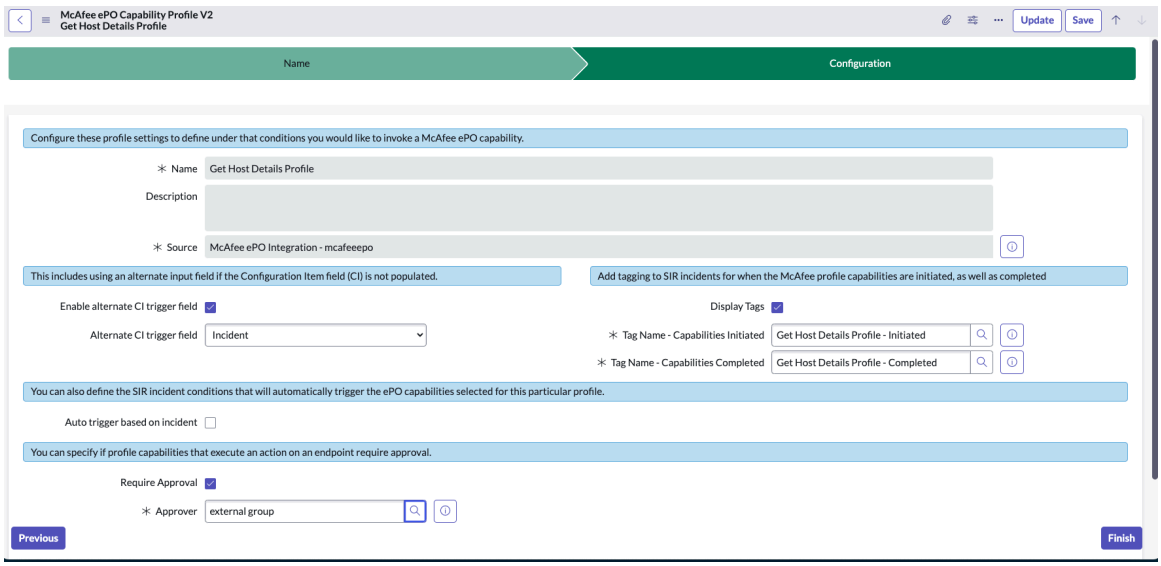
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Balises d'affichage	Les balises de sécurité sont affichées sur les incidents de sécurité. La valeur par défaut est effacée. Lorsque cette case est décochée et que l'option de marquage est désactivée, aucun nom de balise de sécurité n'est affiché sur le formulaire de configuration et les balises ne sont pas affichées sur les incidents de sécurité associés. Pour cet exemple, l'option balises de sécurité est désactivée.
Déclenchement automatique basé sur l'incident	Conditions de filtre. La valeur par défaut est effacée. Lorsque la case est décochée et que l'option est désactivée, le profil doit être invoqué manuellement à partir d'un incident de sécurité. Lorsque cette option est activée, le Créateur de conditions de filtre s'affiche. Vous devez définir les conditions de filtrage afin de spécifier quand le profil s'exécute automatiquement lors de la création d'un incident. Un exemple courant de filtre pour un profil qui exécute des requêtes d'enrichissement est `Catégorie est Activité de code malveillant` et Impact `sur l'entreprise est 1-Critique`. Ces conditions de filtre vous aident à localiser les incidents liés à des types spécifiques d'événements de sécurité et vous aident à limiter le nombre d'incidents de sécurité que vous devez examiner. Ces paramètres de filtre restent enregistrés jusqu'à ce que vous les changiez, et ils peuvent être modifiés pendant l'étape d'incident de prévisualisation et de test de la configuration.
Exiger l'approbation	Option d'approbation de la demande. La valeur par défaut est effacée. Cette option d'approbation est disponible pour tous les profils. En général, les approbations sont utilisées pour les options qui appellent des actions telles que l'isolement de l'hôte et les analyses de programmes malveillants. Lorsque la case est décochée et que cette option est désactivée, aucune demande d'approbation n'est envoyée. Pour cet

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	exemple, aucune autorisation préalable n'est requise pour les requêtes d'enrichissement du système.



3. Pour activer l'option de champ CI alternatif et définir les conditions de filtrage qui invoquent automatiquement ce profil, procédez comme suit.

a. Cochez la case **Activer un champ de déclenchement CI alternatif** .
Le champ de déclenchement CI alternatif s'affiche. Dans cet exemple, en tant qu'utilisateur disposant du rôle sn_si.admin, vous pensez que le champ CI ne sera pas renseigné sur l'incident de sécurité lors de sa création. Sinon, vous pensez que les informations CI pour un nom de domaine complet, un nom d'hôte ou une adresse IP seront renseignées dans le champ `CI identifié` de l'incident de sécurité et vous sélectionnez le champ CI identifié comme alternative. Le CI identifié est sélectionné pour cet exemple, mais vous pouvez utiliser n'importe quel champ de l'incident de sécurité pour l'autre CI.

b. Dans la liste de choix **Champ de déclenchement CI alternatif** qui s'affiche, sélectionnez le champ **CI identifié** .

Tous les champs disponibles sur l'incident de sécurité sont affichés dans la liste, y compris les champs personnalisés. Dans le champ de déclenchement CI alternatif, le `CI identifié` s'affiche.

Lorsque ce profil est invoqué et que le champ CI n'est pas renseigné pour l'incident de sécurité associé lors du déclenchement de l'événement initial, le profil utilise également la valeur du champ CI identifié dans la recherche.

c. Cochez la case **Déclenchement automatique basé sur l'incident** .
Le générateur de conditions de filtre s'affiche. Cette option permet de définir les conditions de filtrage et de spécifier quand le profil est appelé automatiquement lors de la création d'un incident de sécurité.

d. Définissez les conditions d'incident SIR qui déclencheront automatiquement les options ePO sélectionnées pour ce profil particulier.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Si les options de profil qui exécutent une action sur un point de terminaison nécessitent une approbation, cochez la case **Exiger l'approbation** .

f. Sélectionnez une approbation à l'aide de l'icône de recherche.

4. Cliquez sur **Terminer**.
Vous avez configuré le profil pour qu'il se déclenche automatiquement lors de la création de l'incident et qu'un autre champ soit utilisé pour renseigner les résultats de CI correspondants.

Déclencher McAfee ePO manuellement un profil à partir d'un incident de sécurité

Déclencher manuellement un profil d'aptitude à partir d'un Now Platform Réponse aux incidents de sécurité (SIR) incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

Remarque : L'option d'approbations du module d'extension s'affiche Configuration des profils pour l'intégration McAfee ePO uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte.

Pourquoi et quand exécuter cette tâche

Vous pouvez appeler automatiquement une demande d'obtention des détails de l'hôte, d'isolement de l'ordinateur hôte ou de suppression de l'isolement d'un ordinateur si les conditions de déclenchement que vous spécifiez dans le profil correspondent aux conditions des incidents de sécurité. Si vous souhaitez soumettre une demande manuellement, vous pouvez également la soumettre directement à partir d'un incident de sécurité.

Une fois que vous avez activé le profil, en fonction des conditions de déclenchement configurées, vous pouvez afficher les résultats de la requête dans les Now Platform incidents de sécurité. McAfee ePO Les intégrations vous permettent également d'exécuter des options individuelles sur des éléments de configuration (CI) sans utiliser de profil.

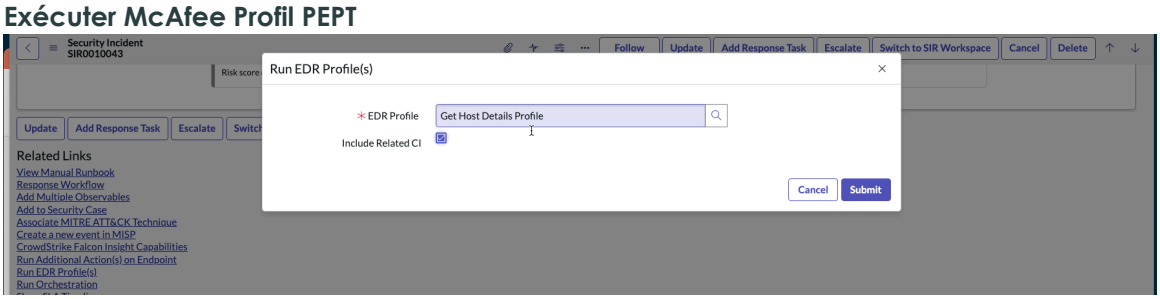
Procédure

1. Accédez à la **Tout** > **Incidents de sécurité** > **Afficher les incidents**.

2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les McAfee ePO informations.

3. Dans la section des listes connexes, sélectionnez **Exécuter le(s) profil(s) EDR**.

Exécuter McAfee Profil PEPT

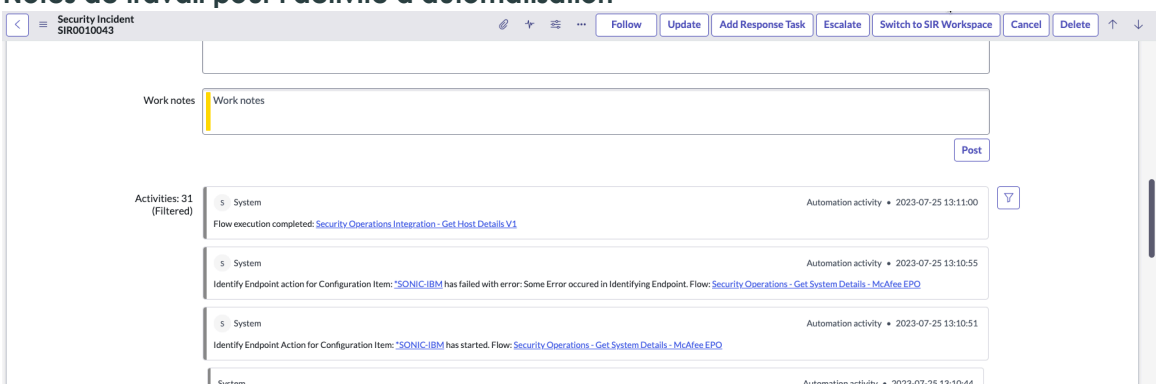


4. Parcourez et sélectionnez un profil dans la liste des profils disponibles.
La liste des profils disponibles est Obtenir les détails de l'hôte, Isoler l'ordinateur de l'hôte et Supprimer l'isolement. Par exemple, sélectionnons Obtenir les détails de l'hôte.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez **Inclure le CI connexe** pour exécuter ce profil sur tous les CI connexes du profil.
   Par exemple, si cinq CI sont associés à l'incident de sécurité, le profil sélectionné s'exécute sur les cinq CI.
6. Cliquez sur **Envoyer**.
   Le profil sélectionné est déclenché manuellement. Vous pouvez passer en revue la section des notes de travail et des activités, ainsi que les balises initiées et terminées par le profil dans la section des notes de travail.

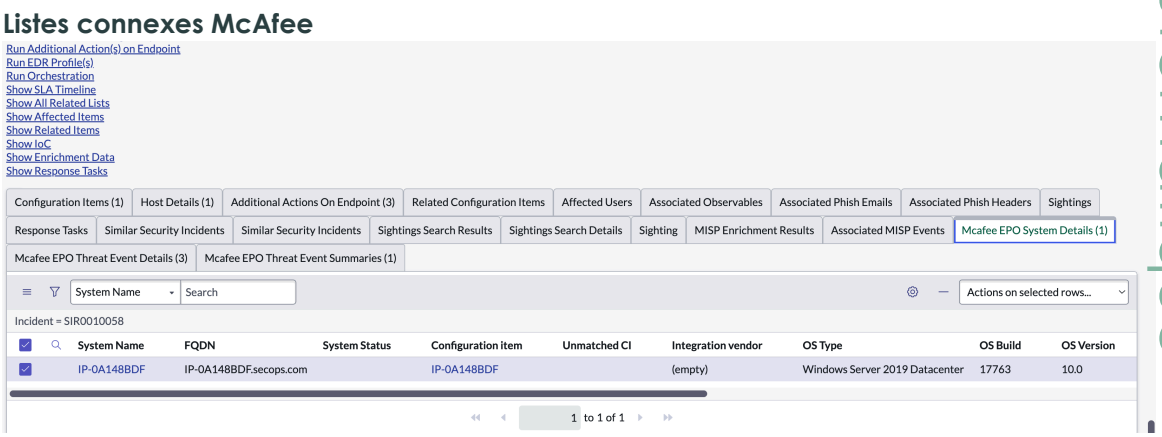
Notes de travail pour l'activité d'automatisation



Les résultats apparaissent sous la forme de listes connexes telles que Obtenir les détails de l'hôte, Isoler l'ordinateur de l'hôte ou Supprimer l'isolement.

Remarque : Toutes les tables de listes connexes étendent les tables de base. Dans cet exemple, les détails du système McAfee ePO sont une table étendue de la table de base Détails de l'hôte.

Listes connexes McAfee



7. Pour exécuter des options individuelles sur un élément de configuration (CI), procédez comme suit :

   a. Dans la liste connexe Éléments de configuration, sélectionnez le CI requis.

   b. Cliquez sur la liste déroulante **Actions sur les lignes sélectionnées...** , puis sélectionnez l'aptitude requise que vous souhaitez exécuter pour le CI sélectionné.
   Par exemple, Isoler l'hôte.

   c. Cliquez sur **Isoler l'hôte** pour l'exécuter sur le CI sélectionné.
   Le CI sélectionné est isolé du réseau.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déclencher des actions supplémentaires dans l'intégration McAfee ePO

Les options Liste des événements de menace et Lancer l'analyse anti-programme malveillant peuvent être déclenchées en exécutant des actions supplémentaires.

Avant de commencer

Rôle requis : sn_si.admin

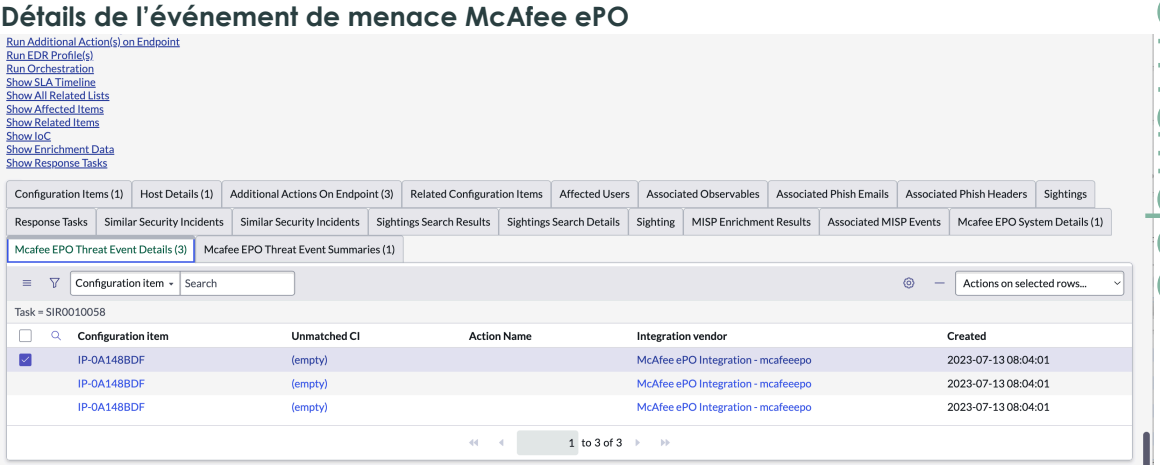
Pourquoi et quand exécuter cette tâche

Vous pouvez configurer et déclencher des actions supplémentaires dans l'intégration activée à l'aide des options **Exécuter des actions supplémentaires sur le**McAfee ePO point de terminaison, qui incluent les options Répertorier les événements de menace et McAfee ePO Lancer l'analyse McAfee ePO de programme malveillant.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité sur lequel vous souhaitez exécuter les actions supplémentaires.
3. Dans la section Liens connexes, cliquez sur **Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison**.
4. Parcourez et sélectionnez l'implémentation de l'aptitude que vous souhaitez déclencher dans la liste des actions supplémentaires.
   Par exemple, McAfee ePO Répertorier les événements de menace.
5. Sélectionnez **Inclure le CI connexe** pour exécuter cette action supplémentaire sur tous les CI connexes du profil.
   Par exemple, si cinq CI sont associés à l'incident de sécurité, le profil sélectionné s'exécute sur les cinq CI.
6. Cliquez sur **Exécuter des actions supplémentaires**.

Détails de l'événement de menace McAfee ePO



Remarque : Toutes les tables de listes connexes étendent les tables de base. Dans cet exemple, la table Détails des événements de menace McAfee ePO est une table étendue de la table de base Actions supplémentaires sur le point de terminaison.

7. Affichez et validez les détails de l'événement de menace McAfee ePO sur les listes connexes.

Utilisation de l'intégration McAfee ePO dans Analyst Workspace

Utilisez l'intégration McAfee ePO pour tirer parti des McAfee ePO options de l'espace de travail d'analyste SIR.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_si.admin

Avant d'utiliser McAfee ePO l'intégration dans l'espace de travail Réponse aux incidents de sécurité, vous devez la ServiceNow Store télécharger et la configurer. Pour plus d'informations, consultez Configurer votre Now Platform instance pour l'intégration McAfee ePO.

Pourquoi et quand exécuter cette tâche

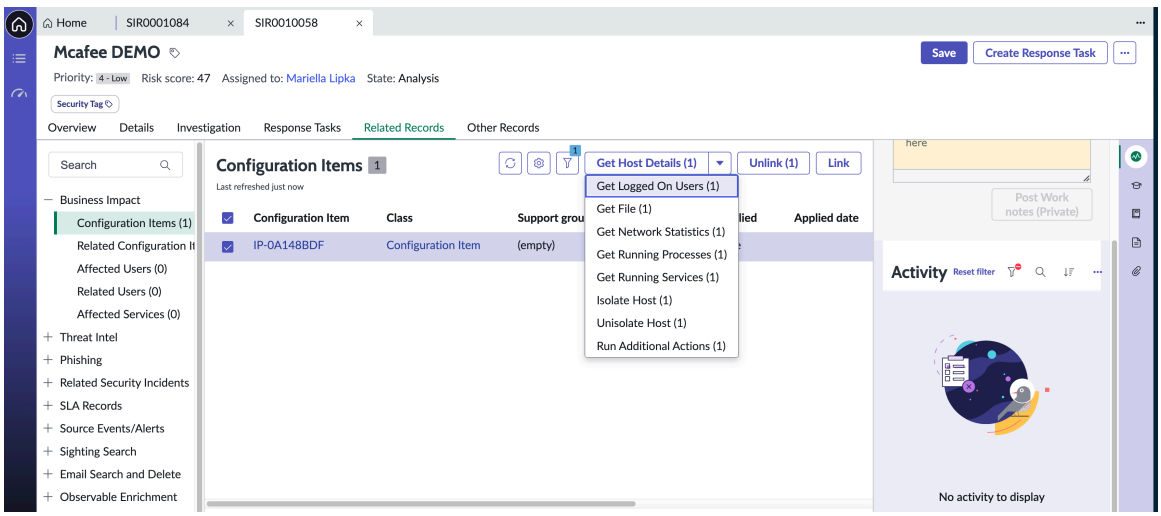
Vous pouvez utiliser l'intégration McAfee ePO pour effectuer des actions de rattrapage sur les points de terminaison en temps réel, utiliser des profils pour recueillir des détails sur l'hôte et effectuer des requêtes ou des actions spécifiques sur le point de terminaison à l'aide de l'espace Réponse aux incidents de sécurité de travail.

L'intégration McAfee ePO permet aux analystes d'utiliser les options suivantes McAfee ePO dans l'espace de Réponse aux incidents de sécurité travail Analyst :

- **Obtenir les détails de l'hôte**
- **Isoler l'hôte**
- **Supprimer l'isolement**
- **Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison**

Procédure

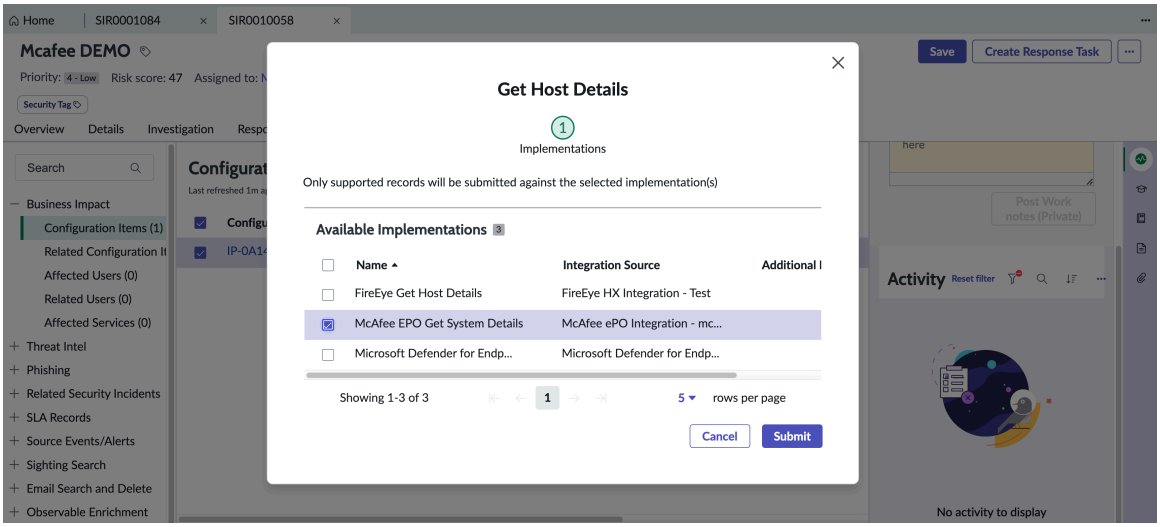
1. Pour ouvrir l'incident de sécurité dans l'espace de travail SIR, cliquez sur **Basculer vers l'espace de travail SIR** sur l'incident de sécurité.
2. Dans l'espace de travail SIR, sélectionnez l'onglet **Enregistrements connexes** .
3. Sélectionnez n'importe quel **élément de configuration**, puis choisissez une aptitude McAfee ePO à déclencher à partir de l'action déroulante de liste connexe.
   Par exemple, Obtenir les détails de l'hôte.



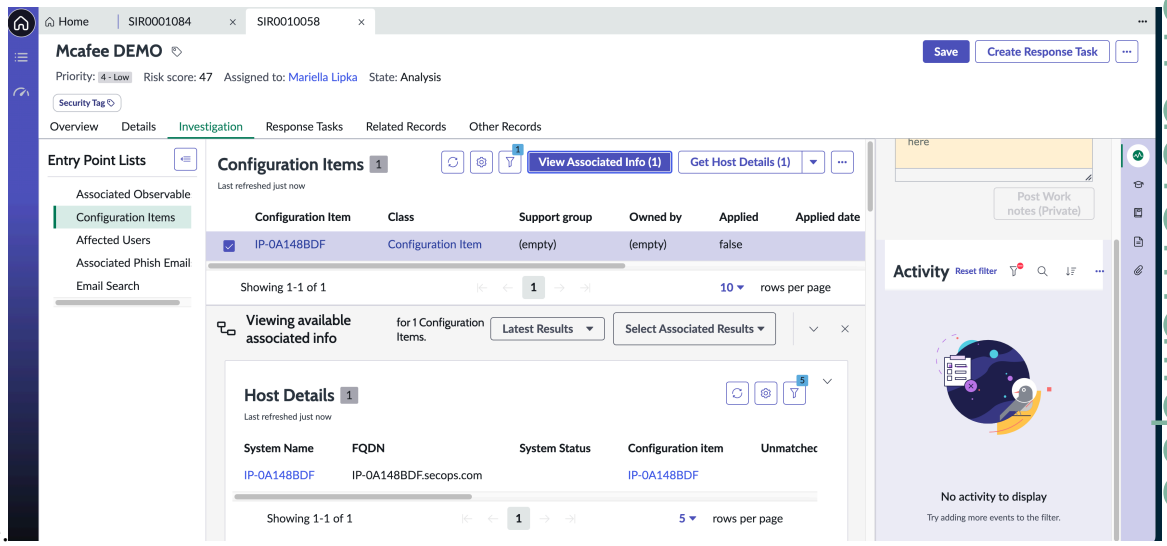
4. Dans la fenêtre contextuelle Obtenir les détails de l'hôte, sélectionnez l'implémentation **de McAfee ePO** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
   L'aptitude Obtenir les détails de l'hôte est invoquée sur le CI. Vous pouvez afficher les notes de travail pour les résultats et les conclusions.
6. Pour afficher les données de l'aptitude déclenchée, sélectionnez l'onglet **Examiner** .
7. Sélectionnez **l'élément de configuration**, puis cliquez sur l'action **Afficher les informations associées** .
   Les informations associées de l'élément de configuration s'affichent. Par exemple, Détails de l'hôte.



8. Cliquez sur **l'élément de configuration** pour afficher les détails de l'hôte.
   De même, vous pouvez essayer d'utiliser l'autre fonctionnalité de McAfee ePO pour vos incidents de sécurité sur l'espace de travail de l'analyste SIR.
9. Vous pouvez utiliser les fonctionnalités de McAfee ePO figurant sur la liste connexe **Endpoint Detection and Reponse (EDR)** pour l'analyse.
10. Parcourez et sélectionnez un profil dans la liste des profils disponibles.
    La liste des profils disponibles est Obtenir les détails de l'hôte, Isoler l'ordinateur de l'hôte et Supprimer l'isolement. Par exemple, sélectionnons Obtenir les détails de l'hôte.
11. Sélectionnez l'implémentation **de McAfee ePO** , puis cliquez sur **Envoyer**.

McAfee ESM - Intégration de l'analyseur d'e-mails

L'intégration ESM - Analyseur d'e-mails est prise en charge par un analyseur d'e-mails qui utilise les notifications par e-mail d'ESM pour créer des incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer McAfee ESM - Intégration de l'analyseur d'e-mails

L'intégration de l'analyseur d'e-mails McAfee ESM utilise les notifications par e-mail d'ESM pour diriger les workflows d'enrichissement et de réponse.

Avant de commencer

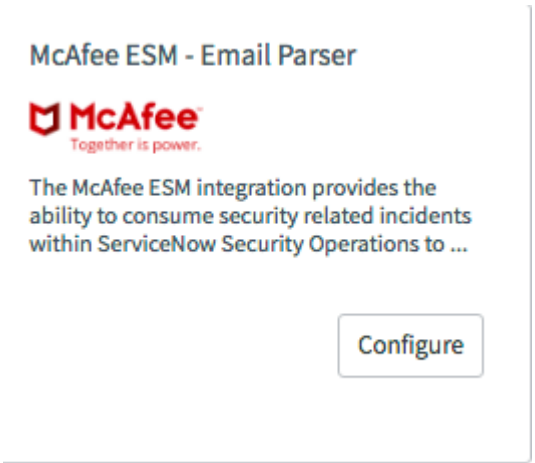
Rôle requis : sn_si_admin

Pourquoi et quand exécuter cette tâche

Un modèle d'analyseur d'e-mails McAfee ESM est fourni pour être utilisé pour l'intégration. Il doit être configuré et activé avant que l'intégration n'ait lieu. La mise à jour de l'analyseur l'active.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.



2. Dans la carte McAfee ESM - Analyseur d'e-mails, cliquez sur **Configurer**.
3. Dans la boîte de dialogue **McAfee ESM - Configuration de l'analyseur d'e-mails** , cliquez sur le lien **Configurer l'analyseur d'e-mails** .
4. Cliquez sur le lien **McAfee ESM** pour modifier les paramètres dans l'analyseur d'e-mail de modèle fourni.
   Renseignez au minimum le champ `L'e-mail provient de` . Pour créer votre propre analyseur d'e-mails, reportez-vous à la section Créer des analyseurs d'e-mails dans Security Operations.
5. Cochez la case **Actif** .
6. Cliquez sur **Mettre à jour** dans le formulaire **Analyseur d'e-mail** .
   L'analyseur d'e-mail est actif. Vous n'avez pas besoin de revenir aux **configurations d'intégration**.

McAfee ESM : intégration de l'enrichissement des incidents

McAfee ESM - L'intégration de l'enrichissement des incidents recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer	Configurer
Intégrations de Réponse aux incidents de sécurité	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Commencez avec l'intégration de l'enrichissement McAfee ESM des incidents
- Créer des enregistrements de configuration de recherche d'observations

Utiliser

- Exécuter une recherche d'observations
- Security Operations Integration - Workflow de recherche de perceptions
- Security Operations - Workflow de recherche d'observations McAfee ESM
- Afficher les détails de la recherche d'observations
- Afficher les résultats de recherche d'observations

Développer

- ServiceNow Opérations de sécurité Directives de développement de l'intégration
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté des opérations de sécurité
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Commencez avec l'intégration de l'enrichissement McAfee ESM des incidents

McAfee ESM protège les terminaux contre les virus, les logiciels espions, les chevaux de Troie et autres menaces de logiciels malveillants et s'intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l'intégration McAfee ESM d'enrichissement d'incident, vous devez la télécharger à ServiceNow Store partir du et ajouter l'URL de base API et les informations d'identification de connexion appropriées.

Avant de commencer

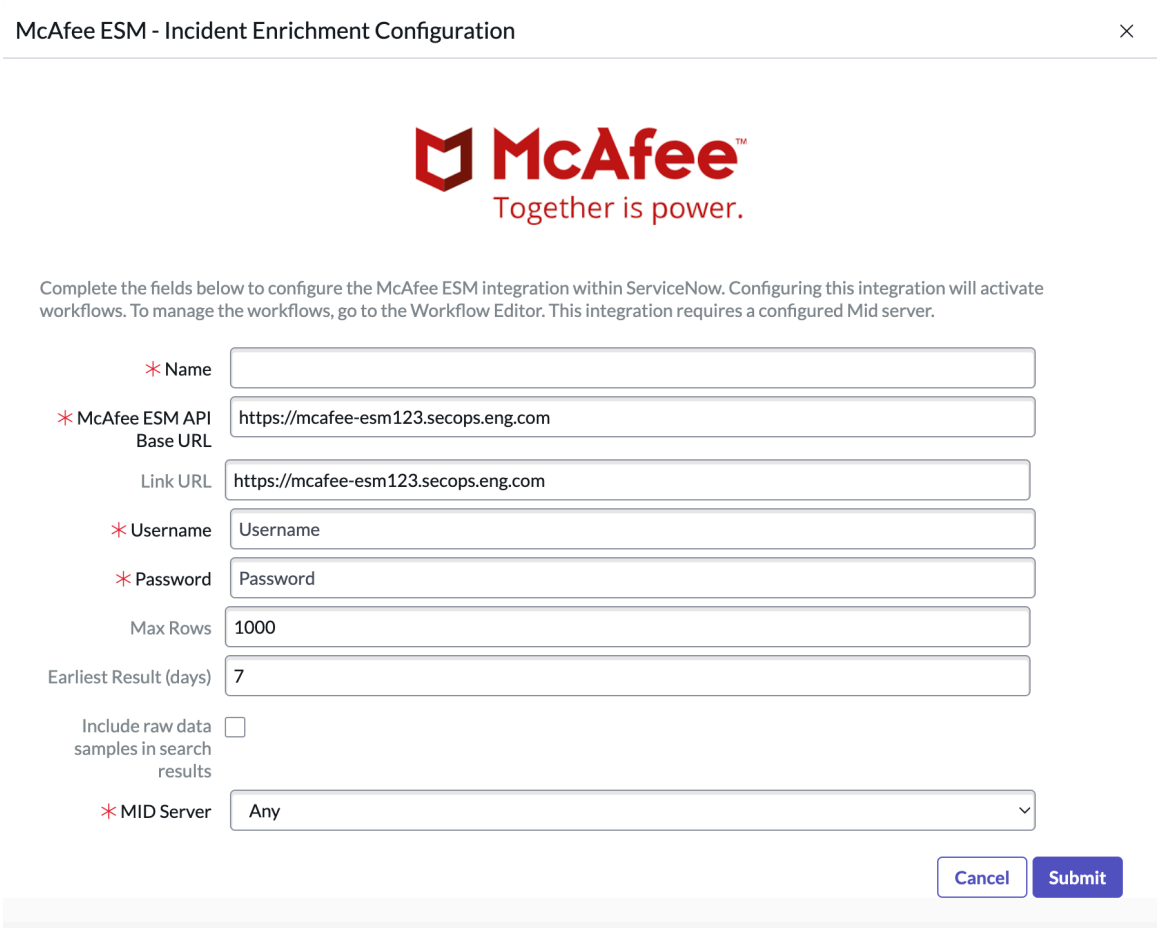
Rôle requis : sn_si_admin

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Intégrations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Sur la carte Enrichissement d'incident McAfee ESM , cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
URL de base de l'API McAfee ESM	URL de base que vous avez acquise sur le site McAfee ESM.
URL de lien	[Facultatif] URL du lien qui renvoie à une instance McAfee ESM, lorsqu'elle est disponible. **Remarque :** Si vous recevez une erreur, veuillez utiliser l'URL de base de l'API McAfee ESM.
Nom d'utilisateur	Votre nom d'utilisateur McAfee ESM.
Mot de passe	Votre mot de passe McAfee ESM.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
de données brutes dans les résultats de recherche	renvoyées dépend du paramètre que vous définissez sur le **nombre de lignes de la propriété de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	Sélectionnez **N'importe lequel** pour utiliser n'importe quel Serveur MID actif ou sélectionnez un nom de Serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

5. Cliquez sur **Envoyer**.
   La carte de configuration de l'intégration s'affiche.
6. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
7. Pour revenir à la liste initiale des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Microsoft Azure Sentinel intégration

Microsoft Azure Sentinel est une solution SIEM (Security Information Event Management) et SOAR (Security Orchestration Automated Response) basée sur le cloud. Vous pouvez utiliser l'intégration Microsoft Azure Sentinel pour ingérer des incidents Azure Sentinel et créer automatiquement des incidents de sécurité dans Réponse aux incidents de sécurité.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

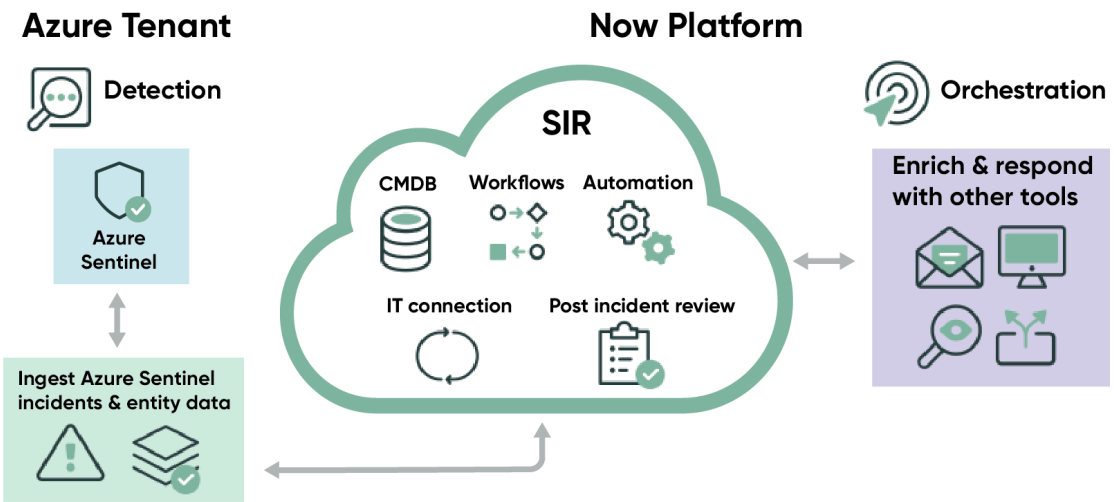
Vue d'ensemble

Consultez le diagramme suivant pour savoir comment Microsoft Azure Sentinel s'intégrer Now Platform Opérations de sécurité aux applications.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Now Platform - Azure Sentinel integration overview



Fonctionnalités principales

Utilisez les fonctionnalités clés de cette intégration pour effectuer les actions suivantes :

- Détectez Microsoft Azure Sentinel les incidents candidats aux incidents de sécurité et automatisez la création de ces incidents de sécurité.
- Mappez Microsoft Azure Sentinel les champs d'incident et d'entité aux champs d'incident SIR de sécurité.
- Filtrer Microsoft Azure Sentinel les incidents.
- Regroupez les incidents en incidents de sécurité ouverts existants afin de ne pas avoir à créer des incidents de sécurité en double.
- Automatisez les mises à jour de l'état des Microsoft Azure Sentinel incidents pour Réponse aux incidents de sécurité afin de pouvoir créer et fermer des incidents de sécurité.

> **Remarque :** ServiceNow Met à jour l'état des Microsoft Azure Sentinel incidents en fonction de la création ou de la fermeture de l'incident de sécurité. Cette mise à jour inclut également des commentaires sur les incidents regroupés et les nouveaux incidents.

- Planifiez l'ingestion d'incident pour créer des incidents de sécurité périodiquement.
- Synchronisez les commentaires d'incident avec SIR les Microsoft Azure Sentinel notes de travail.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
Microsoft site web de la documentation produit	Site web de la documentation produit Microsoft
ServiceNow site web de la documentation produit	Site web de la documentation produit ServiceNow

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise en route de l'intégration Microsoft Azure Sentinel

Activez et configurez le Microsoft Azure Sentinel - Ingestion des incidents module d'extension for Security Operation pour qu'il s'interface avec votre instance et Réponse aux incidents de sécurité votre Now Platform produit.

Avant de commencer

Rôle requis : Microsoft Azure développeur d'application, Microsoft Azure administrateur locataire

Avant de pouvoir utiliser l'intégration Microsoft Azure Sentinel , vous devez la télécharger à ServiceNow Storepartir du fichier .

Pourquoi et quand exécuter cette tâche

Passez en revue la liste de vérification de configuration suivante et vérifiez que vous avez effectué toutes les tâches pour une intégration fluide.

Liste de vérification

Tâche de configuration	Description
Affectez et vérifiez les rôles requis Now Platform et Réponse aux incidents de sécurité .	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • Le rôle administrateur installe l'intégration à partir du ServiceNow Store rôle sn_si.admin et lui attribue le rôle. • Le rôle sn_si.admin effectue les tâches suivantes : ◦ Configure l'intégration. ◦ Crée des profils d'incidents. ◦ Mappe les champs de Microsoft Azure Sentinel données d'incident aux champs d'incident de sécurité. ◦ Planifie l'ingestion d'incident en cours. ◦ Active les mises à jour d'incident lorsqu'un Réponse aux incidents de sécurité incident est créé ou fermé. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst).
Affectez les Microsoft Azure rôles requis.	Les rôles suivants sont nécessaires pour Microsoft Azure enregistrer et configurer votre application : • Développeur d'application pour l'enregistrement de l'application. • Administrateur locataire pour donner des autorisations à l'application en appelant le point de terminaison de consentement de l'administrateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant de configurer cette intégration.	Le module d'extension ServiceNow Hub d'intégration Starter Pack Installer [com.glide.hub.integrations] est requis. Le Réponse aux incidents de sécurité module d'extension (com.snc.security_incident) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si ces applications ne sont pas déjà installées, vous devez installer et activer chaque application une par une dans l'ordre suivant pour garantir une installation fluide : **1.** Réponse aux incidents de sécurité **2.** Interface utilisateur Réponse aux incidents de sécurité **3.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **4.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
Enregistrez et configurez votre application dans le Microsoft Azure portail.	Enregistrez votre application dans le Microsoft Azure portail et accordez à vos utilisateurs un accès en lecture et en écriture à l'application.

Traduction automatique

Enregistrer et configurer le Microsoft Azure portail

Enregistrez votre application dans le Microsoft Azure portail et accordez à vos utilisateurs un accès en lecture et en écriture à l'application.

Avant de commencer

Rôle requis : Microsoft Azure développeur d'application, Microsoft Azure administrateur locataire

Procédure

1. Connectez-vous au Microsoft Azure portail.

2. Recherchez et sélectionnez **Inscriptions d'application**.

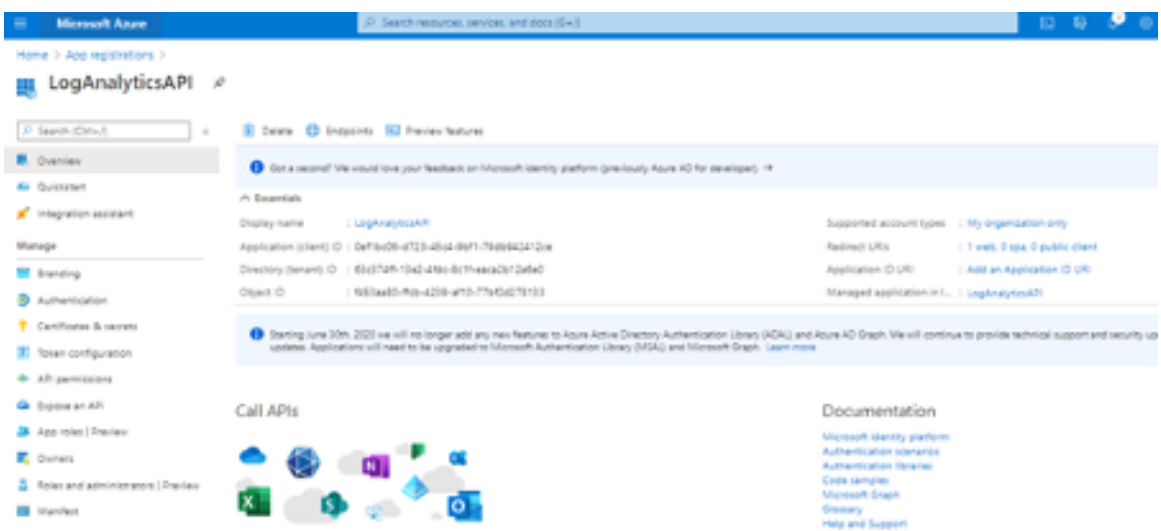
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Nouvelle inscription**.
4. Renseignez les champs du formulaire.

Enregistrer un formulaire d'application

Champ	Description
Nom	Nom d'affichage utilisateur de l'application. Par exemple, LogAnalyticsAPI.
Types de compte pris en charge	Type de compte qui peut utiliser cette application ou accéder à l'API.
URI de redirection	URI de redirection. La réponse d'authentification est dirigée vers cet URI après l'authentification réussie d'un utilisateur.

5. Cliquez sur **Inscrire**.
Une fois l'application enregistrée, la page Vue d'ensemble s'affiche.



6. Accédez à la **Gérer** > **Certificats et secrets**.
7. Dans la section Secrets client, cliquez sur **Nouveau secret client**.
Vous ne pouvez pas afficher le secret client ultérieurement, alors assurez-vous de copier et d'enregistrer le secret client maintenant à cette étape. Si vous oubliez le secret client, vous pouvez en générer un nouveau en suivant les instructions des étapes 4 et 5.
8. Accédez à la **Gérer** > **Autorisations d'API**.
9. Cliquez sur **Ajouter une autorisation**.
10. Dans la fenêtre Demander les autorisations d'API, cliquez sur l'onglet **API utilisées par mon organisation** .
11. Recherchez et sélectionnez le nom de l'application **de l'API d'analyse de journaux** .
12. Dans les autorisations de l'API Log **Analytics, sélectionnez Autorisations d'application**.
L'activation de cette autorisation garantit que l'application s'exécute en tant que service ou démon d'arrière-plan sans utilisateur connecté.
13. Dans la section Données, sélectionnez **Data.Read**
14. Cliquez sur **Ajouter des autorisations**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les autorisations sont mises à jour.

15. Activez l'option **Accorder le consentement de l'administrateur pour le répertoire par défaut** pour l'autorisation d'API Data.Read que vous avez activée à l'étape 13.
16. Recherchez et sélectionnez **les espaces de travail Log Analytics**.
17. Sélectionnez votre espace de travail Sentinel Log Analytics.
    La page Vue d'ensemble de l'espace de travail Sentinel Log Analytics s'affiche.
18. Accédez à la **Contrôle d'accès (IAM)** > **Affectations de rôle**.
19. Cliquez sur **Ajouter**, puis sélectionnez **Ajouter l'affectation d'un rôle**.
20. Renseignez les champs du formulaire.

Formulaire Ajouter une affectation de rôle

Champ	Description
Rôle	Type de compte qui peut utiliser cette application. Sélectionnez **Azure Sentinel Responder**.
Affecter l'accès à	Périmètre des autorisations que vous définissez. Sélectionnez **l'utilisateur**, **le groupe** ou **le principal du service**.
Sélectionner	Application que vous avez créée précédemment à l'étape 4. Par exemple, LogAnalyticsAPI.

21. Cliquez sur **Enregistrer**.

Installer et configurer l'intégration Microsoft Azure Sentinel

Installez et configurez l'intégration Microsoft Azure Sentinel à partir de ServiceNow Store sur votre Now Platform instance pour commencer à ingérer les incidents Azure Sentinel.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Téléchargez l'intégration Microsoft Azure Sentinel à partir de et ServiceNow Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la Microsoft Azure Sentinel mosaïque et cliquez sur **Configurer**.
4. Renseignez les champs du formulaire.

Microsoft Azure Sentinel - Formulaire de configuration de l'ingestion d'incidents

Champ	Description
Nom	Nom de la configuration d'instance Microsoft Azure Cloud .
URL d'identité	URL d'identité pour le Microsoft Azure Cloud locataire. Par exemple, `login.microsoftonline.com`. Pour en

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	savoir plus, consultez la documentation Microsoft Azure .
Gestionnaire de ressources Azure	Point de terminaison Azure Resource Manager pour Microsoft Azure Cloud le locataire. Par exemple, `management.azure.com`. Pour en savoir plus, consultez la documentation Microsoft Azure .
ID de locataire	Microsoft Azure Sentinel ID de locataire. Il s'agit de l'instance à partir de laquelle tous les incidents du Microsoft Azure portail sont récupérés.
ID client	ID client de l'application que vous avez enregistrée dans le Microsoft Azure portail.
Secret client	Secret client pour votre application enregistrée.
ID d'abonnement	ID d'abonnement pour votre application enregistrée.
Nom du groupe de ressources	Nom du groupe de ressources pour votre application enregistrée.
Nom de l'espace de travail	Nom de l'espace de travail de votre application enregistrée.

5. Cliquez sur **Envoyer**.

Résultats
Une fois la configuration validée et envoyée avec succès, chaque configuration du serveur d'ingestion d'incident est enregistrée sous forme de vignette sur la page Intégrations de sécurité.

Créer un profil pour Microsoft Azure Sentinel

Créez un profil d'incident dans votre Now Platform instance et déterminez les Microsoft Azure Sentinel incidents qui conviennent à la création d'incidents de sécurité.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
L'intégration vous permet de créer différents types d'incidents, tels que les tentatives d'accès non autorisé et les programmes malveillants. Ces incidents sont créés en fonction des profils que vous configurez dans l'instance Now Platform . Tous les incidents sont initialement créés pour un type d'incident configuré dans un profil. Les incidents créés peuvent ensuite être filtrés pour spécifier quels incidents créent des incidents de sécurité.

Tous les incidents qui répondent aux critères de sélection de votre Microsoft Azure locataire et qui sont disponibles via l'API Microsoft Azure Sentinel sont initialement ingérés dans votre Now Platform instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Intégration de Microsoft Azure Sentinel** > **Profil d'incident Azure Sentinel**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Microsoft Azure Sentinel - Formulaire de configuration de l'ingestion d'incidents

Champ	Description
Nom	Nom du profil. Ce nom vous aide à identifier le type de profil et est également le nom par défaut de la balise de sécurité associée à ce profil.
Actif	Indicateur indiquant que le profil est actif. Lorsque le profil est actif, cela implique que le Now Platform interroge activement les incidents Azure Sentinel et que les incidents de sécurité correspondants sont créés SIR lorsque les conditions de filtrage sont remplies.
Source	Microsoft Azure locataire que vous avez configuré pour ingérer des incidents. Si vous avez configuré plusieurs locataires, sélectionnez le locataire approprié pour les types d'incidents que vous prévoyez d'ingérer pour le profil.
Ordre	Priorité du flux. La valeur de ce champ indique l'ordre dans lequel les flux sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux doté du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400. La valeur par défaut est 100.
Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

4. Pour accéder à la section Mappage, cliquez sur **Continuer**.

Que faire ensuite

Mappez les champs d'incident individuels Microsoft Azure Sentinel aux champs de l'incident de Now Platform SIR sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mapper les champs d'incident Microsoft Azure Sentinel

Mappez les champs d'incident individuels Microsoft Azure Sentinel aux champs de l'incident SIR de sécurité afin de pouvoir créer des incidents avec les données mappées.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Sur la page de mappage, dans la section Mappage de champs Azure Sentinel, sélectionnez l'une des méthodes d'ingestion d'échantillons.

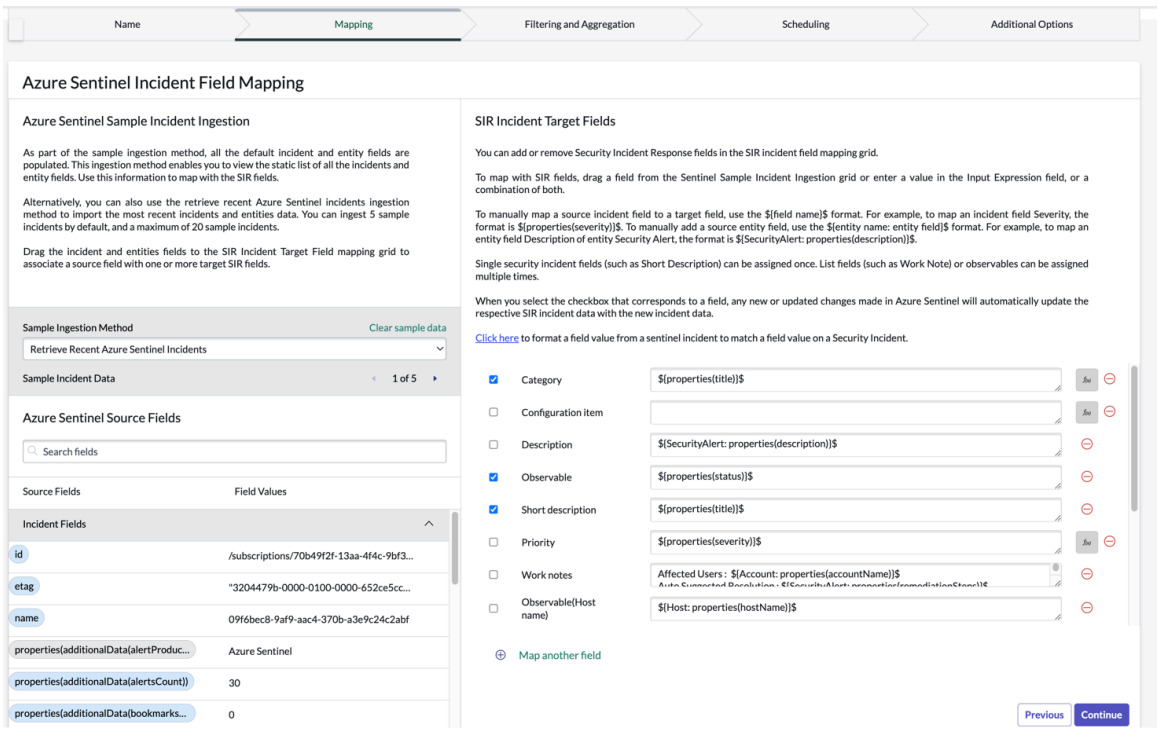
Méthodes d'intégration des exemples

Champ	Description
Tous les champs d'incident et d'entité par défaut	Utilisez cette méthode d'ingestion pour afficher la liste statique de tous les champs d'incidents et d'entité. Cette méthode contient uniquement des noms de champs par défaut sans valeurs. Vous pouvez utiliser ces informations pour les mapper avec les SIR champs.
Récupérer les incidents Azure Sentinel récents	Utilisez cette méthode d'ingestion pour importer les données d'entités et d'incidents les plus récentes. Si l'incident Azure Sentinel contient les données d'entité, celles-ci sont récupérées et disponibles pour le mappage dans la section Champs sources d'Azure Sentinel. Parfois, l'incident Azure Sentinel peut ne pas contenir les données de l'entité, et par conséquent les champs d'entité ne sont pas disponibles pour le mappage dans un tel scénario. Si l'incident Azure Sentinel contient plusieurs alertes, la première alerte qui fait partie de l'incident est affichée dans la section de mappage. Pendant l'ingestion également, les valeurs de champ d'alerte de sécurité les plus précoces sont utilisées. Vous pouvez ingérer 5 échantillons d'incidents par défaut et un maximum de 20 échantillons d'incidents. Les valeurs du champ d'incident d'échantillon sont renseignées lorsque le profil ingère les échantillons d'incidents. Vous pouvez mapper ces incidents aux **champs cibles des incidents SIR**. Les champs et valeurs d'incident apparaissent sous forme d'onglets individuels.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Importer des exemples de données	Cliquez sur **Importer des données d'échantillon** pour importer des échantillons d'incidents à partir d'Azure Sentinel. Ce bouton s'affiche lorsque vous sélectionnez la méthode d'ingestion Récupérer les incidents Azure Sentinel récents. La récupération d'échantillons d'incidents à partir du Microsoft Azure Sentinel serveur peut prendre un moment. Mappez ces incidents récupérés aux champs cibles **de l'incident SIR**. Les champs et valeurs d'incident apparaissent sous forme d'onglets individuels.



2. Pour ajouter des champs aux champs par défaut qui sont affichés sur l'incident de sécurité, procédez comme suit :

a. Dans la section Champs cibles de l'incident SIR, cliquez sur le Bouton Mapper un autre champ.
Il affiche une liste de SIR champs, à partir de laquelle vous pouvez sélectionner un champ pour un nouveau champ à afficher.



b. Dans la colonne Incident de sécurité, développez la liste qui s'affiche, puis sélectionnez un champ.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Plusieurs observables peuvent être affichés sur le même incident de sécurité. Par exemple, le champ **Observable** peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs **Élément de configuration** et **Notes de travail** prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, un message d'erreur s'affiche indiquant que ce champ ne prend pas en charge plusieurs valeurs. De même, si un champ d'un incident de sécurité dispose d'une liste dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affiché dans la liste, le champ ne se renseigne pas sur l'incident de sécurité.

c. Dans la section Champs sources d'Azure Sentinel, faites glisser et déposez votre champ pour le mapper à votre nouveau champ.

d. Lorsque vous cochez la case correspondant à un champ, tout changement nouveau ou mis à jour apporté dans Azure Sentinel met automatiquement à jour les données d'incident SIR respectives avec les nouvelles données d'incident.

Remarque : Dans le système de base, la propriété système sn_sec_sentinel.incident_updates est par défaut définie sur Vrai pour recevoir les Microsoft Azure Sentinel mises à jour relatives aux nouvelles alertes liées à SIR.

- Par défaut, les champs Utilisateurs affectés, Éléments de configuration et Observables sont cochés. Cela signifie que chaque fois que de nouveaux observables ou éléments de configuration associés, ou des utilisateurs affectés sont ajoutés à l'incident, ces informations sont automatiquement extraites et renseignées dans les listes connexes respectives de Security Incident Response (SIR) pendant cet intervalle d'interrogation.
- Pour tous les autres champs, vous devez cocher la case correspondant à un champ pour tout changement nouveau ou mis à jour apporté à l'enregistrement d'incident Azure Sentinel dans Azure Sentinel. Cela mettra automatiquement à jour les données d'incident SIR respectives avec les nouvelles données d'incident.

Important : Une diligence raisonnable est requise avant de sélectionner cette fonctionnalité, car le remplacement des données existantes peut entraîner une instabilité des données avec lesquelles l'analyste peut travailler et toute autre automatisation définie même par les valeurs de champ de l'incident de sécurité peut également être affectée. Il est donc très important de faire preuve de diligence raisonnable avant de sélectionner une fonctionnalité de remplacement.

3. Pour supprimer un champ, utilisez le Supprimer l'élément en regard du champ expression d'entrée dans la section Champs cibles de l'incident SIR.

4. Pour mapper une valeur de champ de la section Champs sources Azure Sentinel à un champ de la section Champs cibles d'incident SIR, utilisez l'une des actions suivantes :

a. Faites glisser le nom du champ (par exemple, ID) et déposez-le en regard d'un nom de champ dans la colonne Champs cibles de l'incident SIR.

Vous pouvez faire correspondre n'importe quelle valeur de la section Champs sources Azure Sentinel à un champ de la section Champs cibles d'incidents SIR. Les champs sont codés par couleur afin que vous ne négligez pas ou ne dupliquiez pas les champs d'incident dans le processus de mappage. Les champs bleu clair indiquent qu'un champ d'incident n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ d'incident entrant à plusieurs champs sur un

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

incident de sécurité. Un champ gris indique qu'un champ a été sélectionné et mappé à un champ sur l'incident de sécurité. De cette façon, vous pouvez visualiser quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si d'autres informations importantes sur l'incident restent non mappées.

b. Vous pouvez ajouter une combinaison de texte et de champ.
Par exemple, `le nom de l'incident est ${name}$`. Ici `, le nom de l'incident peut` être saisi manuellement tandis que `${name}$` est mappé à partir de la section des champs sources d'Azure Sentinel.

c. Vous pouvez saisir et mapper manuellement un incident source ou un champ d'entité à un champ cible.

- Pour mapper manuellement un champ d'incident source, utilisez le format ${field name}$. Par exemple, pour mapper la gravité d'un champ d'incident, le format est`${properties(severity)}$`.
- Pour ajouter manuellement un champ d'entité source, utilisez le format `${entity name : entity field}$` . Par exemple, pour mapper un champ d'entité Description de l'entité Alerte de sécurité, le format est `${SecurityAlert : properties(description)}$`.

Cette intégration classe certains sous-types d'observables. Lorsque vous mappez un champ Azure Sentinel avec le champ observable SIR, l'observable Now Platform est automatiquement classifié. Si vous souhaitez mapper de façon générique l'observable Azure Sentinel entrant au type d'observable dans SIR, faites glisser et déplacez le champ Azure Sentinel dans le champ Observable. Toutefois, si vous connaissez le type d'observable pour l'observable Azure Sentinel entrant dans SIR, effectuez un mappage spécifique au champ Type d'observable SIR . Parmi les exemples de types d'observables spécifiques, citons Observable (nom de domaine), Observable (adresse e-mail), Observable (adresse IP (V4)) et Observable (nom d'hôte SIR).

Si vos champs Azure Sentinel entrants contiennent des MITRE-ATT&CK informations, mappez-les MITRE-ATT&CK au champ Technique. Assurez-vous que le champ Azure Sentinel entrant contient l'ID ou le nom de la MITRE-ATT&CK technique.

Parfois, les valeurs de champ d'incident dans Microsoft Azure Sentinel peuvent ne pas se traduire directement dans les champs de l'incident de sécurité SIR. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez mettre en forme des valeurs similaires, mais pas identiques.

5. Pour formater la traduction d'un champ d'un nouvel champ d'un incident Azure Sentinel afin qu'elle corresponde à une valeur de champ d'un incident de sécurité, cliquez sur le lien **Cliquez ici** dans l'en-tête des **champs cibles de l'incident SIR** .

6. Pour modifier les champs qui prennent en charge la traduction des champs, cliquez sur l'icône Script  des champs pour modifier les champs qui prennent en charge la traduction des champs.
Les champs qui prennent en charge la traduction des champs sont **Catégorie**, **Élément de configuration** et **Priorité**. Par exemple, cliquez sur l'icône  à côté de la catégorie.
L'éditeur de script de traduction de champ Azure Sentinel s'ouvre.

7. Entrez les changements apportés au script et cliquez sur **Mettre à jour** pour enregistrer les changements et revenir à la page Mappage.
Par exemple, pour Catégorie, définissez les éléments suivants dans l'éditeur de script :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
"<Incoming Sentinel Incident Field Value>" : "<Category to assign to
 the Security Incident>".
```

Ce mappage garantit qu'un profil n'utilise que des catégories configurées.

8. Poursuivez votre mappage en ajoutant ou en supprimant des valeurs de champ.
   Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir les critères supplémentaires qu'un incident entrant doit satisfaire pour créer un incident de sécurité.
9. Pour passer à la section Filtrage et agrégation, cliquez sur **Continuer**.

Que faire ensuite

Définissez et définissez des conditions de filtre afin de pouvoir spécifier quels incidents doivent créer des incidents de sécurité. Vous pouvez utiliser les mêmes valeurs de champ (définies dans la section Mappage) dans le générateur de conditions de génération d'incident (dans la section Filtrage et agrégation) pour définir les critères supplémentaires qu'un incident entrant doit satisfaire pour créer un incident de sécurité.

Définition de critères de filtre et d'agrégation

Vous pouvez définir et paramétrer des conditions de filtre afin de pouvoir spécifier quels incidents entrants Microsoft Azure Sentinel doivent créer des incidents de sécurité. Vous pouvez également définir des critères de champ d'incident supplémentaires qui permettent d'ajouter un incident entrant à un incident de sécurité ouvert au lieu de créer un incident.

Définir les conditions de filtrage pour les incidents de sécurité

Définissez les conditions de filtrage de sorte que les incidents de sécurité ne soient créés que lorsque les conditions de filtrage correspondent.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Ce type de filtrage vous aide à isoler les incidents de sécurité et limite le nombre d'incidents de sécurité que vous créez. Si vous définissez des critères de filtrage supplémentaires, seuls les incidents requis sont ingérés sans avoir à modifier la requête ou la configuration de l'incident déclenché.

Procédure

1. Pour définir les critères qu'un incident entrant Microsoft Azure Sentinel doit satisfaire pour qu'un incident de sécurité soit créé, sélectionnez **Filtrer en fonction des conditions**.

   Les options du premier champ des conditions de filtre correspondent aux champs affichés dans la section Ingestion d'échantillons d'incidents Azure Sentinel pour l'incident que vous avez ingéré. Ces champs sont dynamiques et changent en fonction de l'incident que vous ingérez. Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'incident.

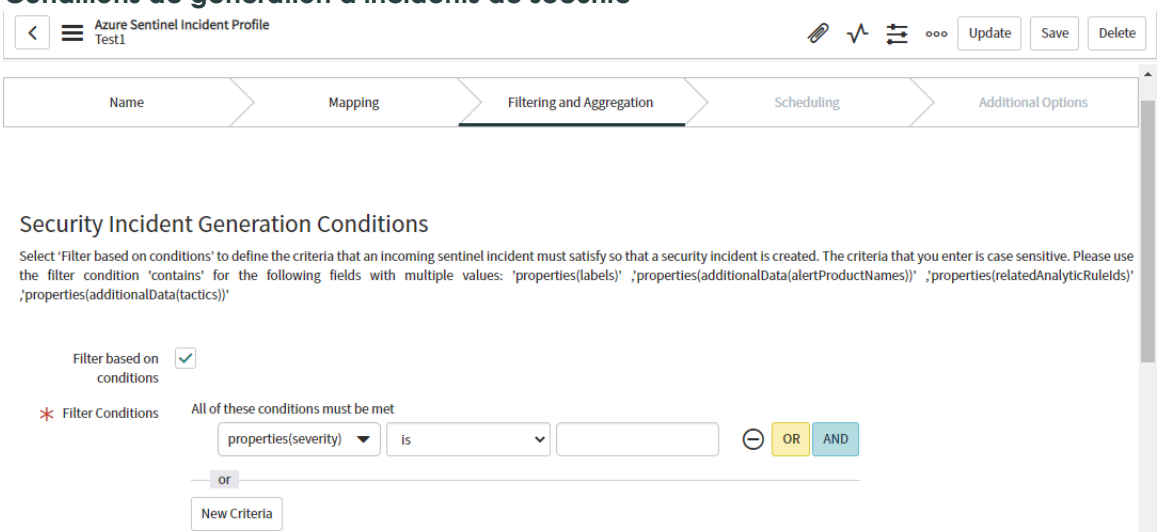
   Utilisez la condition de filtre *contenue* pour les champs à valeurs multiples suivants :

   - properties(labels)
   - properties(additionalData(alertProductNames))
   - properties(relatedAnalyticRuleIds)
   - properties(additionalData(tactics))

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étant donné que la condition de filtre ne peut récupérer que des chaînes, vous devez utiliser la condition de filtre *contient* pour les champs ci-dessus afin de vous assurer que les données sont filtrées correctement.

Conditions de génération d'incidents de sécurité



2. À l'aide des listes et des champs du générateur de conditions, définissez les filtres pour la première ligne.
3. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.

Définir les conditions d'agrégation

Définissez des critères d'agrégation d'incidents supplémentaires qui regroupent un incident entrant en un incident de sécurité SIR existant au lieu de créer des incidents similaires potentiellement dupliqués. Lorsque vous utilisez des critères de valeur de correspondance de champ pour chaque profil, cette agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données des incidents associés sur un seul incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Si un nouvel incident correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation de l'étape de mappage, l'incident est automatiquement ajouté au dernier incident de sécurité ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher tous les incidents agrégés ajoutés dans une liste connexe sur un incident de sécurité.
Tous les incidents regroupés sur un incident de sécurité sont affichés dans la liste connexe Incidents regroupés d'Azure Sentinel. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi des incidents sont ajoutés aux incidents de sécurité existants.

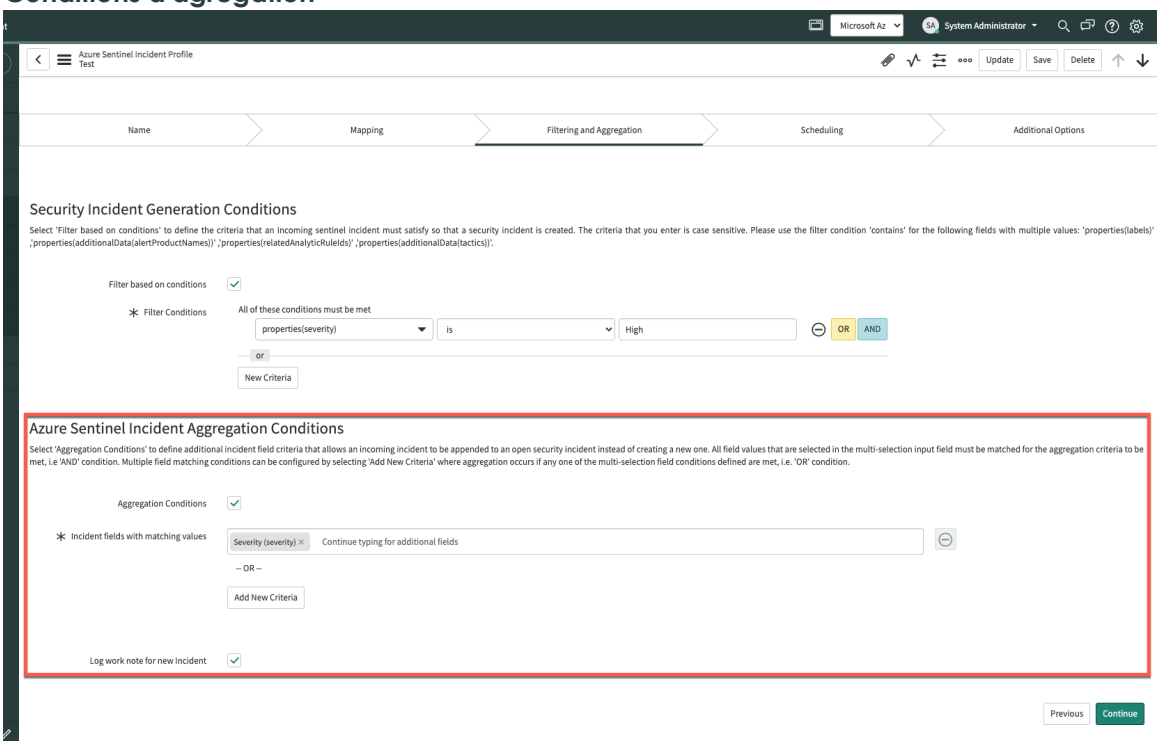
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Pour définir des critères de champ d'incident supplémentaires qui permettent d'ajouter un incident entrant Microsoft Azure Sentinel à un incident de sécurité ouvert au lieu de créer un nouvel incident, sélectionnez l'option **Conditions d'agrégation** comme illustré dans la figure suivante.

Conditions d'agrégation



2. Dans le champ **Champs d'incident avec des valeurs correspondantes** , saisissez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre Now Platform instance.
   Toutes les valeurs de champ que vous avez sélectionnées dans le champ d'entrée de sélection multiple doivent correspondre afin que les critères d'agrégation soient remplis et que cet incident entrant puisse être ajouté à un incident de sécurité existant. Cette sélection implique qu'il s'agit d'une condition *ET* dans laquelle les champs, tels que les observables et les éléments de configuration qui peuvent avoir plusieurs valeurs de champ, leur sont mappés. Si seul un sous-ensemble de valeurs est mis en correspondance, les conditions d'agrégation d'incidents Azure Sentinel ne sont pas remplies et un nouvel incident de sécurité est créé.
3. Pour ajouter plusieurs conditions de correspondance de champ, cliquez sur **Ajouter de nouveaux critères**
   L'agrégation se produit si l'une des conditions de champ de sélection multiple que vous définissez est remplie. Cette sélection implique la condition *OU*.
4. Pour mettre à jour la note de travail d'un nouvel incident lorsqu'elle est ajoutée à un incident de sécurité, sélectionnez **Enregistrer la note de travail pour le nouvel incident**.

   La note de travail consigne l'ajout d'un nouvel incident et inclut un lien vers les détails de l'incident. La note de travail du journal met également à jour d'autres détails que vous ajoutez au champ Note de travail dans votre section de mappage.
5. Cliquez sur **Continuer** pour configurer le calendrier.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Définissez un calendrier pour récupérer les données d'incident et les incidents ingérés qui correspondent aux critères du profil.

Planifier la récupération de l'incident Microsoft Azure Sentinel

Définissez un calendrier pour récupérer les données d'incident et ingérer les Microsoft Azure Sentinel incidents qui correspondent aux critères du profil.

Avant de commencer
Rôle requis : sn_sni.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez planifier la fréquence à laquelle vous souhaitez interroger les Microsoft Azure Sentinel futurs incidents qui correspondent à la configuration du profil d'incident.

Pour activer l'ingestion automatisée d'incidents, vous devez configurer la planification et la récupération des incidents avant d'activer le profil. Pour définir une date et une heure spécifiques pour l'ingestion initiale, activez la **durée d'ingestion de l'incident définie**. L'ingestion suivante est basée sur la période de l'intervalle d'interrogation.

L'intervalle d'interrogation est configuré individuellement pour chaque profil. Les différents intervalles d'interrogation peuvent avoir un impact sur les performances de l'intégration d'incident Microsoft Azure Sentinel . Lors de la planification, prévoyez d'équilibrer la charge du système par rapport à l'urgence d'un incident. Une valeur par défaut d'une minute est définie pour tous les profils. Vous pouvez modifier ce paramètre en fonction de l'urgence de l'incident et de la charge prévue sur votre système.

Toutes les alertes qui sont ajoutées à l'incident dans un intervalle d'interrogation particulier ; un processus est exécuté, puis ajouté aux listes connexes d'alertes Azure Sentinel, et la note de travail est également publiée.

Procédure
1. Renseignez les champs du formulaire de planification.

   Configurez le calendrier pour définir comment et quand vous extrayez les incidents du Microsoft Azure locataire.

Formulaire de planification

Champ	Description
Intégration de l'incident en cours	Ingestion d'incident en cours que l'instance Now Platform extrait du locataire pour les Microsoft Azure nouveaux incidents. Les incidents de sécurité sont créés si des incidents déclenchés sont détectés et que les critères de filtrage de génération d'incident correspondent.
Incrémentation du sondage (minutes)	Fréquence d'interrogation définie en minutes.
Définir le délai d'intégration de l'incident	L'ingestion d'incident basée sur la date et l'heure configurées. Vous pouvez utiliser cette option pour définir une date et une heure spécifiques pour l'ingestion

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	initiale. Les ingestions suivantes sont basées sur la période de l'intervalle d'interrogation.
Délai d'intégration de l'incident d'entrée	Date et heure que vous spécifiez pour l'ingestion de l'incident.
Récupération ponctuelle	Cochez cette case pour autoriser la récupération unique des incidents Azure Sentinel historiques, puis procéder au rapprochement des données. Lorsque vous sélectionnez ce checkox, l'application extrait tous les incidents Azure Sentinel ouverts et fermés pour la période allant jusqu'à 6 mois environ. Lors du traitement des données, les incidents en cours et les données historiques sont tous deux extraits, mais le traitement des incidents en cours prévaut sur l'extraction historique. Sinon, l'extraction historique peut prendre un certain temps en fonction de la durée et du nombre d'incidents que vous ingérez. **Remarque :** Les incidents Azure Sentinel historiques récupérés sont soumis à des vérifications de déduplication afin d'éviter tout doublon dans l'application Security Incident Response.
Depuis date	Date depuis laquelle les incidents historiques sont ingérés à partir d'Azure Sentinel. **Remarque :** Les données sur les incidents sont extraites approximativement des 6 derniers mois.

La page de planification vous permet de définir comment et quand les Microsoft Azure incidents sont extraits du locataire.

2. Pour accéder à la page Options supplémentaires, cliquez sur **Continuer**.

Automatiser les mises à jour et les fermetures d'incidents en fonction de l'état de l'incident SIR

Automatiser les mises à jour et les fermetures d'incidents en fonction de leur SIR état. L'intégration Microsoft Azure Sentinel dispose d'une interface bidirectionnelle qui permet aux deux incidents de créer des incidents de sécurité et de mettre à jour les incidents après la création ou la fermeture de l'incident de sécurité.

Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Renseignez les champs du formulaire.
   Suivez les instructions pour terminer la configuration de mise à jour des incidents lorsque vous créez ou fermez un incident de sécurité dans SIR.

Formulaire Automatisation des mises à jour d'incident

Catégorie	Champ	Description
Mises à jour de création d'incident	Mettre à jour l'état des incidents Azure Sentinel à la création d'un incident SIR	Option qui vous permet d'utiliser la fonctionnalité de mise à jour automatisée des incidents. L'état Microsoft Azure Sentinel de l'incident est mis à jour dans Microsoft Azure l'incident avec les commentaires postérieurs à la création de l'incident SIR dans le Now Platform.
	Mise à jour de l'état de l'incident initial	État de l'incident initial mis à jour dans l'environnement Microsoft Azure Sentinel . Vous **pouvez sélectionner Nouveau** ou **Actif** comme état.
	Commentaires initiaux renvoyés à l'incident	Commentaires initiaux qui sont publiés sur l'incident dans l'environnement Microsoft Azure Sentinel . Modifiez le texte par défaut qui s'affiche dans la section des commentaires en ajoutant ou en modifiant les variables de substitution en utilisant le format ${nom du champ}$ pour n'importe quel champ du formulaire d'incident SIR .
Mises à jour de la clôture de l'incident	Fermer les incidents Azure Sentinel lors de la fermeture de l'incident SIR	Option qui vous permet d'utiliser la fonctionnalité de mise à jour automatisée du statut d'incident. Microsoft Azure Sentinel Les incidents sont fermés dans l'incident Microsoft Azure avec les commentaires donnés après la fermeture de l'incident SIR dans le Now Platform.
	Mise à jour de l'état de l'incident de fermeture	Mise à jour de l'état de l'incident Microsoft Azure Sentinel lorsque celui-ci est fermé dans SIR.
	Commentaires de fermeture renvoyés à l'incident	Commentaires qui sont publiés sur l'incident dans l'incident Microsoft Azure Sentinel lorsque l'incident est fermé dans SIR.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Catégorie	Champ	Description
		Modifiez le texte par défaut qui s'affiche dans la section des commentaires en ajoutant ou en modifiant les variables de substitution en utilisant le format ${nom du champ}$ pour n'importe quel champ du formulaire d'incident SIR .
	Classification des incidents et motif de fermeture	Méthode pour la classification des incidents et le motif de fermeture utilisée pour fermer l'incident dans l'environnement Microsoft Azure Sentinel . Sélectionnez la **méthode par défaut de classification des incidents et de motif de fermeture** pour fermer l'incident dans l'environnement Microsoft Azure Sentinel . Lorsque vous sélectionnez cette méthode, vous devez définir la **classification d'incident par défaut et le motif de fermeture**. Lorsque vous fermez un incident dans SIR, l'état de l'incident dans Azure Sentinel est également fermé avec la **classification d'incident par défaut et le motif de fermeture** spécifiés. Sélectionnez la méthode de **mappage de code de fermeture Classification des incidents et Motif de fermeture-SIR** pour fermer les incidents et mapper les motifs de classification aux SIR codes de fermeture. Vous pouvez mapper plusieurs SIR codes de fermeture à un seul motif de classification. Après avoir fermé un incident à SIR l'aide du code de fermeture, l'état de l'incident dans Azure Sentinel est également fermé avec la classification et le motif de fermeture de l'incident mappés. Si le motif de classification et SIR les codes de fermeture ne sont pas mappés, ou si aucune correspondance n'est trouvée, l'incident est fermé à l'aide du motif de classification par défaut « Indéterminé » dans

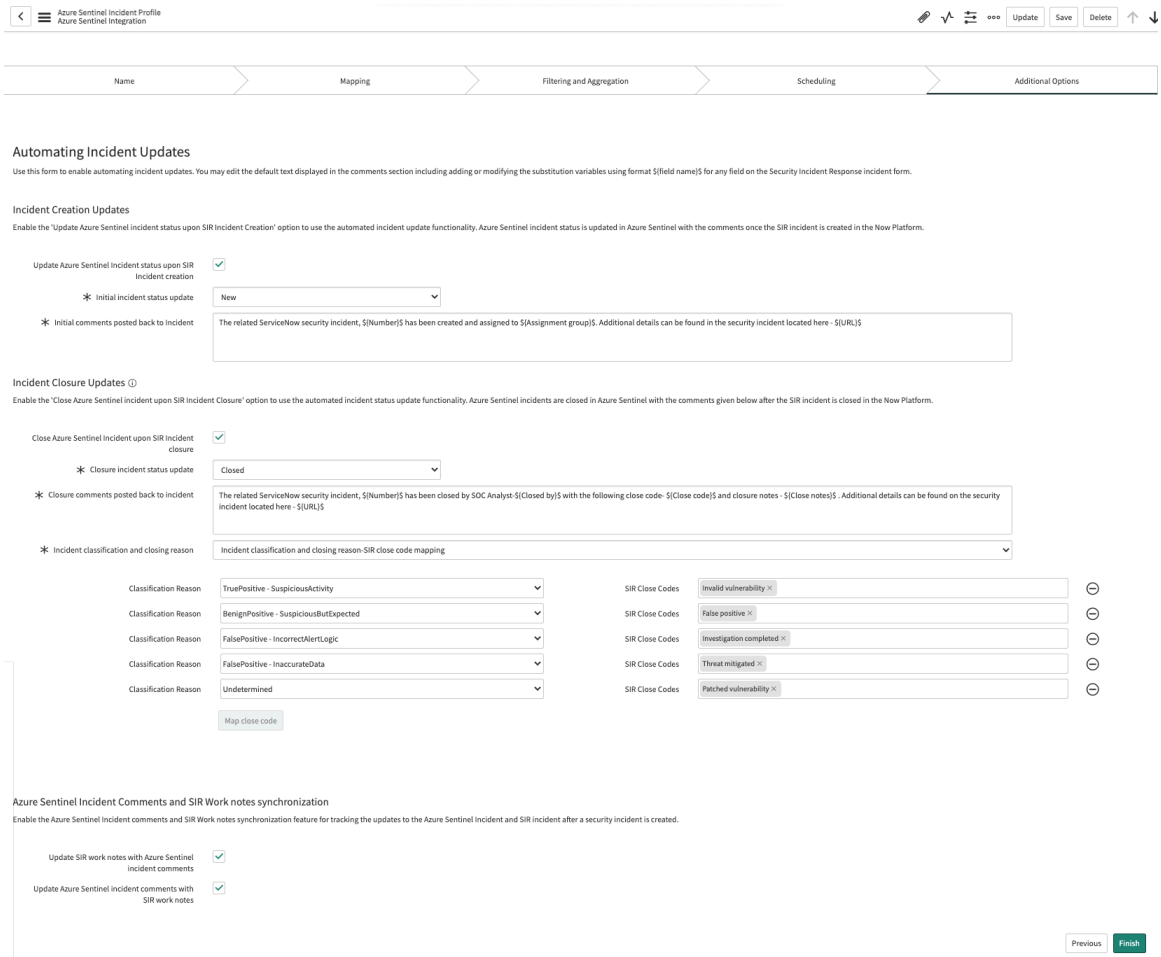
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Catégorie	Champ	Description
		l'environnement Microsoft Azure Sentinel .
Synchronisation des commentaires d'incidents Azure Sentinel et des notes de travail SIR	Mettre à jour les notes de travail SIR avec les commentaires sur l'incident Azure Sentinel	Option que vous pouvez sélectionner pour mettre à jour vos Microsoft Azure Sentinel commentaires dans les notes de SIR travail. Le commentaire dans les SIR notes de travail apparaît avec le préfixe *`Commentaire de Sentinel`*. Le commentaire contient également l'ID Sentinel, les détails de l'analyste et l'horodatage.
	Mettre à jour les commentaires sur l'incident Azure Sentinel avec les notes de travail SIR	Option que vous pouvez sélectionner pour mettre à jour vos SIR notes de travail dans les commentaires d'incident Microsoft Azure Sentinel . Le commentaire dans Microsoft Azure Sentinel apparaît avec le préfixe *`Commentaire de ServiceNow`*.

L'exemple suivant montre les options de configuration disponibles pour automatiser les mises à jour des incidents.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Cliquez sur **Terminer**.

Que faire ensuite
Le profil passe à l'état En attente. Lorsque le message de confirmation indique que l'installation et la configuration sont terminées, vous pouvez activer le profil.

Copier un Microsoft Azure Sentinel profil

Copiez un profil existant et ses paramètres associés au lieu de créer un profil. Lorsque vous créez plusieurs profils, vous pouvez réutiliser les paramètres d'un profil existant en copiant ces profils.

Avant de commencer
Rôle requis : sn_si.admin

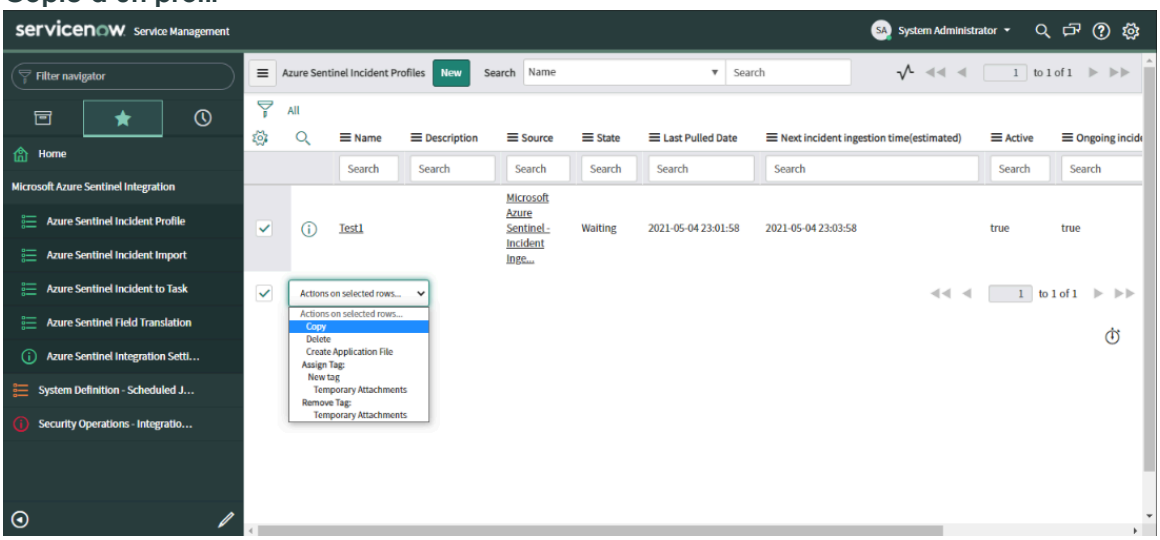
Pourquoi et quand exécuter cette tâche
Lorsque vous copiez un profil, le nom du profil est d'abord modifié pour éviter de créer des profils en double. Le profil copié est également désactivé (défini sur faux) pour éviter de l'activer accidentellement avant d'avoir terminé la configuration. Vous pouvez copier les profils et utiliser les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure

1. Accédez à la **Tout** > **Intégration de Microsoft Azure Sentinel** > **Profil Azure Sentinel**.
2. Dans la liste Profils Azure Sentinel, sélectionnez un profil que vous souhaitez copier, puis dans la liste Actions sur les lignes sélectionnées, cliquez sur **Copier** , comme indiqué dans l'exemple suivant.

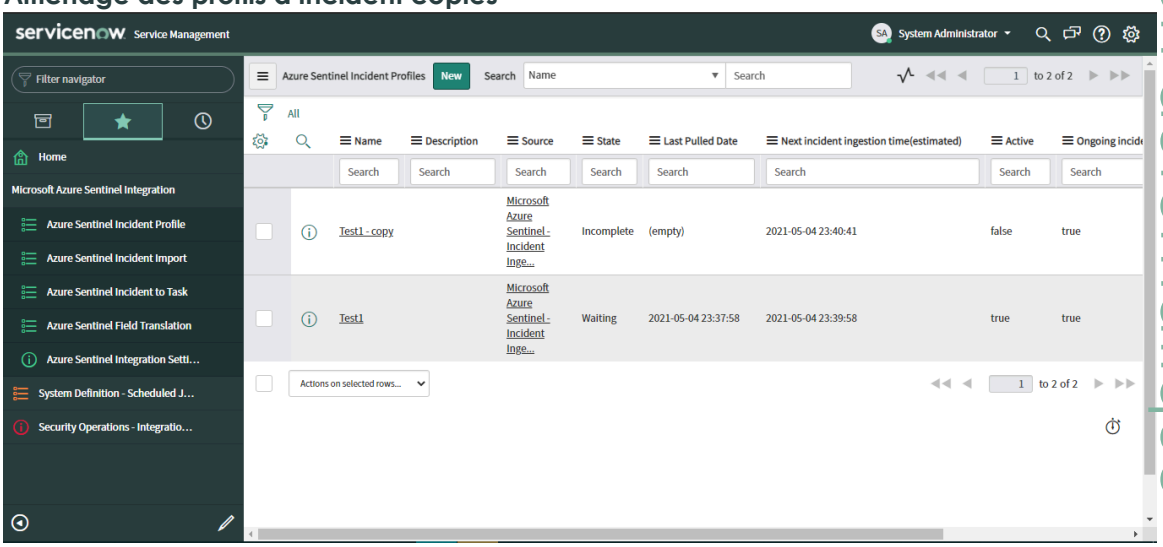
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Copie d'un profil



Le profil est copié et affiché dans la liste, comme illustré dans l'exemple suivant. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient le mot « copier ». Bien que le profil d'origine soit activé (vrai), la copie est désactivée à ce stade (faux). Vous préférez peut-être modifier les valeurs du profil copié et les renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.

Affichage des profils d'incident copiés



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. L'état de la colonne Actif est défini sur faux, ce qui signifie que le profil doit être activé.

SIR Formulaire après une ingestion d'incident

Une fois l'incident Now PlatformMicrosoft Azure Sentinel ingéré, un incident de sécurité est créé et des mises à jour sont apportées à cet enregistrement d'incident de sécurité.

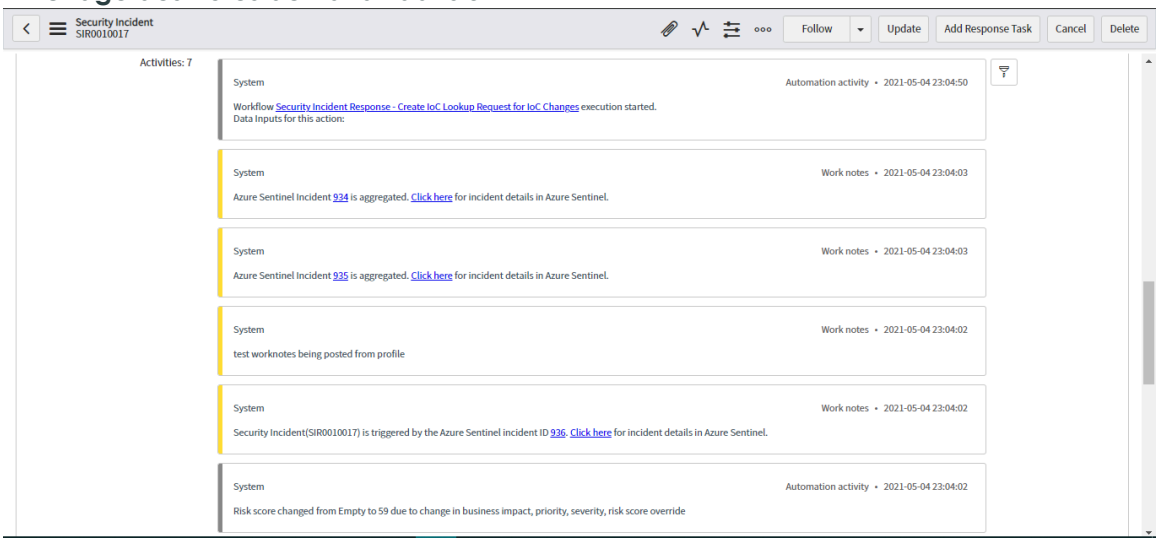
Notes de travail

Une note de travail est publiée lorsqu'un incident est regroupé et si vous avez configuré l'option **Consigner une note de travail pour un nouvel incident** dans les critères d'agrégation d'incidents. L'exemple suivant montre les notes de travail dans SIR.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage des notes de travail dans SIR



Lorsque vous cliquez sur le numéro de l'incident, vous pouvez afficher l'enregistrement d'importation d'incident interne qui contient les données brutes de l'incident. L'exemple suivant montre les données brutes d'incident dans SIR.

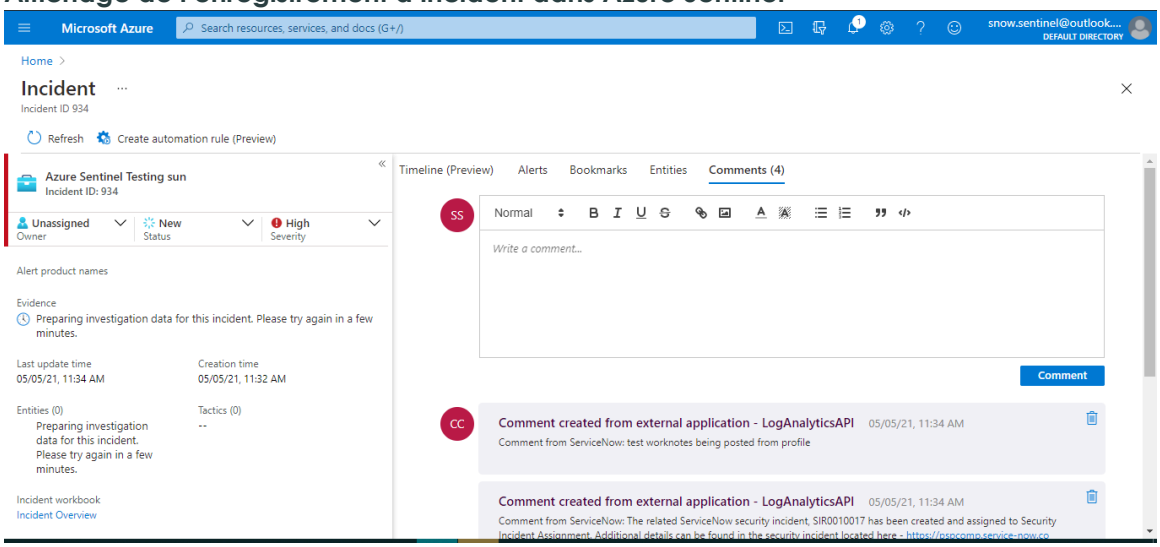
Affichage des données brutes de l'incident dans SIR



Lorsque vous cliquez sur le lien **Cliquer ici** , vous pouvez afficher l'enregistrement dans l'environnement Microsoft Azure Sentinel . L'exemple suivant montre l'enregistrement dans l'environnement Microsoft Azure Sentinel .

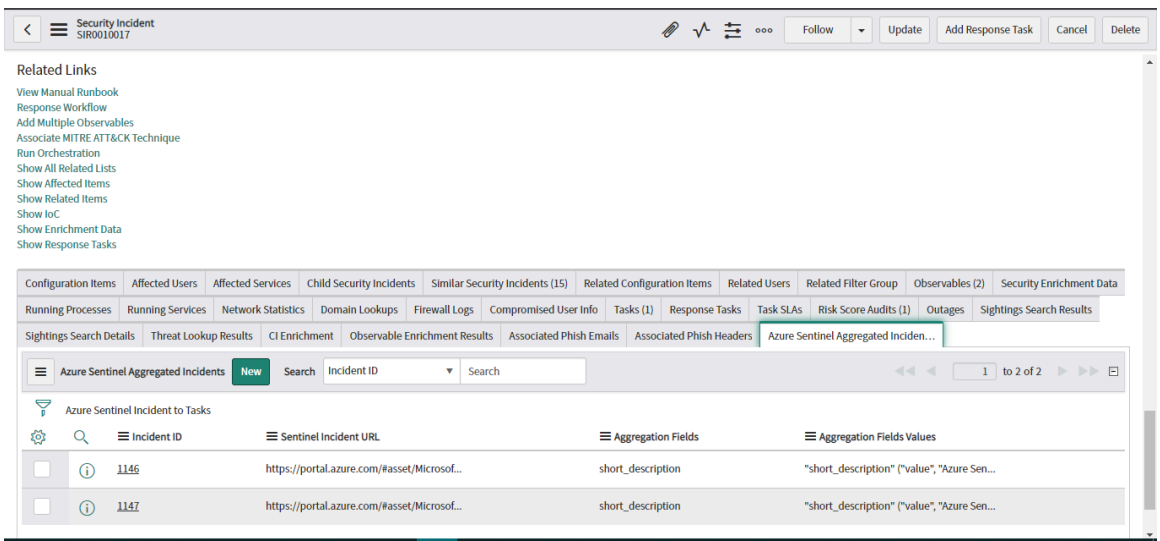
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage de l'enregistrement d'incident dans Azure Sentinel



Incidents Sentinel regroupés

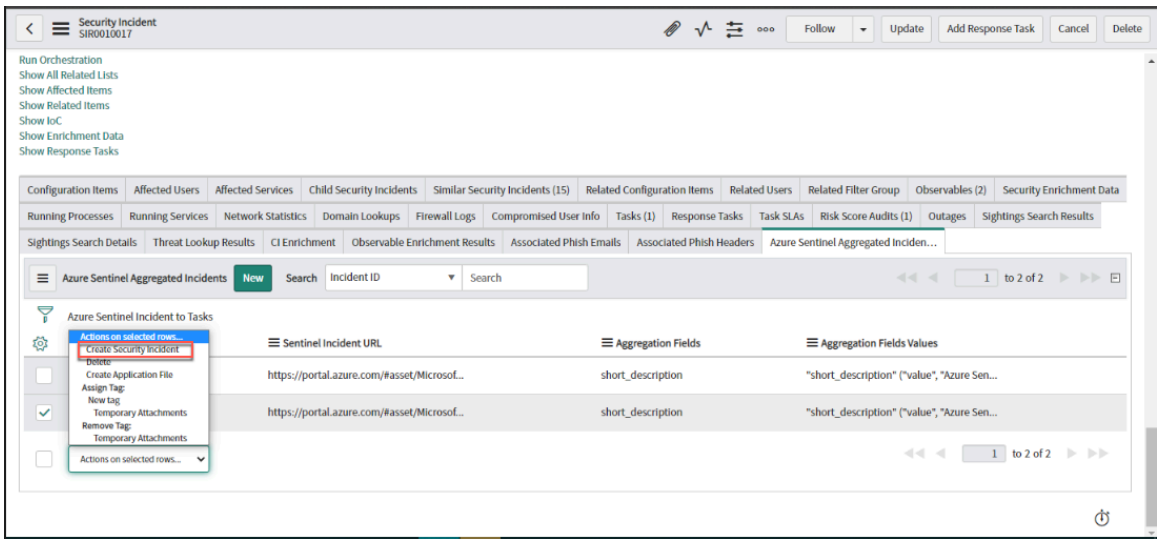
Afficher les incidents Sentinel regroupés : Affichez les incidents regroupés à l'incident de sécurité. Accédez à la **Afficher toutes les listes connexes** > **Incidents Microsoft Azure Sentinel regroupés**.



Créer un incident de sécurité : Sélectionnez un incident dans la liste, cliquez sur le menu **Actions** puis sur **Créer un incident de sécurité**. Cette option crée un nouvel incident de sécurité pour l'incident et cet incident est désagrégé de l'incident de sécurité parent.

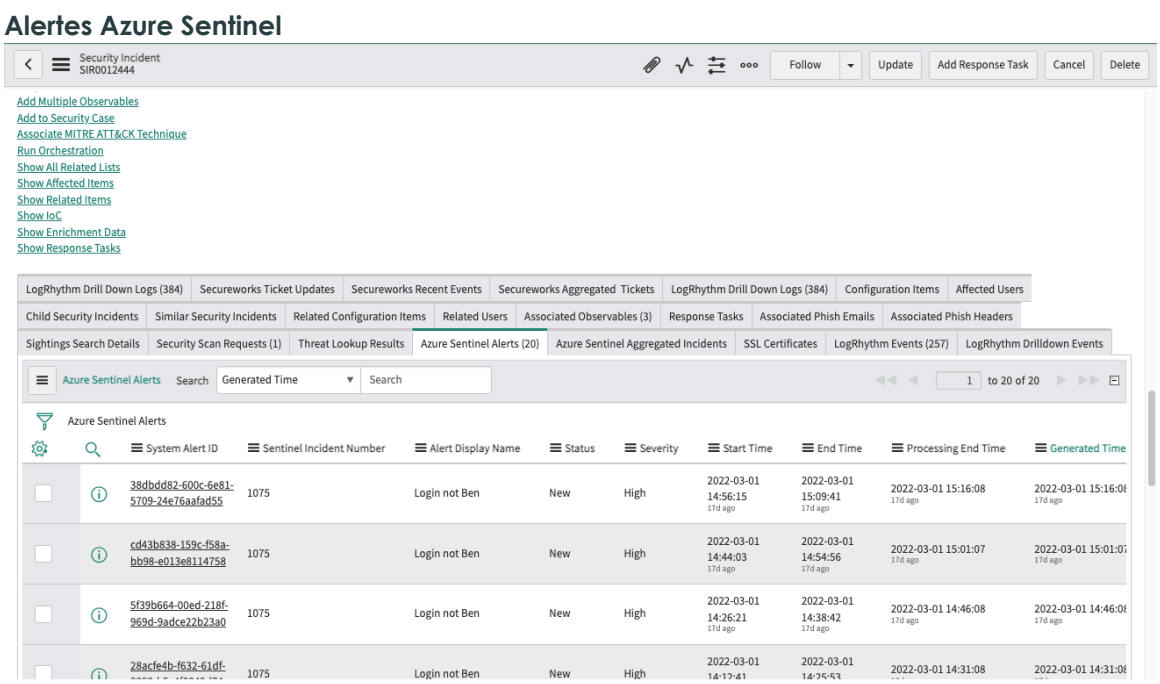
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Alertes Azure Sentinel

Pour afficher les alertes associées à l'incident Sentinel qui a déclenché l'incident de sécurité, accédez à **Afficher toutes les listes connexes** > **Alertes Azure Sentinel**.



Passer en revue les paramètres d'intégration Microsoft Azure Sentinel

Examinez les paramètres d'intégration Microsoft Azure Sentinel afin de pouvoir modifier les propriétés système en fonction de votre environnement.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Intégration de Microsoft Azure Sentinel** > **Paramètres de l'intégration d'Azure Sentinel**.
2. Modifiez les paramètres suivants selon vos besoins.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Microsoft Azure Sentinel Paramètres d'intégration

Nom de la propriété	Description
Appliquez une limite au nombre de jours pendant lesquels des données d'échantillon peuvent être extraites. sn_sec_sentinel.max_nombre_de_jours_pour_les_données_de_l'échantillon	Nombre maximal de jours pendant lesquels vous pouvez extraire des échantillons de données de l'environnement Microsoft Azure Sentinel . Type : nombre entier Valeur par défaut : 7
Recevez des mises à jour liées aux nouvelles alertes liées à SIR. sn_sec_sentinel.incident_updates	Activez l'option pour recevoir les mises à jour des incidents. Type : booléen Valeur par défaut : true
Caractère de délimitation pour diviser les valeurs dans Microsoft Azure Sentinel les mappages de champs. sn_sec_sentinel.delimiter	Caractère de délimitation pour diviser les valeurs dans Microsoft Azure Sentinel les mappages de champs. Type : chaîne Valeur par défaut : ', ' (virgule avec espace)
Appliquez une limite au nombre d'échantillons d'incidents qui peuvent être extraits. sn_sec_sentinel.max_num_of_sample_incident_per_call	Nombre maximal d'échantillons d'incidents à extraire de l'environnement pour l'ingestion Microsoft Azure Sentinel . Type : nombre entier Valeur par défaut : 5 Valeur maximale de l'échantillon : 20
Appliquez une limite au nombre d'incidents sentinel qui peuvent être regroupés en un seul incident. sn_sec_sentinel.max_aggregations_per_si	Limite d'agrégation des incidents pour un incident de sécurité. Par exemple, s'il y a 102 incidents, les 100 premiers sont agrégés aux incident_1 de sécurité et les 2 autres aux incident_2 de sécurité. Type : nombre entier Valeur par défaut : 100
Appliquer une limite au nombre d'incidents de sécurité qui peuvent être créés dans un délai de 24 heures. sn_sec_sentinel.max_si_par_jour	Nombre maximal d'incidents de sécurité qui peuvent être créés en 24 heures dans le Now Platform. Type : nombre entier Valeur par défaut : 1 000

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété	Description
Limite maximale de pagination pour l'extraction des données d'incident dans un appel REST. sn_sec_sentinel.max_page_size	Limite de pagination pour l'extraction des données d'incident dans un appel REST à partir de l'environnement Microsoft Azure Sentinel . Type : nombre entier Valeur par défaut : 100
Valeur de la version de l'API pour les incidents. sn_sec_sentinel.sentinel_security_incident_api_version	Version de l'API Microsoft pour la récupération des incidents Sentinel. Valeur par défaut : 2021-10-01
Valeur de version de l'API pour les alertes. sn_sec_sentinel.sentinel_security_alert_api_version	Version de l'API Microsoft pour la récupération des alertes Sentinel. Valeur par défaut : 2021-10-01
Valeur de version d'API pour les entités. sn_sec_sentinel.sentinel_security_entities_api_version	Version de l'API Microsoft pour la récupération des entités Sentinel. Valeur par défaut : 2021-10-01
sn_sec_sentinel.journalisation.verbosité	Niveau de verbosité du journal de l'application, c'est-à-dire le nom du type d'information. Vous pouvez également mettre à jour la valeur pour les options suivantes : ◦ **erreur** ◦ **avertir** ◦ **info** ◦ **debug** Valeur par défaut : **info**.

3. Cliquez sur **Enregistrer**.
   Vos paramètres d'intégration modifiés sont appliqués à l'intervalle d'interrogation suivant, tel que défini dans le profil.

Séparation de domaine et intégration Microsoft Azure Sentinel

L'application Séparation de domaine est prise en charge. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : basique

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de service de l'application.
- L'application prend en charge Séparation de domaine lors de l'exécution. Séparation de domaine inclut la séparation à partir de l'interface utilisateur, des clés de cache, du reporting, des déploiements et des agrégations.
- Le propriétaire de l'instance doit configurer l'application de sorte qu'elle fonctionne sur plusieurs locataires.

Exemple de cas d'utilisation : lorsqu'un fournisseur de service (SP) utilise la messagerie instantanée pour répondre au message d'un locataire-client, le client doit pouvoir afficher la réponse du SP.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Comment fonctionne Séparation de domaine dans l'intégration Microsoft Azure Sentinel

Procédez comme suit pour réaliser Séparation de domaine :

- Créez un utilisateur avec le rôle sn_si.admin dans le domaine respectif.

  Remarque : Lorsque vous créez le profil, utilisez le sélecteur de domaine pour sélectionner un domaine. Ne créez pas l'utilisateur dans le domaine parent et ne modifiez pas ultérieurement le domaine du profil. Vous devez avoir un utilisateur pour chaque domaine pour votre profil avec le rôle sn_si.admin. Utilisez cet utilisateur pour créer ou modifier les paramètres du profil.

- Désactivez les travaux planifiés existants.
- Répliquez les travaux planifiés suivants pour chaque domaine :
  - Azure Sentinel : extraction des alertes et des entités
  - Synchronisation des commentaires Azure Sentinel
  - Mise à jour de l'état Azure Sentinel
  - Processus du profil Azure Sentinel
  - Données brutes du processus Azure Sentinel
  - Nettoyage des données Azure Sentinel
  - Extraction du commentaire historique Azure Sentinel

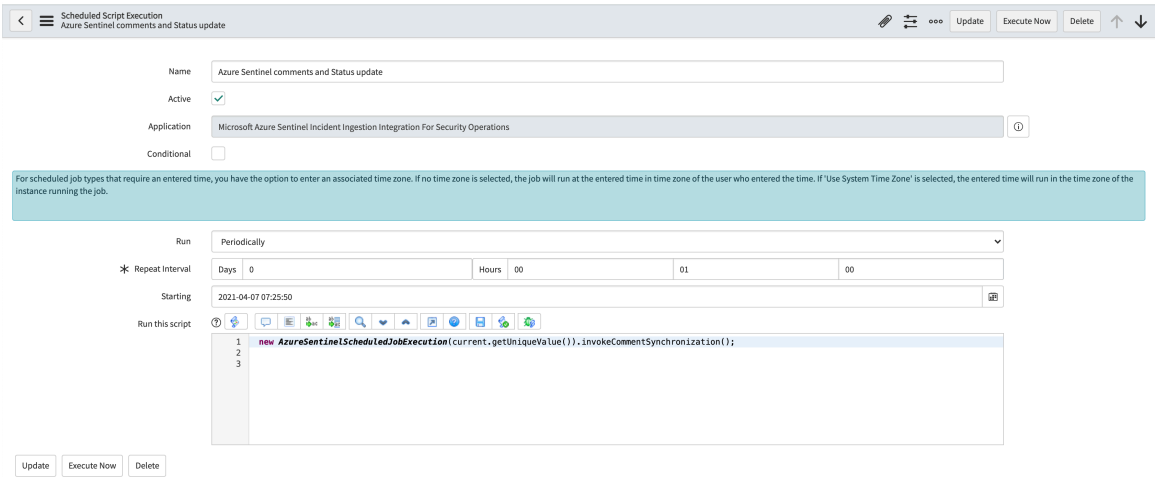
  Remarque : Après avoir répliqué les travaux planifiés, utilisez le navigateur et recherchez le module Politiques d'accès au module, puis affichez les enregistrements récemment créés dont le **script cible** affiche les travaux planifiés nouvellement créés. Modifiez la valeur du champ **Résultat** sur **Suivi**.

- Remplacez **l'utilisateur système Exécuter en tant que** par l'utilisateur disposant du rôle sn_si.admin dans le domaine respectif, puis exécutez la tâche planifiée.

L'exemple suivant montre comment répliquer la tâche de mise à jour de l'état et des commentaires Azure Sentinel et exécuter la tâche en tant qu'utilisateur système.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Information associée

Séparation de domaine pour les fournisseurs de services

Comparaison Microsoft Azure Sentinel et API de sécurité Microsoft Graph intégrations avec SIR

Vous pouvez afficher les différences entre Microsoft Azure Sentinel les API de sécurité Microsoft Graph intégrations et choisir celle qui convient à votre Now Platform instance.

Vue d'ensemble de Microsoft Azure Sentinel - Ingestion des incidents

Microsoft Azure Sentinel est une solution de gestion des événements d'information de sécurité (SIEM) et de réponse automatisée d'orchestration de sécurité (SOAR) basée sur le cloud. Microsoft Azure Sentinel fournit des analyses de sécurité intelligentes et des renseignements sur les menaces dans l'ensemble de l'entreprise. Il offre une solution unique pour la détection des alertes, la visibilité des menaces, la chasse proactive et la réponse aux menaces.

Vue d'ensemble de API de sécurité Microsoft Graph

Il API de sécurité Microsoft Graph s'agit d'un service intermédiaire (ou courtier) qui fournit une interface programmatique unique pour connecter plusieurs fournisseurs de sécurité (natifs de Microsoft ainsi que ServiceNow des partenaires).

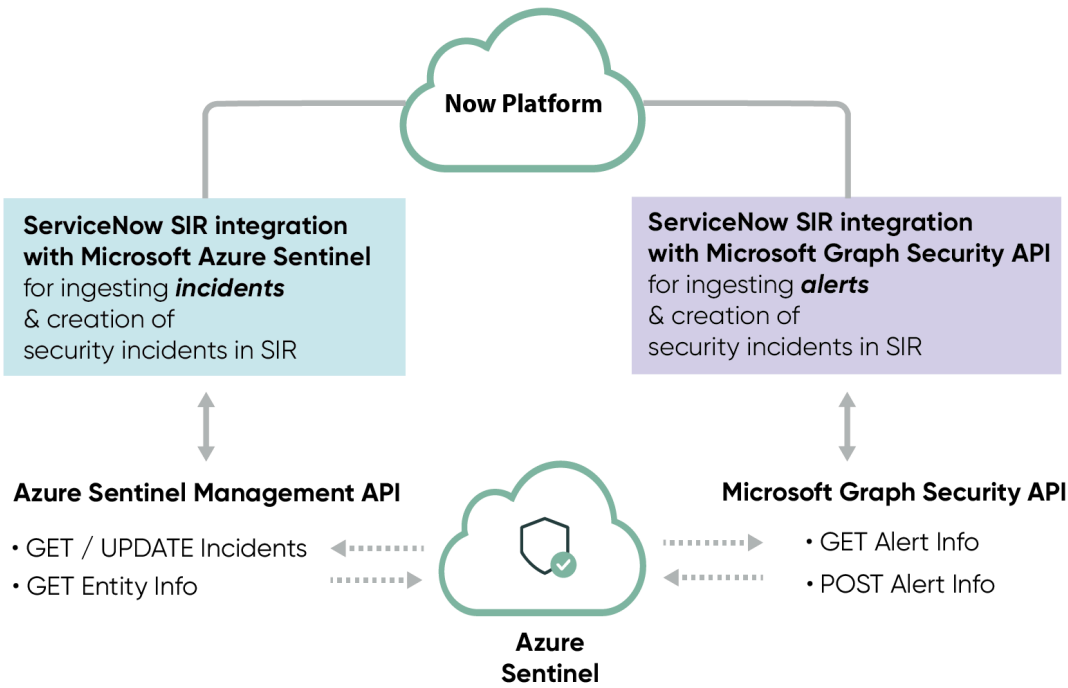
L'intégration API de sécurité Microsoft Graph résout ces problèmes en utilisant la pour se connecter à différentes technologies de sécurité Microsoft telles qu'Azure API de sécurité Microsoft Graph Sentinel, Microsoft Defender Advanced Threat Protection et Azure Advanced Threat Protection. Les alertes des fournisseurs de sécurité Microsoft sont ingérées et les incidents de sécurité sont automatiquement créés dans Réponse aux incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Récapitulatif des différences de fonctionnalités

Azure Sentinel and Graph Security API (Microsoft architecture)



Microsoft Azure Sentinel Vs API de sécurité Microsoft Graph

Microsoft Azure Sentinel	API de sécurité Microsoft Graph
Ingère les Microsoft Azure Sentinel incidents en même temps que les informations sur l'entité (lorsqu'elles sont disponibles) et automatise la création des incidents de sécurité dans SIR.	Ingère les alertes de plusieurs fournisseurs de sécurité (y compris Azure Sentinel) dans un schéma standard et automatise la création des incidents de sécurité dans SIR.
Automatise les mises à jour de l'état des Microsoft Azure Sentinel incidents pour Réponse aux incidents de sécurité afin que vous puissiez créer et fermer des incidents de sécurité. **Remarque :** ServiceNow Met à jour l'état des Microsoft Azure Sentinel incidents en fonction de la création ou de la fermeture de l'incident de sécurité.	Prend en charge les mises à jour d'alerte (changement du statut de l'alerte et fermeture de l'alerte) pour les fournisseurs de sécurité sélectionnés. **Remarque :** Pour plus d'informations sur les API de sécurité Microsoft Graph fournisseurs de sécurité pris en charge, consultez la documentation Microsoft .
Utilisez cette intégration si votre scénario inclut les conditions suivantes :	Utilisez cette intégration si votre scénario inclut les conditions suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Microsoft Azure Sentinel Vs API de sécurité Microsoft Graph (suite)

Microsoft Azure Sentinel	API de sécurité Microsoft Graph
• Une enquête préliminaire sur l'incident est en cours Microsoft Azure Sentinel et une enquête subséquente est en cours SIR • Ingérer les Microsoft Azure Sentinel incidents dans SIR	• Effectuez une enquête sur un incident dans SIR. • Ingérer Microsoft Azure Sentinel les alertes dans SIR. • Les incidents ne sont pas créés dans Microsoft Azure Sentinel.
L'alerte est une entité dans Microsoft Azure Sentinel. Vous ne pouvez pas récupérer d'alertes autonomes ou spécifiques à l'aide de l'API Microsoft Azure Sentinel de gestion. Vous ne pouvez récupérer que les données d'alerte associées à un incident. Les données d'alerte disponibles à l'aide de cette intégration sont plus riches que les données d'alerte disponibles à l'aide du API de sécurité Microsoft Graphfichier .	Les Microsoft Azure Sentinel données d'alerte normalisées sont disponibles. Les Microsoft Azure Sentinel champs d'alerte qui sont mappés en interne dans API de sécurité Microsoft Graphet qui sont disponibles dans API de sécurité Microsoft Graph, peuvent être utilisés dans cette intégration.
	Vous ne pouvez pas mettre à jour les alertes à Microsoft Azure Sentinel l'aide de cette intégration.

Microsoft Defender pour point de terminaison intégration

Il Microsoft Defender pour point de terminaison vous permet d'inspecter, d'analyser et de contenir de manière proactive les menaces connues et inconnues sur n'importe quel point de terminaison.

L'intégration Microsoft Defender pour point de terminaison aide les analystes de sécurité à enquêter efficacement sur les incidents de sécurité et à y remédier, sans avoir à naviguer entre les outils.

Vous pouvez utiliser cette intégration pour créer des configurations permettant de récupérer les détails de l'hôte, les détails des utilisateurs connectés, les détails des ordinateurs connexes et d'autres options d'enrichissement. Vous pouvez demander à ce qu'une machine n'accède pas aux réseaux ou à la retirer de l'isolement. Les demandes peuvent être acceptées ou rejetées par les approbateurs.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Fonctionnalités principales

Microsoft Defender pour point de terminaison présente les principales caractéristiques suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Réalisation d'une recherche de sécurité d'entreprise pour identifier les observables potentiellement malveillants sur les points de terminaison et application de mesures correctives.
- Réalisation d'actions de réponse telles que Isoler l'hôte, Supprimer l'isolation, Limiter l'exécution des applications, Effectuer une analyse antivirus, Limiter la restriction d'application et Arrêter et mettre en quarantaine le fichier.
- Créez ou mettez à jour des indicateurs.
- Procédez à l'enrichissement des observables et récupérez les données associées aux indicateurs.

Microsoft Defender pour point de terminaison

Explorer	Installer	Configurer
Prise en main de Microsoft Defender pour point de terminaison	Installer l'application et configurer une source pour l'intégration	Configurer les profils et les incidents de sécurité pour Microsoft Defender pour point de terminaison
Profil d'aptitude	**Configurations supplémentaires**	**Divers**
Créez un profil d'aptitude pour l'intégration de Microsoft Defender pour point de terminaison.	Configurations supplémentaires que vous pouvez effectuer dans Microsoft Defender pour point de terminaison	Créez et configurez un profil pour la recherche de perceptions et les indicateurs avec Microsoft Defender pour point de terminaison.

Traduction automatique

Enregistrez et configurez le Microsoft Defender pour point de terminaison dans le Microsoft Azure portail

Enregistrez l'application Microsoft Defender pour point de terminaison dans le portail Microsoft Azure et accordez l'accès en lecture et en écriture à l'application.

Avant de commencer

Rôle requis : Développeur d'application, Administrateur locataire.

Procédure

1. Connectez-vous au portail Microsoft Azure.
2. Entrez `les inscriptions d'application` dans la zone de recherche, puis cliquez **sur Cliquer sur Nouvelle inscription**.
3. Entrez un nom pour votre application et l'URI de redirection, puis cliquez sur **Enregistrer**. Un exemple de nom est `Microsoft Defender pour point de terminaison`. L'URI de redirection est utilisé lors de l'octroi du consentement administrateur pour l'application.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sur la page **Inscriptions de l'application** , sélectionnez l'application que vous avez enregistrée à l'étape 3.
5. Sous Gérer, sélectionnez **Certificats et secrets**.
6. Pour créer un secret client, sélectionnez **Nouveau secret client**.
7. Copiez le secret client et enregistrez-le.

   Si vous avez oublié le secret client, vous pouvez générer un nouveau secret client.

8. Accédez à la **Gérer** > **Autorisations d'API**.
9. Cliquez sur **Ajouter une autorisation**.
10. Dans la fenêtre Demander les autorisations d'API, cliquez sur l'onglet **API utilisées par mon organisation** .
11. Recherchez et sélectionnez **WindowsDefenderATP**.
12. Dans les autorisations WindowsDefenderATP, sélectionnez **Autorisations d'application**. L'activation de cette autorisation garantit que l'application s'exécute en tant que service ou démon d'arrière-plan sans utilisateur connecté.
13. Ajoutez les autorisations suivantes au niveau de l'application et accordez le consentement de l'administrateur pour les autorisations d'API nouvellement ajoutées.

Autorisation	Nom d'affichage de l'autorisation
Ordinateur.Lecture.Tout	Lire tous les profils de machine
Utilisateur.Lecture.Tout	Lire les profils d'utilisateurs
Machine.Isoler	Isoler la machine
Machine.RestrictExecution	Restreindre l'exécution de code
Machine.Scan	Machine de numérisation
Machine.StopAndQuarantine	Arrêter et mettre en quarantaine
URL. Lire.Tout	URL de lecture
Fichier.Lecture.Tout	Lire les profils des fichiers
Ip.Lecture.Tout	Lire les profils d'adresses IP
Ti.Lectureécriture.Tout	Indicateurs de lecture et d'écriture

Traduction automatique

Démarrer l'intégration Microsoft Defender pour point de terminaison

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform® instance avant d'installer l'application Microsoft Defender pour point de terminaison à partir du ServiceNow Store.

Avant de commencer

Rôle requis : administrateur

Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application pour garantir une installation et une configuration fluides.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis : **1.** Vous devez disposer du rôle d'administrateur système (admin) pour installer l'application pour l'intégration. **2.** Vous devez disposer du rôle d'administrateur d'incident de sécurité (sn_si.admin) pour configurer l'intégration, créer, activer et supprimer des profils. **3.** Vous devez avoir le rôle d'analyste des incidents de sécurité (sn_si.analyst) pour travailler avec les incidents de sécurité. Un utilisateur disposant de ce rôle peut initier n'importe laquelle des options disponibles dans l'intégration.
Vérifiez que les applications principales de ServiceNow qui sont requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si ces applications ne sont pas déjà installées, vous devez installer et activer chaque application une par une dans l'ordre suivant pour garantir une installation fluide : **1.** Réponse aux incidents de sécurité **2.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **3.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
Avant d'activer l'option d'approbation pour les profils, vérifiez que vous avez créé un groupe d'approbation.	Un workflow d'approbation facultatif est disponible pour isoler les ordinateurs hôtes, les restaurer sur le réseau et exécuter des actions supplémentaires sur le point de terminaison. Si votre organisation souhaite un niveau supplémentaire de contrôle sur ces actions, activez l'option Exiger l'approbation pendant la configuration des profils. Dans un scénario où le profil est disponible, la configuration du profil pour approbation est prioritaire. Dans un scénario où le profil n'est pas disponible, les approbations sont traitées en fonction des paramètres par défaut. En tant qu'administrateur de sécurité, vous pouvez configurer l'approbation tout en configurant les profils et les paramètres par défaut. Un groupe d'approbation doit être

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	disponible dans la liste Groupes de votre instance. Pour surveiller et traiter les demandes soumises par les utilisateurs disposant du rôle sn_si.analyste, chaque membre du groupe d'approbation doit accéder à Mes approbations dans le Now Platform®. Les approbateurs peuvent également trouver les demandes soumises exclusivement pour Microsoft Defender pour point de terminaison l'intégration sous le module Approbations. Pour plus d'informations sur la création d'un groupe d'utilisateurs, consultez Créer un groupe d'utilisateurs .

Que faire ensuite

Vous avez correctement configuré votre Now Platform® instance pour l'intégration Microsoft Defender pour point de terminaison . L'étape suivante consiste à installer l'application Microsoft Defender pour point de terminaison à partir de ServiceNow Store pour l'intégration.

Installer l'application et configurer une source pour l'intégration

Installez et configurez l'intégration Microsoft Defender pour point de terminaison à partir de ServiceNow Store sur votre Now Platform instance. Commencez à créer des profils d'aptitude à l'aide des configurations.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Téléchargez l'intégration de Microsoft Defender pour point de terminaison à partir de et ServiceNow Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette Microsoft Defender pour point de terminaison, puis cliquez sur **Configurer**.
4. Renseignez les champs suivants du formulaire.

Configurer Microsoft Defender pour point de terminaison

Nom	Nom de la configuration d'instance Microsoft Defender pour point de terminaison .
URL de base	URL de base du service pour Microsoft Defender pour point de terminaison
ID de locataire	ID Microsoft Defender pour point de terminaison du locataire. Toutes les actions seront effectuées sur cette instance.
ID client	ID client de l'application que vous avez enregistrée dans le portail Microsoft Azure.

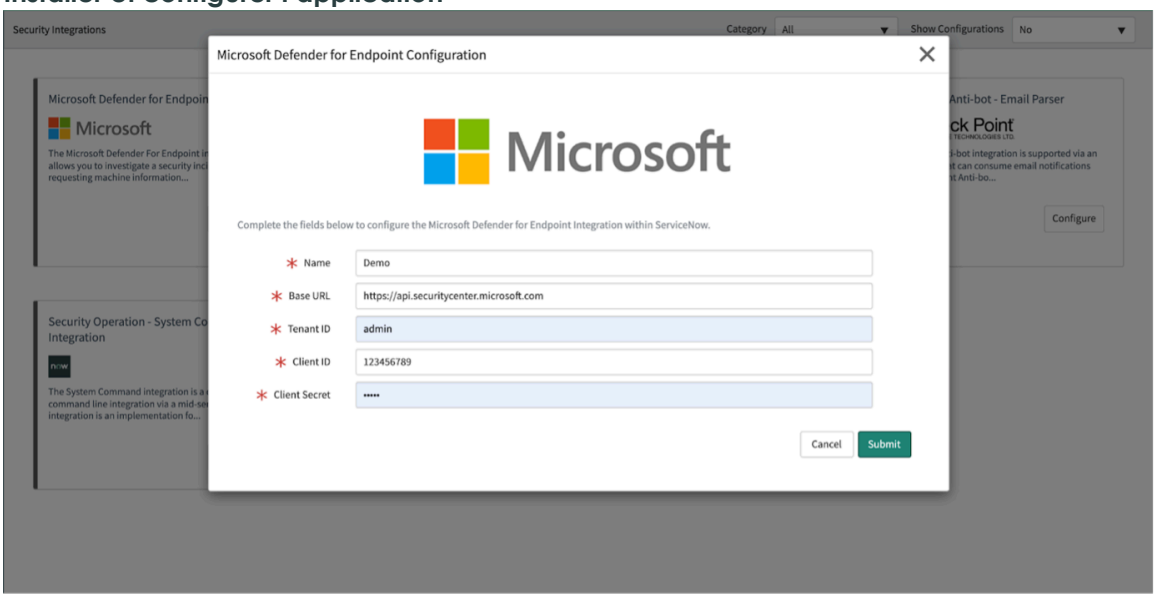
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Secret client	Secret client pour votre application enregistrée.

5. Cliquez sur **Envoyer**.

Installer et configurer l'application



Résultats
La Microsoft Defender pour point de terminaison liste des configurations s'affiche avec votre nouvel enregistrement de configuration. Vous avez terminé la configuration pour le Microsoft Defender pour point de terminaisonfichier .

Microsoft Defender pour point de terminaison Paramètres par défaut

Vous devez effectuer d'autres paramètres de configuration une fois l'installation terminée.

Une fois l'installation terminée, vous trouverez le module Paramètres par défaut sous l'application Microsoft Defender pour point de terminaison , dans le volet de navigation de gauche. Il contient les paramètres par défaut des différentes Microsoft Defender pour point de terminaison fonctionnalités.

Rôles requis : sn_si.admin, sn_si.analyst (lecture seule).

Configurations supplémentaires

Les paramètres de configuration supplémentaires sont les suivants :

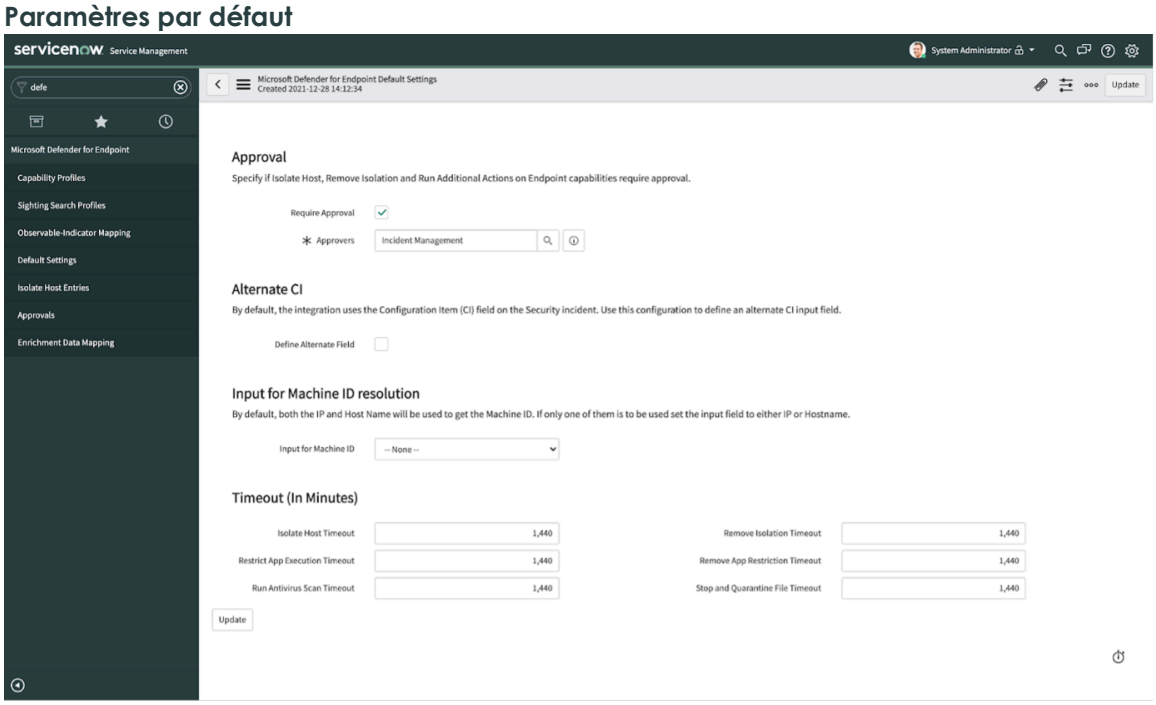
- **Approbation** : cette approbation concerne spécifiquement les actions Isoler l'hôte, Supprimer l'isolement de l'hôte et d'autres actions telles que Restreindre l'exécution des applications, Supprimer la restriction d'application et Exécuter une analyse antivirus. Vous pouvez utiliser cette approbation uniquement lorsque les actions sont déclenchées directement à partir de la liste connexe et s'il n'existe aucun profil existant. S'il existe des profils pour ces options, la configuration de l'approbation dans le profil est prioritaire.
  - **Exiger l'approbation** : lorsque vous activez **l'option Exiger l'approbation**, le champ Approbateurs est disponible sur le formulaire.
  - **Approbateurs** : liste des groupes d'approbateurs. Après avoir soumis une demande, le groupe doit obtenir l'approbation du groupe.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **CI alternatif** : si vous cochez cette case, la liste des champs disponibles permet de transmettre un CI alternatif à l'option. Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité. Cette configuration s'applique uniquement à l'aptitude Exécuter des actions supplémentaires sur le point de terminaison. Utilisez cette configuration pour définir un champ d'entrée CI alternatif pour la seule fonctionnalité Exécuter des actions supplémentaires sur le point de terminaison. Pour les autres options, utilisez la configuration de la section profil. Si les profils ne définissent pas d'autre CI, les options prennent le champ CI du formulaire d'incident de sécurité.
- **Entrée pour la résolution de l'ID de l'agent** : par défaut, l'adresse IP et le nom d'hôte sont utilisés pour obtenir l'ID de l'agent. Si vous comptez n'utiliser qu'un seul d'entre eux, définissez le champ d'entrée sur IP ou Nom d'hôte.
- **Délai d'expiration** :
  - **Délai d'isolement de l'hôte (en minutes) :** Indique le seuil d'exécution des options Isoler l'hôte.
  - **Supprimer le délai d'isolement (en minutes) :** Indique le seuil d'exécution pour l'option Supprimer le délai d'isolement
  - **Restreindre le délai d'exécution de l'application (en minutes) :** Indique le seuil d'exécution de l'option Restreindre l'exécution de l'application.
  - **Supprimer le délai d'expiration de la restriction d'application (en minutes) :** Indique le seuil d'exécution de l'aptitude Supprimer la restriction d'application.
  - **Exécuter le délai d'expiration de l'analyse antivirus (en minutes) :** Indique le seuil d'exécution de l'aptitude Exécuter l'analyse antivirus.
  - **Délai d'arrêt et de mise en quarantaine du fichier (en minutes) :** Indique le seuil d'exécution pour l'aptitude Arrêter et mettre en quarantaine un fichier.

Paramètres par défaut



Mapper les types d'indicateurs Microsoft Defender pour point de terminaison

Mappez le type d'observable ServiceNow avec le type d'indicateur Microsoft Defender pour point de terminaison . Ce mappage sera utilisé dans les actions d'enrichissement d'observable et de création d'indicateur dans Microsoft Defender.

Traduction automatique

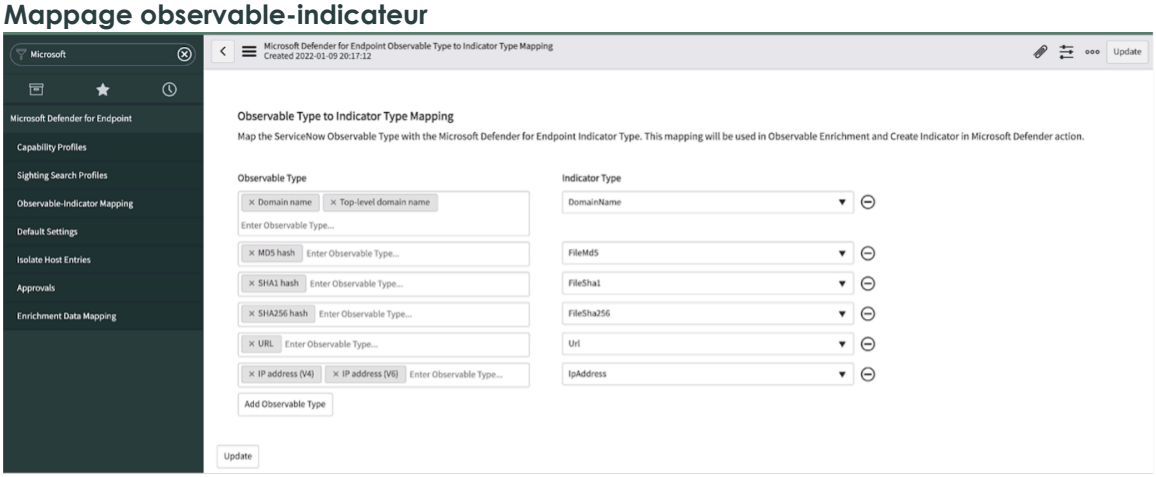
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.admin ou sn_si.analyst (lecture seule)

Pourquoi et quand exécuter cette tâche
Dans un scénario où le type d'observable n'est pas mappé à un type d'indicateur, ces observables ne sont pas éligibles pour l'enrichissement des observables et la création d'indicateurs dans Microsoft Defender pour point de terminaison.

Procédure
1. Accédez à la **Microsoft Defender pour point de terminaison** > **Mappage observable-indicateur**.

Mappage observable-indicateur



2. Ajoutez ou mettez à jour un type d'observable de l'une des façons suivantes :
   - Pour ajouter un nouveau mappage, cliquez sur **Ajouter un type d'observable**.
   - Pour mettre à jour l'observable sur le mappage de type d'indicateur, cliquez sur une ligne existante.
3. Pour enregistrer le mappage, cliquez sur **Mettre à jour**.

Créer un profil d'aptitude pour l'intégration Microsoft Defender pour point de terminaison

Créez un profil et sélectionnez les Microsoft Defender pour point de terminaison options que vous souhaitez qu'il exécute.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Les profils sont créés pour regrouper ou regrouper les options, ce qui aiderait les analystes à effectuer facilement l'enquête ou le rattrapage. Vous pouvez ajouter les fonctionnalités suivantes au profil :

- Obtenir les détails de l'hôte
- Obtenir les utilisateurs connectés
- Isoler l'hôte
- Supprimer l'isolement

Vous ne pouvez pas associer les options Isoler l'hôte et Supprimer l'isolement de l'hôte avec d'autres options lors de la création d'un profil. Les profils pour ces fonctionnalités doivent être créés individuellement. D'autre part, les fonctionnalités Obtenir les détails de l'hôte et

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Obtenir les utilisateurs connectés peuvent être regroupées. Vous pouvez créer des profils individuellement ou en les matraquant en totalité ou en parties selon vos besoins.

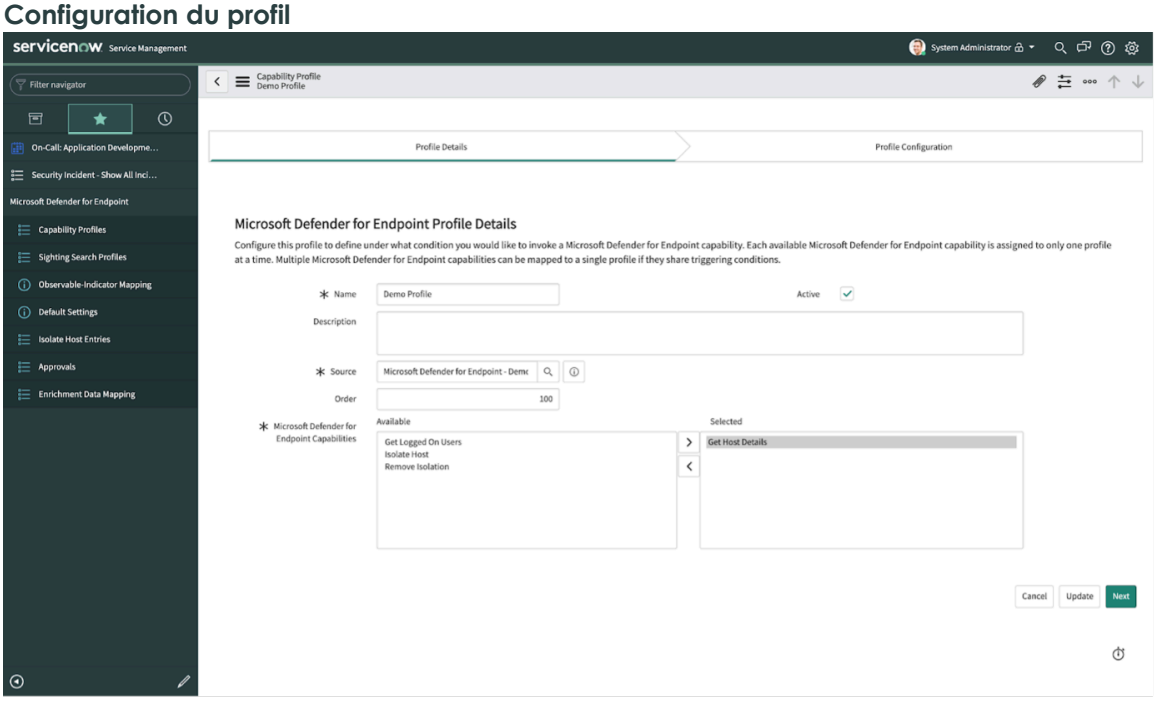
Remarque : Une fois qu'une option est incluse dans un profil, elle ne peut être incluse dans aucun autre profil provenant de la même source.

Procédure

1. Accédez à la **Microsoft Defender pour point de terminaison** > **Profils d'aptitude**.

   La liste des profils d'aptitude de Microsoft Defender pour point de terminaison s'affiche.

Configuration du profil



2. Cliquer sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire de profil d'aptitude

Champ	Description
Nom	Nom du profil d'aptitude Microsoft Defender pour point de terminaison . Ce nom vous permet d'identifier le type de profil et de le décrire.
Description	Informations supplémentaires sur le profil qui le décrivent plus en détail.
Source	Nom de la Microsoft Defender pour point de terminaison source. Seules les sources configurées sont disponibles dans la liste.
Fonctionnalités de Microsoft Defender pour point de terminaison	Options du Microsoft Defender pour point de terminaison profil. Sélectionnez les options que vous souhaitez pour ce profil dans la colonne Disponible et déplacez-les vers la colonne Sélectionné.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ordre	Priorité du flux. La valeur par défaut est 100. La valeur de ce champ indique l'ordre dans lequel les flux sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux doté du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400.
Actif	Option pour indiquer que le profil est actif. Une fois le profil actif, il est automatiquement déclenché lorsqu'un incident de sécurité correspondant aux conditions de filtrage spécifiées dans la configuration est créé.

4. Pour passer à la configuration du profil, cliquez sur **Suivant**.

Que faire ensuite

L'étape suivante consiste à configurer votre profil. Avant de configurer les paramètres du profil, vous préférerez peut-être examiner les profils de manière et les conditions configurées et déclenchantes. Pour plus d'informations, consultez Conditions de déclenchement dans un élément de configuration.

Conditions de déclenchement dans un élément de configuration

Une fois que vous avez créé un profil et sélectionné les Microsoft Defender pour point de terminaison options que vous souhaitez qu'il exécute, configurez les paramètres du profil afin que le profil s'exécute uniquement lorsqu'un ensemble de conditions spécifiques est rempli.

Comment déclencher des conditions dans un élément de configuration

Vous pouvez définir des conditions de déclenchement afin que le profil s'exécute automatiquement chaque fois qu'un incident de sécurité correspondant à la condition de déclenchement est créé. Si la condition de déclenchement n'est pas définie, ces profils peuvent être exécutés manuellement en cliquant sur le formulaire Exécuter le(s) profil(s) EDR sur l'incident de sécurité, puis en sélectionnant le profil.

Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité. Cette valeur est utilisée pour faire correspondre les ID de vos actifs avec les informations stockées dans le Now Platform Base de données de gestion des configurations (CMDB)fichier . Lorsqu'un incident de sécurité est créé et qu'un profil est exécuté automatiquement ou manuellement, le CMDB est recherché pour récupérer le nom d'hôte ou l'adresse IP en fonction de la valeur du champ CI. Le nom d'hôte ou adresse IP est utilisé pour résoudre l'ID Microsoft Defender pour point de terminaison de l'agent afin d'identifier le point de terminaison.

Dans l'idéal, une valeur correspondante est trouvée dans la base de données et les données sont collectées à partir de la Microsoft Defender pour point de terminaison console pour l'actif correspondant. Les données des différentes options sont extraites dans votre Now Platform Base de données de gestion des configurations (CMDB) instance et affichées dans les listes connexes d'un incident de sécurité. Lorsque le champ Élément de configuration (CI) n'est pas renseigné sur l'incident de sécurité avec un nom d'hôte ou une adresse IP qui

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

correspond à la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité qui contient soit le nom d'hôte, soit l'adresse IP pour effectuer la résolution de l'ID de l'agent.

Au cours de l'étape de configuration de la configuration du profil, vous pouvez sélectionner un autre champ CI pour l'identification du point de terminaison afin de vous assurer que vous êtes en mesure d'identifier le point de terminaison sur Microsoft Defender pour point de terminaison. Vous pouvez sélectionner n'importe quel champ de l'incident de sécurité comme champ de déclenchement CI alternatif, y compris les champs personnalisés que vous créez. En sélectionnant cet autre champ CI comme copie de sauvegarde, vous vous assurez que vos profils s'exécutent même si le champ CI n'est pas renseigné pour l'incident de sécurité associé à la création de l'incident.

Remarque : Les autres champs CI ne sont pris en compte que pour les options qui peuvent être ajoutées à un profil. Ces fonctionnalités incluent Obtenir les détails de l'hôte, Obtenir les utilisateurs connectés, Isoler l'hôte et Supprimer l'isolement. Pour toutes les actions supplémentaires, le CI alternatif doit être configuré dans le module Paramètres par défaut.

Configurer les profils et les incidents de sécurité pour l'intégration Microsoft Defender pour point de terminaison

Créez un profil et sélectionnez les Microsoft Defender pour point de terminaison options que vous souhaitez qu'il exécute. Vous devez configurer les paramètres de manière à ce que le profil ne puisse être déclenché que dans les conditions définies.

Avant de commencer
Rôle requis : sn_si.admin, sn_si.analyst (lecture seule)

Pourquoi et quand exécuter cette tâche
Configurez le profil de manière à ce qu'il s'exécute uniquement lorsque les conditions que vous spécifiez sont remplies. Si nécessaire, vous pouvez sélectionner un autre champ d'entrée pour le champ Élément de configuration (CI) et définir des conditions de filtrage afin que le profil puisse être déclenché automatiquement lors de la création d'un incident de sécurité répondant aux conditions de déclenchement.

Remarque : Vous ne pouvez accéder à la page Configuration du profil qu'après avoir accédé à la page Détails du profil.

Procédure

1. Accédez à la **Microsoft Defender pour point de terminaison** > **Profils d'aptitude**.
2. Après avoir rempli la section Détails du profil, cliquez sur **Suivant**.
   Examinez et configurez les sections.
3. Dans la section Définir des critères d'incident (automatisation), sélectionnez l'option **Définir des critères d'incident** pour déclencher Microsoft Defender pour point de terminaison automatiquement les options du profil.
   Définir des critères d'incident (automatisation) : définissez les conditions d'incident de sécurité qui déclencheraient automatiquement les options Microsoft Defender pour point de terminaison pour le profil. Si vous ne sélectionnez pas l'option **Définir un critère d'incident** , le profil et les options sous-jacentes peuvent être invoqués manuellement à partir de l'incident de sécurité.

   Remarque : Les options Isoler l'hôte et Supprimer l'isolement de l'hôte ne peuvent pas être déclenchées automatiquement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans les **Conditions de filtre**, sélectionnez le champ requis.

b. Ajoutez **de nouveaux critères** et définissez également **la conditionOU** ou ET.

4. Dans la section Approbations, cochez la case **Exiger l'approbation** pour fournir un niveau de contrôle supplémentaire.

   Si vous sélectionnez cette option, vous avez plus de contrôle lors de l'utilisation des fonctionnalités de Microsoft Defender pour point de terminaison pour isoler les ordinateurs hôtes, les restaurer sur le réseau, obtenir des fichiers.

   L'option Approbations de la configuration du profil s'affiche uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte, respectivement.

5. Dans la section Configuration supplémentaire, sélectionnez l'option **Définir un champ alternatif** pour définir un autre champ d'entrée.
   Configuration supplémentaire : lorsque le champ Élément de configuration (CI) n'est pas renseigné sur l'incident de sécurité avec un nom d'hôte ou une adresse IP qui correspond à la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour interroger les API de Microsoft Defender pour point de terminaison.

   Remarque : Pour plus d'informations, consultez Conditions de déclenchement dans un élément de configuration.

   a. Sélectionnez l'option **Définir un autre champ** .

   b. Sélectionner le champ d'entrée dans le **Champ de déclenchement CI alternatif**.

6. Dans la section Balises, cochez la case **Balise d'affichage** pour activer le balisage des incidents de sécurité, le nom du profil est préfixé lors de l'activation de la balise.

   Vous pouvez éventuellement baliser les incidents de sécurité avec des balises pour les balises de profil initié, de profil terminé et de profil ayant échoué. Par défaut, cette option est désactivée pour tous les profils.

7. Cliquer sur **Fermer**.

Vérifier les filtres de condition de déclenchement

Validez le profil et vérifiez que les filtres de condition de déclenchement que vous avez configurés fonctionnent comme prévu.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Pourquoi et quand exécuter cette tâche

Après avoir activé le profil, en fonction des conditions de déclenchement configurées, vous pouvez afficher les résultats de la requête dans les Now Platform® incidents de sécurité.

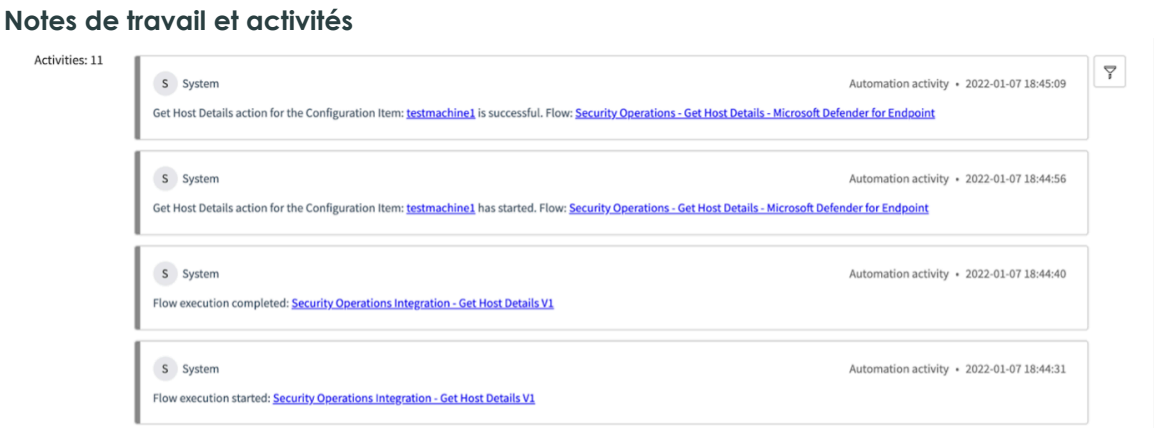
Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Pour créer un nouvel incident de sécurité, sélectionnez **Nouveau**.
3. Pour déclencher le profil respectif, indiquez les conditions de filtre indiquées dans le profil d'aptitude.
4. Cliquer sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Pour valider la section des notes de travail et des activités, affichez et vérifiez les enregistrements balisés avec les balises de profil initié, de profil terminé ou de profil ayant échoué.



6. Pour valider toutes les données des listes connexes, cliquez sur **Afficher toutes les listes connexes**.
7. Cliquez sur un onglet **de liste connexe** pour valider les détails.
   Par exemple, Détails de l'hôte.

Déclencher les Microsoft Defender pour point de terminaison options à partir des liens connexes

Déclenchez manuellement un profil d'aptitude après avoir examiné un incident de sécurité à partir des liens connexes.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Pourquoi et quand exécuter cette tâche

En plus d'exécuter le profil pour le CI ou le CI alternatif de l'incident de sécurité, vous pouvez également exécuter le profil pour les valeurs CI présentes dans la liste connexe Élément de configuration en sélectionnant **Inclure le CI connexe** dans la boîte de dialogue. Cela récupère également les données des valeurs CI présentes dans la liste connexe. Vous pouvez également exécuter le profil uniquement pour les valeurs CI présentes dans la liste connexe.

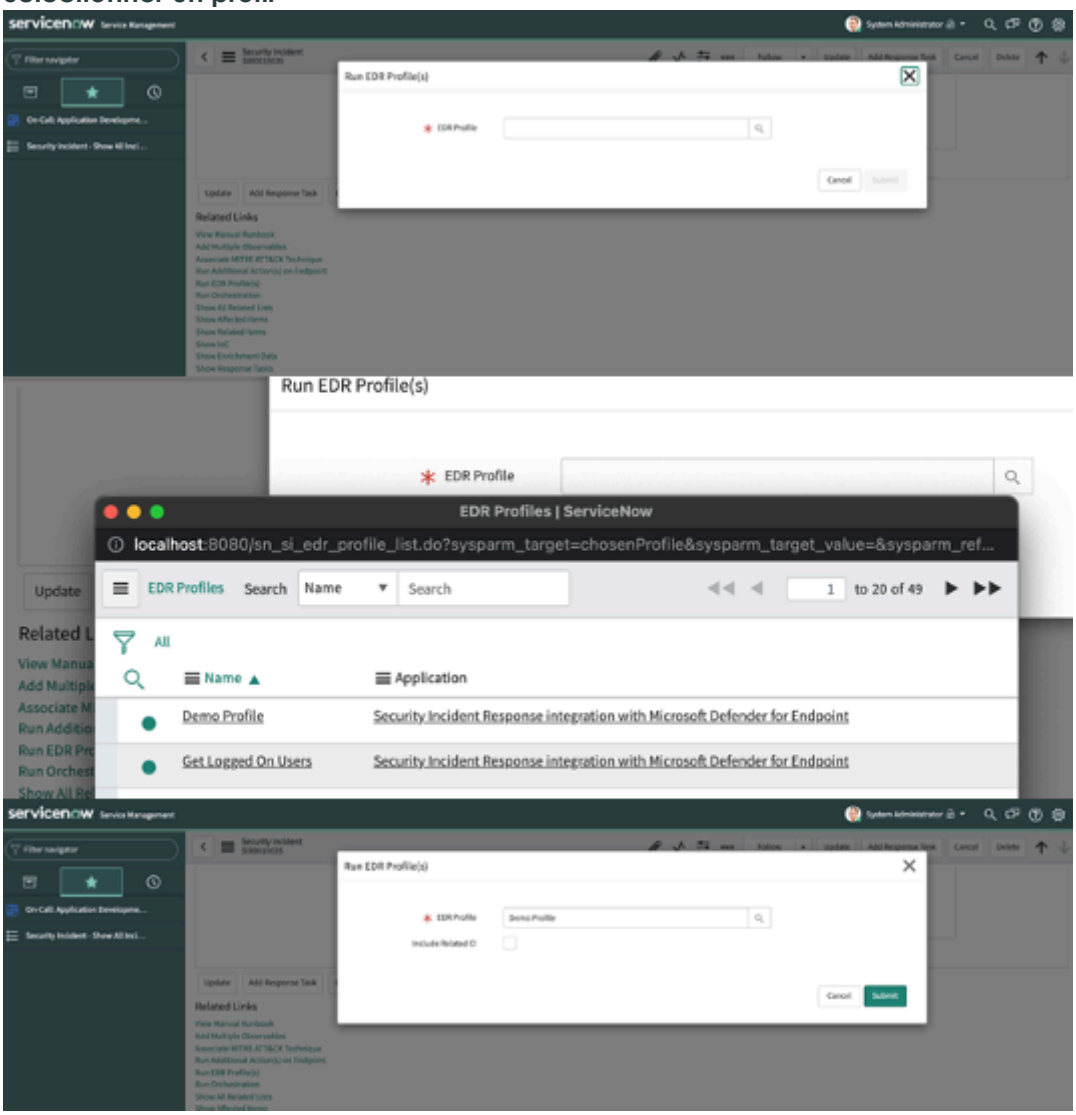
Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les Microsoft Defender pour point de terminaison informations.
3. Dans la section Liens connexes, cliquez sur **Exécuter le(s) profil(s) EDR**.
4. Parcourez et sélectionnez un profil dans la liste des profils disponibles, puis cliquez sur **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sélectionner un profil



Le profil sélectionné est déclenché manuellement.

5. Validez la section des notes de travail et des activités.
6. Affichez les balises et validez les données dans les listes connexes.

Déclencher la liste connexe De l'élément Microsoft Defender pour point de terminaison de configuration

Déclenchez manuellement un profil d'aptitude à partir de la liste connexe des éléments de configuration.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les Microsoft Defender pour point de terminaison informations.
3. Cliquer sur **Afficher toutes les listes connexes**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur la liste connexe Élément de configuration.
5. Sélectionnez les éléments de configuration ajoutés.
6. Dans les **actions** sur les lignes sélectionnées, sélectionnez une option.
   L'aptitude sélectionnée est déclenchée manuellement.
7. Validez la section des notes de travail et des activités.
8. Affichez les balises et validez les données dans les listes connexes.

Configurations supplémentaires dans Microsoft Defender pour point de terminaison

L'intégration Microsoft Defender pour point de terminaison prend en charge l'exécution d'actions supplémentaires au-delà des actions standard.

Le Microsoft Defender pour point de terminaison prend en charge les configurations supplémentaires suivantes :

Configurer l'option Isoler l'hôte dans Microsoft Defender pour point de terminaison

Isolez l'hôte de l'accès au réseau en Microsoft Defender pour point de terminaison fonction de la gravité de l'attaque. L'isolement de l'hôte du réseau vous permet d'empêcher toute autre activité malveillante ou attaque potentielle sur d'autres hôtes.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Exigences relatives à l'option Isoler l'hôte

Option	Obligatoire	Description
Isoler l'hôte	Type d'isolement	(Obligatoire) Type d'isolement (complet ou sélectif).
	Commentaire	(Obligatoire) Commentaire à associer à l'action.

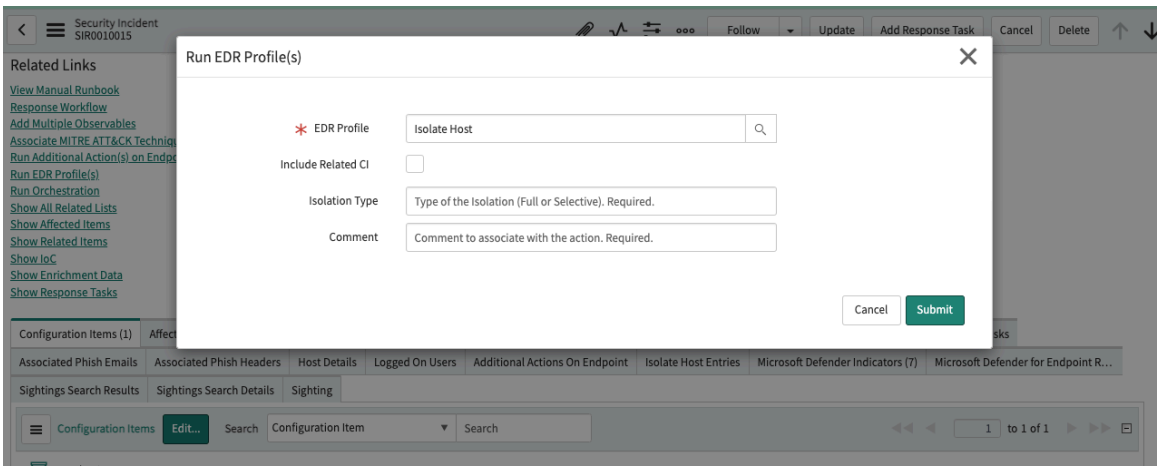
Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations sur Microsoft Defender pour point de terminaison.
3. Dans la section Liens connexes, cliquez sur **Exécuter le(s) profil(s) EDR**.
4. Parcourez et sélectionnez un profil avec **l'option Isoler l'hôte** sélectionnée dans la liste des profils disponibles, puis cliquez sur **Soumettre**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Isoler l'hôte



Vous pouvez également procéder comme suit :

a. Dans la section Listes connexes, cliquez sur **Afficher toutes les listes connexes**.

b. Cliquez sur la liste connexe **Élément de configuration** .

c. Sélectionnez **Isoler l'hôte** , puis sélectionnez les options correspondantes.

5. Validez l'activité d'automatisation et la section d'activités, et assurez-vous que les données sont conformes aux attentes.
6. Affichez les données et validez les détails d'isolement de l'hôte sur les listes connexes.

Configurer l'option Supprimer l'isolement de l'hôte dans Microsoft Defender pour point de terminaison

Si nécessaire, supprimez l'isolement d'un hôte précédemment isolé du réseau dans Microsoft Defender pour point de terminaison. Vous pouvez empêcher toute autre activité malveillante ou attaque potentielle sur d'autres hôtes.

Avant de commencer

Exigences relatives à l'aptitude Supprimer l'isolement

Option	Entrée requise	Description
Supprimer l'isolement	Commentaire	(Obligatoire) Commentaire à associer à l'action.

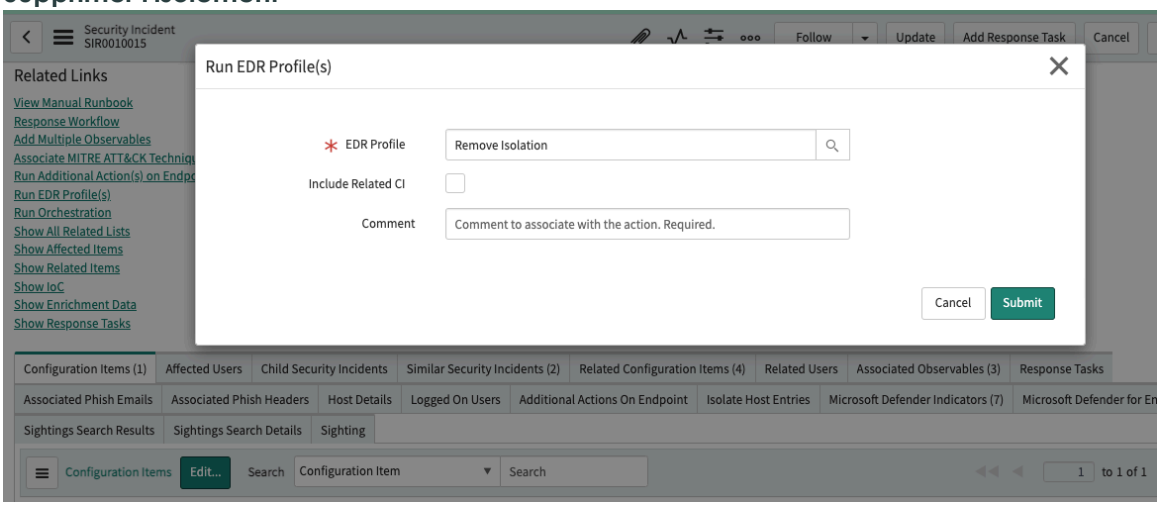
Rôle requis : sn_si.admin ou sn_si.analyst

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations sur Microsoft Defender pour point de terminaison.
3. Dans la section Liens connexes, cliquez sur **Exécuter le(s) profil(s) EDR**.
4. Parcourez et sélectionnez un profil avec **l'option Supprimer l'isolement** sélectionnée dans la liste des profils disponibles, puis cliquez sur **Soumettre**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Supprimer l'isolement



Vous pouvez également procéder comme suit :

a. Cliquez sur **Afficher toutes les listes connexes** dans la section Listes connexes.

b. Cliquez sur la liste connexe **Élément de configuration** .

c. Sélectionnez **Supprimer l'isolement** et sélectionnez les options correspondantes.

5. Validez l'activité et la section Activités d'automatisation.

6. Affichez les données et validez les détails d'isolement de l'hôte sur les listes connexes.

7. Validez les activités d'automatisation de l'exécution.

Configurer l'aptitude Exécuter l'analyse antivirus dans Microsoft Defender pour point de terminaison

Lancez à distance une analyse antivirus pour identifier et corriger les logiciels malveillants susceptibles d'être présents sur un appareil compromis. Exécutez l'analyse dans le cadre du processus d'enquête ou de réponse.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Configuration requise pour l'aptitude Exécuter l'analyse antivirus

Entrée	Description
Type d'analyse	(Obligatoire) Type d'analyse (complète ou rapide).
Commentaire	(Obligatoire) Commentaire à associer à l'action.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.

2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations sur Microsoft Defender pour point de terminaison.

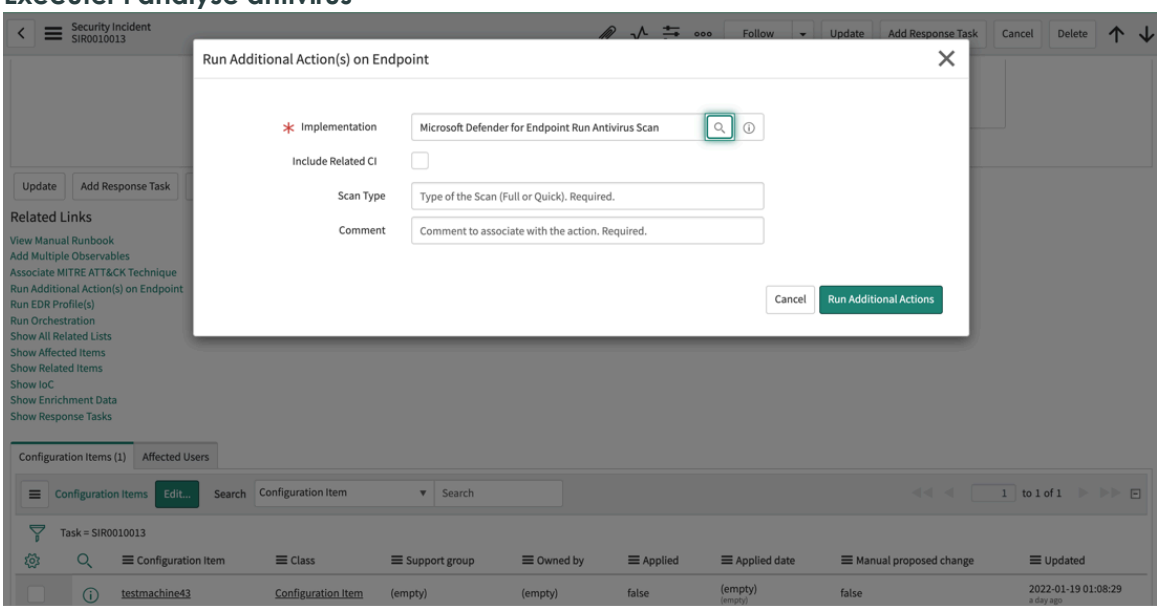
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans la section Liens connexes, cliquez sur **Exécuter des actions supplémentaires sur le point de terminaison**.

b. Parcourez et sélectionnez l'aptitude requise.
Par exemple, cliquez sur **Exécuter l'aptitude d'analyse antivirus** .

Exécuter l'analyse antivirus



Vous pouvez également procéder comme suit :

a. Dans la section Listes connexes, cliquez sur **Afficher toutes les listes connexes**.

b. Cliquez sur la liste connexe **Élément de configuration** .

c. Sélectionnez les éléments de configuration ajoutés et, dans Actions sur les lignes sélectionnées, sélectionnez **Exécuter des actions supplémentaires sur le point de terminaison**.
Une fois que vous avez sélectionné l'implémentation de l'aptitude **Exécuter l'analyse antivirus**, les champs **d'entréeType d'analyse supplémentaire** et Commentaire s'affichent.

3. Sélectionnez le **type d'analyse** que vous souhaitez exécuter (rapide ou complet) et ajoutez un commentaire avant d'exécuter l'analyse.
4. Pour lancer l'analyse antivirus, cliquez sur **Exécuter une action supplémentaire**.
5. Affichez les activités d'automatisation de l'exécution et validez-les.
6. Validez l'état de l'action sur les listes connexes Actions supplémentaires sur le point de terminaison.

Configurer l'option Restreindre l'exécution d'application dans Microsoft Defender pour point de terminaison

Pour contenir une attaque, restreignez ou verrouillez un appareil et empêchez les tentatives ultérieures d'exécution de programmes potentiellement malveillants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Exigences relatives à l'aptitude Restreindre l'exécution de l'application

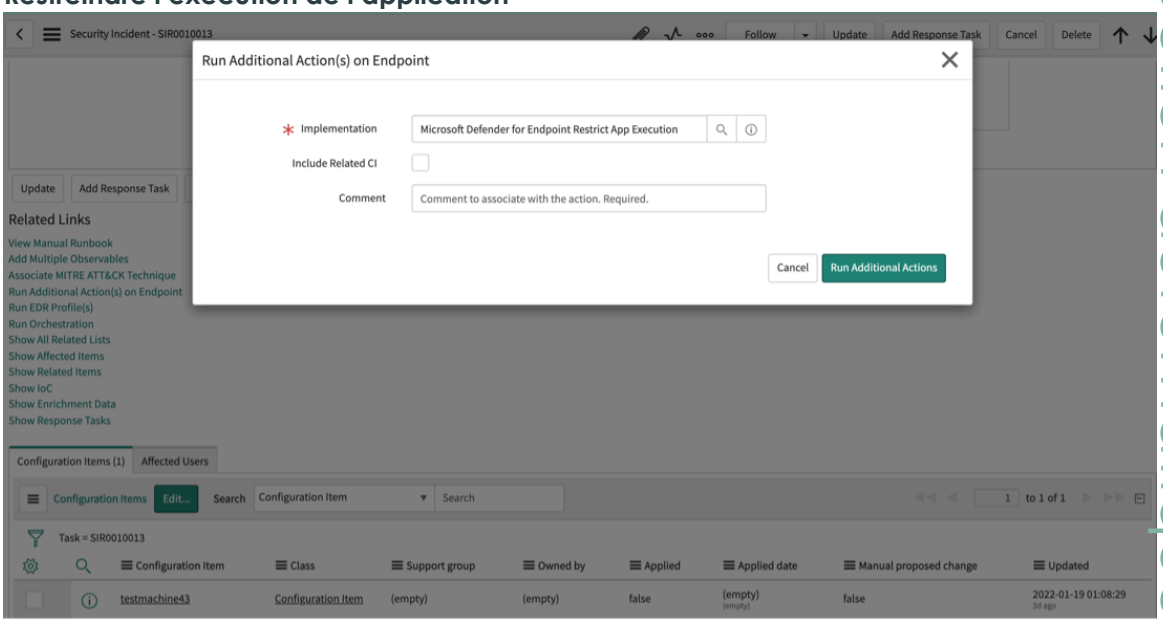
Entrée	Description
Commentaire	(Obligatoire) Commentaire à associer à l'action)

Rôle requis : sn_si.admin ou sn_si.analyst

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations sur Microsoft Defender pour point de terminaison.
   a. Dans la section Liens connexes, cliquez sur **Exécuter des actions supplémentaires sur le point de terminaison**.
   b. Parcourez et sélectionnez l'option **Restreindre l'exécution de l'application** .

Restreindre l'exécution de l'application



Vous pouvez également procéder comme suit :

   a. Dans la section Listes connexes, cliquez sur **Afficher toutes les listes connexes**.
   b. Cliquez sur la liste connexe **Élément de configuration** .
   c. Sélectionnez les éléments de configuration ajoutés.
   d. Dans Actions sur les lignes sélectionnées, sélectionnez **Exécuter des actions supplémentaires sur le point de terminaison**.
3. Pour activer Restreindre l'exécution de l'application sur l'ordinateur, cliquez sur **Exécuter une action supplémentaire**.
4. Affichez les activités d'automatisation de l'exécution et validez-les.
5. Validez l'état de l'action sur les listes connexes Actions supplémentaires sur le point de terminaison.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'aptitude Supprimer la restriction d'application dans Microsoft Defender pour point de terminaison

Si nécessaire, supprimez les restrictions de n'importe quelle application sur l'appareil.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

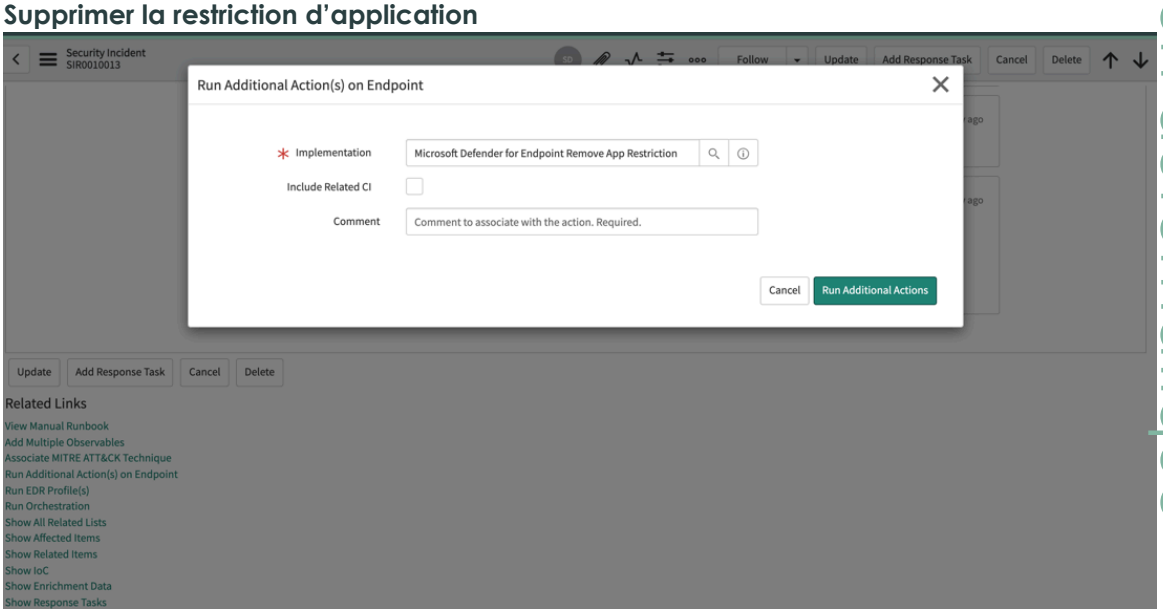
Configuration requise pour l'aptitude Supprimer la restriction d'application

Entrée	Description
Commentaire	(Obligatoire) Commentaire à associer à l'action)

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations sur Microsoft Defender pour point de terminaison.
   a. Dans la section Liens connexes, cliquez sur **Exécuter des actions supplémentaires sur le point de terminaison**.
   b. Parcourez et sélectionnez l'option **Supprimer la restriction d'application** .

Supprimer la restriction d'application



Vous pouvez également procéder comme suit :

   a. Dans la section Listes connexes, cliquez sur **Afficher toutes les listes connexes**.
   b. Cliquez sur la liste connexe **Élément de configuration** .
   c. Sélectionnez les éléments de configuration ajoutés.
   d. Sélectionnez **Exécuter des actions supplémentaires sur le point de terminaison**.
   Le champ d'entrée Commentaire supplémentaire s'affiche.
3. Pour supprimer la restriction d'application, cliquez sur **Exécuter une action supplémentaire**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Affichez les activités d'automatisation de l'exécution et validez-les.
5. Validez l'état de l'action sur les listes connexes Actions supplémentaires sur le point de terminaison.

Configurer l'option Obtenir les ordinateurs connexes à partir de Defender dans Microsoft Defender pour point de terminaison

Obtenir la liste des ordinateurs associés à des observables spécifiques.

Avant de commencer

Remarque : Les types d'observables pris en charge sont le nom de domaine, le hachage SHA1 et le nom d'utilisateur.

Rôle requis : sn_si.admin ou sn_si.analyst

Pourquoi et quand exécuter cette tâche

Vous pouvez récupérer la liste des ordinateurs qui ont accédé aux observables particuliers. Vous pouvez stocker la liste dans la table Détails des ordinateurs associés Microsoft Defender pour point de terminaison. Vous pouvez déclencher l'aptitude Obtenir les ordinateurs connexes à partir de Defender à partir de la liste connexe Observables associés.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations sur Microsoft Defender pour point de terminaison.



3. Dans la section Liens connexes, cliquez sur **Afficher IoC**.
4. Cliquez sur la liste connexe Observables associés.
5. Sélectionnez les observables associés.
6. Dans la liste Actions, sélectionnez l'option **Obtenir les ordinateurs connexes à partir de Defender** .
7. Validez l'activité et la section Activités d'automatisation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Affichez les données et validez les détails des ordinateurs connexes Microsoft Defender pour point de terminaison sur les listes connexes.
9. Affichez les activités d'automatisation de l'exécution et validez-les.

Configurer l'option Arrêter et mettre en quarantaine le fichier dans Microsoft Defender pour point de terminaison

Arrêtez et mettez en quarantaine les fichiers de la plateforme Microsoft Defender.

Avant de commencer

Types d'observables pris en charge : hachage SHA1.

Exigences relatives à l'option Arrêter et mettre en quarantaine les fichiers

Entrée	Description
Commentaire	(Obligatoire) Commentaire à associer à l'action)

Rôle requis : sn_si.admin ou sn_si.analyst

Pourquoi et quand exécuter cette tâche

Vous pouvez exécuter l'action Arrêter et mettre en quarantaine le fichier sur les observables particuliers de type SHA1 uniquement. Stockez les détails dans la table Actions supplémentaires sur le point de terminaison. Vous pouvez déclencher l'aptitude Arrêter et mettre en quarantaine le fichier à partir de la liste connexe Détails des ordinateurs associés Microsoft Defender pour point de terminaison.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations sur Microsoft Defender pour point de terminaison.
3. Dans la section Liens connexes, cliquez sur **Afficher toutes les listes connexes**.
4. Cliquez sur la liste connexe Détails des ordinateurs connexes Microsoft Defender pour point de terminaison.
5. Sélectionnez un ou plusieurs enregistrements.
6. Dans les **actions** sur les lignes sélectionnées, sélectionnez l'option **Arrêter et mettre en quarantaine le fichier** .
7. Validez l'activité et la section Activités d'automatisation.
8. Affichez les données et validez les données sur les listes connexes.
9. Affichez les activités d'automatisation de l'exécution et validez-les.

Créer et configurer un profil pour la recherche de perceptions avec l'intégration Microsoft Defender pour point de terminaison

Créez et configurez automatiquement le profil de recherche de perceptions à l'aide du Microsoft Defender pour point de terminaison.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le workflow de recherche de perceptions pour effectuer les recherches de perceptions. Ce workflow accepte une liste d'observables, trouve toutes les options d'implémentation, crée les requêtes basées sur les configurations de recherche de perception et exécute les recherches basées sur le workflow configuré.

Le Microsoft Defender pour point de terminaison fournit un profil de recherche de perception du système de base qui vous permet de configurer les recherches de perception automatiques. Avec ce profil, vous pouvez accéder aux informations de perception observables connexes d'une organisation et également voir les observations d'autres organisations.

Procédure

1. Accédez à la **Intégrations** > **Configuration de la recherche de détections**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs suivants du formulaire.

Formulaire de configuration de la recherche de perceptions

Champ	Description
Nom	Nom du profil de recherche de perceptions.
Est une recherche enregistrée	Option permettant d'enregistrer la configuration de la recherche. Les requêtes de configuration de recherche enregistrées sont des exemples de requêtes. Vous pouvez les remplacer par les paramètres de votre environnement et créer des configurations de recherche enregistrées supplémentaires si nécessaire.
Source de recherche de perceptions	La source configurée pour la recherche de perceptions dans Microsoft Defender pour point de terminaison l'intégration.
Rechercher	Chaîne de recherche native qui forme une requête.
Actif	Option permettant d'activer la configuration de recherche enregistrée. Seules les configurations de recherche actives peuvent effectuer une recherche d'observations.
Type d'observable	Type de catégorie de l'observable. Par exemple, adresse IP, valeur de hachage, URL et nom de domaine.
Nombre maximum d'observables par recherche	Nombre maximal d'observables que vous pouvez afficher à partir d'une requête de recherche. Définissez cette valeur sur 1 pour cette intégration.
Paramètres de la recherche de perceptions	Paramètres permettant de définir des requêtes plus complexes qui incluent la logique et d'autres opérateurs pris

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	en charge par le magasin de journaux spécifié.

4. Cliquez sur **Envoyer**.

Effectuer une recherche manuelle de perception dans Microsoft Defender pour point de terminaison

Sélectionnez un ou plusieurs observables et effectuez une recherche de perception manuelle pour Microsoft Defender pour point de terminaison déterminer la récurrence d'une menace dans le temps.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.analyst

Pourquoi et quand exécuter cette tâche

Les types d'observables pris en charge sont les suivants :

- Nom du domaine
- Adresse IP (V4)
- Adresse IP (V6)
- Hachage MD5
- Hachage SHA1
- Hachage SHA256

Procédure

1. Accédez aux **incidents de sécurité**.
2. Ouvrez un SIR existant ou créez-en un nouveau.
3. Dans les liens connexes, cliquez sur **Afficher IoC**.
4. Cliquez sur les listes connexes Observables associés.
5. Sélectionnez les observables.
6. Dans la liste Actions, cliquez sur **Exécuter l'enrichissement des observables**.
7. Sélectionnez les observables sous **Action** sur les lignes sélectionnées, puis cliquez sur **Exécuter la recherche de perceptions**.

> **Remarque :** La recherche de perception est prise en charge pour les types d'observables Nom de domaine, Adresse IP (V4), Adresse IP (V6), Hachage MD5, Hachage SHA1 et Hachage SHA256 respectivement.

8. Spécifiez le délai de la recherche, puis cliquez sur **Rechercher**.

> **Remarque :** Microsoft Defender pour point de terminaison prend en charge la recherche de perception uniquement pour les 30 derniers jours. Si votre requête de plage est antérieure aux 30 derniers jours, la recherche de perception ne récupère aucune donnée. Si votre requête de plage chevauche les 30 derniers jours, les observations des 30 derniers jours seulement sont récupérées, et si votre requête de plage est dans les 30 derniers jours, les observations de l'heure de début définie à l'heure actuelle sont récupérées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Une fois la recherche terminée, validez les résultats et les détails dans les listes connexes.
10. Cliquez sur **Détails de la recherche de perception** pour afficher les détails de la recherche de perception.
11. Cliquez sur **l'onglet Perception** pour plus de détails et sur l'onglet **Résultats de recherche de perceptions** pour obtenir les résultats de la recherche.

    Vous pouvez afficher des informations supplémentaires relatives à l'observation particulière dans le champ **Résumé** .

Procéder à un enrichissement automatique des observables dans Microsoft Defender pour point de terminaison

Effectuez un enrichissement automatique des observables dans Microsoft Defender pour point de terminaison pour enrichir les observables avec des informations supplémentaires provenant de diverses sources.

Avant de commencer

Vérifiez que vous avez activé la propriété système **Réponse aux incidents de sécurité** . Cette option déclenche l'option d'enrichissement des observables dans SIR, chaque fois qu'un observable est associé à un incident de sécurité.

Rôle requis : sn_si.admin, sn_si.analyst

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser cette option au cours des enquêtes de réponse à un incident pour contenir une menace identifiée. Lorsque de nouveaux observables sont associés à l'incident de sécurité, vous pouvez activer l'exécution automatique de l'enrichissement des observables dans Microsoft Defender pour point de terminaison.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations sur Microsoft Defender pour point de terminaison.
3. Validez l'activité d'automatisation une fois que les nouveaux observables ont été associés à l'incident de sécurité.
4. Affichez les résultats de l'enrichissement dans la liste connexe Indicateurs de l'incident de sécurité.
   Vous pouvez utiliser la table suivante pour plus d'informations sur l'enrichissement des observables.

Indicateur Microsoft Defender

Champ	Description
ID de l'indicateur	Identité de l'entité de l'indicateur. Cliquez sur **Ouvrir** pour afficher l'enregistrement en détail dans l'instance Now Platform
Observable	Observable associé au résultat.
Titre	Titre de l'indicateur.
Type d'indicateur	Type de l'indicateur.
Action	Action effectuée par l'indicateur.
Action recommandée	Actions recommandées pour l'indicateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Fournisseur de l'intégration	Intégration de la source Defender à partir de laquelle les données sont récupérées.
Date d'expiration	Délai d'expiration de l'indicateur.
Date de récupération	Date de création de l'enregistrement d'enrichissement.

Effectuer un enrichissement manuel de l'observable dans Microsoft Defender pour point de terminaison

Sélectionnez un ou plusieurs observables et effectuez un enrichissement manuel des observables pour enrichir les observables avec des informations supplémentaires provenant de .Microsoft Defender pour point de terminaison

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

L'intégration Microsoft Defender pour point de terminaison permet l'enrichissement des observables pour tous les types d'observables mappés dans le module Mappage observable-indicateur.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations sur Microsoft Defender pour point de terminaison.
3. Cliquez sur **Afficher toutes les listes connexes**.
4. Cliquez sur l'onglet **Observables associés** .
5. Sélectionnez les observables.
6. Dans la liste Actions, cliquez sur **Exécuter l'enrichissement des observables**.
7. Sélectionnez une **source** Microsoft Defender pour point de terminaison et déplacez-la vers la colonne **Sélectionnée** pour spécifier l'implémentation que vous souhaitez utiliser pour enrichir les observables sélectionnés.
8. Cliquez sur **Envoyer**.
9. Pour valider l'état de l'exécution, affichez les notes de travail.
10. Pour afficher les résultats, cliquez sur l'onglet **Indicateur Microsoft Defender** .
    Vous pouvez utiliser la table suivante pour plus d'informations sur l'enrichissement des observables.

Indicateur Microsoft Defender

Champ	Description
ID de l'indicateur	Identité de l'entité de l'indicateur. Cliquez sur **Ouvrir** pour afficher l'enregistrement en détail dans l'instance Now Platform
Observable	Observable associé au résultat.
Titre	Titre de l'indicateur.
Type d'indicateur	Type de l'indicateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Action	Action effectuée par l'indicateur.
Action recommandée	Actions recommandées pour l'indicateur.
Fournisseur de l'intégration	Intégration de la source Defender à partir de laquelle les données sont récupérées.
Date d'expiration	Délai d'expiration de l'indicateur.
Date de récupération	Date de création de l'enregistrement d'enrichissement.

Créer des indicateurs dans Microsoft Defender pour point de terminaison

Créez des indicateurs à partir des observables associés de l'incident de sécurité à l'aide de .Microsoft Defender pour point de terminaison

Avant de commencer

Rôle requis : sn_si.admin, sn_si.analyst

Pourquoi et quand exécuter cette tâche

L'intégration Microsoft Defender pour point de terminaison permet d'enrichir les observables pour tous les types d'observables qui sont mappés dans le module de mappage Observable-Indicateur.

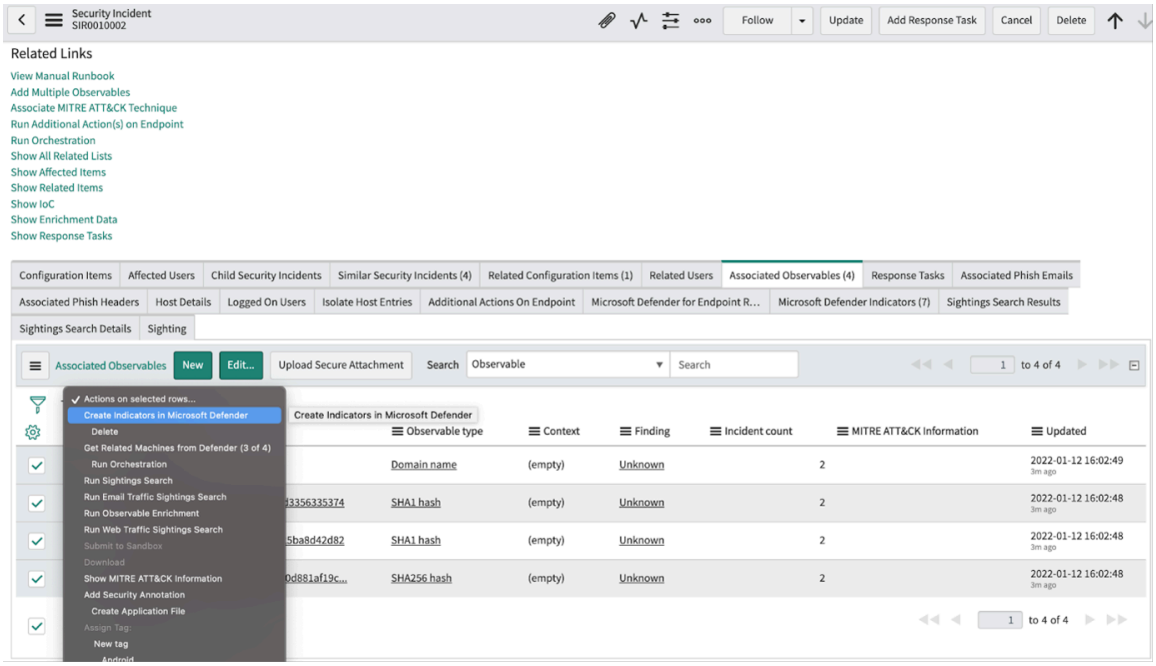
La création d'indicateurs vous permet de définir une liste d'indicateurs pour la détection, ainsi que pour bloquer la prévention et les réponses. Vous pouvez créer les indicateurs à partir de l'observable associé à l'incident de sécurité.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour lesquels vous souhaitez créer des indicateurs dans Microsoft Defender pour point de terminaison.
3. Cliquez sur les listes connexes Observables associés.
4. Ajoutez des observables existants ou créez-en de nouveaux.
5. Sélectionnez les observables.
6. Dans **Actions** sur les lignes sélectionnées, cliquez sur **Créer un indicateur dans Microsoft Defender**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Renseignez les champs du formulaire.

Champ	Description
Observables sélectionnés	Observables qui sont affectés. Cette action peut être utilisée pour créer des indicateurs pour plusieurs observables. Si vous souhaitez désélectionner un observable, vous pouvez le faire en désélectionnant les observables dans la liste. **Remarque :** Si les types d'observables pris en charge ne sont pas mappés, les indicateurs ne sont pas créés dans Microsoft Defender pour ces observables.
Titre	Titre de l'indicateur.
Description	Description de l'indicateur.
Délai d'expiration	Délai d'expiration de l'indicateur.
Actions recommandées	Actions recommandées qui doivent être effectuées pour l'indicateur.
Source	Configuration de l'intégration pour créer l'indicateur.
Action	Actions qui seront effectuées si l'indicateur est détecté dans l'organisation. Les valeurs possibles sont les suivantes : ◦ **Avertissement** ◦ **Bloc** ◦ **Audit**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ **'BlockAndRemediate'** ◦ **Autorisé**
Application	L'application Microsoft Defender pour point de terminaison associée à l'indicateur. Ce champ ne s'applique qu'à un nouvel indicateur et ne peut pas être utilisé pour un indicateur existant.
Gravité	Gravité de l'indicateur. Les valeurs possibles sont les suivantes : ◦ **Faible** ◦ **Moyen** ◦ **Élevé**
Noms de groupes RBAC	Noms de groupes RBAC auxquels l'indicateur est appliqué. Les noms figurent dans une liste séparée par des virgules.

8. **Cliquez sur Créer un indicateur**
9. Validez l'activité et les messages de l'interface utilisateur.
10. Cliquez sur l'onglet **Indicateur Microsoft Defender** pour afficher les résultats.

Mettre à jour les indicateurs dans Microsoft Defender pour point de terminaison

Mettez à jour les indicateurs existants à Microsoft Defender pour point de terminaison partir du menu contextuel de la liste ou de la vue de formulaire de l'indicateur Microsoft Defender respectivement.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.analyst

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Cliquez sur **Afficher toutes les listes connexes** , puis cliquez sur l'onglet **Indicateurs Microsoft Defender** .

Remarque :

Vous devez configurer la liste connexe des indicateurs Microsoft Defender, qui apparaîtraient dans les listes connexes des incidents de sécurité. Pour plus d'informations, consultez Actions d'interface utilisateur du formulaire.

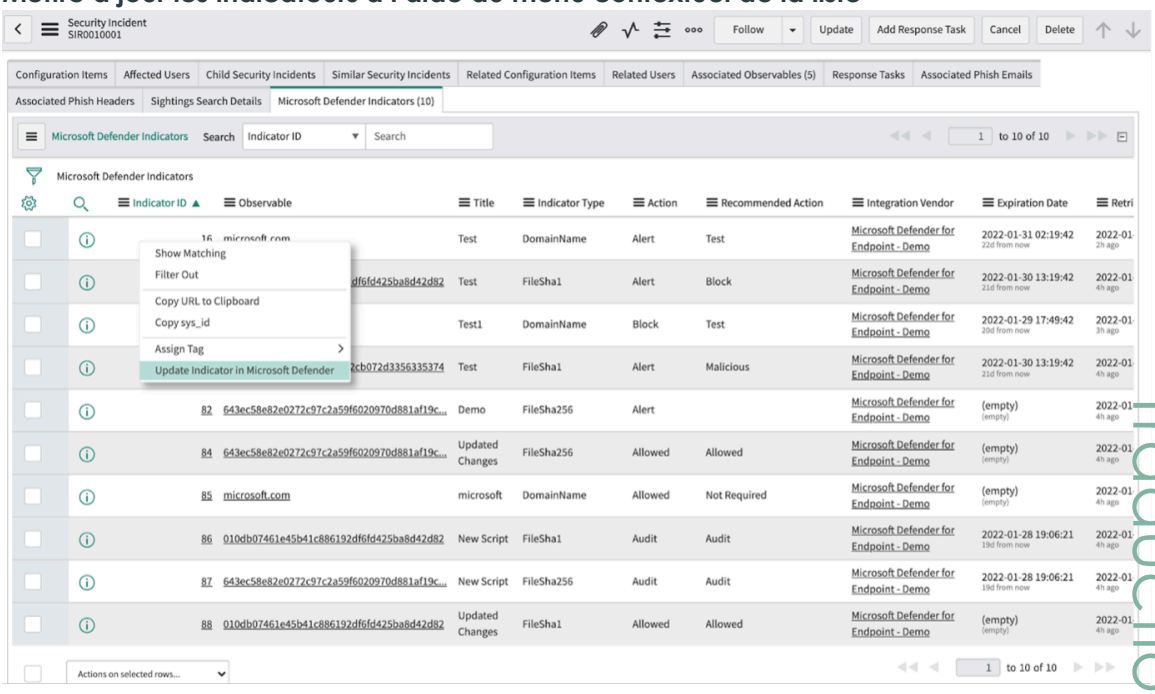
3. Mettez à jour les indicateurs Microsoft Defender pour point de terminaison de l'une des manières suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

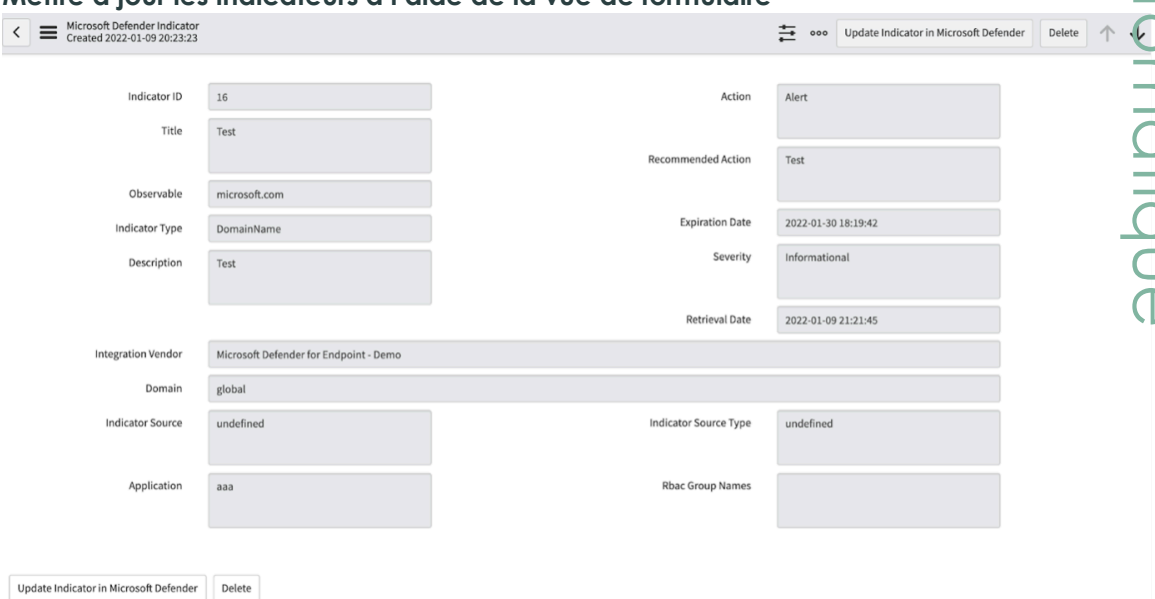
◦ Pour mettre à jour les indicateurs à partir du menu contextuel de la liste, sélectionnez la ligne de l'indicateur que vous souhaitez mettre à jour, puis cliquez sur **Mettre à jour l'indicateur dans l'option Microsoft Defender** .

Mettre à jour les indicateurs à l'aide du menu contextuel de la liste



◦ Pour mettre à jour les indicateurs à partir de la vue de formulaire, cliquez sur **Mettre à jour l'indicateur dans Microsoft Defender** dans la vue de formulaire.

Mettre à jour les indicateurs à l'aide de la vue de formulaire



4. Renseignez les champs du formulaire.

Formulaire d'indicateur Microsoft Defender

Champ	Description
Titre	Titre de l'indicateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Description de l'indicateur.
Délai d'expiration	Délai d'expiration de l'indicateur.
Actions recommandées	Actions recommandées à effectuer pour l'indicateur.
Source	Configuration de l'intégration pour créer l'indicateur.
Action	Actions effectuées si l'indicateur est détecté dans l'organisation. Les valeurs possibles sont les suivantes : ◦ **Avertissement** ◦ **Bloc** ◦ **Audit** ◦ **Bloquer et rattraper** ◦ **Autorisé**
Application	L'application Microsoft Defender pour point de terminaison associée à l'indicateur. Ce champ ne s'applique qu'à un nouvel indicateur et ne peut pas être utilisé pour un indicateur existant.
Gravité	Gravité de l'indicateur. Les valeurs possibles sont les suivantes : ◦ **Faible** ◦ **Moyen** ◦ **Élevé**
Noms de groupes RBAC	Noms des groupes RBAC auxquels l'indicateur est appliqué. Les noms figurent dans une liste séparée par des virgules.

5. Cliquez sur **Mettre à jour l'indicateur**.
6. Validez l'activité et les messages de l'interface utilisateur.

Séparation de domaine dans l'intégration Microsoft Defender pour point de terminaison

L'intégration de Séparation de domaine est prise en Microsoft Defender pour point de terminaison charge. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Prise en charge : basique

Procédez comme suit pour Séparation de domaine :

1. Créez un utilisateur avec le rôle sn_si.admin dans le domaine correspondant.
2. Exécutez les procédures d'intégration Microsoft Defender pour point de terminaison dans le domaine approprié.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de la limite de taux dans l'intégration Microsoft Defender pour point de terminaison

Configurez la limite de débit de l'API et le délai d'expiration de la limite de taux pour l'intégration Microsoft Defender pour point de terminaison .

Avant de commencer

Rôle requis : sn_si.admin, sn_si.analyst (lecture seule)

Procédure

1. Dans le filtre de navigation, saisissez `sys.properties.list`.
   La liste exhaustive des propriétés de la table Propriétés système [sys_properties] s'affiche.
2. Recherchez et modifiez les propriétés suivantes en fonction de vos besoins.

Nom de la propriété	Description
sn_sec_defender_ep.rate_limit_timeout_in_minutes	Si une demande ne s'exécute pas dans le délai spécifié, l'exécution est interrompue et un message d'erreur approprié s'affiche. Valeur par défaut : 75.
sn_sec_defender_ep.request_per_hour_limit	Si l'appel d'API configuré est effectué sur le même point de terminaison dans l'heure, la demande est mise en file d'attente jusqu'à ce que le seuil soit atteint ou que le délai configuré soit atteint. Valeur par défaut : 1500.
sn_sec_defender_ep.request_per_minute_limit	Si l'appel d'API configuré est effectué sur le même point de terminaison dans la minute, la demande est mise en file d'attente jusqu'à ce que le seuil soit atteint ou que le délai configuré soit atteint. Valeur par défaut : 100.
sn_sec_defender_ep.import_indicator_request_per_minute_limit	Si l'appel d'API configuré est effectué sur le point de terminaison dans la minute, la demande est mise en file d'attente jusqu'à ce que le seuil soit atteint ou que le délai configuré soit atteint. Valeur par défaut : 30.

Microsoft Exchange Online intégration

Pour l'application d'intégration Microsoft Exchange Online par ServiceNow, le Now Platform® Réponse aux incidents de sécurité produit (SIR) est intégré au Microsoft Exchange Online service, l'un des services basés sur le cloud de la Microsoft suite de produits Office 365. L'analyste de votre centre des opérations de sécurité (SOC) peut rechercher des menaces liées à la sécurité dans votre environnement de messagerie d'entreprise, et supprimer et corriger les e-mails d'hameçonnage grâce à des fonctionnalités de recherche et de suppression d'e-mails.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble

En tant qu'analyste des incidents de sécurité, vous exécutez l'intégration à partir de l'interface de l'analyste de sécurité, et le workflow renvoie les détails des e-mails qui correspondent aux critères de recherche. Les recherches d'e-mails sont basées sur des critères qui incluent des lignes d'objet ainsi que les adresses e-mail de l'expéditeur et du destinataire. Une fois la recherche d'e-mails terminée, vous pouvez supprimer les Microsoft Exchange Online e-mails suspects du service. Un processus d'approbation facultatif peut être configuré pour demander l'approbation avant de supprimer les e-mails.

Cette intégration de recherche et de suppression d'e-mails peut être utilisée avec un runbook ou un workflow de réponse au phishing plus large. Une fois qu'un utilisateur ou un employé de l'entreprise a reçu un e-mail suspect et l'a signalé à l'équipe de réponse anti-hameçonnage ou à la boîte de réception de l'entreprise, l'e-mail signalé est transféré à l'et Now Platform classé comme incident de sécurité. Après avoir vérifié qu'un e-mail est une attaque de hameçonnage, en tant qu'analyste responsable de l'enquête sur les incidents de hameçonnage, vous pouvez lancer une recherche d'e-mails pour déterminer si d'autres utilisateurs professionnels ont reçu cet e-mail d'hameçonnage. La recherche vous permet de localiser les e-mails associés à la même campagne d'hameçonnage et d'identifier d'autres victimes potentielles qui ont peut-être reçu l'e-mail, l'ont lu et ont potentiellement cliqué sur une URL malveillante ou ouvert une pièce jointe.

Fonctionnalités principales

L'intégration comprend les fonctionnalités clés suivantes :

- Configurez les critères de recherche des menaces d'hameçonnage dans Réponse aux incidents de sécurité en fonction des combinaisons des champs d'expéditeur, de destinataire et d'objet des e-mails.
- Pour les recherches d'e-mails longues et volumineuses, l'analyste des incidents de sécurité est informé par e-mail lorsque la recherche est terminée avec succès, ainsi que du nombre de messages correspondants.
- L'état des messages individuels vous informe si les destinataires ont lu ou supprimé des e-mails suspects.
- S'ils sont configurés, des processus d'approbation facultatifs garantissent que les e-mails suspects ne sont pas supprimés sans autorisation préalable.
- Une piste d'audit complète pour les demandes de suppression, qui inclut le nombre d'e-mails supprimés, est consignée dans les notes de travail des incidents de sécurité.
- Si le balisage est configuré, les balises de sécurité sont enregistrées lorsque les workflows de recherche et de suppression d'e-mails sont lancés et exécutés avec succès sur les incidents de sécurité.

Versions prises en charge Microsoft Exchange Online

Cette intégration prend en charge Microsoft Exchange Online les services qui font partie de la Microsoft suite Office 365. L'intégration ne prend pas en charge les environnements Exchange hébergés Microsoft . Microsoft exécute des Microsoft Exchange Online services sur la version Exchange 2016.

Prérequis

Le module d'extension com.snc.si_dep est requis pour n'importe quelle Now Platform version. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour garantir une installation fluide :

1. Cadre de travail de Security Integration
2. Security Support Common
3. Orchestration de support de sécurité
4. Réponse aux incidents de sécurité

Architecture d'intégration et connexion des systèmes

Pour plus d'informations sur l'architecture de l'intégration, y compris les termes clés et les détails de connexion des systèmes externes, reportez-vous Architecture d'intégration et connexion de systèmes externes pour l'intégration Microsoft Exchange Onlineà .

Liste de vérification

Les sujets suivants sont numérotés. Suivez les rubriques répertoriées ci-dessous dans l'ordre dans lequel elles sont présentées pour une installation et une configuration fluides de l'application.

Pour obtenir une liste de contrôle imprimable de ces étapes, reportez-vous à la section Liste de vérification pour l'intégration Microsoft Exchange Online. Vous pouvez utiliser cette liste pour surveiller votre progression au fur et à mesure que vous accomplissez les tâches de bout en bout de l'installation de l'intégration, de la configuration et de la vérification des résultats.

Configurez votre Microsoft compte Azure pour l'intégration ServiceNow Microsoft Exchange Online

Effectuez les tâches de configuration suivantes dans votre Microsoft portail Azure avant d'installer l'application ServiceNow pour cette intégration. Ce compte permet au locataire d'accéder aux détails de l'e-mail Microsoft Exchange Online .

Avant de commencer

Rôle requis : Microsoft administrateur du portail Azure

Ce compte est nécessaire pour accéder au locataire afin de recueillir des détails supplémentaires sur les Microsoft Exchange Online e-mails et de supprimer des e-mails. Ce compte est configuré dans le Microsoft portail Azure.

Les images utilisées dans les tâches suivantes sont privilégiées et exclusives et sont utilisées avec l'autorisation de Microsoft. Ce contenu est susceptible d'être mis à jour par Microsoft. Pour vérifier que vous avez accès au contenu le plus récent, consultez le site Web de la documentation Microsoft .

Dans les images suivantes, `ServiceNow Inc.` s'affiche pour le nom du compte dans les exemples pour le portail Azure. Dans votre compte du portail Azure, le nom de la société de votre compte dans le portail Azure s'affiche.

Procédure

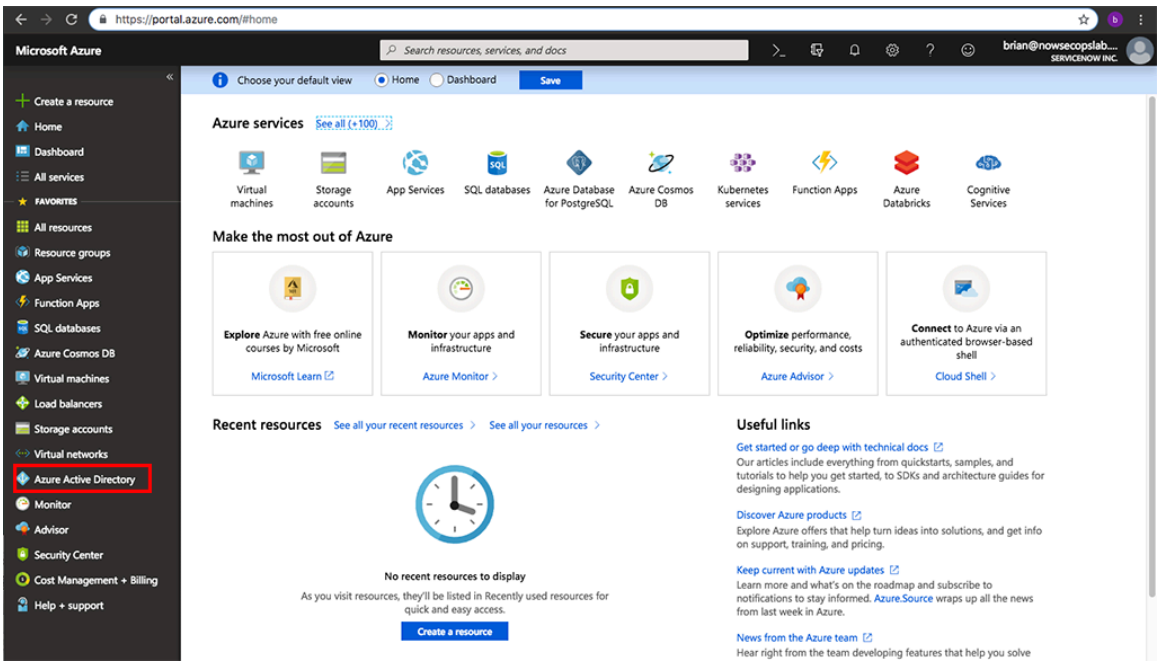
Si vous n'avez pas créé d'ID d'application pour l'authentification OAuth dans le Microsoft portail Azure, procédez comme suit.

Traduction automatique

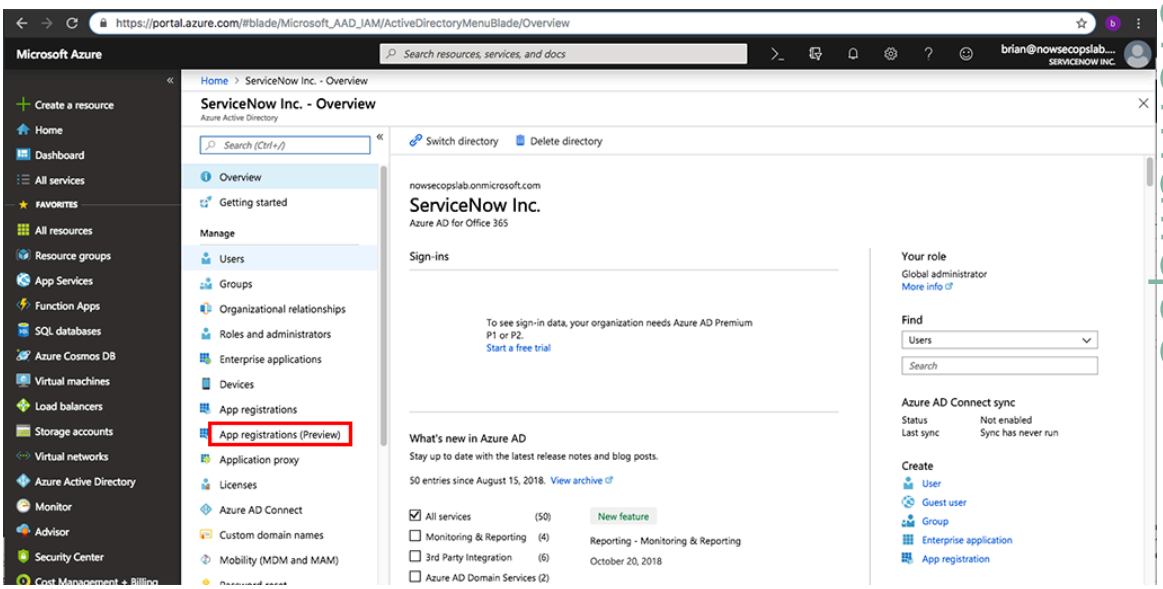
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Connectez-vous au Microsoft portail Azure à l'aide de vos informations d'identification d'administrateur du portail Azure.

b. Dans le panneau de navigation de gauche du volet Accueil, cliquez sur **Azure Active Directory**.



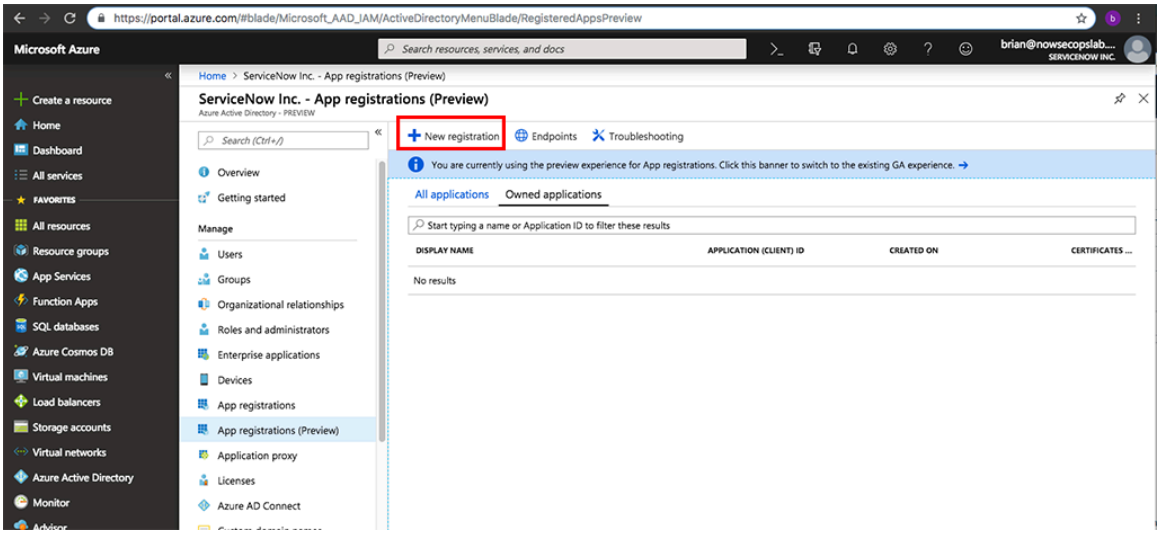
c. Dans le volet Vue d'ensemble qui s'affiche, cliquez sur **Inscriptions d'applications (aperçu).**



d. Dans le volet Inscriptions d'applications (aperçu) qui s'affiche, cliquez sur **Nouvelle inscription**.

Traduction automatique

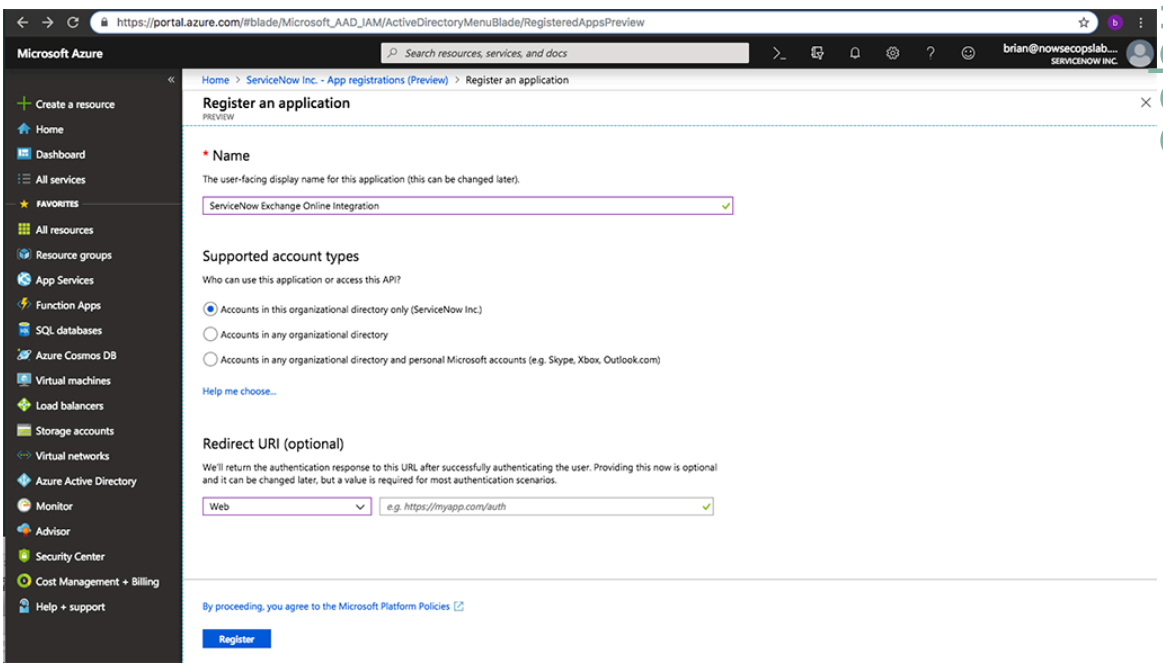
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



e. Remplissez le formulaire Enregistrer une demande qui s'affiche.

Un exemple de formulaire rempli est affiché après le tableau.

Champ	Description
Nom	Nom de l'application. Dans cet exemple, `l'intégration de ServiceNow Exchange Online` est saisie.
Types de compte pris en charge	Pour ce compte, dans Types de comptes pris en charge, cliquez sur **Comptes dans ce répertoire d'organisation uniquement ServiceNow Inc.).** Ce domaine est utilisé pour les recherches d'e-mails.
URL de redirection (facultatif)	Si vous saisissez une valeur pour ce champ, elle n'est pas utilisée par l'intégration.

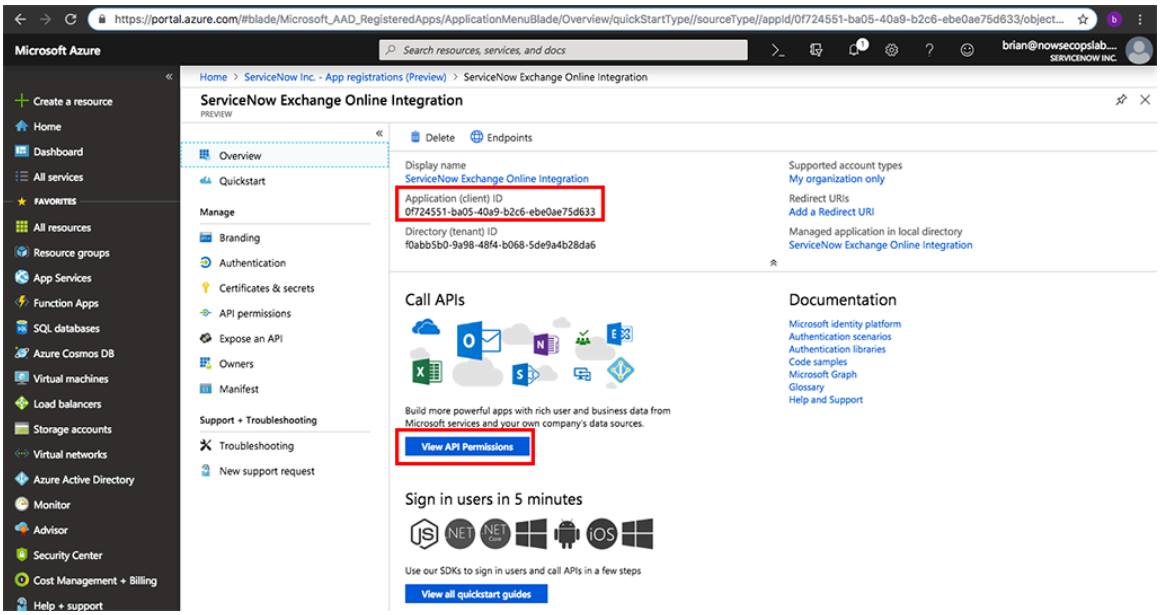


Traduction automatique

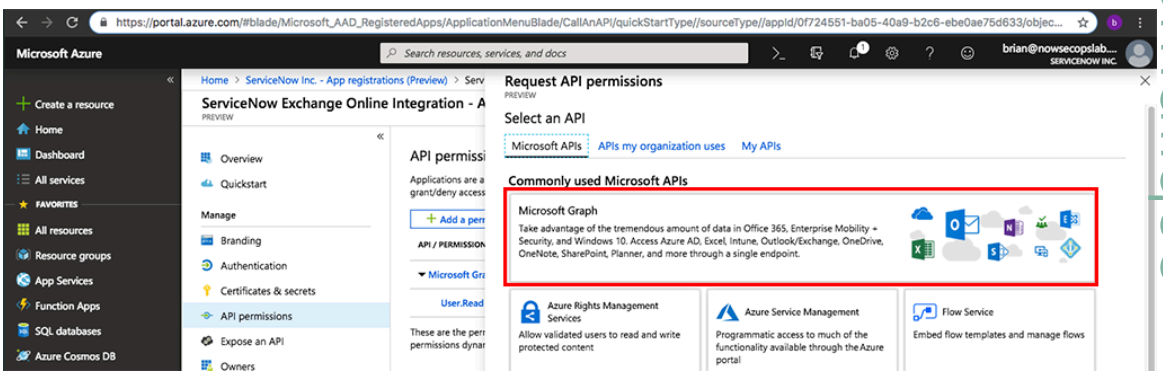
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Cliquez sur **Inscrire**.
Un ID d'application est créé. Cet ID est similaire à un nom d'utilisateur. Vous saisissez cette valeur sur la page de configuration dans le champ **ID de l'application OAuth** lors de l'étape de configuration de votre Now Platform instance décrite à la section Configurer l'intégration Microsoft Exchange Online avec votre Now Platform instance.

g. Une fois l'ID d'application (client) affiché dans le volet Intégration de ServiceNow Exchange Online, cliquez sur **Afficher les autorisations d'API**.



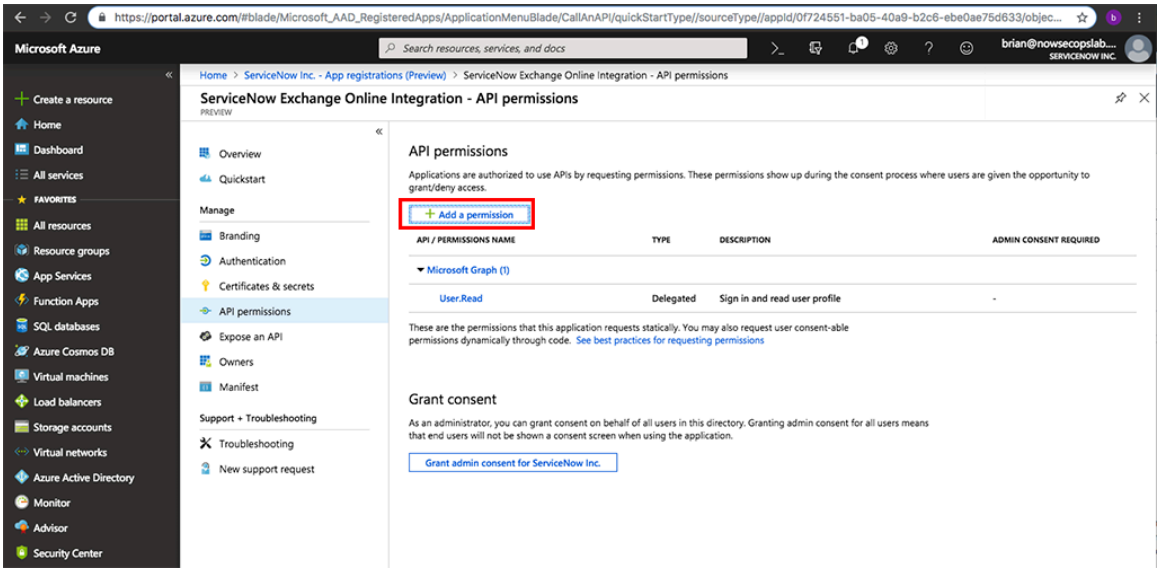
h. Dans le volet des autorisations de l'API de demande qui s'affiche, cliquez sur **Microsoft Graph**.



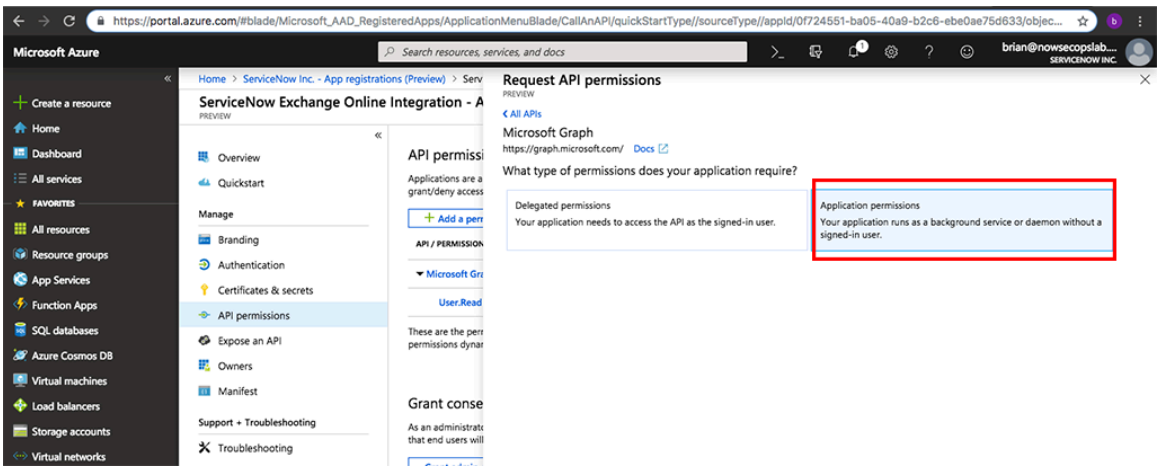
i. Dans le volet des autorisations de l'API d'Intégration de ServiceNow Exchange Online qui s'affiche, cliquez sur **Ajouter une autorisation**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



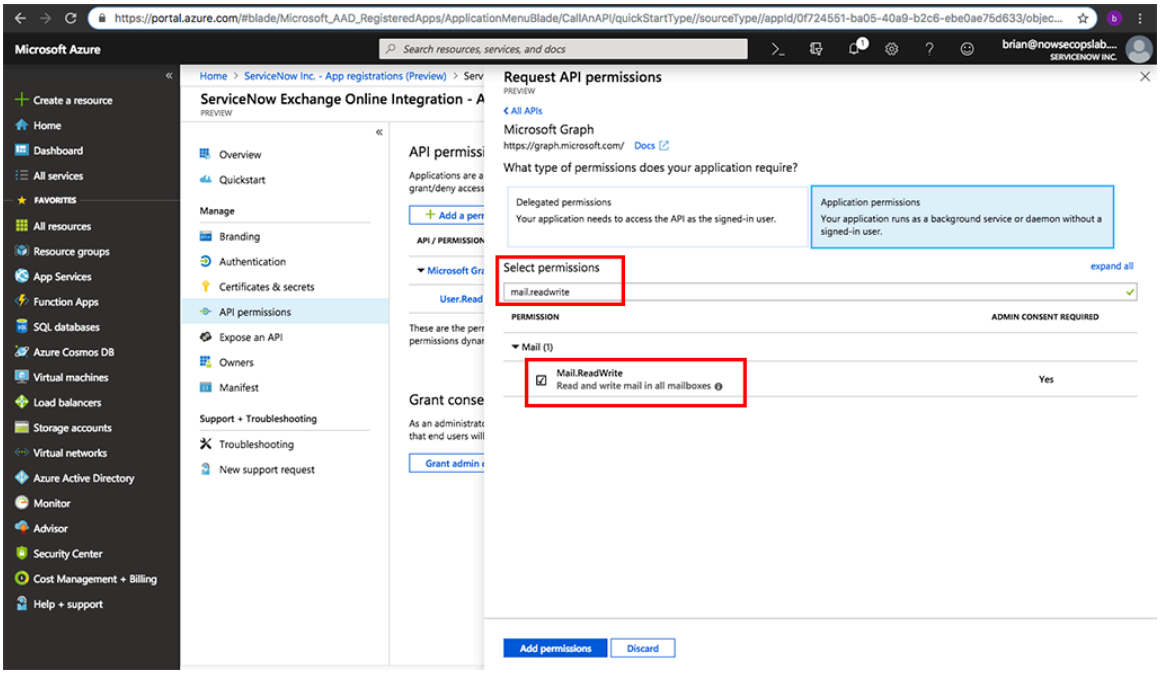
j. Dans le volet des autorisations d'API de demande qui s'affiche, cliquez sur **Autorisations d'application**.



k. Dans le champ Select Permissions (Sélectionner les autorisations) qui s'affiche, saisissez **Mail.ReadWrite** et cochez la case **Mail.ReadWrite** .

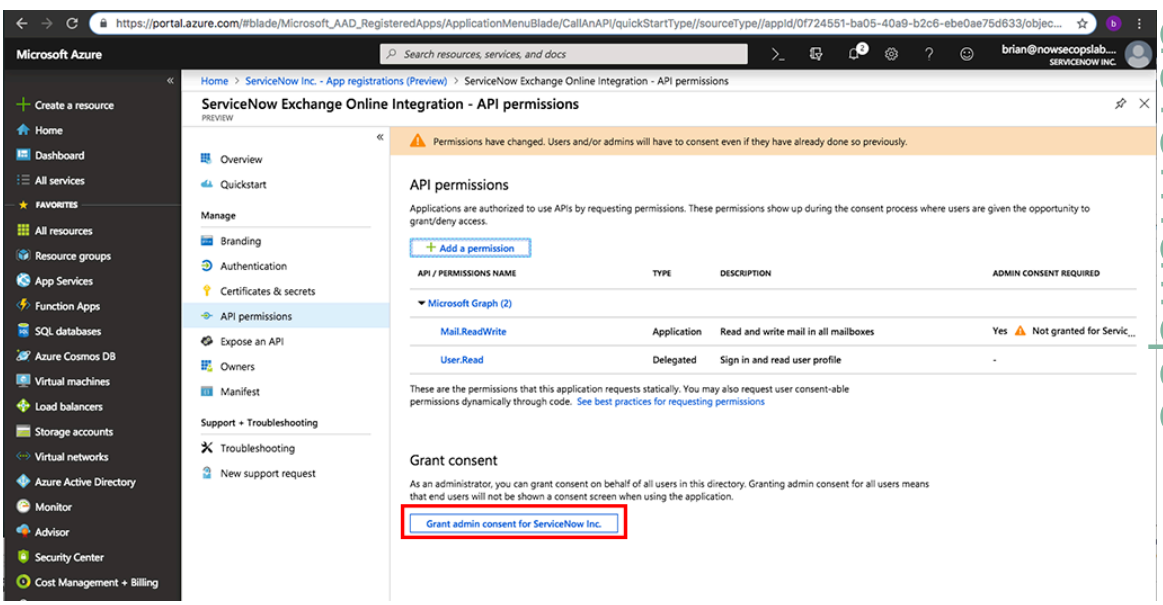
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



l. Cliquez sur **Ajouter des autorisations**.

m. Dans le volet des autorisations de l'API d'Intégration de ServiceNow Exchange Online qui s'affiche, cliquez sur **Accorder le consentement de l'administrateur pour <nom de votre organisation>**.

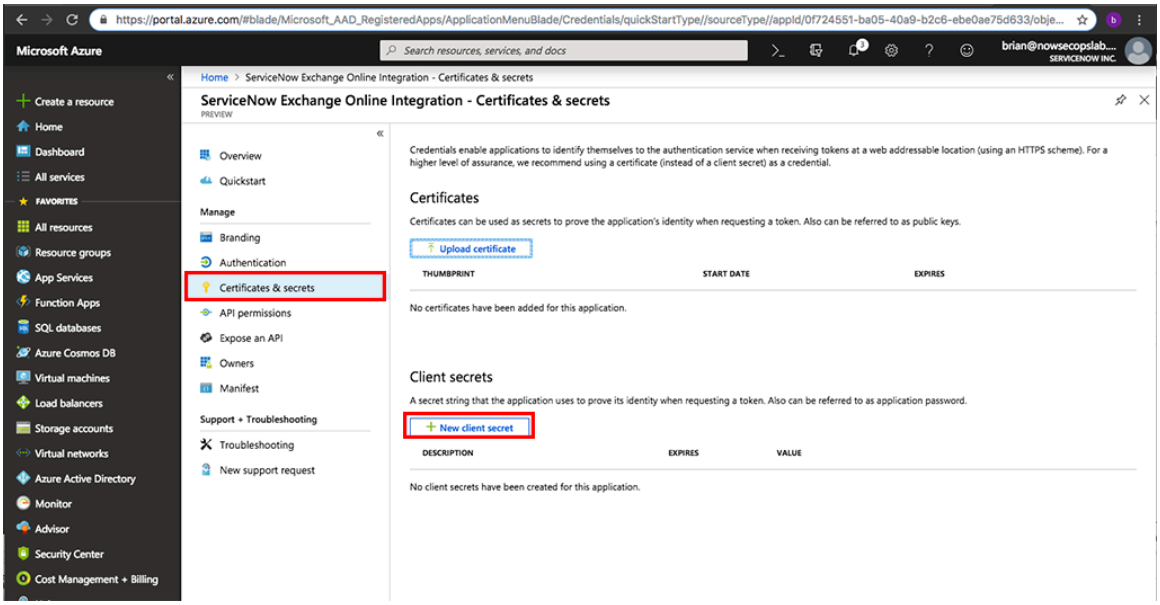


n. Pour confirmer la sélection d'API précédente (Microsoft Graph API) que vous avez entrée, cliquez sur **Confirmer**.

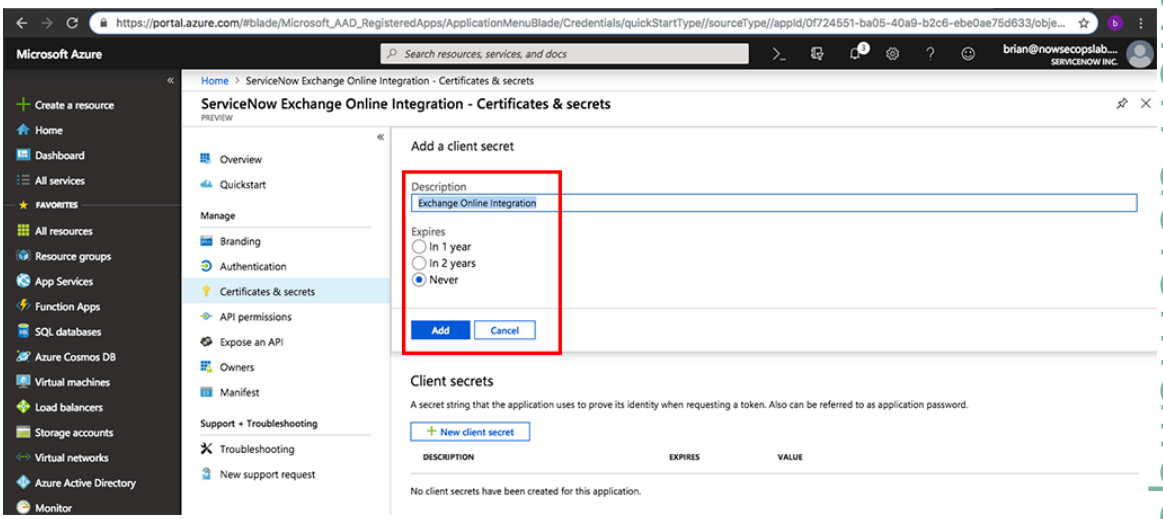
o. Dans le volet Intégration de ServiceNow Exchange Online - Certificats et secrets, cliquez sur **Certificats et secrets** , puis sur **Nouveau secret client** (mot de passe).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



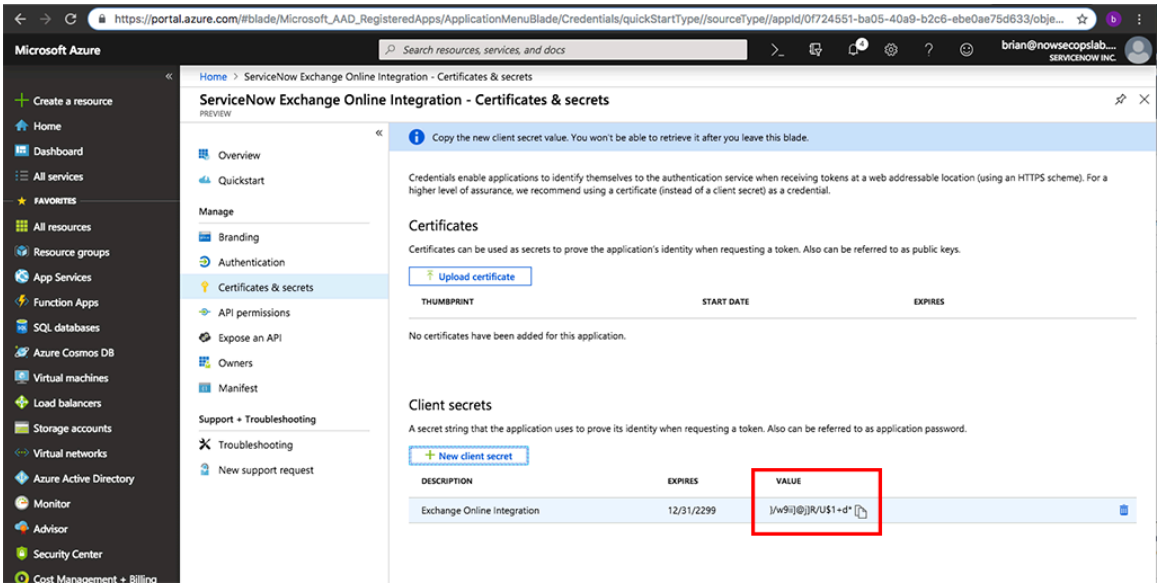
p. Dans le formulaire qui s'affiche dans le volet Intégration de ServiceNow Exchange Online - Certificats et secrets, saisissez le nom de l'application dans le champ `Description` , cliquez sur une option d'expiration, puis cliquez sur **Ajouter**.



Dans le volet Certificats et secrets qui s'affiche, dans la section **Secrets client** , sous `Valeur`, la ligne est renseignée avec le nouveau secret client (mot de passe). Conservez ce mot de passe en lieu sûr. Lorsque vous quittez cette page, cette valeur de mot de passe n'est plus visible. Vous saisissez ce mot de passe dans le champ **Secret du client OAUTH** sur la page de configuration lors de l'étape de configuration de l'intégration dans votre Now Platform instance. Les étapes de configuration de l'intégration sont décrites à la section Configurer l'intégration Microsoft Exchange Online avec votre Now Platform instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous avez créé avec succès un ID d'application pour l'authentification OAuth dans le Microsoft portail Azure.

Que faire ensuite

Vous êtes prêt à configurer votre Now Platform® instance pour l'intégration.

Configurer l'authentification basée sur certificat ou l'authentification par application uniquement

Une intégration initiale est requise pour l'authentification à l'aide d'objets d'application. Application et Principal de service sont utilisés de manière interchangeable, mais une application est semblable à un objet de classe tandis qu'un principal de service est semblable à une instance de la classe.

Pour plus d'informations sur les objets principaux d'application et de service dans Azure Active Directory, consultez Objets principaux d'application et de service dans Azure Active Directory . Pour obtenir un flux visuel détaillé sur la création d'applications dans Azure AD, consultez Créer une application Azure Active Directory et un principal de service pouvant accéder aux ressources .

Pour configurer l'authentification basée sur certificat ou l'authentification via l'application uniquement, procédez comme suit :

1. Enregistrez l'application dans Azure AD.
2. Affectez des autorisations d'API à l'application.

   Pour que l'objet d'application ait accès aux ressources, il doit disposer de l'autorisation d'application `Exchange.ManageAsApp` et `Mail.ReadWrite`.

3. Générez un certificat auto-signé et accordez l'accès à la clé privée.

   Créez et configurez un certificat X.509 auto-signé, qui est utilisé pour authentifier votre application auprès d'Azure AD, tout en demandant le jeton d'accès de l'application uniquement. Les certificats de nouvelle génération (CNG) ne sont pas pris en charge pour l'authentification d'application uniquement avec Exchange. Les certificats GNC sont créés par défaut dans les versions modernes de Windows. Vous devez utiliser un certificat provenant d'un fournisseur de clé CSP. `(-provider = 'Fournisseur de chiffrement fort de Microsoft')`.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Joignez le certificat à l'application Azure AD.
5. Affectez des rôles Azure AD à l'application.

   Le rôle Azure AD d'administrateur `de conformité` doit être affecté à l'application.

6. Créez un nouveau principal de service.

Étape 1 : enregistrer l'application dans Azure AD

1. Ouvrez le portail Azure AD .
2. Dans la zone **de recherche** en haut de la page, tapez **Inscriptions d'application**.
3. Sélectionnez **Inscriptions d'applications** dans les résultats de la section Services.

   Vous pouvez également accéder à la page Inscriptions de **l'application** à l'aide de https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade .

4. Sur la page **Inscriptions de l'application** , sélectionnez **Nouvelle inscription**.
5. Sur la page**Enregistrer une application** , configurez les paramètres suivants :

Champ	Description
Nom	Entrez quelque chose de descriptif. Par exemple, ExO PowerShell CBA.
Types de compte pris en charge	Vérifiez que **seuls les comptes de ce répertoire organisationnel (<VotreNomOrganisation> uniquement : locataire unique)** sont sélectionnés. Pour rendre l'application mutualisée pour les scénarios délégués Exchange Online, sélectionnez la valeur Comptes dans n'importe quel répertoire d'organisation (Tout répertoire Azure AD : mutualisé).

6. Une fois l'inscription de l'application terminée, sélectionnez **S'inscrire** et fermez la page de l'application.

Étape 2 : attribuer des autorisations d'API à l'application

Les procédures décrites dans cette section remplacent les autorisations par défaut qui ont été automatiquement configurées pour la nouvelle application. L'application n'a pas besoin des autorisations par défaut qui ont été remplacées.

1. Sur la page de l'application, sélectionnez **Manifeste sous Gestion** .
2. Dans la page Manifeste, recherchez l'entrée `requiredResourceAccess` (à la ligne 47 ou environ).
3. Modifiez les valeurs `resourceAppId`, `resourceAccess ID` et `resourceAccess` type comme indiqué dans l'extrait de code suivant :

```
"requiredResourceAccess": [
  {
   "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
  "resourceAccess": [
   {
    "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
    "type": "Role"
   }
  ]
 },
 {
  "resourceAppId": "00000003-0000-0000-c000-000000000000",
  "resourceAccess": [
   {
    "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
    "type": "Role"
   }
  ]
 }
],
```

4. Sélectionnez **Enregistrer**.
5. Sur la page **Manifest** , sélectionnez **Autorisations d'API** sous Gestion.
6. Sur la page **des autorisations d'API** , renseignez les champs.

Champ	Description
Nom API/autorisations	Vérifiez que la valeur `Exchange.ManageAsApp` and `Mail.ReadWrite` s'affiche.
Statut	La valeur incorrecte actuelle **n'est pas accordée pour <Organisation>** et cette valeur doit être modifiée. Sélectionnez **Accorder le consentement administrateur pour <Organisation>**, lisez la boîte de dialogue de confirmation qui s'ouvre, puis sélectionnez **Oui**. La valeur État doit maintenant être **Accordée pour <Organisation>**.

7. Fermez la page des autorisations d'API actuelle (et non l'onglet du navigateur) pour revenir à la page des inscriptions d'applications.

Étape 3 : générer un certificat autosigné et accorder l'accès à la clé privée

Créez un certificat x.509 auto-signé en procédant comme suit :

- Utilisez les applets de commande New-SelfSignedCertificate , Export-Certificate et Export-PfxCertificate dans une session Windows PowerShell avec élévation de privilèges (exécutée en tant qu'administrateur) pour demander un certificat auto-signé et l'exporter vers `.cer` et `.pfx` (SHA1 par défaut). Par exemple :

```
# Create certificate
$mycert = New-SelfSignedCertificate -DnsName
 "snowsecops.onmicrosoft.com" -CertStoreLocation
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(2) -KeySpec
 KeyExchange -Provider "Microsoft Strong Cryptographic Provider"

# Generate password fro private key
$mypwd = ConvertTo-SecureString -String '<password>' -Force
 -AsPlainText

# Export certificate to .pfx file
$mycert | Export-PfxCertificate -FilePath mycert.pfx -Password $mypwd

# Export certificate to .cer file
$mycert | Export-Certificate -FilePath mycert.cer
```

- Fournissez un accès par clé privée à l'utilisateur du service MID en procédant comme suit :
  1. Ouvrez **MMC (Microsoft Management Console).**
  2. À partir de la console MMC (Microsoft Management Console), accédez à **Certificats (ordinateur local)** > **Personnel** > **Certificats**.

     (Si MMC n'a pas d'élément de menu, ajoutez-le en accédant à **Fichier** > **Ajouter Supprimer le composant logiciel enfichable**.
  3. Cliquez avec le bouton droit de la souris sur le certificat que vous avez généré.
  4. Développer **Toutes les tâches** > **Gérer les clés privées**
  5. Ajoutez **l'utilisateur du service MID** à la liste des accesseurs.

Étape 4 : joindre le certificat à l'application Azure AD

Après avoir enregistré le certificat avec votre application, vous pouvez utiliser l'empreinte digitale pour l'authentification.

1. À la fin de l'étape 2, sélectionnez votre application dans l'onglet **Applications détenues** de la page **Inscription des applications**.

   Si vous devez revenir à la page **d'enregistrement des applications** , utilisez https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/%7E/RegisteredApps , vérifiez que l'onglet **Applications possédées** est sélectionné, puis sélectionnez votre application.
2. Sélectionnez **Certificats et secrets** sous Gérer.
3. Sur la page **Certificats et secrets** qui s'ouvre, sélectionnez Télécharger le **certificat**.
4. Accédez au certificat autosigné (`fichier .cer`) que vous avez créé à l'étape 3.
5. Lorsque vous avez terminé, sélectionnez **Ajouter**.

   Le certificat est maintenant affiché dans la section Certificats.
6. Notez `CertificateThumbPrint` et fermez la page actuelle **Certificats et secrets** .

Étape 5 : affecter des rôles Azure AD à l'application

1. Ouvrez le portail Azure AD .
2. Dans le champ **de recherche** en haut de la page, recherchez **Rôles et administrateurs**.
3. Sélectionnez des **rôles et des administrateurs Azure AD** dans les résultats de la section Services.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez également accéder à la page **Rôles et administrateurs Azure AD** à l'aide de https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade .

4. Sur la page **Rôles et administrateurs Azure AD** , recherchez et sélectionnez l'un des rôles pris en charge en cliquant sur le nom du rôle (et non sur la case à cocher) dans les résultats.

   Recherchez et sélectionnez le rôle **d'administrateur de conformité** .

5. Sur la page **Affectations** , sélectionnez **Ajouter des affectations**.
6. Dans la fenêtre contextuelle **Ajouter des devoirs** , recherchez et sélectionnez l'application que vous avez créée à l'étape 1.
7. Lorsque vous avez terminé, sélectionnez **Ajouter**.
8. Revenez à la page **Affectations** , vérifiez que le rôle a été affecté à l'application.

Étape 6 : créer un nouveau principal de service

Important : Assurez-vous d'être connecté à **PowerShell Sécurité et conformité** avant de terminer les étapes de création d'un nouveau principal de service. La création d'un nouveau principal de service sans connexion à PowerShell ne fonctionnera pas (votre ID d'application Azure et votre ID d'objet sont nécessaires pour créer le nouveau principal de service).

1. Exécutez la commande suivante pour stocker les détails de l'application Azure que vous avez enregistrée à l'étape 1 (`<AppName>`) dans une variable :

```
Install-Module -Name AzureAD
Import-Module -Name AzureAD
Connect-AzureAD
$AADApp = Get-AzureADServicePrincipal -SearchString"<AppName>"
```

   Pour obtenir des informations détaillées sur la syntaxe et les paramètres, consultez Get-AzureADServicePrincipal .

2. Dans la même fenêtre PowerShell, connectez-vous à PowerShell Sécurité et conformité :

```
Import-Module ExchangeOnlineManagement
Connect-IPPSSession -CertificateThumbPrint
 "<Your_Certificate_ThumbPrint>" -AppID $AADApp.AppId -Organization
 "<Your_organization>
```

   Exécutez les commandes suivantes pour créer un objet principal de service pour l'application Azure :

```
New-ServicePrincipal -AppId $AADApp.AppId -ObjectId $AADApp.ObjectId
 -DisplayName "<Descriptive Name>"
```

   Pour plus d'informations sur la syntaxe et les paramètres, consultez New-ServicePrincipal .

Configurer votre Now Platform® instance pour l'intégration Microsoft Exchange Online

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform® instance avant d'installer l'application Microsoft Exchange Online . Consultez la liste de vérification et vérifiez que vous avez terminé ces tâches avant de télécharger et d'installer Microsoft Exchange Online l'application pour l'intégration afin de garantir une installation et une configuration fluides.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform® et Réponse aux incidents de sécurité (SIR).	Les rôles suivants ServiceNow sont requis : • L'administrateur système (admin) installe les applications et attribue le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) configure l'application pour l'intégration. Si nécessaire, le rôle d'administrateur d'incident de sécurité attribue également à l'analyste d'incident de sécurité (sn_si.analyst) les rôles de lecture et d'écriture des e-mails (sn_sec_cmn.cap_email_write et sn_sec_cmn.cap_email_read). Les rôles (sn_sec_cmn.cap_email_read) et (com.snc.security_incident) sont installés avec le Réponse aux incidents de sécurité produit. Ils sont affectés par défaut à l'administrateur d'incident de sécurité et peuvent être réaffectés si nécessaire. • L'analyste des incidents de sécurité (sn_si.analyst) effectue des recherches d'e-mails et supprime des e-mails. Ce rôle vérifie également que les e-mails ont été supprimés et fonctionne avec les incidents de sécurité. ◦ Le rôle write permet au sn_si.analyst de modifier, de créer et d'effectuer des recherches d'e-mails et de supprimer des messages. Il n'existe pas de rôle distinct requis pour supprimer des messages. ◦ Le rôle de lecture permet au sn_si.analyst d'afficher les résultats sur les listes connexes relatives aux incidents de sécurité. **Remarque :** Le sn_si.analyst doit disposer des rôles (sn_sec_cmn.cap_email_read) et (sn_sec_cmn.cap_email_write) pour afficher les résultats de recherche d'e-mails et créer et effectuer des requêtes de recherche d'e-mails. Si elles ne sont pas affectées, les étapes suivantes décrivent comment affecter les rôles (sn_sec_cmn.cap_email_read) et

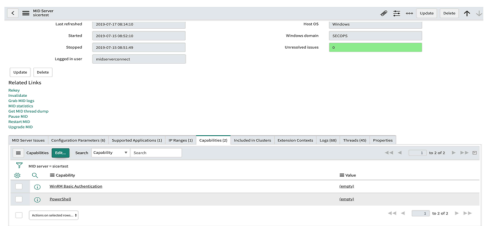
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	(sn_sec_cmn.cap_email_write) à l'analyste des incidents de sécurité. Pour plus d'informations sur l'affectation de rôles dans , reportez-vous à Réponse aux incidents de sécuritéla section Rôles installés avec SIR.
Vérifiez que vous avez configuré un Windows serveur MID dans votre Now Platform instance.	Le serveur MID est requis dans votre Now Platform environnement. Bien que le produit et le Microsoft Exchange OnlineNow Platform soient tous deux des offres cloud, un serveur MID est requis pour cette intégration. Le script PowerShell s'exécute à partir d'un Windows serveur dans l'environnement du client pour se connecter au Microsoft Exchange Online serveur via un MID Server. À partir de la version 10.5 et ultérieure de Pour Microsoft Exchange OnlineOpérations de sécurité l'intégration, vous devez installer le module Exchange Online PowerShell V2 dans le serveur MID. Pour plus d'informations, consultez la documentation Microsoft sur le module Exchange Online PowerShell V2 . Une connexion HTTPS sortante du MID Server est nécessaire pour que l'intégration récupère les Microsoft Exchange Online informations du locataire de service. Pour plus d'informations sur Serveur MID, voir Serveur MID Vous testez la connexion entre votre instance et le Serveur MID Windows après l'installation de l'application lors de l'étape de configuration de l'intégration.
Configurer le Windows Serveur MID pour gérer Microsoft Exchange Online les requêtes	• Configurez l'authentification basée sur certificat Exchange Online sur le fichier .Serveurs MID • Affectez les options d'authentification basée sur les certificats Exchange Online et PowerShell au(x) MID Server désigné(s).

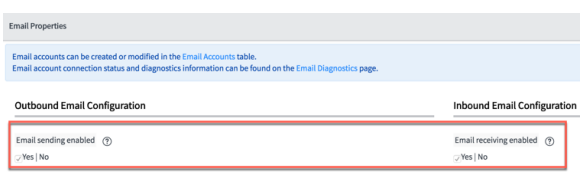
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	Dans votre environnement de serveur MID actuel, si vous avez défini les options sur **TOUS** pour chaque serveur MID, **l'authentification basée sur un certificat Exchange Online** est ajoutée automatiquement pour tous les serveurs MID. Dans ce cas, tous les MID Server de votre environnement peuvent recevoir Microsoft Exchange Online des demandes de recherche d'intégration. Pour vous assurer que les demandes de recherche sont envoyées uniquement aux MID Server désignés et pour éviter un acheminement de recherche incorrect, cliquez sur **Modifier** et suivez les étapes suivantes : • Supprimez l'aptitude **TOUT** de tout serveur MID qui ne dispose pas de la fonctionnalité **d'authentification basée sur un certificat Exchange Online** requise. • Sélectionnez les options requises comme indiqué ci-dessous, puis cliquez sur **Enregistrer**.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Le Réponse aux incidents de sécurité module d'extension Dependency (com.snc.si_dep) est requis et installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Orchestration de support de sécurité Pour en savoir plus sur la configuration de votre Now Platform instance pour l'intégration, consultez et .
Si votre organisation prévoit d'utiliser Now Platform des notifications par e-mail, vérifiez	Suivez ces étapes pour vérifier que l'option d'envoi et de réception d'e-mail est activée

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
que l'option d'envoi/réception d'e-mail est activée.	dans votre Now Platform® instance. Cette aptitude informe les utilisateurs par e-mail lorsque des recherches et des demandes de suppression ont été lancées et terminées avec succès. 1. Accédez à la **Propriétés d'e-mail** > **Administration** > **Propriétés d'e-mail**. 2. Dans la configuration des messages sortants, vérifiez que les `options Envoi d'e-mail activée` et `Réception d'e-mail activée sont sélectionnées`. Cette aptitude d'envoi/réception d'e-mail est requise pour que votre analyste d'incident de sécurité reçoive des notifications par e-mail envoyées par le Now Platform®. Si la fonctionnalité d'approbation de suppression est activée, les demandes de suppression d'e-mails sont également envoyées aux approbateurs par e-mail. Outre l'activation de cette propriété d'e-mail, aucune autre configuration n'est requise pour envoyer et recevoir des e-mails dans le Now Platform®fichier .
	

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

En tant qu'administrateur d'incident Now Platform de sécurité (sn_si.admin), les rôles de lecture et d'écriture des e-mails (sn_sec_cmn.cap_email_read) et (sn_sec_cmn.cap_email_write) vous sont automatiquement affectés lorsque vous téléchargez le Réponse aux incidents de sécurité produit (SIR). En tant qu'administrateur des incidents de sécurité, vous affectez ces rôles à l'analyste des incidents de sécurité (sn_si.analyst) ou à un autre rôle. Si vous n'avez pas affecté ces rôles à l'analyste des incidents de sécurité ou à un autre rôle, procédez comme suit pour les affecter.

Procédure

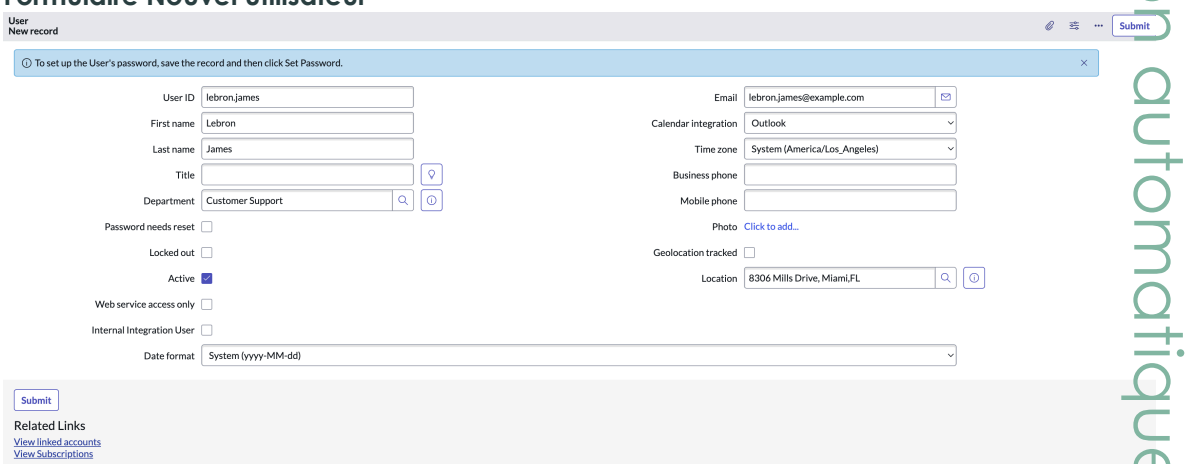
1. Accédez à la **Organisation** > **Utilisateurs**.
2. Cliquez sur le module **Utilisateurs** .
   a. Cliquez sur **Nouveau** dans la liste Utilisateurs qui s'affiche.
   b. Sur le formulaire Nouvel utilisateur qui s'affiche, remplissez le formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
UserID	ID d'utilisateur pour le rôle d'analyste Now Platform des incidents de sécurité, par exemple, `jferguson`.
E-mail	Adresse e-mail de l'entreprise. Les notifications de résultats de recherche d'e-mails et de confirmation de suppression d'e-mails sont envoyées à cette adresse e-mail. Pour cet exemple, `jferguson@servicenow.com` est utilisé, mais n'importe quelle adresse e-mail d'entreprise peut être utilisée pour recevoir ces notifications par e-mail selon les besoins de votre organisation.
Prénom	Prénom
Nom de famille	Nom de famille
Titre	`Analyste des incidents de sécurité`, `analyste de la sécurité` ou `analyste du centre des opérations de sécurité (SOC)`, par exemple.

Formulaire Nouvel utilisateur



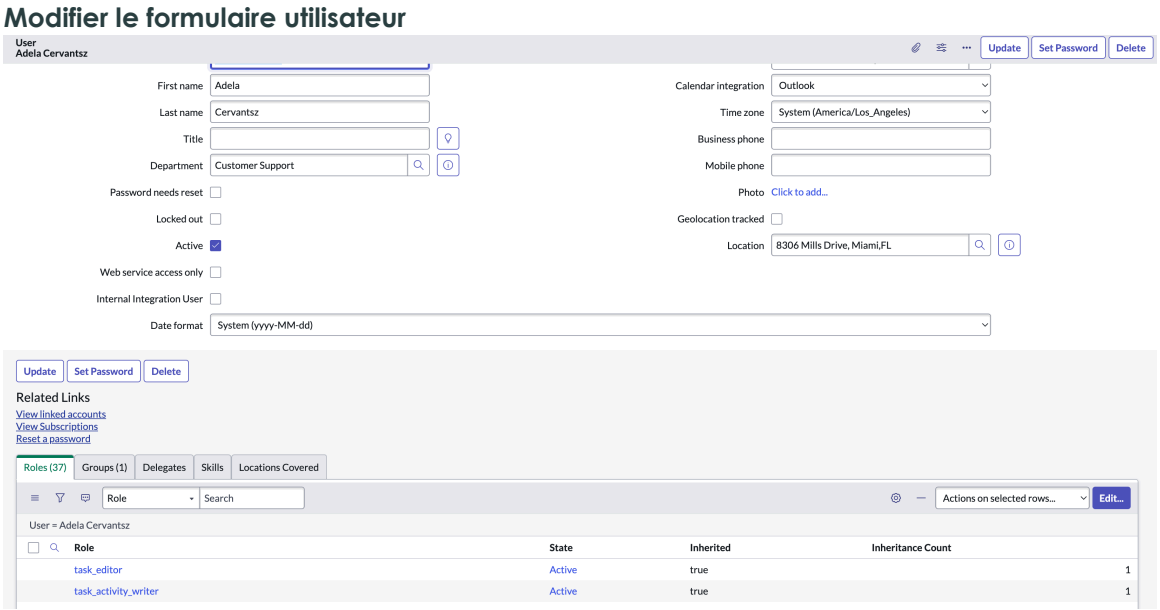
c. Cliquez sur **Envoyer**.
Le nouvel utilisateur apparaît dans la liste Utilisateurs.

3. Dans la liste Utilisateurs de la colonne ID d'utilisateur, cliquez sur le nom de l'utilisateur auquel vous souhaitez affecter les rôles `sn_sec_cmn.cap_email_read` et `sn_sec_cmn.cap_email_read`.

4. Dans l'enregistrement ouvert dans la section Liens connexes, cliquez sur **Modifier**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



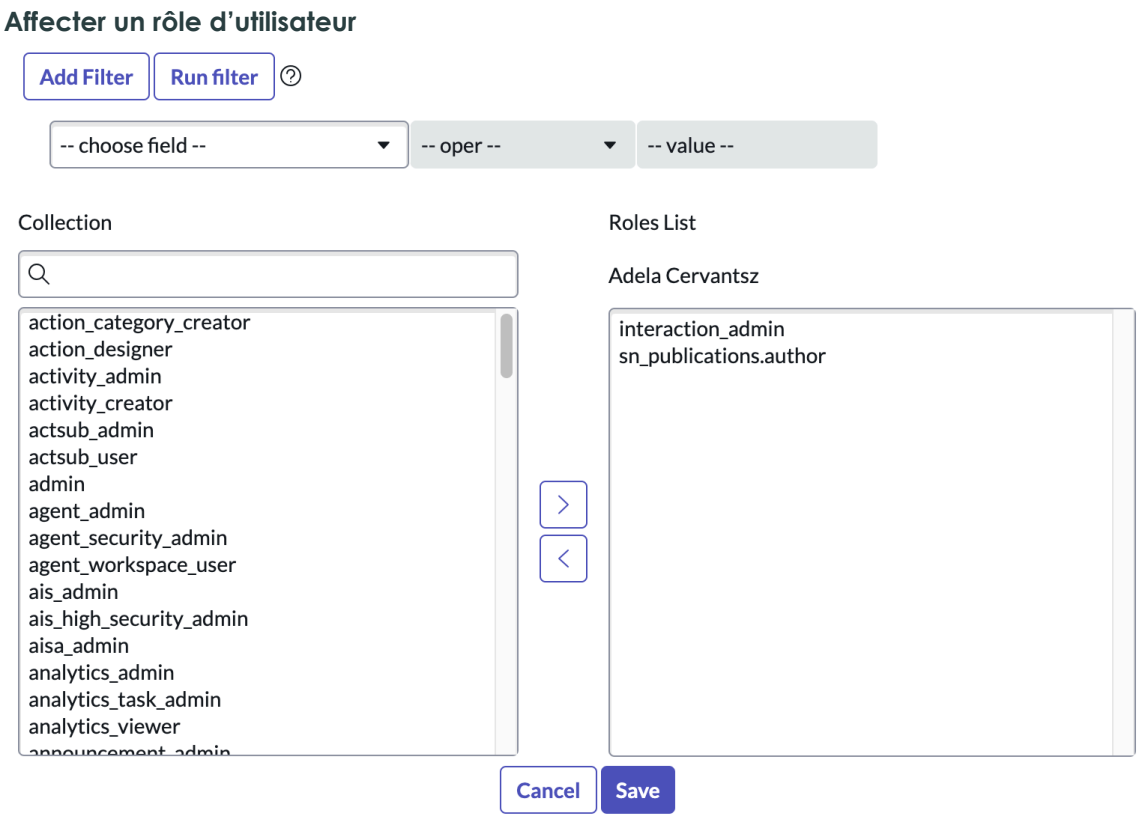
5. Sur le formulaire `Modifier les membres` qui s'affiche, saisissez `sn_sec_cmn.cap_email_read` dans le champ de collection.

> **Remarque :** La colonne sous le champ se remplit automatiquement. Si le rôle sn_si.analyst n'est pas affecté à l'utilisateur, saisissez également `sn_si.analyst` dans le champ Collecte. Dans la figure suivante, le rôle sn_si.analyst a déjà été attribué à Joe Ferguson.

6. Dans la colonne Collecte, sélectionnez, puis déplacez `sn_sec_cmn.cap_email_read`, `sn_sec_cmn.cap_email_read` et `sn_si.analyst` (s'ils ne sont pas déjà affectés) vers la liste des rôles.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Cliquez sur **Enregistrer**.
   Les rôles `sn_sec_cmn.cap_email_read` et `sn_sec_cmn.cap_email_read` sont affectés à l'analyste de la sécurité (jferguson).
8. Ajoutez des utilisateurs et affectez des rôles en fonction des besoins de votre organisation.
9. Facultatif : Si vous souhaitez activer l'aptitude d'approbation pour les demandes de suppression d'e-mails, procédez comme suit pour créer un groupe d'approbation.

   a. Accédez à la **Administration utilisateurs** > **Groupes**.

   b. Dans la liste Groupes qui s'affiche, cliquez sur **Nouveau**.

   c. Renseignez les champs du formulaire.

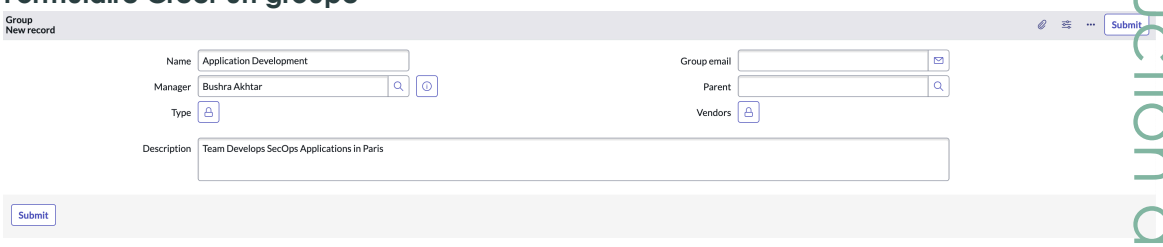
Champ	Description
Nom	Nom du groupe qui traite une approbation lorsqu'une demande de suppression d'e-mail est soumise, `par exemple, les approbateurs Exchange Online`.
E-mail de groupe	Entrez une adresse e-mail si vous souhaitez une liste de distribution d'e-mails de groupe ou l'adresse e-mail du point de contact, tel que le gestionnaire de groupe. (Optional) Laissez ce champ vide si vous souhaitez que des notifications par e-mail

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	soient envoyées aux adresses e-mail individuelles de chaque utilisateur du groupe.
Responsable	(Facultatif) Nom du gestionnaire de groupe. Cliquez sur l'icône de recherche pour afficher la liste.
Parent	(Facultatif) Si ce groupe a un parent, l'autre groupe dont il est membre.
Type	(Facultatif) Définissez des catégories de groupes.
Fournisseurs	(Facultatif) Affectez le rôle vendor_manager aux utilisateurs impliqués dans le processus de gestion des fournisseurs de votre organisation.
Description	(Facultatif) Informations supplémentaires sur le groupe.

Formulaire Créer un groupe



Pour plus d'informations sur la création de groupes et l'affectation de rôles, voir Créer un groupe d'utilisateurs .

d. Cliquez sur **Envoyer**.
Dans la colonne `Nom` , le nouveau groupe s'affiche dans la liste Groupes.

Vous pouvez ajouter d'autres utilisateurs à ce groupe. Un utilisateur hérite des rôles de tous les groupes auxquels il appartient. Vous pouvez également affecter des rôles directement à un utilisateur. Pour en savoir plus, consultez la rubrique Gestion des rôles . Chaque utilisateur peut approuver les demandes de suppression d'e-mails soumises par l'analyste de sécurité. Un seul utilisateur est requis pour approuver ou rejeter la demande.

Si votre organisation souhaite un niveau de contrôle supplémentaire sur la suppression des e-mails avec cette intégration, activez l'option d'approbation facultative. Cochez la case **Activer** de l'onglet `Paramètres supplémentaires` au cours de l'étape de configuration pour activer les approbations. Dans l'exemple précédent, chaque utilisateur du groupe `d'approbateurs Exchange Online` est disponible pour traiter les demandes de suppression par notification par e-mail.

Installer l'application Microsoft Exchange Online pour l'intégration ServiceNow Microsoft Exchange Online

Avant d'exécuter l'intégration sur votre instance, installez l'application Microsoft Exchange Online pour l'intégration à partir du ServiceNow Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Avant d'installer l'application à partir de sur votre Now Platform instance, effectuez toutes les tâches répertoriées dans les listes de ServiceNow Store vérification des prérequis.

Rôle requis : administrateur

Important :

- L'authentification basée sur un certificat Microsoft Exchange Online est prise en charge sur Microsoft Exchange Online for Security Operations version 10.5.4 ou ultérieure.
- Si vous installez des données de démonstration, une configuration de démonstration sans informations d'identification est automatiquement créée. Cela peut entraîner des erreurs. Pour plus de détails, voir KB0755880 .

Procédure

1. Si vous n'avez pas installé l'application pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois que vous avez installé l'application à ServiceNow Storepartir du , configurez-la pour qu'elle se connecte à votre Now Platform instance.

Information associée

Configurez votre Microsoft compte Azure pour l'intégration ServiceNow Microsoft Exchange Online

Configurer l'authentification basée sur certificat ou l'authentification par application uniquement

Configurer votre Now Platform instance pour l'intégration Microsoft Exchange Online

Configurer l'intégration Microsoft Exchange Online avec votre Now Platform instance

Une fois que vous avez installé l'application à ServiceNow Storepartir du , configurez-la pour qu'elle se connecte à votre Now Platform instance. Cette activation active les workflows de recherche et de suppression.

Avant de commencer

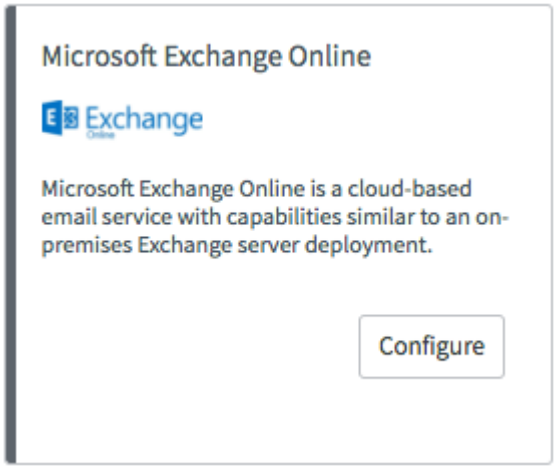
Rôle requis : sn_si.admin

Procédure

1. Dans votre Now Platform instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
2. Localisez la Microsoft Exchange Online tuile.
3. Cliquez sur **Configurer**.

Traduction automatique

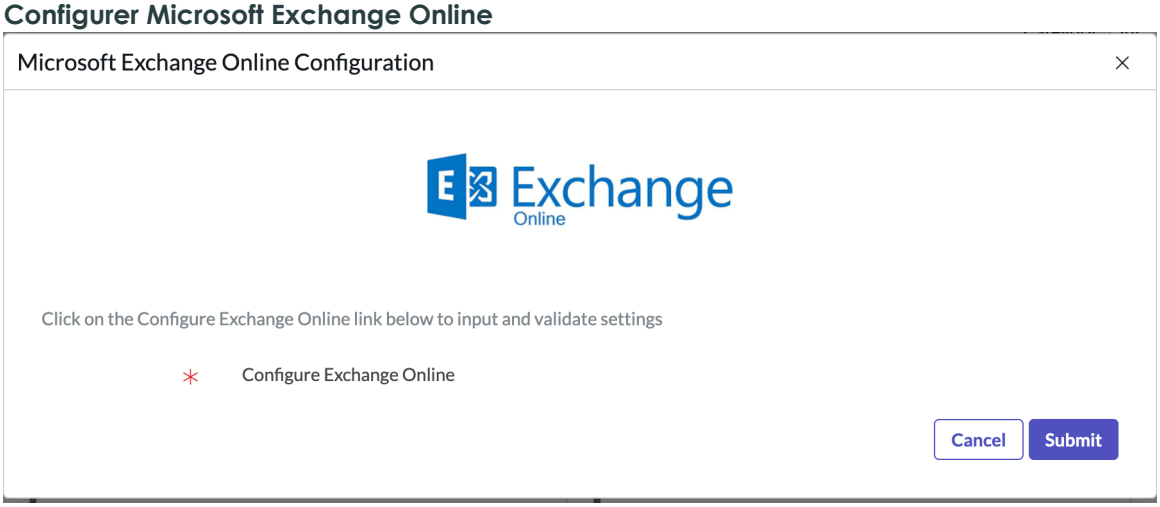
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans la boîte de dialogue Configuration qui s'affiche Microsoft Exchange Online , cliquez sur **Configurer Exchange Online**.

   Vous trouverez ci-dessous un exemple de formulaire rempli et validé.

Configurer Microsoft Exchange Online



Option	Description
Onglet Paramètres de connexion	
Locataire	Le Microsoft Exchange Online locataire sur lequel vous souhaitez effectuer des recherches. Ce texte est le nom unique qui apparaît après @ pour les adresses e-mail de votre organisation. Pour cet exemple, `snowsecops.onmicrosoft.com` est le locataire (domaine).
Empreinte du certificat	L'empreinte d'un certificat est un hachage d'un certificat, calculé sur toutes les données du certificat et sa signature. Les empreintes digitales sont utilisées comme identifiants uniques pour les certificats, dans les applications lors de la prise de décisions de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	confiance, dans les fichiers de configuration et affichées dans les interfaces.
ID de l'application OAuth	L'ID d'application (client) qui a été généré pour le compte que vous avez créé dans le Microsoft portail Azure. Pour plus d'informations, consultez Configurez votre Microsoft compte Azure pour l'intégration ServiceNow Microsoft Exchange Online.
Secret client OAuth	Mot de passe (secret client) pour le compte que vous avez créé dans le Microsoft portail Azure. Pour plus d'informations, consultez Configurez votre Microsoft compte Azure pour l'intégration ServiceNow Microsoft Exchange Online.
Onglet Paramètres supplémentaires	
Fenêtre de recherche d'e-mail (jours)	L'historique des recherches d'e-mails est compris en nombre de jours. L'intégration recherche les e-mails qui ont été envoyés ou reçus sur le Microsoft Exchange Online serveur pour le nombre de jours calendaires que vous entrez. Vous devez saisir une valeur comprise entre 1 et 30. 30 jours est le nombre maximum de jours que vous pouvez saisir par défaut pour une recherche. La saisie d'un nombre faible de jours dans la plage de la fenêtre de recherche améliore le délai de réponse, mais il est possible que vous ne puissiez pas capturer tous les messages correspondants. Ce paramètre global s'applique à toutes les recherches. Avant d'exécuter la recherche par e-mail, il n'existe aucun paramètre vous permettant de modifier cette valeur pour des recherches individuelles.
Durée de recherche maximale	Utilisez cette option pour définir le seuil du délai d'expiration de recherche. Si le seuil de délai est atteint, la recherche se termine et aucun résultat n'est affiché. Vous pouvez spécifier une valeur par défaut de 90 minutes et une valeur maximale de 240 minutes. En définissant ce seuil, vous pouvez éviter les boucles de recherche interminables qui pourraient entraîner des problèmes de performances sur le Microsoft Exchange Online locataire et l'instance ServiceNow .
Balisage	Balise de sécurité. Cette valeur est sélectionnée par défaut.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Lorsque cette option est activée, les balises de sécurité sont automatiquement appliquées aux incidents de sécurité associés lorsque les options de recherche et de suppression sont lancées et terminées avec succès. Les noms de balises par défaut sont affichés, mais les noms et les couleurs des balises peuvent être modifiés. Pour plus d'informations, consultez Modifier les balises de sécurité dans Now Platform pour l'intégration Microsoft Exchange Online.
Récupérer les e-mails supprimés	Cette valeur est sélectionnée par défaut. Cet élément s'applique uniquement aux e-mails que vous avez supprimés à l'aide de cette intégration. Si vous ne souhaitez pas que les utilisateurs de votre organisation aient accès aux e-mails que vous avez supprimés, vérifiez que la case n'est pas cochée. Si la case n'est pas cochée, les e-mails que vous supprimez à l'aide du workflow de cette intégration sont définitivement supprimés et placés dans le dossier Purges. Ce dossier est un sous-dossier dans le dossier Microsoft Exchange Online Éléments récupérables auquel un utilisateur ne peut normalement pas accéder. Si vous souhaitez que les utilisateurs récupèrent les e-mails que vous supprimez, cochez cette case. Si cette case est cochée, selon la façon dont le compte de l'utilisateur est configuré dans Microsoft Exchange Online, les e-mails que vous supprimez à l'aide du workflow de cette intégration sont placés dans le dossier Éléments supprimés de la boîte aux lettres de l'utilisateur. Si un compte est configuré de manière à ce que l'utilisateur puisse afficher le dossier Éléments supprimés dans sa boîte aux lettres, il peut récupérer les e-mails que vous supprimez de son compte Microsoft Exchange Online. Pour plus d'informations, voir Récupérer des éléments ou des e-mails supprimés dans Outlook Web App .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

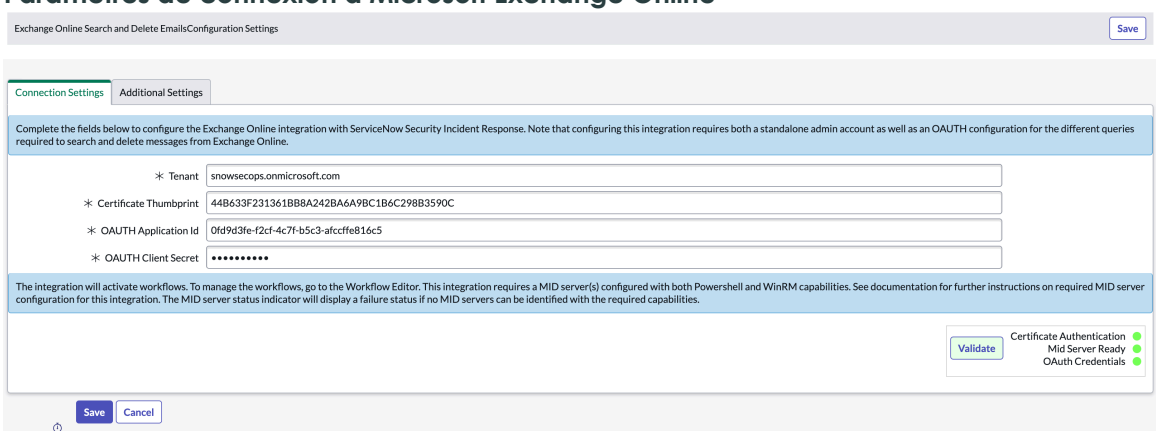
Option	Description
Notification d'achèvement de la recherche	Sélectionnez cette option pour activer les notifications lorsque la recherche est terminée. Si la case **Activer** est cochée, vous recevrez des notifications si des e-mails correspondants sont trouvés. Si la case n'est pas cochée, les notifications d'achèvement de la recherche ne sont pas envoyées.
Approbations	Demandez l'approbation pour supprimer des e-mails. La valeur par défaut est effacée. Lorsque la case est décochée, le processus d'approbation facultatif permettant de demander une autorisation préalable avant de supprimer des e-mails du Microsoft Exchange Online service est désactivé. Vérifiez que cette case n'est pas cochée si vous souhaitez accorder à votre analyste d'incident de sécurité l'autorisation de supprimer des e-mails sans demander d'autorisation préalable. Si cette option est activée, une demande est envoyée par e-mail à chaque membre d'un groupe d'approbation. Dans la liste, sélectionnez un groupe d'approbation. Pour plus d'informations sur la création d'un groupe d'approbation, reportez-vous à Configurer votre Now Platform instance pour l'intégration Microsoft Exchange Online. Une fois qu'une demande est soumise à un groupe d'approbation, une seule approbation du groupe est requise pour terminer la demande. Tout membre du groupe d'approbation dispose d'un pouvoir d'approbation. Le fait d'avoir un groupe composé de plusieurs personnes ayant une autorisation d'approbation garantit que ces demandes sont traitées en temps opportun.
Notifications de défaillance	Cochez la case pour activer les notifications d'échec lorsque l'action de recherche ou de suppression échoue en raison d'informations d'identification OAuth non valides. Si cette option est activée, les notifications d'échec sont envoyées par e-mail à chaque membre du groupe de notifications d'échec lorsque les informations d'identification OAuth ne sont pas valides.

Traduction automatique

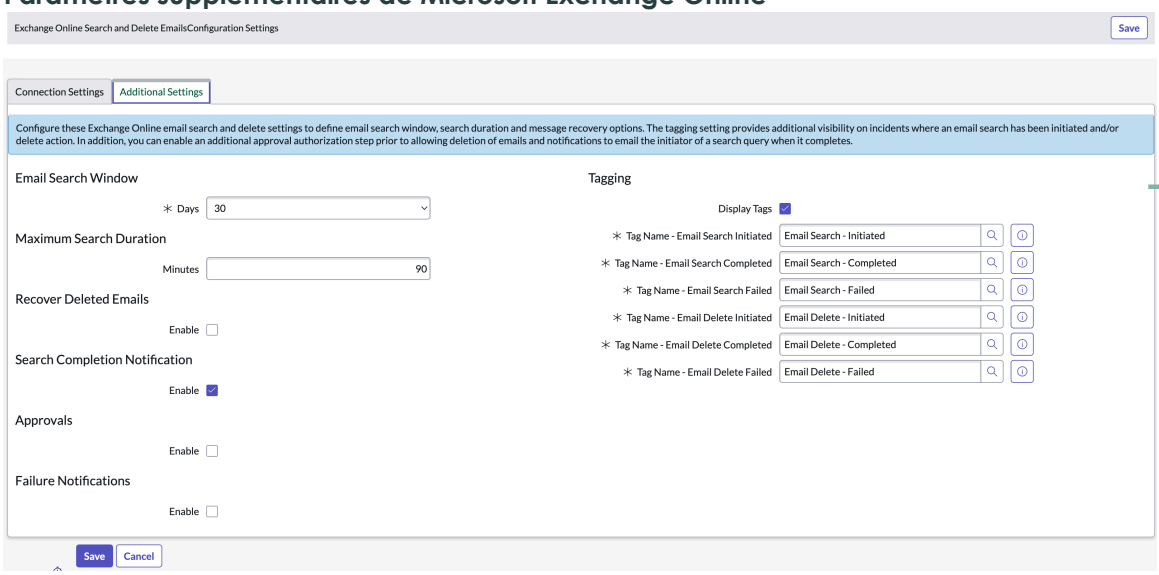
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Si la case n'est pas cochée, aucune notification de défaillance n'est envoyée.
Seuil de résultat d'e-mail	À partir de la version 10.3 ou ultérieure, vous pouvez spécifier un seuil de suppression d'e-mail pour les approbations. Si le nombre d'e-mails supprimés est supérieur ou égal à la valeur spécifiée ici, la demande de suppression doit être approuvée avant que l'action de suppression ne soit invoquée. Si la valeur de seuil est définie sur 1, chaque demande de suppression doit être approuvée.

Paramètres de connexion à Microsoft Exchange Online



Paramètres supplémentaires de Microsoft Exchange Online



5. Choisissez-en un pour continuer.

Option	Description
Enregistrer	Enregistrez vos modifications. Cette action ne vérifie pas votre connexion.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Dans l'onglet Paramètres de connexion, cliquez sur Valider.	Cette action valide votre authentification de certificat, votre connexion au MID Server et vos informations d'identification OAuth. Si vos informations d'identification sont valides, le bouton **Valider** et les deux indicateurs sont verts.

Trouble?
Si un message d'erreur s'affiche ou si un ou plusieurs des indicateurs à droite du bouton Valider sont rouges, vérifiez que les informations d'identification du compte utilisateur que vous avez saisies sont valides. Entrez vos informations d'identification et cliquez à nouveau sur **Enregistrer** .

Échec de la validation

Reportez-vous au tableau suivant pour plus d'informations sur le bouton **Valider** et les icônes colorées.

État du bouton et des indicateurs de validation	Description
Le bouton Valider est vert et tous les petits indicateurs colorés sont verts.	Indique que la connexion au Serveur MID et les informations d'identification (authentification de certificat et OAuth) sont valides.
Le bouton Valider est rouge clair avec une bordure bleue et un ou tous les petits indicateurs colorés sont orange.	La validation est en cours. La validation peut prendre quelques instants de plus.
Le bouton Valider est rouge clair et un ou tous les petits indicateurs colorés sont rouges.	• Le bouton Authentification basée sur certificat Exchange Online ou Informations d'identification OAuth est rouge : indique que l'authentification basée sur certificat Exchange Online ou les informations d'identification OAuth ne sont pas valides. • Les boutons Authentification basée sur certificat Exchange Online et Serveur MID prêt sont rouges : indique que le Serveur MID n'est pas accessible et que, par conséquent, l'authentification basée sur un certificat Exchange Online via le Serveur MID a échoué. • L'indicateur d'authentification basée sur un certificat Exchange Online est rouge, mais le bouton Serveur MID prêt est vert : indique que le Serveur MID est actif et configuré correctement, mais que l'authentification basée sur le certificat Exchange Online est incorrecte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir des critères de recherche d'e-mails et demander une recherche sur le Microsoft Exchange Online service

En tant qu'utilisateur disposant du rôle sn_si.analyste, définissez les critères de recherche et soumettez une demande de recherche d'e-mails basée sur les détails d'un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

Les chiffres de cette procédure sont affichés avec **les formulaires à onglets** sélectionnés dans les paramètres du système. Pour plus d'informations sur la sélection et l'effacement des formulaires à onglets, consultez la section intitulée Afficher les formulaires à onglets dans Configuration de la mise en page du formulaire sur le site web de la documentation produit ServiceNow .

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

L'état des messages individuels qui correspondent à la requête de recherche et les résultats de la recherche sont signalés dans l'enregistrement d'incident de sécurité. Si les notifications par e-mail sont activées, vous pouvez afficher les résultats de la recherche à partir d'un message par e-mail.

Les critères de recherche peuvent inclure les adresses de l'expéditeur du message, l'adresse du destinataire ou le nom de l'objet. Les combinaisons suivantes des paramètres de recherche Objet, Expéditeur et Destinataire du message sont souvent utilisées pour trouver des e-mails liés au phishing qui peuvent faire partie d'une seule campagne d'hameçonnage :

- Recherchez tous les e-mails originaux envoyés par un compte d'hameçonnage : Recherchez par expéditeur.
- Recherchez tous les e-mails originaux d'une seule campagne d'hameçonnage : effectuez une recherche par objet et par expéditeur.
- Retrouvez tous les e-mails reçus pour une même campagne d'hameçonnage (originaux et transférés, n'importe quel expéditeur) : Recherche par objet.
- Recherchez tous les e-mails transférés pour un seul e-mail d'hameçonnage provenant d'un seul utilisateur : Recherche par destinataire + objet.
- Rechercher tous les e-mails liés au phishing envoyés à un seul utilisateur : Recherche par expéditeur + destinataire.

Remarque : Les recherches sont effectuées sur les e-mails envoyés ou reçus au cours des 30 derniers jours calendaires, sauf si une fenêtre de recherche plus courte est configurée lors de la configuration initiale. Une recherche d'e-mails réussie est requise avant de pouvoir supprimer des e-mails.

L'exemple suivant vous montre comment lancer une recherche à partir d'un Now Platform incident de sécurité. Un incident de sécurité est créé sur la base de l'e-mail d'origine d'une attaque de phishing présumée dans le Microsoft Exchange Online serveur de votre organisation. Pour cet exemple, les critères de recherche sont Expéditeur (De) plus Objet, où De est `phisher@cbazyx.com` et Objet est `Connexion à votre compte`.

Les résultats des recherches sur les sujets sont renvoyés lorsque la recherche trouve des chaînes de texte contenant des mots clés qui correspondent aux critères de recherche entrés. Dans cet exemple, l'objet est `de vous connecter à votre compte`. Utilisez l'opérateur **ET** pour séparer les conditions de recherche De et Objet afin de renvoyer des résultats pour tous les messages électroniques contenant ces critères de recherche donnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

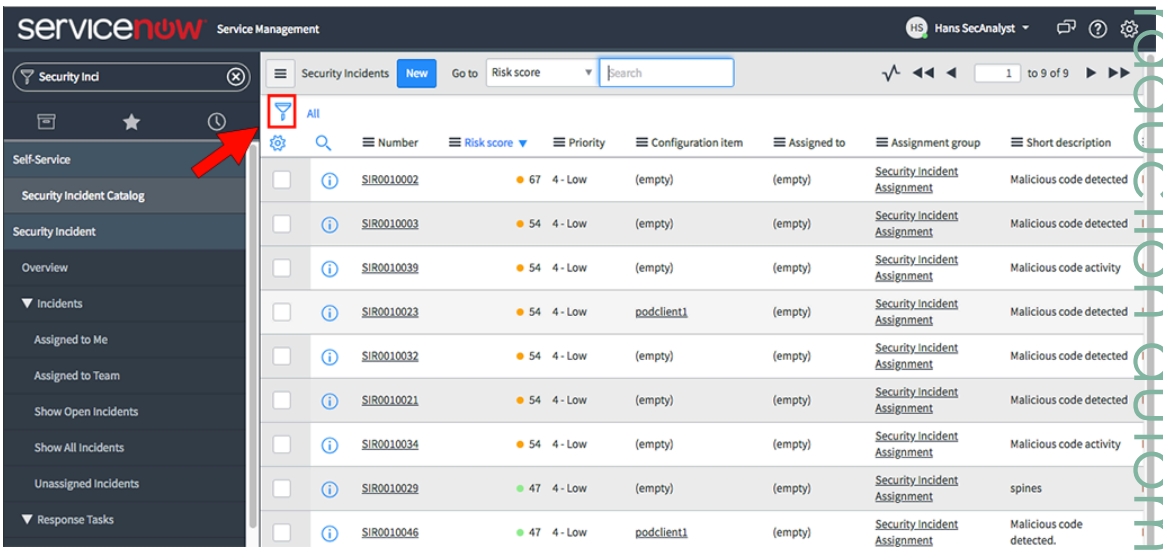
Les étapes suivantes décrivent comment configurer une recherche qui ne trouve que les e-mails contenant du texte de ligne d'objet envoyé par un compte d'hameçonnage spécifique.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents** et localisez l'incident de sécurité sur lequel vous travaillez.
2. Vous pouvez également suivre les étapes suivantes pour définir et exécuter un filtre afin que seuls les incidents de sécurité créés par des événements d'hameçonnage soient affichés.

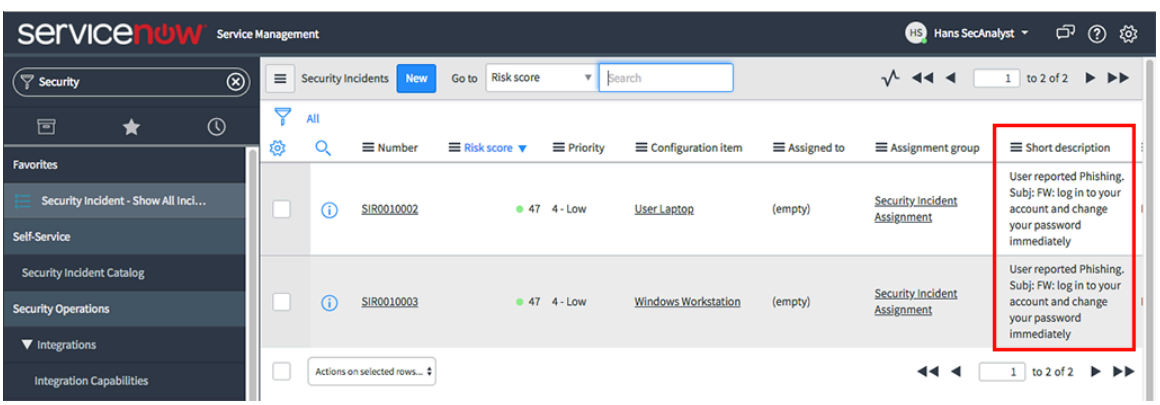
   a. Accédez à la **Incident de sécurité** > **Afficher les incidents** pour ouvrir la liste des incidents de sécurité.

   b. Dans le coin supérieur gauche de la liste qui s'affiche, cliquez sur l'icône de filtre.



   c. Dans les champs qui s'affichent, sélectionnez **Description brève** > **contient** dans les listes de choix, saisissez ensuite **Hameçonnage signalé** par les utilisateurs et cliquez sur **Exécuter**.

   Les incidents de sécurité liés au phishing sont affichés.



Traduction automatique

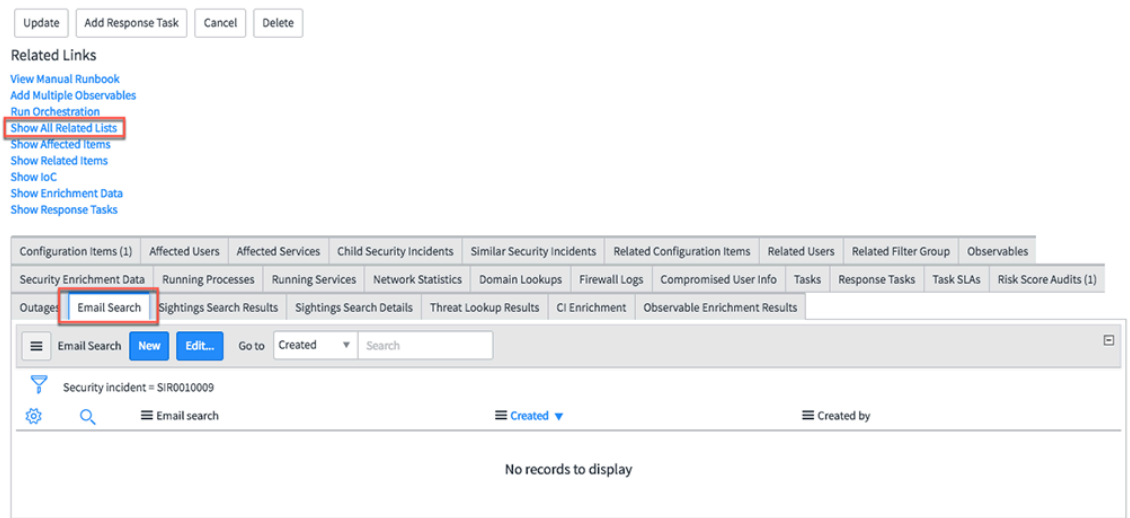
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Utilisez le texte de la colonne Brève description pour vous aider à localiser l'incident de sécurité sur lequel vous travaillez.

e. Dans la colonne Nombre, cliquez sur un incident de sécurité pour ouvrir un enregistrement.

3. Faites défiler l'écran jusqu'au bas de l'enregistrement d'incident de sécurité et cliquez sur la liste connexe Recherche d'e-mail.

Si la liste connexe Recherche d'e-mail n'est pas affichée, cliquez sur le lien connexe **Afficher toutes les listes connexes** pour afficher cette liste connexe.



4. Dans la liste connexe Recherche d'e-mail, cliquez sur **Nouveau** pour créer un enregistrement de recherche d'e-mail.
Le formulaire Recherche d'e-mail s'affiche. Si vous souhaitez réexécuter cette requête de recherche pour le même incident associé au hameçonnage avec des modifications mineures, vous pouvez réutiliser cet enregistrement de requête de recherche. Toutefois, il est peu probable que vous utilisiez cette recherche pour un autre incident associé au hameçonnage, car les campagnes d'hameçonnage sont dynamiques et les champs Expéditeur et Message changent souvent.

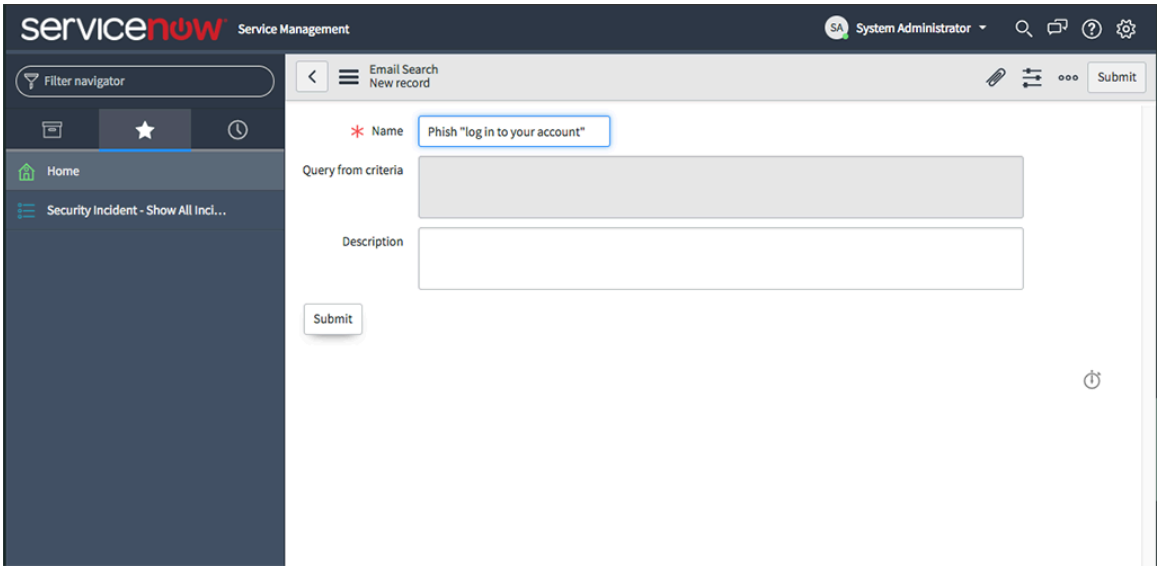
5. Facultatif : Pour modifier un enregistrement de requête de recherche existant, cliquez sur **Modifier**.

6. Renseignez les champs du formulaire Recherche d'e-mail.

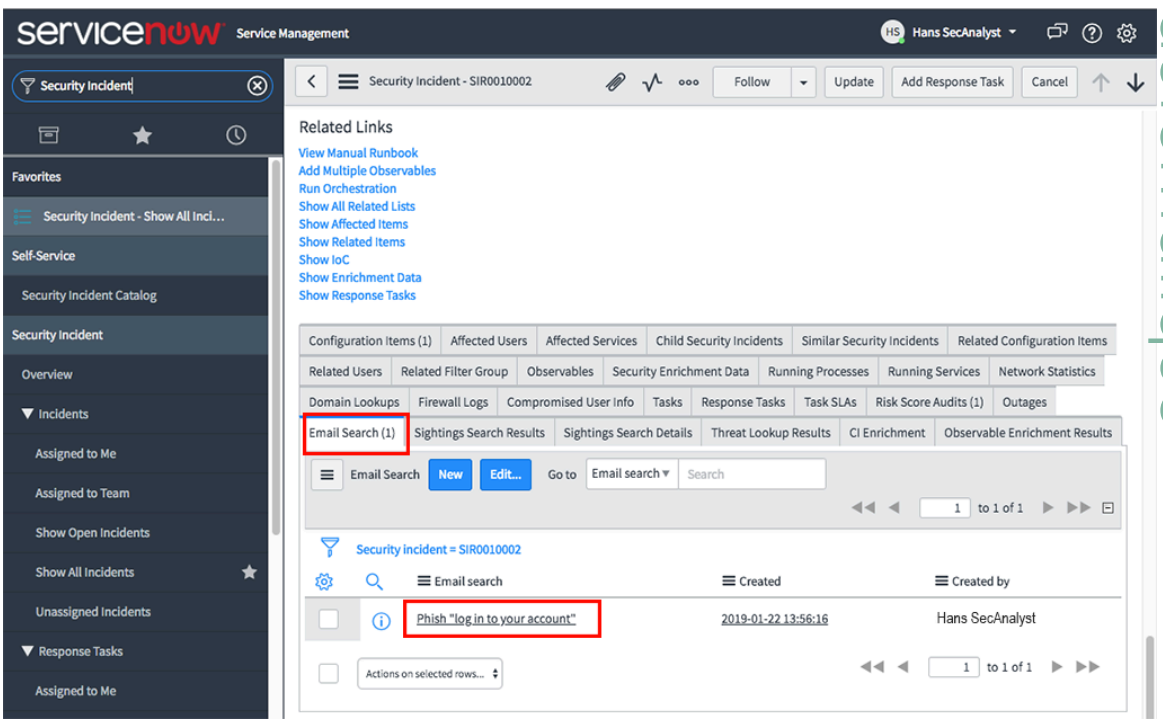
Champ	Description
Nom	Informations permettant de décrire le type de recherche. Dans cet exemple, un nom pour une recherche De + Sujet est `Hameçonnage « connectez-vous à votre compte ».`
Description	Informations sur la recherche dans le serveur de messagerie. Un exemple pour cette recherche est `From=phisher@cbazyx.com + Subject=connectez-vous à votre compte`.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



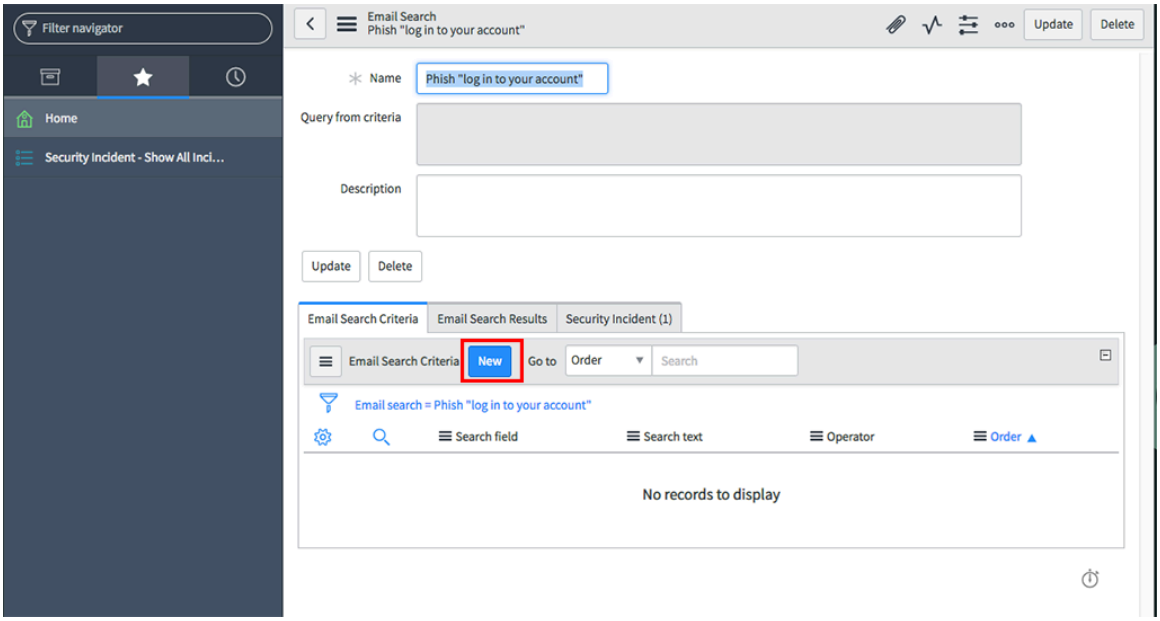
7. Cliquez sur **Envoyer**.
   L'incident de sécurité s'affiche et le nom de la recherche d'e-mail s'affiche dans la colonne Recherche d'e-mail de la liste connexe Recherche d'e-mail. Avant de pouvoir utiliser cette nouvelle requête de recherche, des critères de recherche doivent être définis pour l'enregistrement de recherche.
8. Pour définir les critères de recherche, avec la liste connexe Recherche d'e-mail sélectionnée, dans la colonne Recherche d'e-mail, cliquez sur **Hameçonnage « se connecter à votre compte** ».



9. Dans l'enregistrement de recherche d'e-mail qui s'affiche, cliquez sur la liste connexe Critères de recherche d'e-mail, puis cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Renseignez les champs du formulaire Critères de recherche d'e-mail.

Le tableau ci-dessous un exemple de formulaire rempli.

Champ	Description
Recherche d'e-mail	Le champ est renseigné automatiquement avec le nom que vous avez saisi pour l'enregistrement de recherche d'e-mail.
Icône de recherche	Chercher à l'aide d'une liste. Liste des recherches enregistrées. Cliquez sur l'icône pour ouvrir une liste des recherches d'e-mails enregistrées. Cliquez sur un élément de cette liste pour supprimer la recherche actuelle et sélectionner une recherche d'e-mails précédemment enregistrée.
Icône d'informations	Icône utilisée pour afficher l'enregistrement de recherche d'e-mail. Cliquez sur l'icône pour afficher l'enregistrement de recherche d'e-mail.
Champ de recherche	Critère de recherche (**Objet**, **De** ou **Destinataire**). Sélectionnez le critère de recherche dans la liste de choix et définissez une valeur que vous souhaitez rechercher dans le champ de texte. Pour cet exemple, commencez par De `phisher@cbazyx.com` (l'adresse e-mail de l'expéditeur de l'e-mail d'hameçonnage).
Actif	Option permettant d'activer la recherche. La recherche est activée par défaut.

Traduction automatique

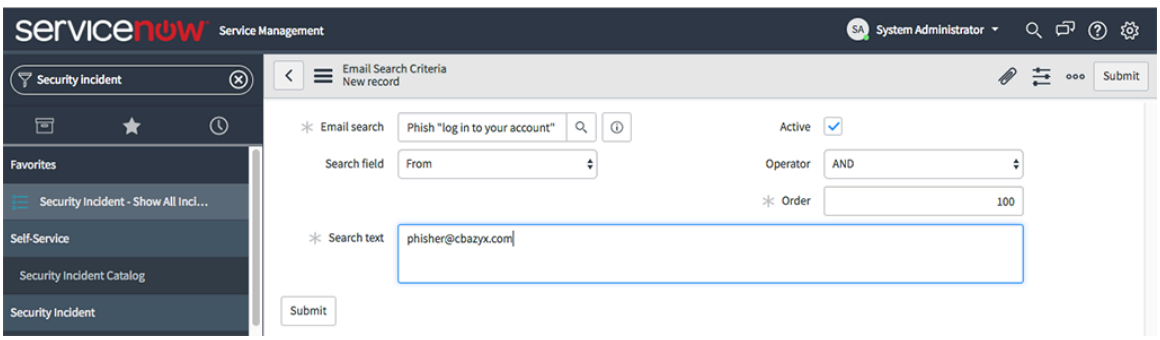
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si vous désactivez cette option, cet enregistrement n'est pas inclus dans une recherche.
Opérateur	Opérateurs (**ET, OU**) pour affiner votre recherche. **ET** : le système recherche les conditions séparées par **ET** et renvoie des résultats uniquement si toutes les conditions sont remplies. Pour la recherche de l'expéditeur et de l'objet, utilisez l'opérateur **ET** afin que les deux conditions de recherche soient réunies lors de la recherche d'e-mails. Pour cet exemple, utilisez l'opérateur **AND** de sorte que la requête soit De (Expéditeur) = `phisher@cbazyx.com` **ET** Objet = `Connectez-vous à votre compte`. **OU** : le système recherche et renvoie des résultats si l'une des conditions séparées par **OU** est remplie. Par exemple, de (expéditeur) = `phisher@cbazyx.com` **OU** de (expéditeur) = `phisher-2@cbazyx.com`.
Ordre	Si vous entrez plus de deux conditions de recherche, utilisez l'ordre pour classer les conditions par ordre de priorité. 100 est la valeur par défaut. Entrez une valeur comprise entre 1 et 100 pour chaque condition, par exemple, 100, 95, 90, 80. La condition dont le numéro est le plus bas affecté a la priorité de recherche la plus élevée dans un groupe de conditions.
Texte de recherche	Les valeurs de texte (mots clés) pour la recherche (adresses e-mail ou lignes d'objet). Le champ de recherche contient le texte utilisé dans la recherche, par exemple `phisher@cbazyx.com`. Pour que la recherche renvoie des résultats précis pour les recherches de l'expéditeur (De) et du destinataire, les chaînes de recherche doivent correspondre exactement. Pour les recherches par sujet, la chaîne de recherche peut contenir des mots-clés qui font partie d'une chaîne plus grande. Par exemple, un objet peut contenir la chaîne de recherche exacte qui correspond à un en-tête de message de transfert ou de réponse, par exemple

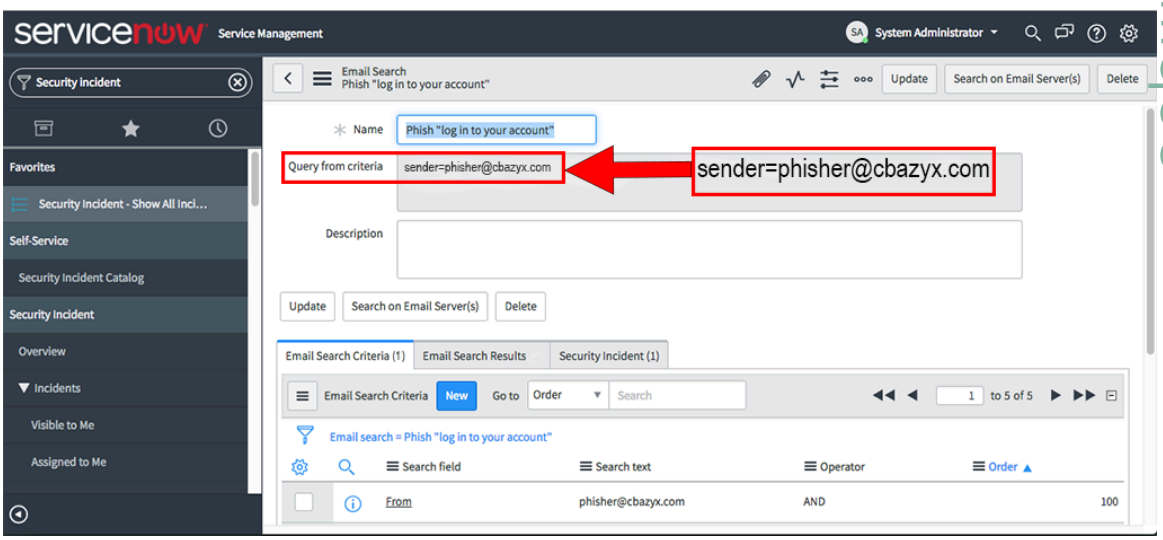
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	`FW : connectez-vous à votre compte et changez immédiatement votre mot de passe.` Par exemple, `Connectez-vous à votre compte` sont des mots-clés exacts dans la chaîne `Connectez-vous à votre compte et changez votre mot de passe immédiatement.` Aucune désignation de caractère générique (*) n'est requise pour prendre en charge un type de recherche Contenant . Actuellement, il n'existe aucune méthode de filtrage permettant de faire correspondre une chaîne de recherche exacte qui ne fait pas partie d'une chaîne de texte plus grande.



11. Cliquez sur **Envoyer**.
L'enregistrement de recherche d'e-mail s'affiche. Dans le champ **Requête à partir de critères** , les critères de recherche que vous avez ajoutés pour l'expéditeur (De) s'affichent.

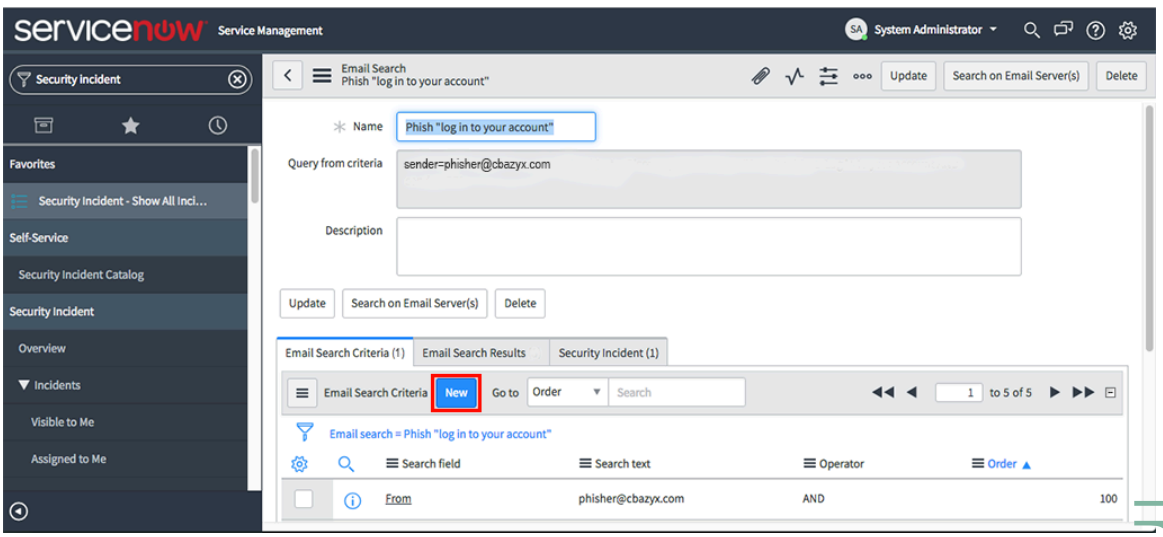


12. Pour mettre à jour ces critères de recherche d'e-mails avec plus d'informations afin que la requête inclue la condition objet plus expéditeur souhaitée, suivez les étapes pour ajouter une autre condition de recherche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

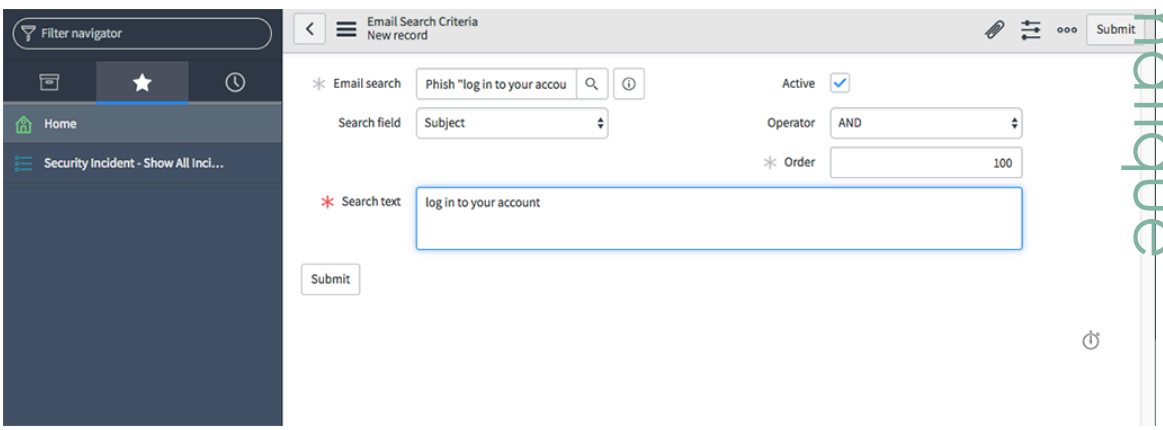
a. Dans la liste connexe Critères de recherche d'e-mail, cliquez sur **Nouveau**.



b. Dans la liste des **champs de recherche**de l'enregistrement Critères de recherche d'e-mail qui s'affiche, sélectionnez **Objet**.

c. Dans la liste Opérateur, sélectionnez**ET** ou **OU.**
Si vous sélectionnez **OU**, la recherche renvoie des résultats si les mots clés de la chaîne de texte de la ligne d'objet correspondent ou si la condition d'adresse e-mail est respectée. **AND** est sélectionné pour cet exemple afin que la recherche renvoie des résultats uniquement pour les e-mails qui contiennent les mots clés de la chaîne de texte de l'objet et qui correspondent à l'adresse e-mail de l'expéditeur.

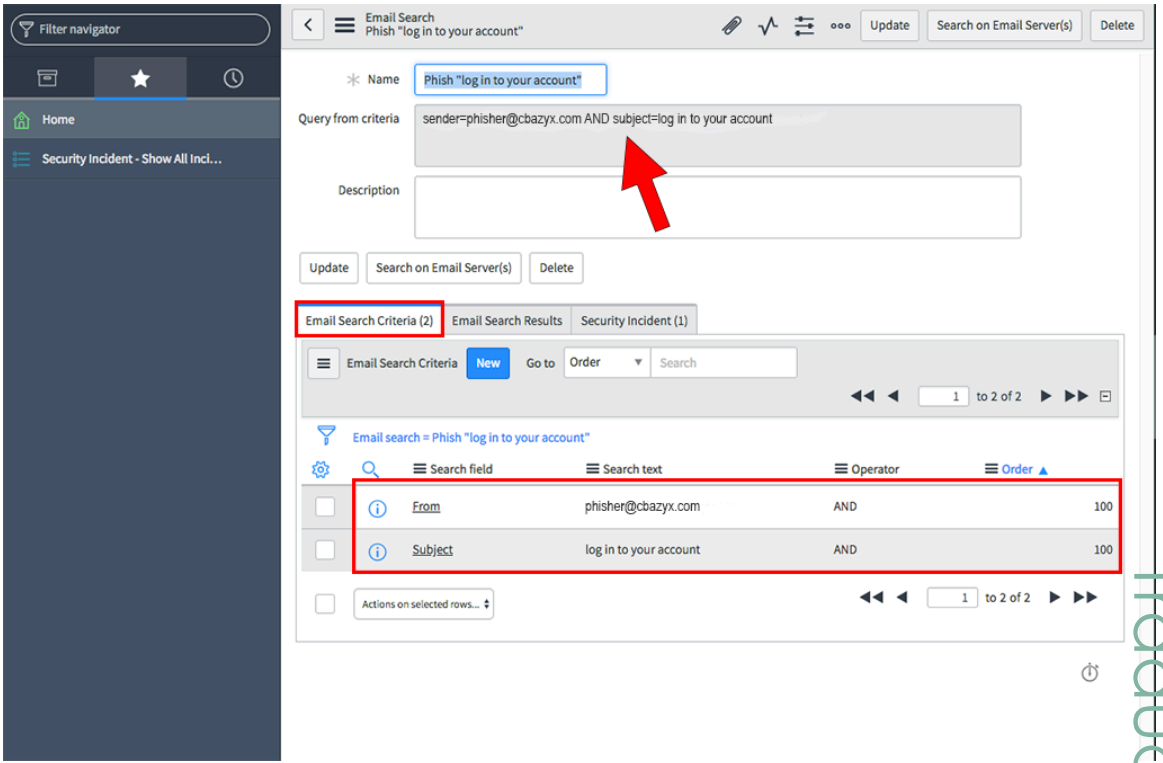
d. Dans le champ **Texte de recherche** , saisissez la valeur du texte de la ligne `d'objet, connectez-vous à votre compte`.



e. Cliquez sur **Envoyer**.
La nouvelle condition est affichée dans la liste connexe Critères de recherche d'e-mail, et les deux conditions sont affichées dans le champ **Demander à partir de critères** séparés par l'opérateur **ET** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



f. Facultatif : Si vous avez plusieurs conditions de recherche et que vous sélectionnez **ET** pour séparer chaque condition, définissez la valeur d'ordre pour les classer par ordre de priorité.

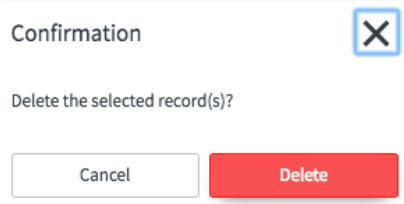
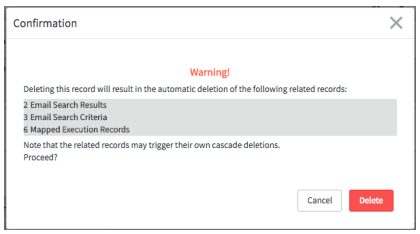
g. Continuez d'ajouter, de modifier ou de supprimer des critères de recherche comme vous le souhaitez, puis cliquez sur **Mettre à jour** pour enregistrer vos changements apportés à l'enregistrement.

13. Choisissez une option pour continuer.

Option	Description
Mettre à jour	Mettez à jour et enregistrez vos changements apportés à l'enregistrement.
Rechercher sur les serveurs de messagerie	Lancez une recherche sur les serveurs avec les critères que vous avez enregistrés dans l'enregistrement Critères de recherche d'e-mail.
Supprimer	Supprimez cet enregistrement de recherche d'e-mail de votre Now Platform instance. Cette action ne supprime pas les e-mails réels. Il supprime uniquement l'enregistrement de recherche utilisé pour trouver des messages. Une boîte de dialogue s'affiche. Si vous cliquez sur **Supprimer**, les résultats de recherche d'e-mails et les critères de recherche d'e-mails de cet enregistrement de recherche sont supprimés.

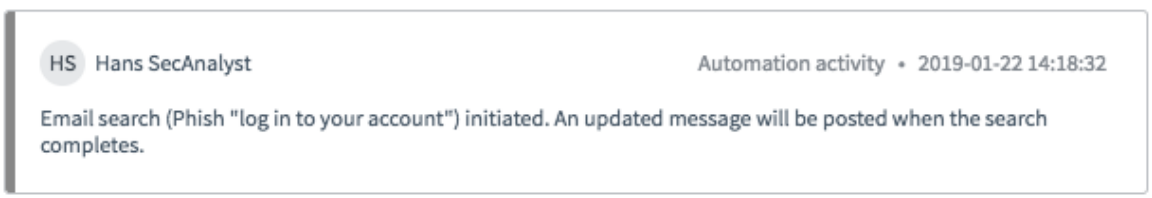
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	 Si un enregistrement comporte des résultats de recherche, l'avertissement suivant s'affiche. 

14. Pour lancer une recherche d'e-mails, dans l'enregistrement de recherche d'e-mails, cliquez sur **Rechercher sur les serveurs de messagerie**.
Un message s'affiche pour indiquer que la demande de recherche est envoyée.

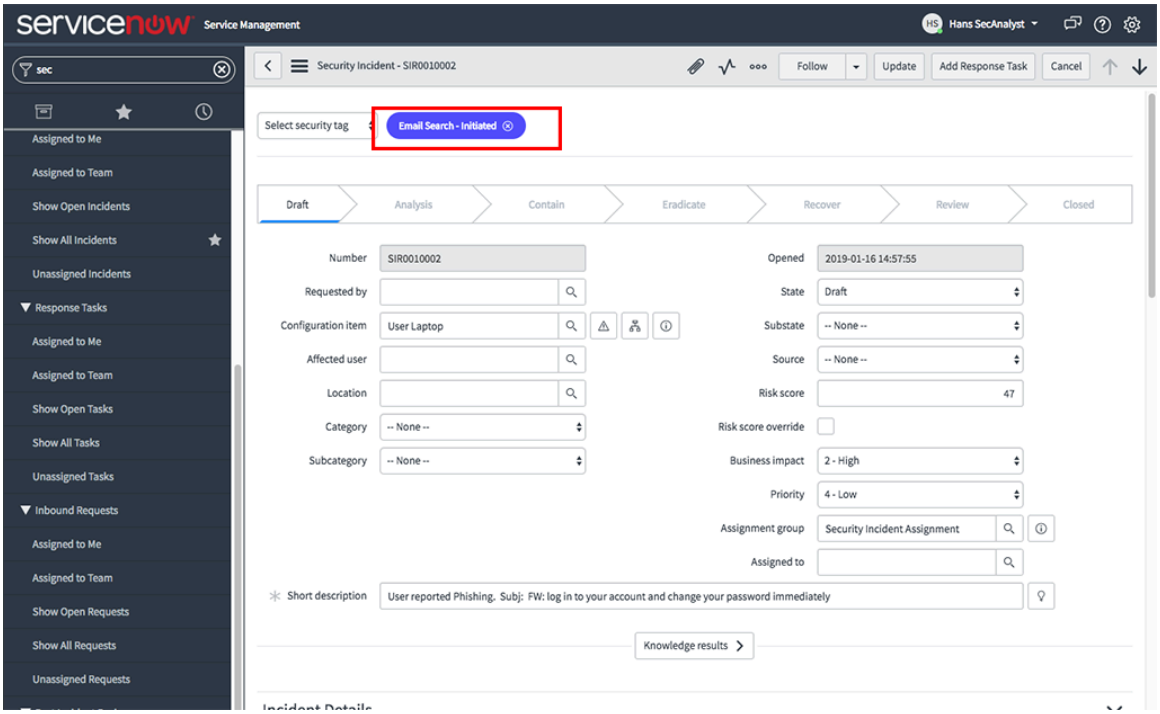
Sur l'enregistrement d'incident de sécurité, une note de travail s'affiche indiquant qu'une recherche a été lancée.



Si le balisage est activé, en haut de l'enregistrement d'incident de sécurité, la balise de sécurité `Recherche d'e-mail - Initiée` s'affiche.

Traduction automatique

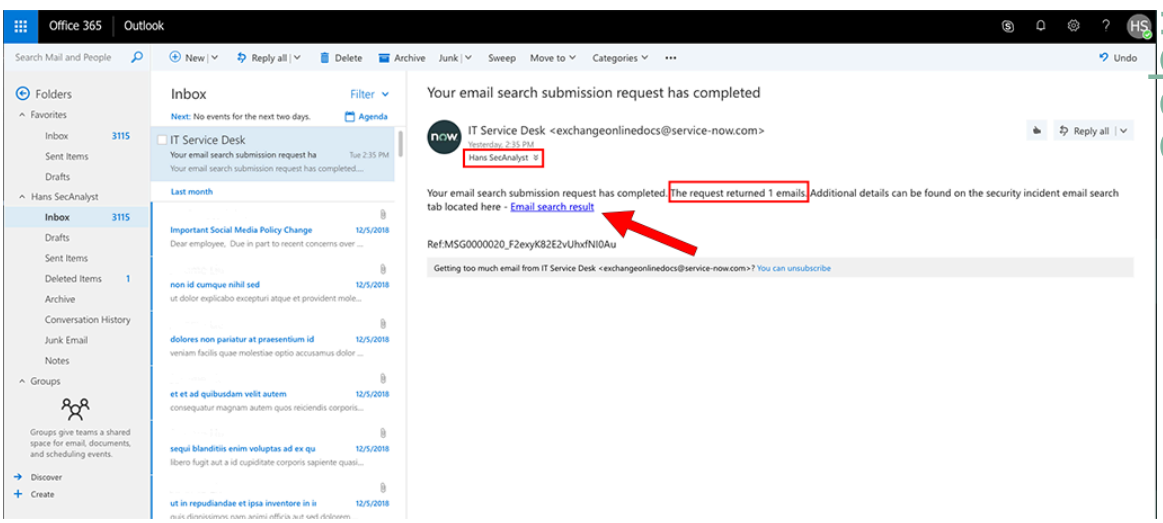
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois la recherche terminée avec succès, si les notifications par e-mail sont activées, un e-mail est envoyé à l'adresse e-mail de la personne qui a initié la recherche.

Dans cet exemple, c'est l'utilisateur disposant du rôle sn_si.analyst, `Hans SecAnalyst`, qui a soumis cette recherche. L'image suivante montre que cette notification est envoyée à un compte dans Microsoft Exchange Online. Toutefois, ces notifications peuvent être envoyées à un autre service de messagerie, selon les besoins.

Cette notification vous permet d'afficher tous les résultats correspondants qui nécessitent un suivi et une suppression. L'exemple suivant montre qu'il existe un e-mail qui correspond aux critères de recherche. Un lien de résultat de recherche d'e-mail vers l'enregistrement des résultats de recherche d'e-mail dans votre Now Platform instance est également fourni. Si vous souhaitez afficher l'enregistrement de recherche, cliquez sur ce lien.



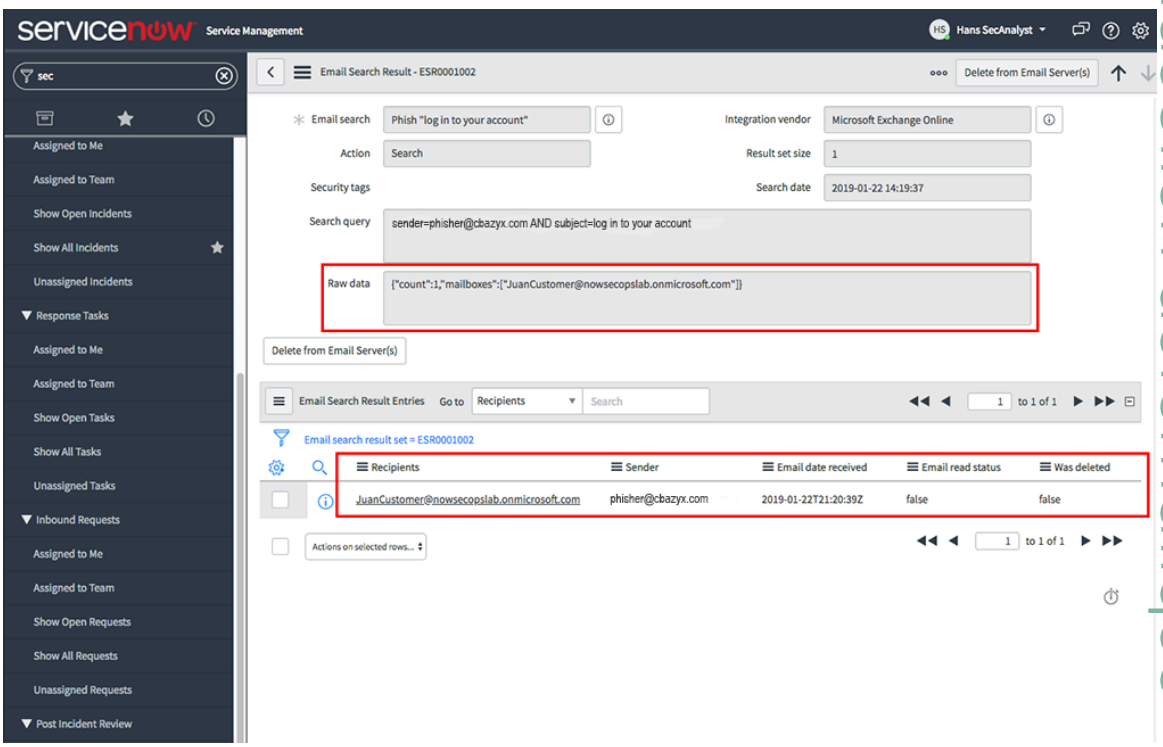
15. À partir de cet e-mail, pour afficher les résultats de la recherche, cliquez sur le lien **de résultat de recherche d'e-mail** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'enregistrement des résultats de recherche d'e-mail s'affiche. Dans cet enregistrement, vous pouvez vérifier et examiner les données suivantes.

- Dans le champ **Données brutes** , le nombre d'e-mails correspondant au nombre d'e-mails qui correspondaient aux critères de recherche `{"count » :1}`, ainsi que les adresses des boîtes aux lettres où les e-mails ont été trouvés sont affichés `["JuanCustomer@nowsecopslab.onmicrosoft.com"]`.
- Dans la colonne Destinataires, le destinataire est (`JuanCustomer@nowsecopslab.onmicrosoft.com`).
- Dans la colonne `Expéditeur` , la source de l'e-mail est affichée.
- Dans la colonne `Date de réception de l'e-mail` , la date et l'heure de réception de l'e-mail sont affichées pour vous aider à suivre les chronologies des campagnes d'hameçonnage.
- Dans la colonne `État de lecture de l'e-mail` , l'e-mail de cet exemple n'a pas été lu (`faux`). Si un e-mail a été lu, `vrai` s'affiche.
- Dans la colonne `A été supprimé` , l'e-mail de cet exemple n'a pas été supprimé. Si un e-mail a été supprimé, `vrai` s'affiche.

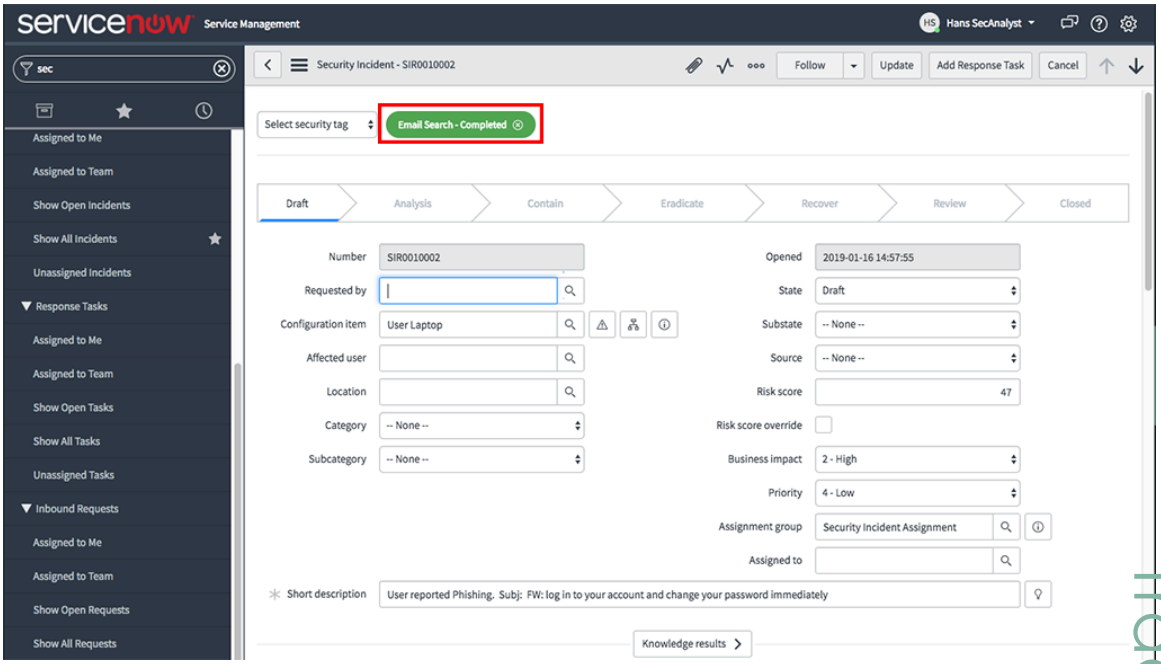


16. Pour afficher les résultats de la recherche de l'incident de sécurité, vous pouvez également suivre les étapes suivantes.

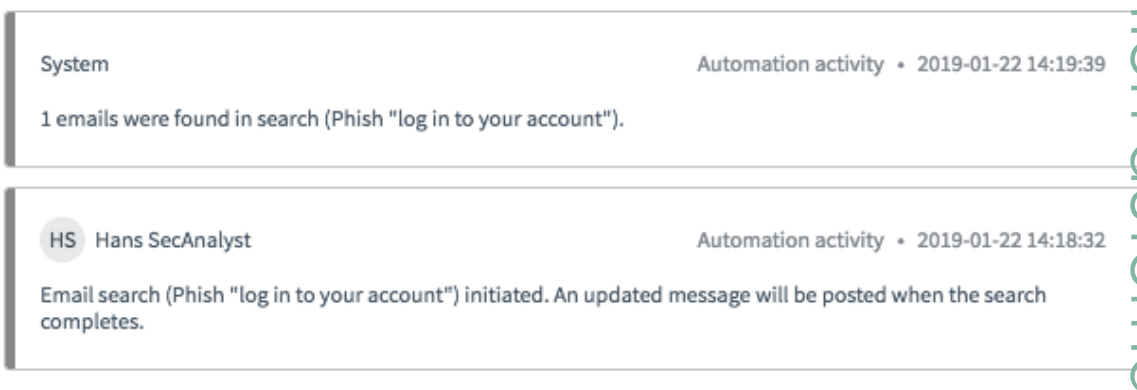
a. Accédez à la **Incident de sécurité** > **Incidents** et ouvrez l'incident de sécurité sur lequel vous travaillez.
En haut de l'enregistrement, lorsque la recherche est terminée avec succès, la balise de sécurité `Recherche d'e-mail - Terminée` remplace la balise `de sécurité Recherche d'e-mail - Initiée` .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Des notes de travail indiquent que la recherche a été effectuée avec succès et qu'un e-mail correspondant a été trouvé.

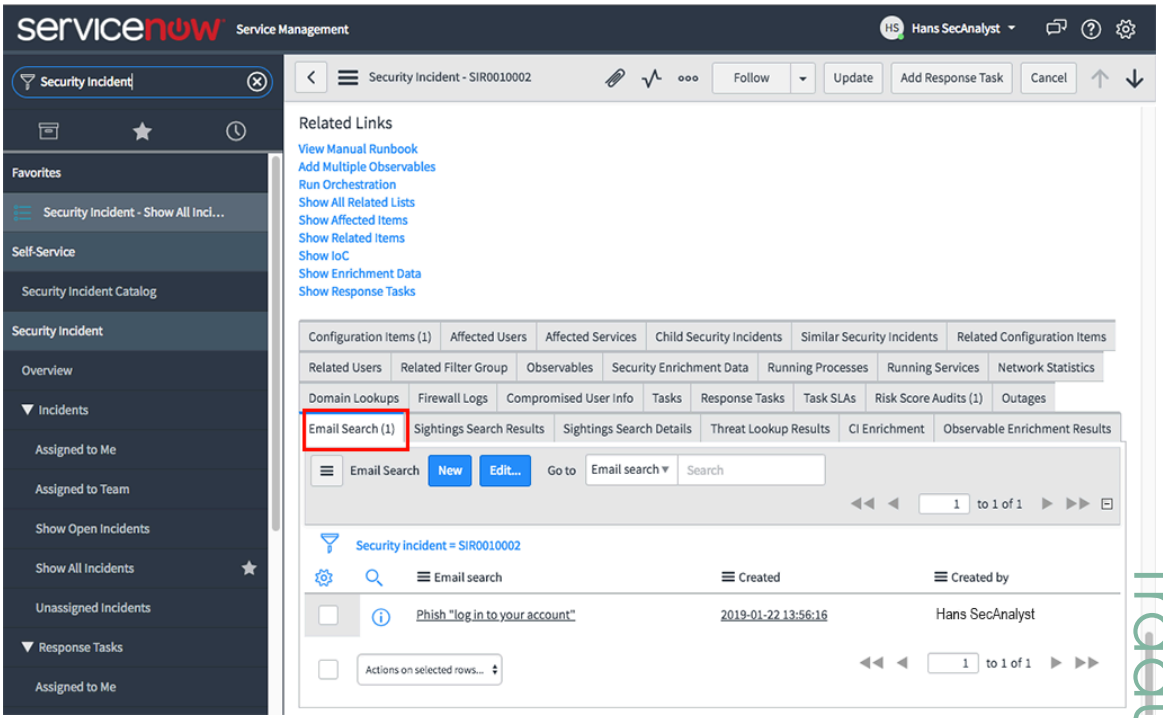


b. Faites défiler l'écran jusqu'au bas de l'enregistrement d'incident de sécurité et cliquez sur la liste connexe Recherche d'e-mail.

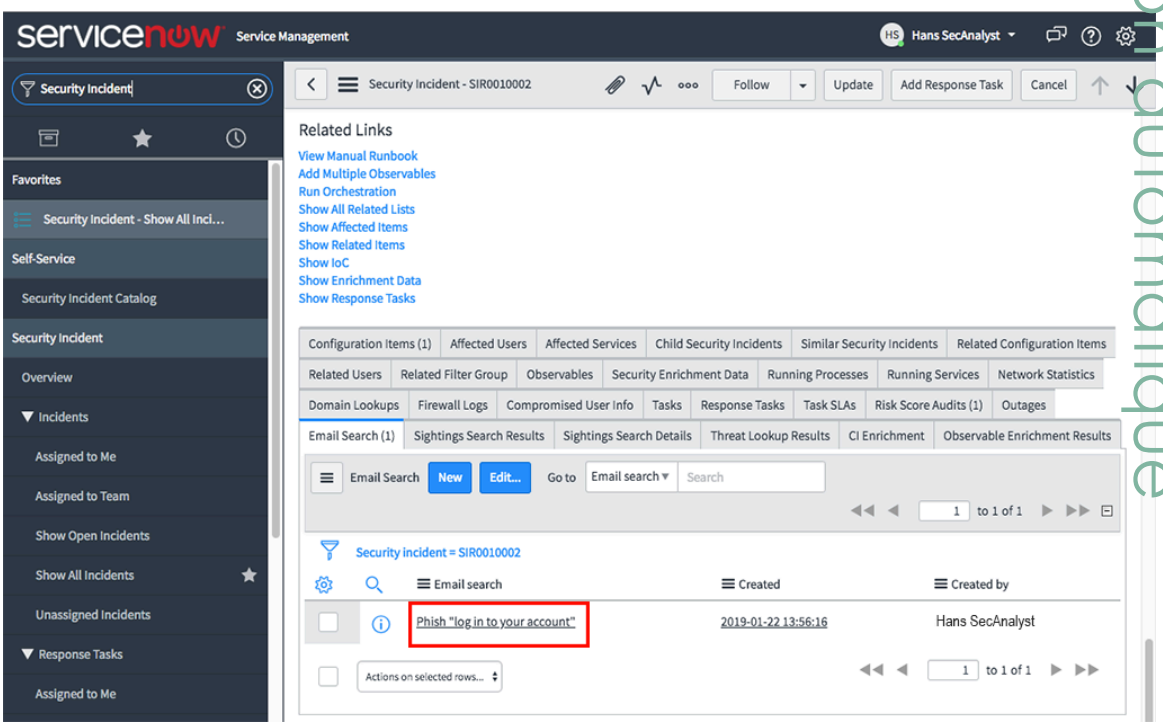
Si la liste connexe Recherche d'e-mail n'est pas affichée, cliquez sur le lien connexe**Afficher toutes les listes connexes** pour afficher cette liste connexe.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Après avoir sélectionné la liste connexe Recherche d'e-mail, cliquez sur le nom de votre recherche dans la colonne Recherche d'e-mail.



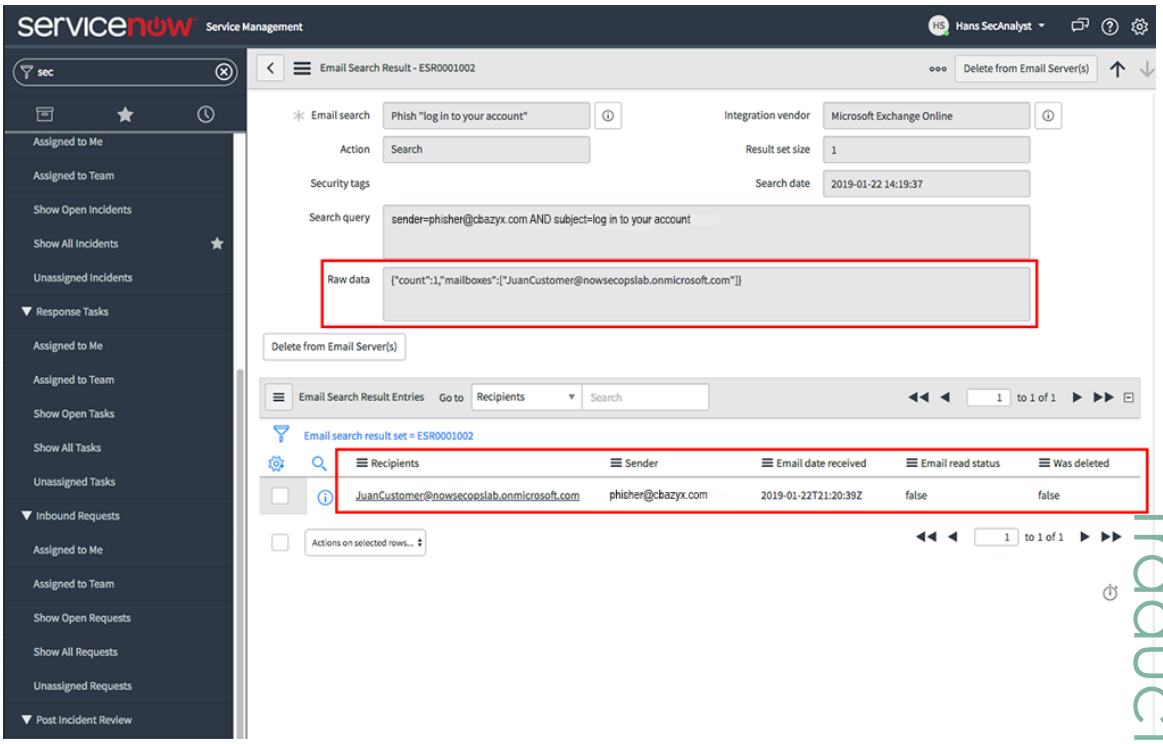
d. Dans l'enregistrement Recherche d'e-mail, cliquez sur la liste connexe Résultats de recherche d'e-mail.

e. Dans la colonne Date de recherche, cliquez sur la date de votre recherche pour afficher les données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'enregistrement des résultats de recherche d'e-mail s'affiche.



Une fois qu'une recherche d'e-mails est terminée avec succès, évaluez les résultats. Si vous déterminez que des e-mails doivent être corrigés, vous pouvez les supprimer ou demander leur approbation.

Demander l'approbation de suppression des e-mails sur le service Microsoft Exchange Online

Une fois qu'une recherche d'e-mails est effectuée avec succès et que les messages correspondants sont identifiés, vous pouvez supprimer définitivement tous les e-mails suspects du service Microsoft Exchange Online associés à l'incident de sécurité et à la campagne de hameçonnage.

Avant de commencer

Rôle requis : sn_si.analyst

Le système effectue des suppressions sur vos derniers résultats de recherche réussis.

Pourquoi et quand exécuter cette tâche

Si les approbations et les notifications par e-mail sont activées, envoyez une demande de suppression des e-mails à un groupe d'approbation avant la suppression des e-mails.

Les résultats de la recherche d'e-mails s'affichent avec tous les messages qui ont été reçus. Pour s'assurer que les e-mails d'hameçonnage sont correctement supprimés, les résultats de la suppression sont publiés dans les notes de travail de l'incident de sécurité associé. Si le balisage est activé, une balise de sécurité s'affiche également sur l'incident de sécurité associé. Si l'e-mail n'est pas supprimé avec succès, vous en êtes également informé dans les notes de travail.

En fonction des politiques de votre organisation, vous devrez peut-être demander une approbation avant de supprimer les e-mails d'hameçonnage. Le processus d'approbation de suppression nécessite des informations sur le nombre d'e-mails à supprimer et, éventuellement, l'accès à d'autres détails de messages. Pour traiter la demande de suppression, dans une notification par e-mail, un approbateur reçoit le nombre de messages électroniques correspondants, le lien d'incident de sécurité pour accéder aux détails

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

complets du message et les liens d'approbation ou de rejet. Les liens contenus dans cet e-mail permettent à un approbateur d'accepter ou de rejeter la demande de suppression de la notification par e-mail. Une piste d'audit complète avec horodatage est également disponible pour suivre le moment où l'état d'approbation a changé dans les notes de travail. Si un groupe d'approbation est affecté, un utilisateur du groupe peut traiter la demande pour l'ensemble du groupe. Chaque membre du groupe d'approbation reçoit une notification par e-mail pour la demande.

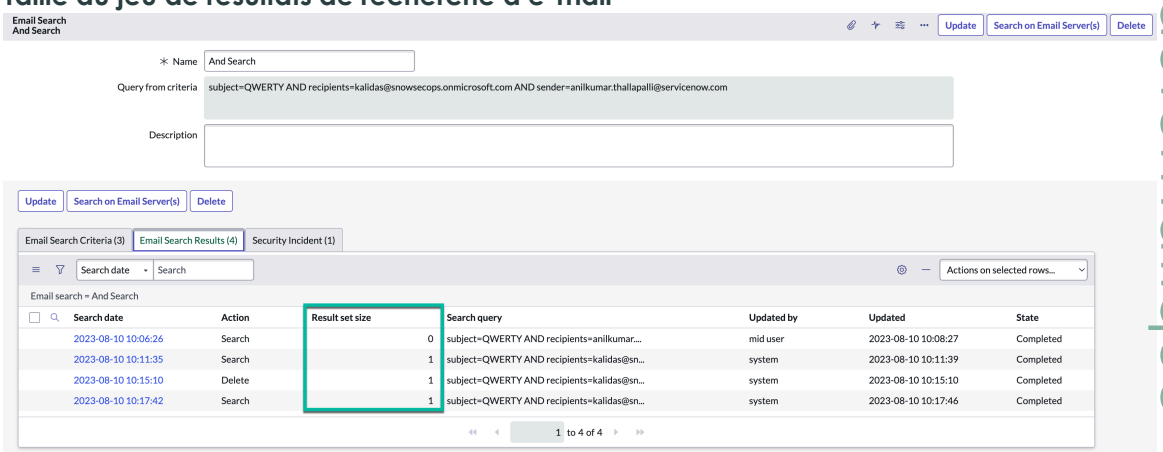
En tant qu'utilisateur disposant du rôle sn_si.analyst, si vous déterminez que des e-mails doivent être corrigés, suivez les étapes requises pour supprimer les e-mails. Si les approbations sont activées, demandez l'approbation pour supprimer les e-mails du Microsoft Exchange Online service.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité > Afficher tous les incidents**.
2. Cliquez sur la liste connexe **Recherche d'e-mail** .
3. Après avoir sélectionné la liste connexe Recherche d'e-mail, cliquez sur le nom de votre recherche dans la colonne Recherche d'e-mail.
   Les résultats de la recherche sont affichés dans la liste connexe Résultats de recherche d'e-mail.

   Pour cet exemple, cette recherche a permis de trouver des e-mails qui correspondent à vos critères de recherche. Deux actions de recherche sont répertoriées dans l'enregistrement. Une recherche n'a aucune correspondance (0) et l'autre recherche a une correspondance d'e-mail (1).

Taille du jeu de résultats de recherche d'e-mail

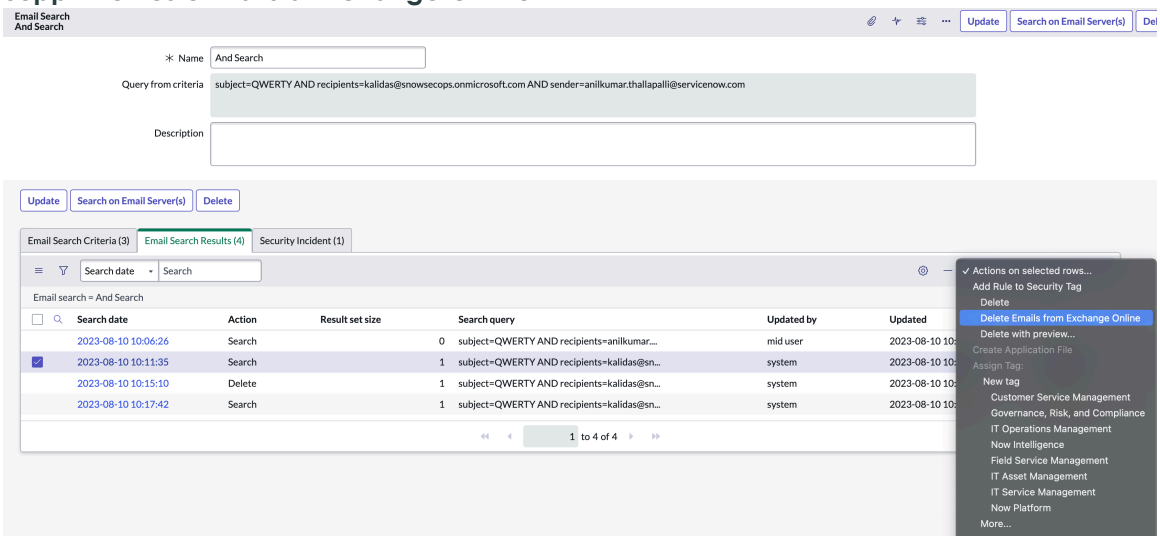


4. Pour supprimer des éléments d'e-mail associés à une recherche, cochez la case correspondante d'un ensemble de résultats de recherche à gauche de la colonne Date de recherche.
   Vous pouvez sélectionner un seul jeu de résultats ou plusieurs jeux de résultats dans la liste.
5. Sélectionnez les jeux de résultats que vous voulez supprimer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Supprimer les e-mails d'Exchange Online

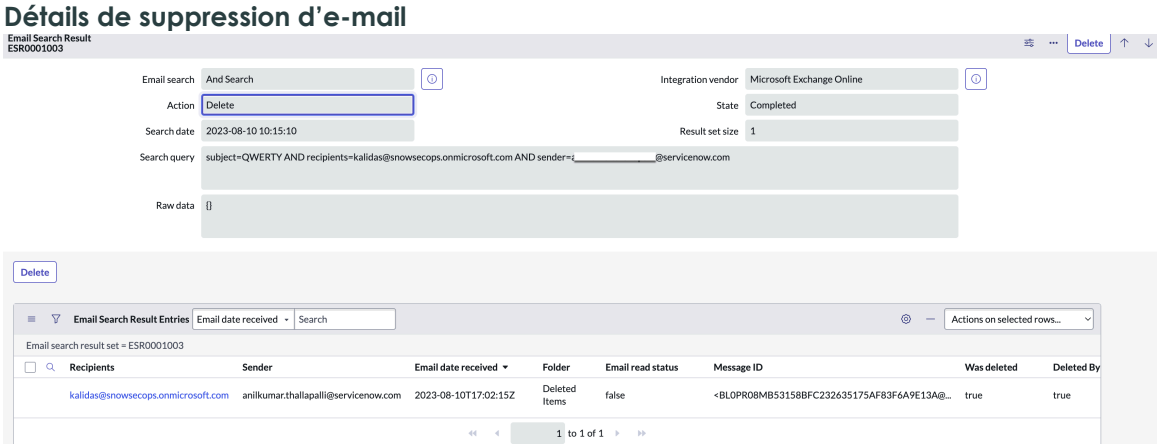


6. En bas de la liste connexe Résultats de recherche d'e-mail, à partir de la liste Actions sur les lignes sélectionnées, sélectionnez **Supprimer les e-mails d'Exchange Online** pour supprimer tous les éléments d'e-mail associés à un ou plusieurs jeux de résultats du serveur Exchange Online.
   Si un jeu de résultats contient plusieurs e-mails, vous n'avez pas besoin d'ouvrir l'enregistrement Résultat de recherche d'e-mail et de sélectionner des e-mails individuels pour les supprimer. Tous les `éléments` d'e-mails ayant un état faux dans la colonne A été supprimé de l'enregistrement Résultat de recherche d'e-mail sont supprimés une fois que vous avez sélectionné **Supprimer les e-mails d'Exchange Online**.

   Si un élément d'e-mail d'un jeu de résultats a déjà été supprimé, l'état de la colonne A été supprimé de l'enregistrement Résultat de recherche d'e-mail est `vrai`. Ces éléments ne sont pas supprimés à nouveau.

   Si l'option d'approbation est désactivée au cours de l'étape de configuration, une fois que vous avez sélectionné **Supprimer les e-mails d'Exchange Online**, les e-mails associés au jeu de résultats sont supprimés. Le jeu de résultats lui-même n'est pas supprimé. Toutefois, l'état de tous les éléments d'e-mail supprimés du jeu de résultats est mis à jour sur `vrai` dans la colonne A été supprimé de l'enregistrement Résultat de recherche d'e-mail. Pour en savoir plus sur la fonctionnalité d'approbation, reportez-vous à la section Configurer l'intégration Microsoft Exchange Online avec votre Now Platform instance.

Détails de suppression d'e-mail

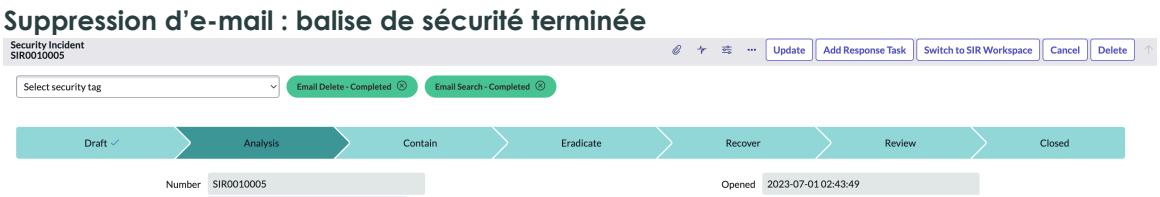


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ces e-mails sont supprimés du Microsoft Exchange Online locataire sur lequel vous avez effectué les recherches. Une note de travail s'affiche si les e-mails sont supprimés avec succès.

Sur l'enregistrement d'incident de sécurité, la balise de sécurité `Suppression d'e-mail - Terminé` s'affiche.

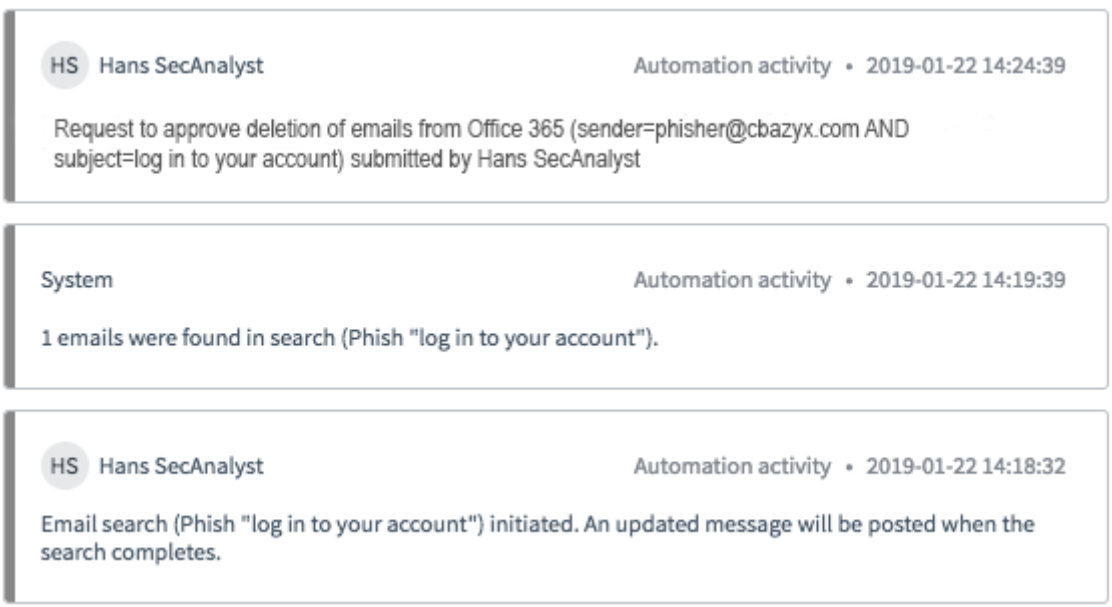


Si les approbations sont désactivées pour les demandes de suppression, vous avez supprimé avec succès les Microsoft Exchange Online e-mails du locataire.

Si les approbations sont activées pour les demandes de suppression au cours de l'étape de configuration, une fois que vous avez sélectionné **Supprimer les e-mails d'Exchange Online**, une notification par e-mail est envoyée à chaque membre du groupe d'approbation que vous avez sélectionné au cours de l'étape de configuration.

Si le balisage est activé pendant l'étape de configuration, la balise de sécurité `Suppression d'e-mail - Initiée` s'affiche sur l'enregistrement d'incident de sécurité connexe. Pour en savoir plus sur le balisage, reportez-vous à la section Configurer l'intégration Microsoft Exchange Online avec votre Now Platform instance.

Des notes de travail indiquent qu'une demande de suppression d'e-mails est soumise par l'utilisateur disposant du rôle sn_si.analyst (`Hans SecAnalyst`).



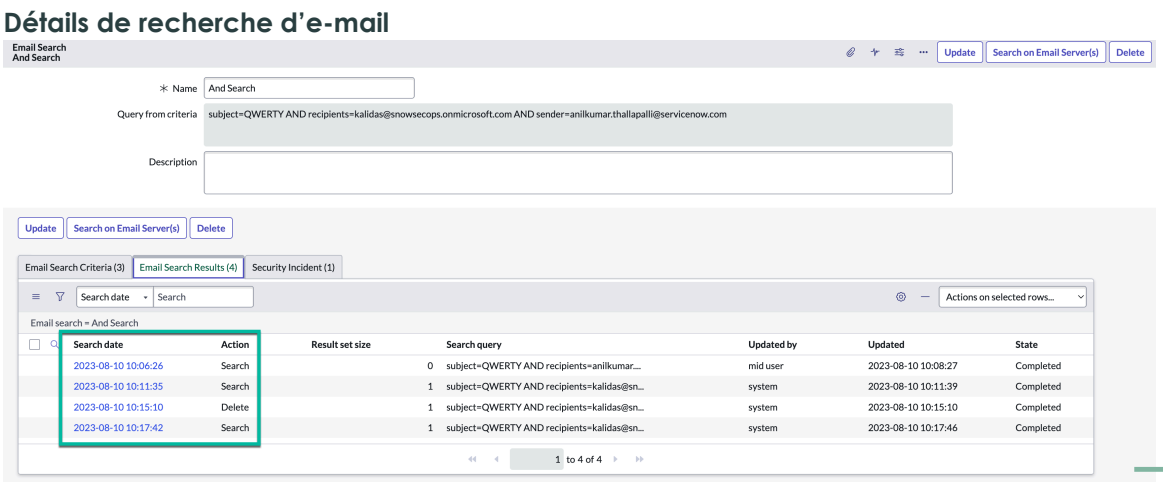
Si les approbations sont activées, l'étape suivante consiste à traiter la demande de suppression.

7. Si vous souhaitez également afficher les détails et les éléments d'e-mail individuels d'un enregistrement de recherche avant de le supprimer ou d'envoyer une demande de suppression, procédez comme suit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Une fois la liste connexe Résultats de recherche d'e-mail sélectionnée, dans la colonne Date de recherche, cliquez sur la date d'une recherche que vous souhaitez examiner.



Les informations suivantes sur les e-mails s'affichent :

- Destinataires
- Expéditeur
- Date de réception de l'e-mail
- État de lecture de l'e-mail (`vrai` ou `faux`)
- A été supprimé (`vrai | faux`)
- Supprimé par intégration (`vrai | faux`)

> **Remarque :**
>
> La valeur est définie sur Vrai lorsque l'e-mail est supprimé lorsque l'analyste lance la suppression des serveurs de messagerie.
>
> Les notes de travail sont mises à jour avec le nombre total d'enregistrements supprimés, qui inclut les enregistrements supprimés par l'intégration et l'utilisateur.

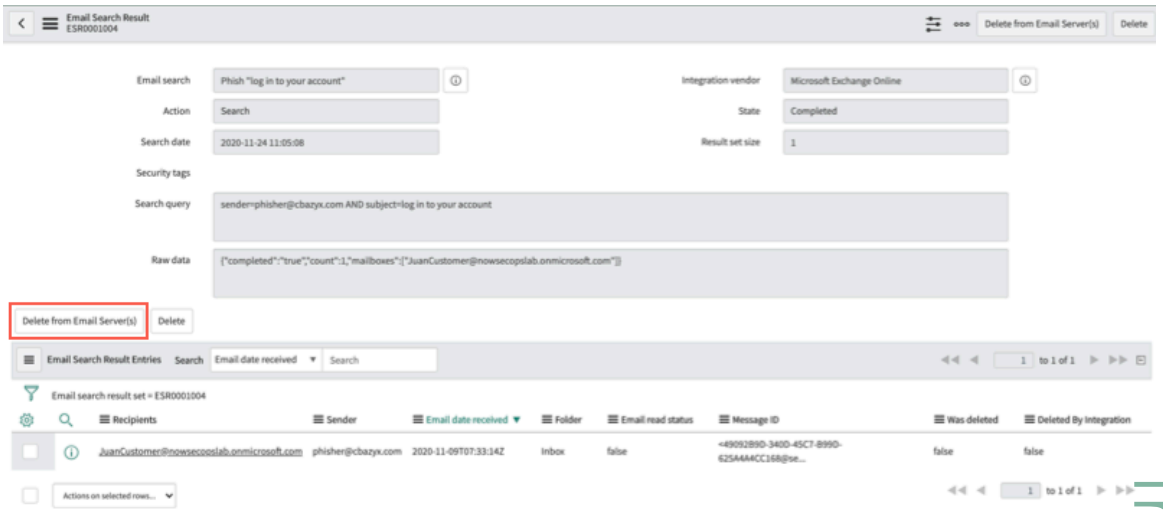
b. Après avoir examiné les données, pour supprimer tous les e-mails, ou envoyer une demande de suppression de tous les e-mails, cliquez sur **Supprimer des serveurs de messagerie**.

Comme décrit dans l'exemple précédent, si plusieurs e-mails sont répertoriés dans l'enregistrement des résultats de recherche, vous n'avez pas besoin de sélectionner les e-mails individuels pour les supprimer. La demande de suppression supprime tous les e-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

mails associés à la recherche lorsque `la valeur faux` est affichée dans la colonne A été supprimé des derniers résultats de recherche.



Si les approbations sont activées, cela signifie que vous avez soumis une demande de suppression d'e-mails. Les balises de sécurité et les notes de travail sont affichées sur l'enregistrement d'incident de sécurité connexe, comme décrit dans l'exemple précédent. En tant qu'approbateur, l'étape suivante consiste à traiter la demande de suppression.

Approuver les demandes de suppression d'e-mail pour l'intégration Microsoft Exchange Online

Si l'option d'approbation est activée dans votre Now Platform instance, les demandes de suppression d'e-mails sont envoyées à chaque membre du groupe d'approbation par e-mail. Vous sélectionnez le groupe d'approbation au cours de l'étape de configuration. Les approbations fournissent à votre organisation un niveau supplémentaire de contrôle sur la suppression des e-mails.

Avant de commencer

Vérifiez que l'option **Approbations** est sélectionnée dans l'onglet Paramètres supplémentaires du formulaire Paramètres de configuration de la recherche et de la suppression d'e-mails Exchange Online.

Vérifiez que vous avez activé les options **Envoi d'e-mail activé**et **Réception d'e-mail activée** dans votre instance pour les Now Platform demandes d'approbation. Pour plus d'informations, consultez Configurer votre Now Platform instance pour l'intégration Microsoft Exchange Online.

Lorsque l'utilisateur disposant du rôle sn_si.analyst soumet des demandes de suppression par e-mail, ces demandes sont envoyées par défaut par e-mail à sn_si.admin. Si vous avez créé un groupe d'approbation, chaque membre du groupe reçoit une notification. Les approbateurs peuvent traiter les demandes de suppression d'e-mail directement à partir de la notification par e-mail. Les demandes peuvent également être traitées à partir des enregistrements de résultats de recherche d'e-mail dans Now Platform les instances. Cette rubrique présente les deux méthodes d'approbation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les informations suivantes décrivent la demande dans la notification par e-mail :

Numéro d'enregistrement du résultat de recherche d'e-mail

Numéro unique affecté à l'enregistrement de recherche par le Now Platform dans le cadre de la piste d'audit.

Nom de l'analyste ayant soumis la demande

Nom de la personne qui a soumis la demande dans le cadre de la piste d'audit.

Lien vers l'incident de sécurité

Un lien vers l'incident de sécurité lié à l'événement d'hameçonnage. Affichez l'incident de sécurité avec les notes de travail, les recherches d'e-mails et les résultats de recherche d'e-mails directement à partir de l'e-mail.

Approuver ou rejeter les liens

Liens pour approuver ou rejeter la demande à partir de la notification par e-mail. Une fois que vous avez cliqué sur l'un ou l'autre des liens, le système lance automatiquement le workflow connexe et une note de travail est ajoutée à l'enregistrement de l'incident de sécurité.

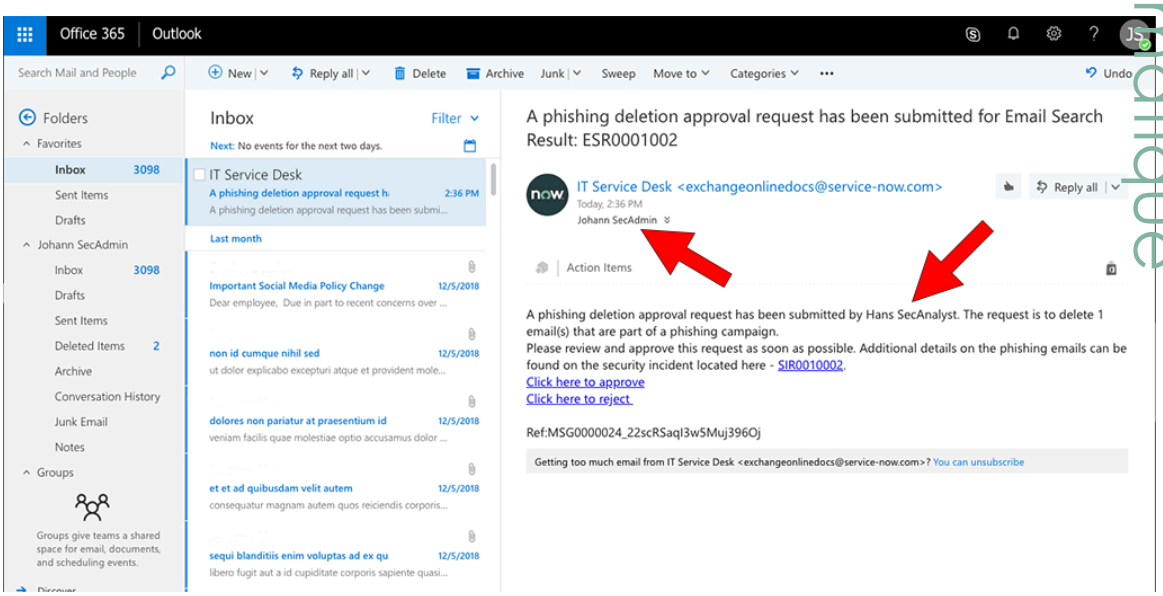
Rôle requis : sn_si.admin ou tous les membres d'un groupe d'approbation affecté.

Procédure

1. Pour traiter la demande de suppression de la notification par e-mail, procédez comme suit.

   a. En tant qu'approbateur, recherchez l'e-mail de notification dans le compte de messagerie que vous avez configuré dans votre Now Platform compte d'utilisateur.

   Dans cet exemple, l'utilisateur disposant du rôle sn_si.analyst (Hans SecAnalyst) soumet une demande pour supprimer un e-mail. Johann SecAdmin est membre du groupe d'approbation.



   b. Dans la notification par e-mail, choisissez une option pour continuer.

Traduction automatique

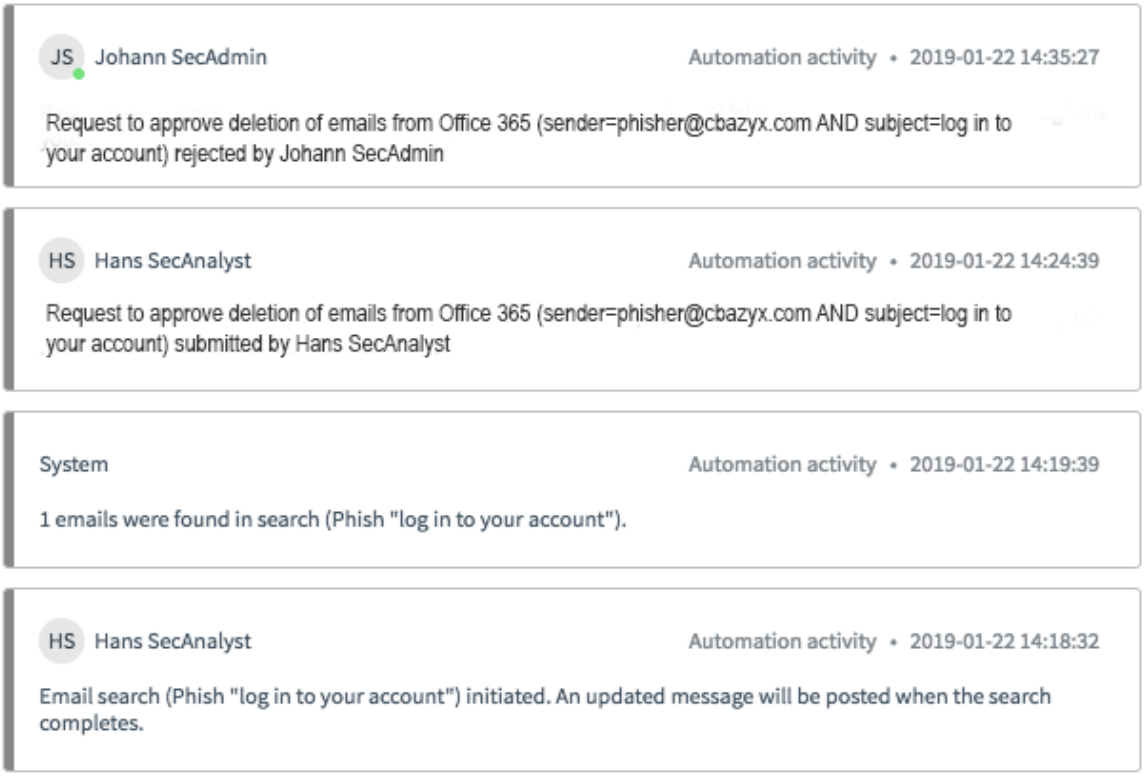
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Cliquez sur le lien Cliquez ici pour approuver Approuver	Approuvez la demande de suppression. Tous les éléments d'e-mail ayant un état `faux` dans la colonne A été supprimé qui sont associés à l'enregistrement des résultats de recherche sont automatiquement supprimés du Microsoft Exchange Online locataire. L'état de tous les éléments d'e-mail du jeu de résultats est mis à jour sur `vrai` dans la colonne A été supprimé de l'enregistrement de résultat de recherche d'e-mail. Une note de travail est publiée dans l'enregistrement d'incident de sécurité avec le nombre d'e-mails supprimés avec succès. Si le balisage est activé, la balise `Suppression d'e-mail : balise terminée` remplace la balise `Suppression d'e-mail : initiée`.
Cliquez sur le lien Cliquez ici pour rejeter	Rejetez la demande de suppression. Une note de travail est publiée avec le nom de la personne qui a rejeté la demande. Après le rejet d'une demande, en tant qu'utilisateur disposant du rôle sn_si.analyst, vous devez soumettre une nouvelle demande de suppression si vous déterminez que les e-mails doivent être supprimés.
Cliquez sur le lien vers l'enregistrement d'incident de sécurité (SIR0010002)	Examinez l'incident de sécurité connexe et toutes les données de recherche connexes avant de traiter la demande.

L'image suivante montre un exemple de piste d'audit créée par les notes de travail sur l'enregistrement d'incident de sécurité connexe pour cet exemple. Lorsque la demande est rejetée à partir de la notification par e-mail par un approbateur, une note de travail est publiée par la personne qui a rejeté la demande. Johann SecAdmin rejette cette demande.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Dans le Now Platform cas de la personne qui a rejeté la demande (Johann SecAdmin), dans **Libre-service > Mes approbations**, `Rejeté` s'affiche dans la colonne État.

Une fois qu'une demande est rejetée par un membre unique du groupe d'approbation, en tant qu'utilisateur disposant du rôle sn_si.analyst, vous devez soumettre une nouvelle demande de suppression de ces e-mails si vous déterminez qu'ils doivent être supprimés.

Dans cet exemple, une fois la demande rejetée, l'utilisateur disposant du rôle sn_si.analyst envoie une nouvelle demande.

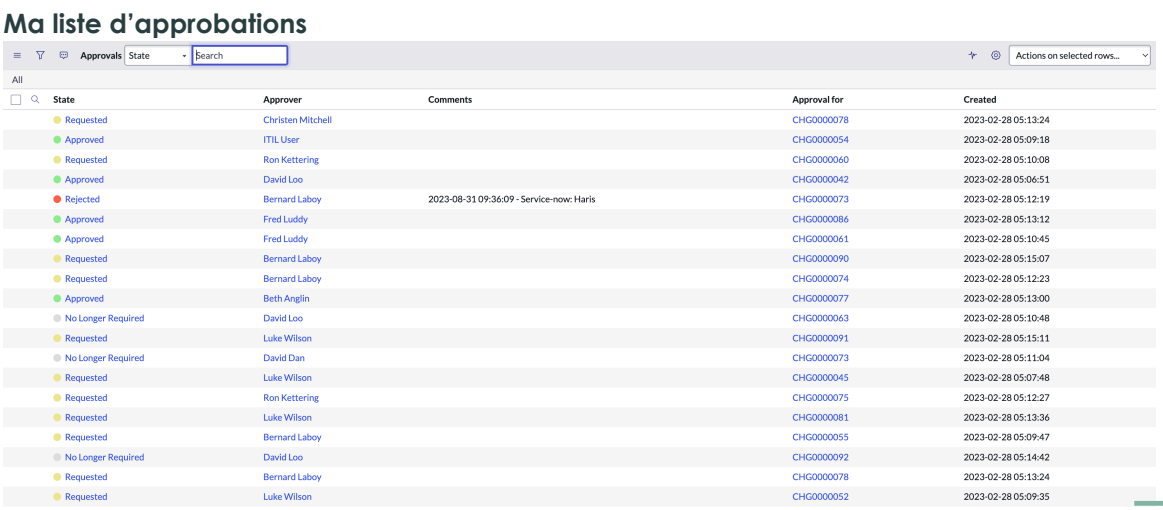
Un autre membre du groupe d'approbation, John Approver, reçoit un e-mail similaire à celui affiché dans l'exemple précédent. John Approver peut également traiter cette demande.

2. Les approbateurs peuvent également accéder à **Libre-service > Mes approbations** dans leurs Now Platform instances pour afficher et traiter les demandes de suppression. Pour traiter une demande à partir de **Mes approbations**, procédez comme suit.

Traduction automatique

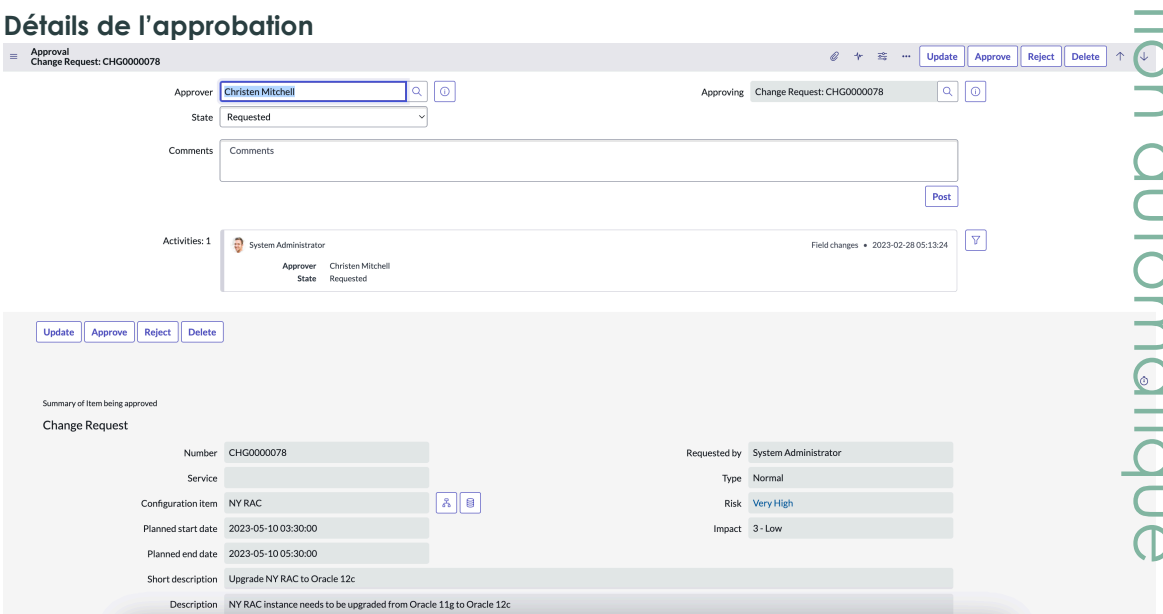
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Libre-service > Mes approbations**.



b. Dans la colonne État, cliquez sur l'élément demandé.

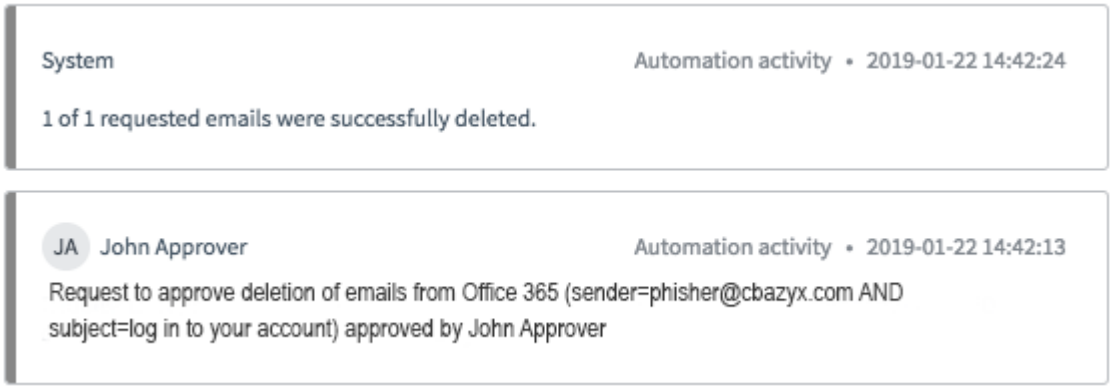
L'enregistrement d'approbation qui s'affiche répertorie les données relatives à la recherche, à la demande de recherche et aux résultats de la recherche.



c. Dans cet enregistrement, cliquez sur **Approuver** pour approuver la demande. Une fois la demande approuvée, le système lance le workflow de suppression pour supprimer les e-mails. L'image suivante montre un exemple de piste d'audit créée par les notes de travail sur l'enregistrement d'incident de sécurité connexe pour cet exemple. Une fois que cette demande de suppression est soumise à nouveau, elle est approuvée. Quelle que soit la méthode utilisée pour approuver une demande, le nombre d'e-mails supprimés avec succès est publié dans une note de travail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois les e-mails supprimés avec succès, dans l'enregistrement d'incident de sécurité connexe, si le balisage est activé, la balise `Suppression d'e-mail : terminée` remplace la balise `Suppression d'e-mail : initiée`.

Entrante **Libre-service > Mes approbations** pour l'approbateur (John Approver), l'état passe de `Demandé` à `Approuvé`.

Entrante **Libre-service > Mes approbations** pour les autres membres du groupe d'approbation (par exemple, Johann SecAdmin), l'état devient `N'est plus nécessaire` une fois la demande approuvée.

3. Pour confirmer que les e-mails sont également supprimés dans l'enregistrement Résultat de recherche d'e-mail de l'enregistrement d'incident de sécurité connexe, procédez comme suit.

a. Accédez à la **Incidents de sécurité > afficher tous les incidents** et localisez l'incident de sécurité lié au hameçonnage.
Les listes connexes s'affichent au bas de l'enregistrement.

b. Cliquez sur la liste connexe **Recherche d'e-mail** .

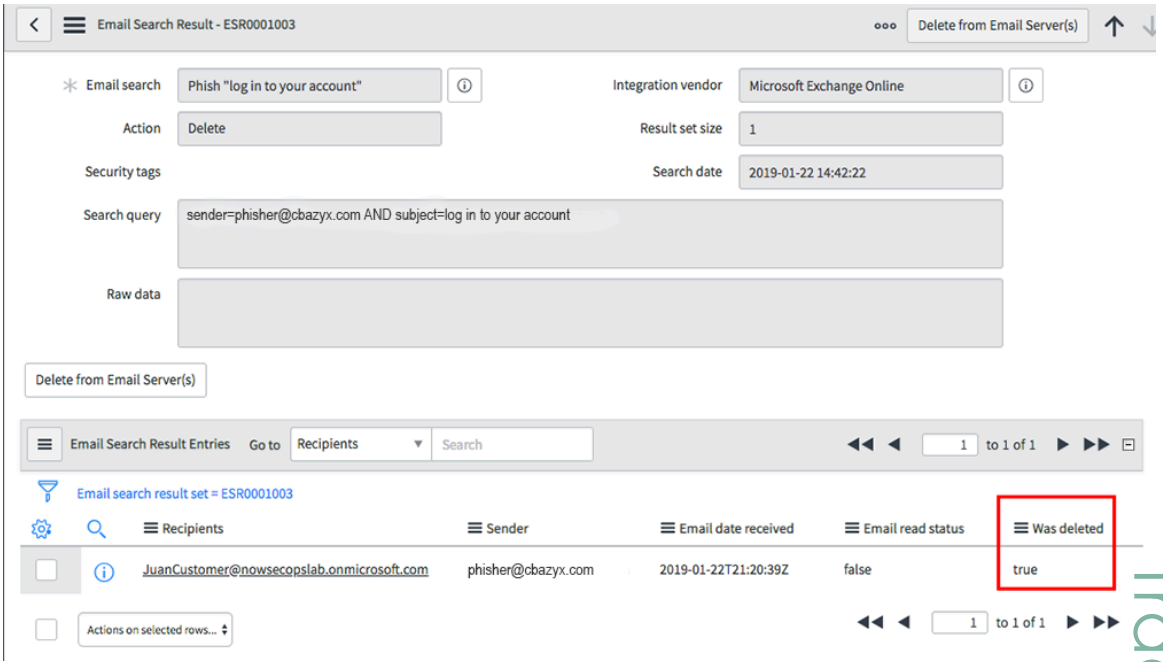
c. Cliquez sur le nom de la recherche dans la colonne Recherche d'e-mails (`Phish « connectez-vous à votre compte »`).
L'enregistrement de recherche d'e-mail s'affiche. Si la liste connexe Recherche d'e-mail n'est pas visible, cliquez sur le lien **Afficher toutes les listes connexes**.

d. Cliquez sur la liste connexe **Résultats de recherche d'e-mail** .
Dans la colonne Date de recherche, les actions de recherche et de suppression d'e-mails sont affichées avec les dates correspondantes.

e. Dans la colonne Rechercher une date, cliquez sur l'élément qui correspond à l'action de suppression.
Dans l'enregistrement Résultat de recherche d'e-mail qui s'affiche, l'état de la colonne A été supprimé indique que l'e-mail est supprimé (`vrai`).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous avez approuvé avec succès les demandes de suppression d'e-mail à partir d'une notification par e-mail et d'un enregistrement d'approbation, et vous avez confirmé que les e-mails sont supprimés. Pour en savoir plus sur la localisation de l'enregistrement Résultat de recherche d'e-mail, reportez-vous à la section Définir des critères de recherche d'e-mails et demander une recherche sur le Microsoft Exchange Online service.

Architecture d'intégration et connexion de systèmes externes pour l'intégration Microsoft Exchange Online

L'architecture Microsoft Exchange Online d'intégration a été développée pour prendre en charge les fonctionnalités de recherche et de suppression des menaces par e-mail dans le Microsoft Exchange Online service. Cette introduction explique pourquoi il existe des étapes de configuration que vous devez effectuer dans vos Microsoft comptes avant d'installer l'application ServiceNow .

L'architecture d'intégration est basée sur l'évaluation des interfaces de programmation d'applications actuellement disponibles et sur la consultation du personnel d'intégration Microsoft . Ces informations, ainsi que la Now Platform terminologie clé relative au et au Microsoft Exchange Online service, sont fournies pour clarifier le fonctionnement conceptuel de l'intégration.

Termes clés utilisés pour cette intégration

Les termes clés suivants sont utilisés lors de l'installation et de la configuration. Pour plus d'informations sur les conditions suivantes, consultez le site web de la documentation produit ServiceNow et le site web de la documentation Microsoft .

Now Platform

Un produit d'entreprise ServiceNow Il Now Platform s'agit de la base sur laquelle les composants individuels, tels que Security Incident Response (SIR), IT Service Management (ITSM) et d'autres produits sont construits.

Réponse aux incidents de sécurité (SIR)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application Now Platform qui suit la progression des incidents de sécurité, depuis la détection et l'analyse initiale, en passant par le confinement, l'éradication et la récupération, jusqu'à l'examen final et la fermeture post-incident.

Microsoft Exchange Online

Offre de service de messagerie pour Microsoft Exchange Online, qui fait partie de la suite de Microsoft produits Office 365.

API du graphique global

L'API fournie par Microsoft qui est utilisée pour accéder aux informations de la boîte de réception dans Microsoft Exchange Online.

Authentification basée sur certificat

Cette authentification permet aux clients d'autoriser ou d'exiger des utilisateurs qu'ils s'authentifient directement avec des certificats X.509 sur leur Azure Active Directory (Azure AD) pour les applications et la connexion au navigateur.

Authentification OAuth

ID créé dans le portail Azure, utilisé pour collecter des détails supplémentaires de messages Microsoft électroniques et pour supprimer des e-mails dans Microsoft Exchange Online.

Hôte Windows

Le type spécifique d'ordinateur virtuel utilisé dans cette intégration.

Serveur MID

Application Now Platform qui facilite la communication et le mouvement de données entre le et des Now Platform applications, sources de données et services externes. Un serveur MID est généralement requis pour l'intégration avec des technologies locales, mais un serveur MID peut être déployé dans certains cas entre le et une offre basée sur le Now Platform cloud lorsqu'un composant fourni par le client est requis pour l'intégration. Pour cette Microsoft Exchange Online intégration de services, le serveur MID facilite la communication entre le Now Platform serveur et le serveur PowerShell.

Serveur PowerShell

Le serveur PowerShell est une application Microsoft qui nécessite les informations d'identification de votre compte Microsoft.

Administrateur d'incident de sécurité (sn_si.admin)

L'utilisateur ayant le rôle sn_si.admin supervise la configuration de l'intégration au produit SIR dans votre Now Platform instance. L'utilisateur disposant de ce rôle approuve également les demandes de suppression d'e-mails par défaut et attribue le rôle sn_si.analyst si nécessaire. L'utilisateur disposant de ce rôle a également un contrôle total sur toutes les Gestion des services données.

Analyste des incidents de sécurité (sn_si.analyst)

L'utilisateur disposant du rôle sn_si.analyst interagit avec les incidents de sécurité dans le produit SIR et les analyse.

Connexion à des systèmes externes pour la recherche et la suppression d'e-mails

Cette application utilise le service PowerShell Centre de sécurité et de conformité Office 365 et le service Global Graph API pour récupérer des informations à partir du locataire de service Office 365 Exchange Online. Une connexion HTTPS sortante du MID Server vers cet environnement est nécessaire pour que l'intégration fonctionne correctement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'architecture d'intégration prend en charge une fonctionnalité de recherche et de suppression d'e-mails dans le Microsoft Exchange Online service. L'architecture d'intégration cible les e-mails d'hameçonnage ainsi que d'autres menaces par e-mail susceptibles de compromettre la sécurité de votre organisation. Pour obtenir des e-mails qui correspondent à un critère de requête de recherche donné, le Now Platform se connecte à un Microsoft Exchange Online locataire de service à l'aide d'un serveur MID qui exécute PowerShell sur un serveur Windows.

Une fois le Now Platform connecté au Microsoft Exchange Online service, l'intégration prend en charge les niveaux suivants de recherches d'e-mails :

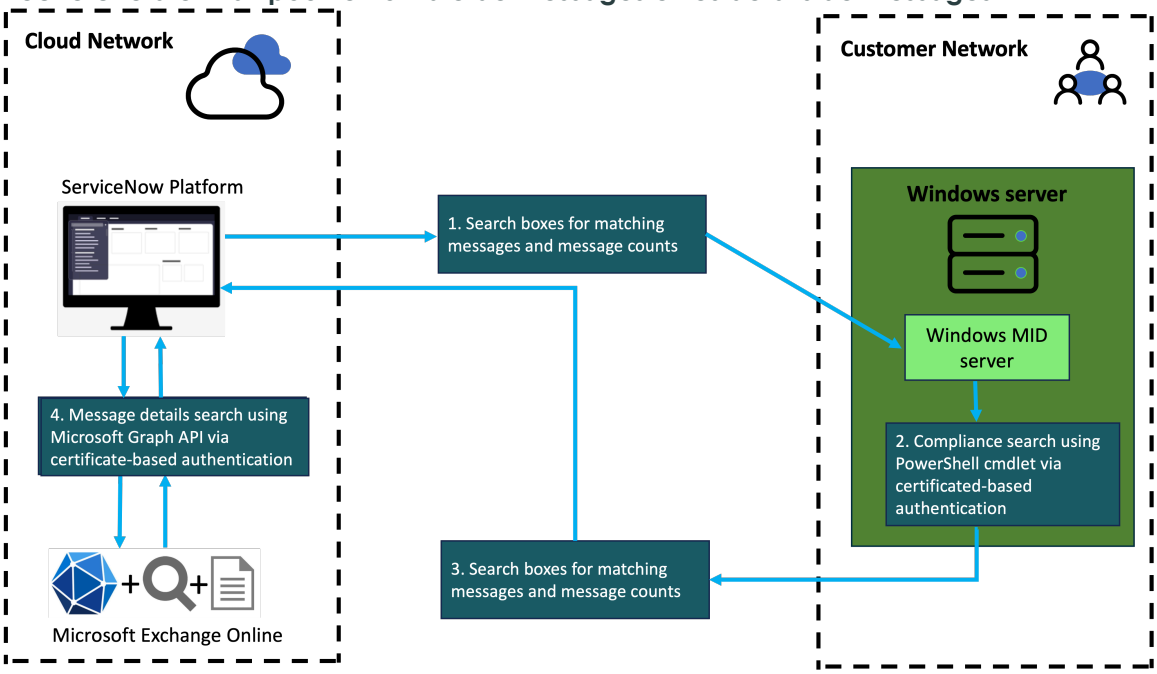
- Les messages correspondants : Cette recherche est effectuée via l'applet de commande Microsoft PowerShell via un serveur MID Windows qui est un composant de .Now Platform Cette recherche est basée sur des critères que vous configurez dans le Now Platform formulaire à partir d'un incident de sécurité. Le premier composant de la recherche renvoie tous les e-mails qui correspondent aux critères de recherche que vous avez configurés, ainsi que les adresses de boîtes aux lettres spécifiques dans lesquelles ces messages se trouvent dans Microsoft Exchange Online. Les paramètres de recherche pris en charge sont l'objet du message électronique, l'expéditeur et le destinataire (valeur affichée dans le champ Destinataire d'un message électronique).
- Détails du message : Une fois que la recherche initiale basée sur l'applet de commande PowerShell a identifié les messages correspondants, cette recherche récupère des informations supplémentaires sur les messages à l'aide de l'API Microsoft Global Graph. Les résultats de l'e-mail renvoyé incluent les détails de message suivants :
  - État de lecture : l'état Vrai ou Faux suit le moment où les utilisateurs ont lu des e-mails.
  - Adresse de l'expéditeur.
  - Adresse du destinataire : ces adresses comprennent des individus, un groupe et des personnes qui sont en copie conforme et en cci sur les messages.
  - État de suppression : l'état Vrai ou Faux suit les e-mails supprimés.
  - ID du message : identificateur alphanumérique des messages électroniques.

Le flux de données de base de l'e-mail recherche le nombre de messages et les détails des messages est illustré dans la figure suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche d'e-mail pour le nombre de messages et les détails de messages



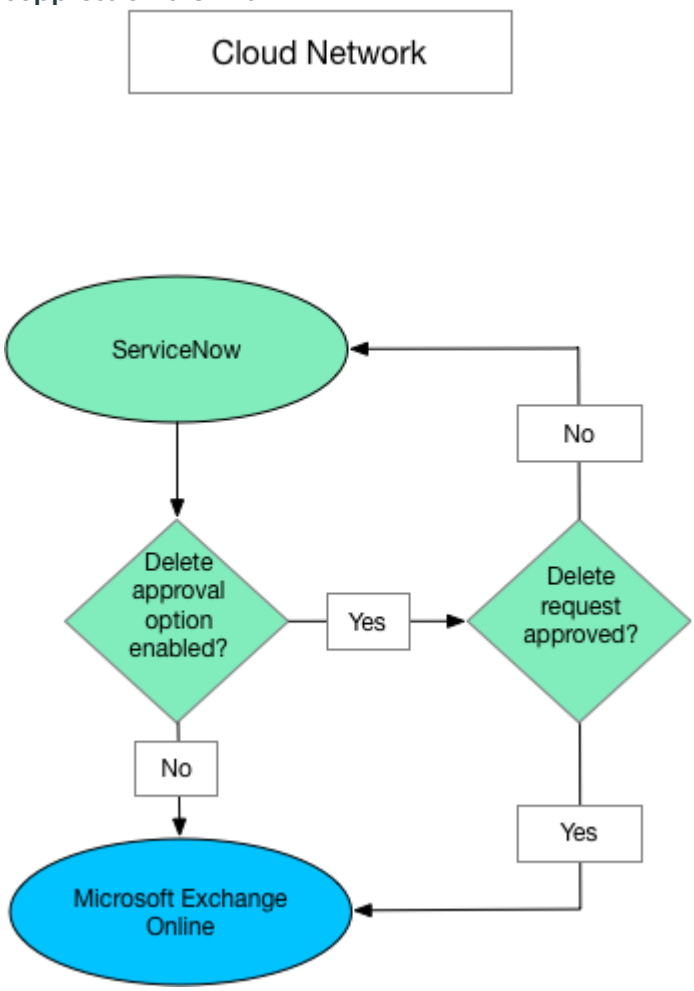
Pour la suppression des e-mails, l'intégration utilise l'API Global Graph. La récupération des e-mails supprimés est disponible en option lors de l'étape de configuration et est décrite plus en détail dans Configurer l'intégration Microsoft Exchange Online avec votre Now Platform instance.

Le flux de données pour la suppression des e-mails avec le processus d'approbation préconfiguré est illustré dans la figure suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suppression d'e-mail



Workflows

L'application Microsoft Exchange Online de recherche et de suppression d'e-mails inclut les workflows suivants :

- Exchange Online : suppression des e-mails
- Obtenir les détails de la messagerie Exchange Online.
- Microsoft Exchange Online -Recherche et suppression d'e-mails.

Pour plus d'informations, reportez-vous à la section Prise en main des workflows .

Vous êtes maintenant prêt à configurer les comptes requis pour l'intégration.

Récupérer les e-mails supprimés sur le Microsoft Exchange Online service

(Facultatif) En tant qu'administrateur Microsoft Exchange, vous pouvez récupérer les e-mails supprimés si votre rattrapage d'incident nécessite que vous récupériez les e-mails supprimés par le workflow de cette intégration.

Avant de commencer

Pour en savoir plus sur la façon dont cette intégration supprime des e-mails, reportez-vous à la section Configurer l'intégration Microsoft Exchange Online avec votre Now Platform instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur le rôle d'administration dans le produit Office 365, y compris des informations sur la Microsoft récupération d'éléments supprimés dans une boîte aux lettres d'utilisateur, voir À propos du rôle administrateur Exchange Online .

Rôle requis : admin, administrateur Microsoft Exchange

Pourquoi et quand exécuter cette tâche

Si vous sélectionnez l'option **Récupérer les e-mails supprimés** dans l'onglet Paramètres supplémentaires lors de l'étape de configuration, vous activez la récupération des e-mails supprimés dans votre Microsoft Exchange Online locataire. Les e-mails supprimés à l'aide du workflow de suppression de cette intégration sont placés dans le sous-dossier Éléments supprimés du dossier Éléments récupérables dans la boîte aux lettres de l'utilisateur sur le Microsoft Exchange Online service. Si le compte de l'utilisateur est configuré dans Microsoft Exchange Online le locataire afin que l'utilisateur puisse afficher le dossier Éléments supprimés, l'utilisateur peut récupérer ces e-mails à l'aide du Microsoft service Outlook sur le Web. L'administrateur peut également récupérer les Microsoft Exchange Online e-mails supprimés dans le dossier Éléments supprimés d'un utilisateur. Pour plus d'informations, voir Récupérer des éléments supprimés ou des e-mails dans Outlook Web App .

Rôle requis : Microsoft Exchange Online administrateur ou Microsoft administrateur général pour récupérer les e-mails supprimés.

Rôle requis : sn_si.admin dans le Now Platform pour activer l'option Récupérer les e-mails supprimés.

Rôle requis : sn_si.analyste dans le pour terminer une recherche réussie d'e-mails et vérifier que les e-mails sont correctement supprimés avant la Now Platform récupération.

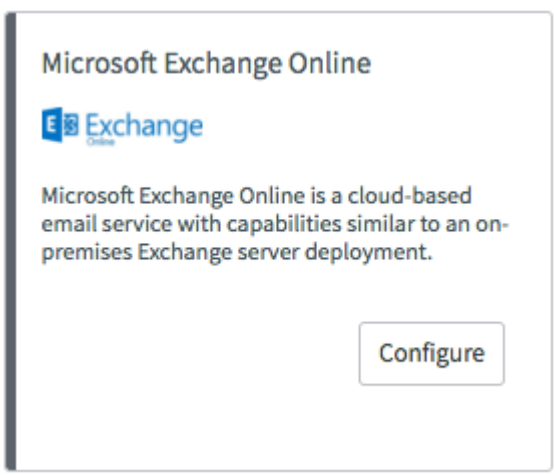
Procédure

Pour activer l'option de récupération d'e-mail, procédez comme suit.

a. Accédez à la **Security Operations** > **Intégrations** > **Configurations**.

b. Localisez la Microsoft Exchange Online tuile.

c. Cliquez sur **Configurer**.

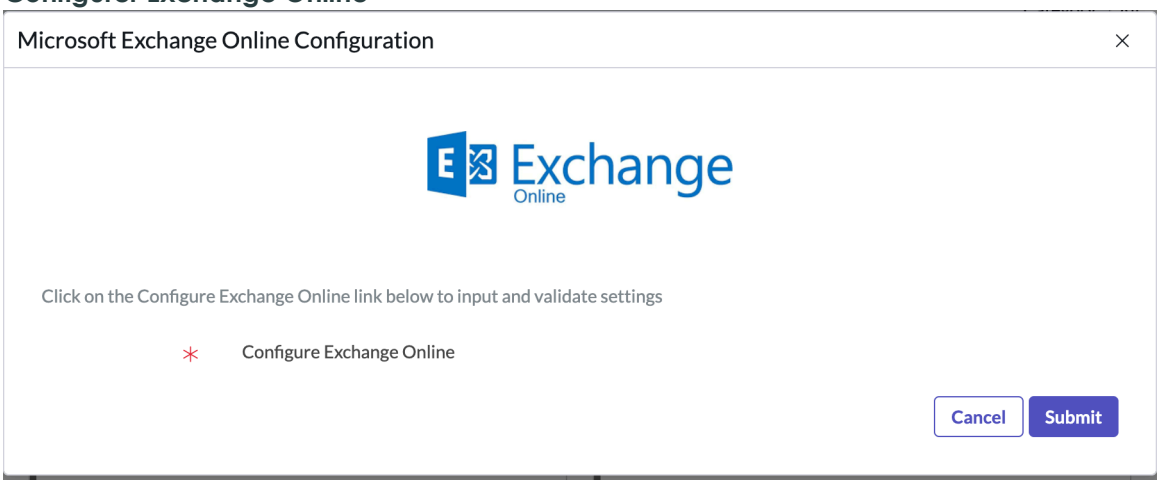


d. Dans la boîte de Microsoft Exchange Online dialogue Configuration qui s'affiche, cliquez sur **Configurer Exchange Online**.

Traduction automatique

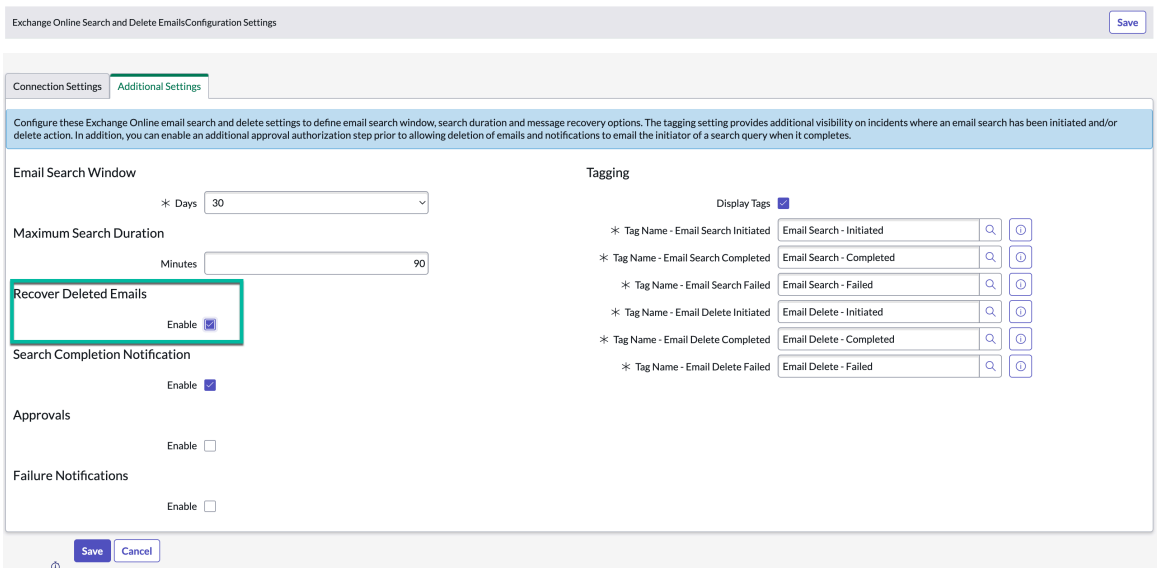
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Exchange Online



e. Dans l'onglet `Paramètres supplémentaires`, sous `Récupérer les e-mails supprimés`, cochez la case **Activer** .

Récupérer les e-mails supprimés



f. Vérifiez tous les autres paramètres et cliquez sur **Soumettre**.

g. Pour vérifier que la recherche et la suppression des e-mails sont effectuées avec succès pour les e-mails que vous souhaitez récupérer, accédez à l'incident de sécurité qui a journalisé les workflows de recherche et de suppression d'e-mails.

h. Localisez les notes de travail et vérifiez que le système a correctement supprimé les messages.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. En tant qu'administrateur Microsoft Exchange Online ou administrateur général, connectez-vous à votre Microsoft compte Office 365.

j. Suivez les étapes décrites dans Récupérer des éléments ou des e-mails supprimés dans Outlook Web App sur le site web de la Microsoft documentation.

Modifier les balises de sécurité dans Now Platform pour l'intégration Microsoft Exchange Online

Vous pouvez modifier les noms et les couleurs des balises de sécurité dans votre Now Platform® instance pour l'intégration Microsoft Exchange Online . Ces balises de sécurité vous aident à identifier rapidement quand la recherche d'e-mail se termine ou échoue. Ils identifient également quand des demandes de suppression d'e-mails sont lancées et quand les éléments d'e-mail sont supprimés avec succès.

Avant de commencer

Par défaut, les balises de sécurité sont activées dans votre Now Platform® instance si vous sélectionnez l'option **Balises d'affichage** au cours de l'étape de configuration. Vous pouvez modifier les couleurs et les noms des balises, et affecter des balises à des groupes de balises de sécurité pour vous aider à les organiser dans votre Now Platform® instance. Par exemple, vous pouvez modifier les couleurs des balises de sorte que la balise de début d'une fonctionnalité soit d'une couleur et que la balise de complétion soit d'une autre couleur pour correspondre aux autres balises de sécurité activées dans votre Now Platform® instance. Ces différentes couleurs peuvent vous aider à identifier rapidement quand les workflows commencent et se terminent avec succès. Si vous décidez que vous n'avez pas besoin d'une balise spécifique, sans désactiver le balisage pour l'intégration, vous pouvez également désactiver une seule balise de l'enregistrement de balise. Si elle est désactivée, cette balise n'apparaît plus sur les incidents de sécurité associés. Pour plus d'informations sur la configuration de groupes de balises de sécurité et de balises, consultez Configurer des groupes de balises de sécurité et des balises sur le site web de la documentation produit ServiceNow .

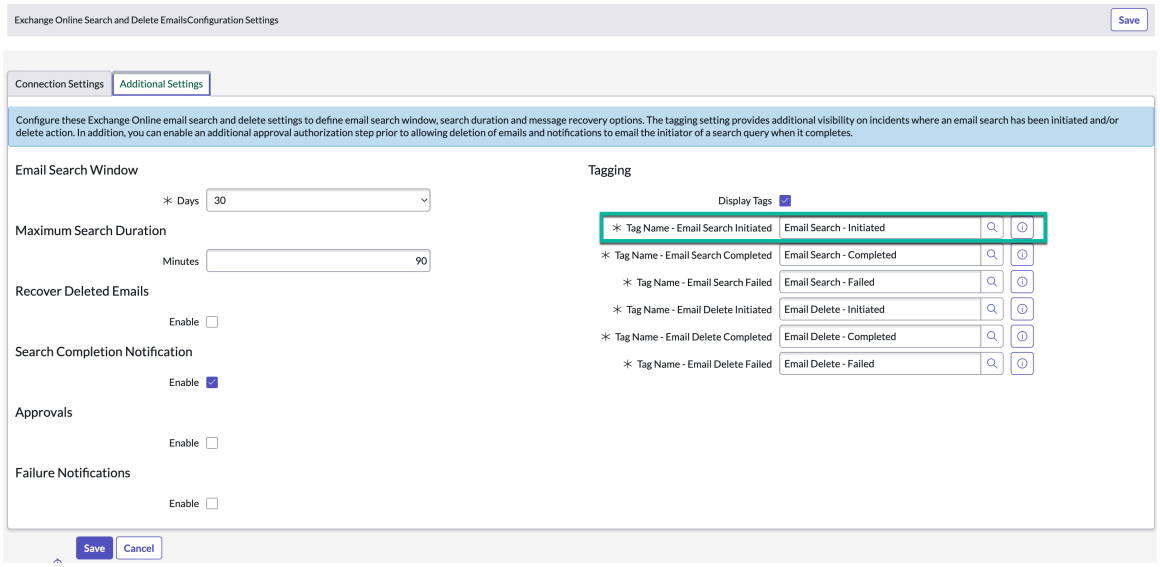
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Intégrations** > **Paramètres Exchange Online**.
2. Cliquez sur l'onglet **Paramètres supplémentaires** pour le sélectionner.
3. Dans l'onglet qui s'affiche, si l'option **Afficher les balises** est décochée, sélectionnez-le pour afficher les noms des balises.
4. Une fois les noms des balises affichés, cliquez sur l'icône d'informations à droite d'une balise.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



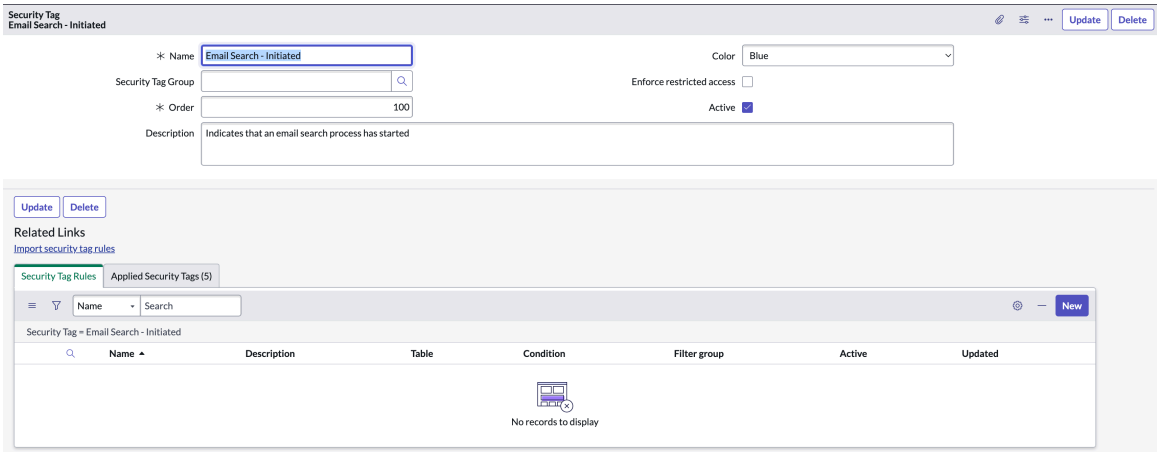
5. Dans la boîte de dialogue Balise de sécurité qui s'affiche, cliquez sur **Ouvrir l'enregistrement**.
6. Dans l'enregistrement qui s'affiche, modifiez les champs.

Option	Description
Nom	Nom unique de la balise de sécurité.
Couleur	Couleur de balise de sécurité. Sélectionnez une couleur dans la liste de choix.
Groupe de balises de sécurité	Nom du groupe de balises de sécurité. Cliquez sur l'icône d'informations pour afficher les groupes disponibles. La valeur par défaut est le groupe de balises Meta.
Appliquer l'accès restreint	Sélectionnez cette option pour affecter les rôles de lecture et d'écriture nécessaires aux utilisateurs pour lire ou écrire dans les enregistrements qui ont cette balise de sécurité. La valeur par défaut est effacée.
Ordre	Spécifier l'ordre dans lequel la balise apparaît sur les formulaires ou dans une liste. La valeur par défaut est 100. Pour définir l'ordre dans la liste, saisissez une valeur. Par exemple, 100, 200, 300, 400. La balise dont le numéro est le plus bas est affichée en premier dans la liste. Le profil avec le numéro le plus élevé est affiché en dernier.
Actif	Activez ou désactivez cette balise. La valeur par défaut est sélectionnée (active)
Description	Description de la balise.

7. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous avez maintenant modifié avec succès l'enregistrement de balise pour une balise de sécurité.

Liste de vérification pour l'intégration Microsoft Exchange Online

Utilisez cette liste de vérification pour vous guider dans les tâches de bout en bout de l'intégration. La liste de vérification suivante comprend les tâches de configuration et d'installation, ainsi que des exemples de cas d'utilisation et de résultats attendus pour l'application.

Avant de commencer

Suivez la progression de l'installation, de l'installation et de la configuration de l'intégration à l'aide de la table suivante. Terminez toutes les tâches d'une étape avant de passer à l'étape suivante. Chaque étape identifie les rôles requis pour effectuer les tâches et référence les rubriques numérotées du guide d'installation et de configuration pour cette intégration.

Rôles requis : les rôles sont répertoriés pour chaque étape dans la table suivante.

Procédure

Pour suivre votre progression en vue de l'intégration, suivez les étapes de la table dans l'ordre dans lequel elles sont présentées

Liste de vérification

☐	En tant qu'administrateur Microsoft Office 365, configurez votre Microsoft compte Office 365. Créez un compte d'API qui autorise l'accès au centre de sécurité et de conformité dans Microsoft Office 365.
☐	En tant qu'administrateur Microsoft Azure, configurez votre Microsoft compte Azure. Créez un compte qui utilise un ID d'application pour collecter des détails supplémentaires sur les e-mails et supprimer des e-mails. Pour connaître la procédure de configuration du compte, reportez-vous à la section Configurez votre Microsoft compte Azure pour l'intégration ServiceNow Microsoft Exchange Online.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

☐	En tant qu'administrateur Now Platform , configurez votre Now Platform instance pour l'intégration. Pour les tâches et plus d'informations, reportez-vous à la section Configurer votre Now Platform instance pour l'intégration Microsoft Exchange Online. **a.** Affectez Now Platform des rôles. **b.** Configurez un Serveur MID dans votre Now Platform instance. **c.** Installez Now Platform (SIR) et Opérations de sécurité les applications à partir de et ServiceNow Store activez-les sur votre instance. **d.** Activez les options d'envoi et de réception d'e-mail. **e.** Affectez le rôle de lecture et d'écriture d'e-mail au sn_si.analyst. **f.** Créez un groupe d'approbation.
☐	En tant qu'administrateur Now Platform , installez l'application pour l'intégration à partir du ServiceNow Store. Pour connaître la procédure d'installation, reportez-vous à la section Installer l'application Microsoft Exchange Online pour l'intégration ServiceNow Microsoft Exchange Online.
☐	En tant que sn_si.admin, renseignez les onglets des paramètres de configuration pour établir la connectivité et activer les workflows de recherche et de suppression. Pour les paramètres de connexion et de configuration, reportez-vous à la section Configurer l'intégration Microsoft Exchange Online avec votre Now Platform instance.
☐	En tant que sn_si.analyste, configurez les critères de recherche des e-mails et demandez une recherche des e-mails correspondants sur le Microsoft Exchange Online serveur. Pour obtenir un exemple, reportez-vous à Définir des critères de recherche d'e-mails et demander une recherche sur le Microsoft Exchange Online service. **a.** Localisez les incidents de sécurité liés à des événements d'hameçonnage. **b.** Définissez des critères de recherche d'e-mails. **c.** Demander une recherche d'e-mails. **d.** Localisez les résultats de recherche et les détails des messages sur les listes connexes de l'incident de sécurité.
☐	En tant que sn_si.analyst, supprimez les Microsoft Exchange Online e-mails du serveur. Pour obtenir un exemple, reportez-vous à Demander l'approbation de suppression des e-mails sur le service Microsoft Exchange Online.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	a. Localisez l'incident de sécurité avec les résultats de la recherche. **b.** Supprimez des e-mails ou demandez l'approbation pour supprimer des e-mails. **c.** Vérifiez que les e-mails sont supprimés des résultats publiés dans les notes de travail et les listes connexes sur l'incident de sécurité.
☐	En tant que sn_si.admin ou en tant que membre d'un groupe d'approbation, traitez les demandes de suppression d'e-mail via des notifications par e-mail. Pour obtenir un exemple, reportez-vous à Approuver les demandes de suppression d'e-mail pour l'intégration Microsoft Exchange Online.

Vous avez terminé avec succès les étapes de configuration et vérifié les résultats attendus pour l'intégration.

Dépanner l'intégration de Microsoft Exchange Online

Une fois que vous avez correctement configuré l'application Microsoft Exchange Online et configuré votre Now Platform instance, si vous rencontrez des problèmes de recherche d'e-mails, vous pouvez exécuter des tests de diagnostic basés sur des critères spécifiques.

Avant de commencer
Rôle requis : administrateur

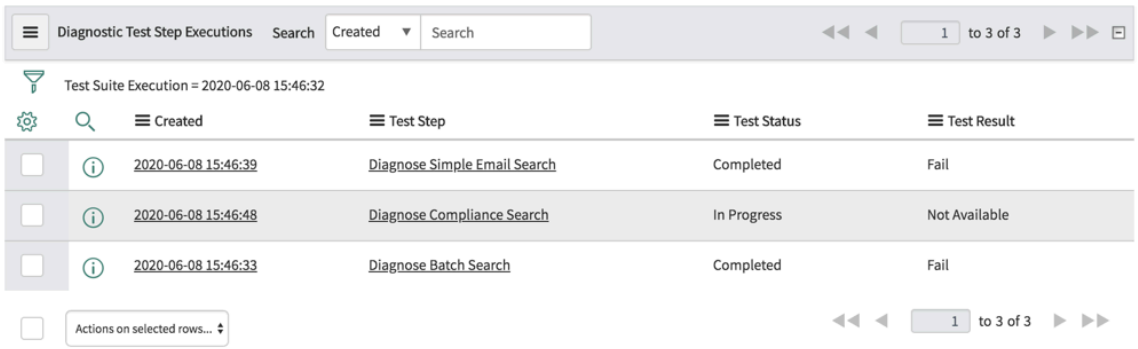
Pourquoi et quand exécuter cette tâche
Les résultats de ces tests peuvent aider le support client à identifier et à ServiceNow résoudre les problèmes.

Procédure

1. Accédez à la **Tout** > **Diagnostics d'Exchange Online** > **Initier des tests de diagnostic**.
2. Renseignez les champs suivants :
   - Saisissez l'expéditeur et une ou plusieurs adresses e-mail du destinataire pour affiner les critères de recherche et fournir des résultats plus précis.
   - Spécifiez le sujet pour lequel les tests de diagnostic sont effectués. Il s'agit d'un champ obligatoire.
3. Cliquez sur **Envoyer**.
4. Pour afficher les résultats des tests de diagnostic, accédez à **Diagnostics d'Exchange Online** > **Afficher les résultats des tests de diagnostic**.
   La colonne État affiche les états suivants :
   - Terminé - Réussi : les tests ont été effectués avec succès.
   - Terminé – Échecs : les tests ont été effectués avec quelques erreurs.
   - En cours : les tests sont toujours en cours d'exécution et ne sont pas terminés.
5. Cliquez sur l'exécution de la suite de tests de diagnostic pour afficher les détails de l'exécution du test.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

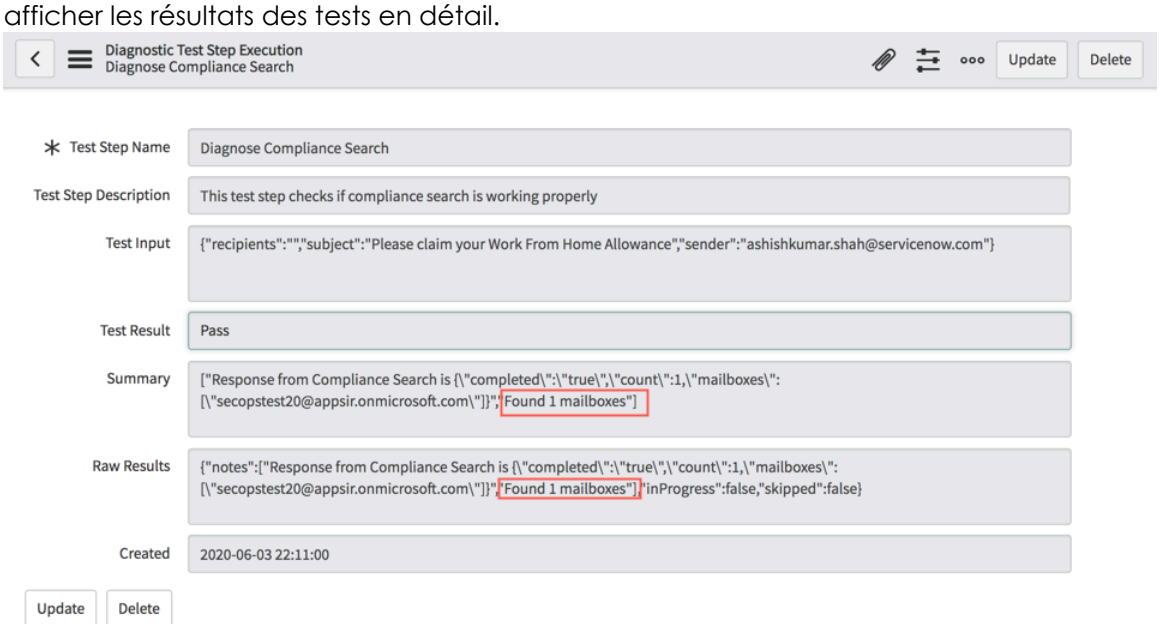


Les types de tests de diagnostic suivants sont exécutés :

- Diagnostiquer la recherche de conformité : génère une liste des boîtes aux lettres des destinataires en effectuant une recherche de conformité.
- Diagnostiquer la recherche d'e-mail simple : recherche les boîtes aux lettres d'e-mail en effectuant des appels REST distincts pour rechercher chaque dossier du destinataire.
- Recherche par lots de diagnostic : recherche des boîtes de réception dans une requête par lots, en combinant plusieurs recherches dans un seul appel REST.

Pour effectuer les tests 2 et 3, vous devez spécifier les adresses e-mail du destinataire dans la page Initier les tests de diagnostic. S'ils ne sont pas spécifiés, les tests ne seront pas effectués.

6. Cliquez sur le lien Créé dans la page Exécution de la suite de tests de diagnostic pour afficher les résultats des tests en détail.



L'image ci-dessus montre les résultats détaillés de l'exécution de l'étape de test de recherche de conformité Diagnostiquer et montre le nombre de boîtes aux lettres trouvées dans la recherche.

Important : Pour connaître les scénarios de dépannage et les problèmes supplémentaires, consultez KB1501969 : Configuration et dépannage de l'authentification basée sur certificat pour l'intégration d'Exchange Online

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration de Microsoft Exchange sur site

L'intégration Microsoft Exchange sur site fournit des outils permettant aux analystes de sécurité de contenir et d'éradiquer les menaces d'hameçonnage et de harponnage dans les instances locales.

Explorer	Configurer
Intégrations de Réponse aux incidents de sécurité	Prise en main de l'intégration Microsoft Exchange On-Premises
Utiliser Rechercher et supprimer les e-mails d'hameçonnage	**Développer** • ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide • Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service et assistance client	

Prise en main de l'intégration Microsoft Exchange On-Premises

L'intégration Microsoft Exchange sur site fournit des outils aux analystes de sécurité pour contenir et corriger les menaces d'hameçonnage et de harponnage dans les instances locales. Avant de pouvoir utiliser l'intégration Microsoft Exchange locale, vous devez la télécharger à ServiceNow Store partir du et identifier les serveurs Exchange et MID appropriés.

Avant de commencer

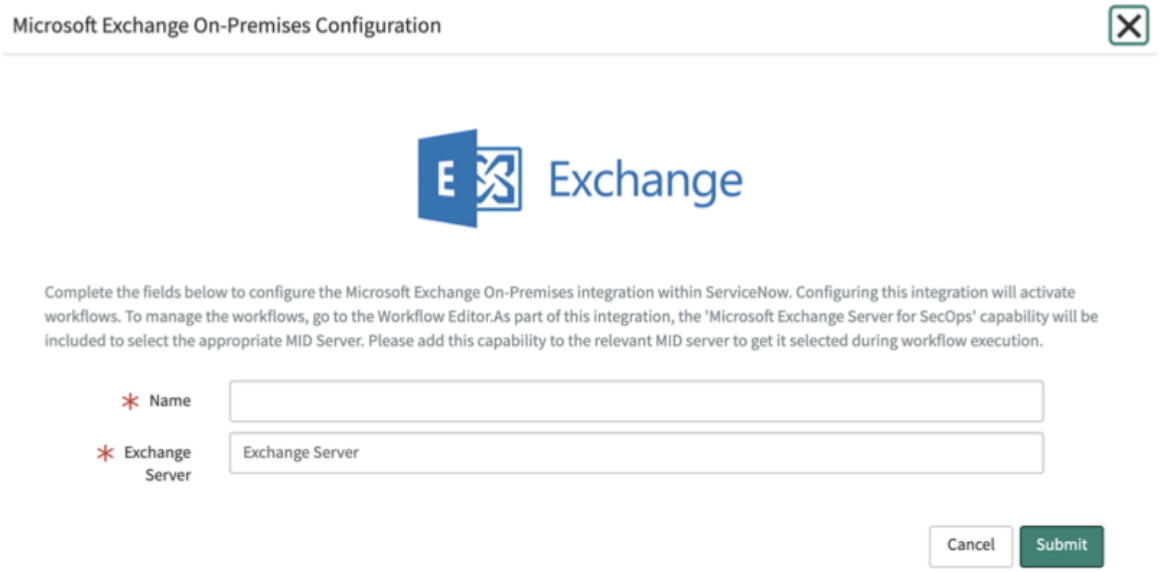
Rôle requis : sn_si_admin

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation du système d'exploitation terminée, accédez à **Security Operations** > **Intégrations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Dans la Microsoft Exchange carte On-Premises, cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



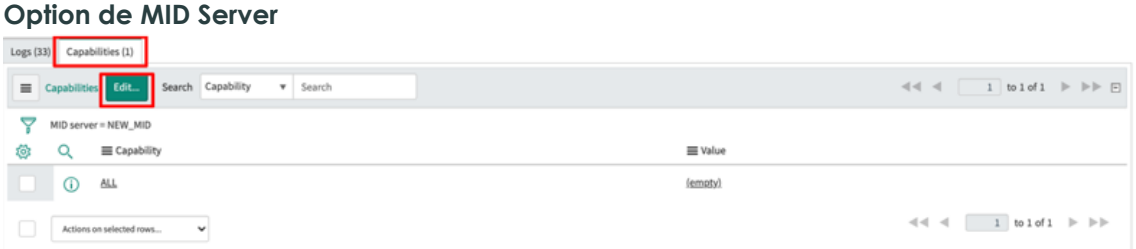
4. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
Serveur Exchange	Spécifiez le serveur Exchange à utiliser.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

5. Cliquez sur **Envoyer**.
   La carte de configuration de l'intégration s'affiche.
6. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
7. Pour revenir à la liste initiale des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .
8. Accédez à la **Orchestration** > **Serveurs MID**.
9. Ouvrez l'enregistrement et vérifiez que l'état du MID Server accessible au serveur Exchange et **son option État** est définie sur **Actif** et **l'option Validé** est définie sur **Oui**.
10. Ajoutez l'option de serveur MID :
    - Sélectionnez le MID Server respectif auquel ajouter l'option.
    - Cliquez sur la liste connexe **Options** , puis cliquez sur **Modifier**.

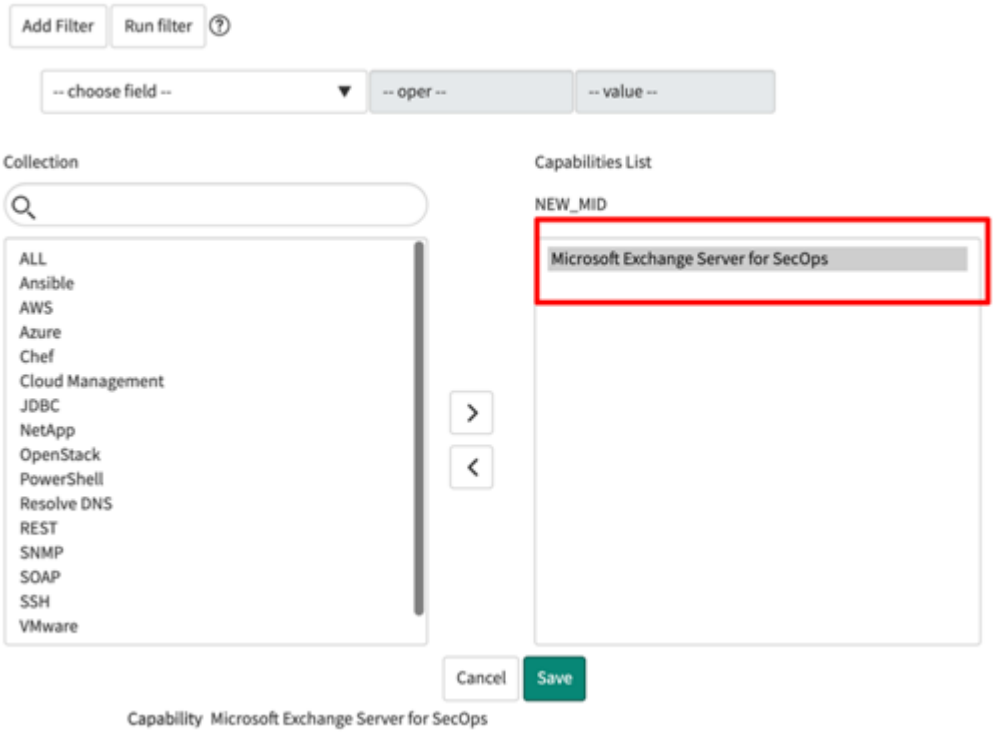
Option de MID Server



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Supprimez **tout** et ajoutez **Microsoft Exchange Server pour SecOps**.



- Sélectionnez les **plages IP** dans la section **Listes connexes** et définissez la valeur sur **TOUS** ou sur n'importe quelle valeur souhaitée.
- Sélectionnez les **applications prises en charge** dans la section **Listes connexes** et définissez la valeur sur TOUT ou Orchestration.
- **Enregistrez** l'enregistrement.

11. Validez les connexions et les informations d'identification.
12. Une fois les informations d'identification validées, la configuration sur l'instance ServiceNow est terminée et vous pouvez effectuer des opérations de recherche et de suppression d'e-mails à l'aide de cette intégration.

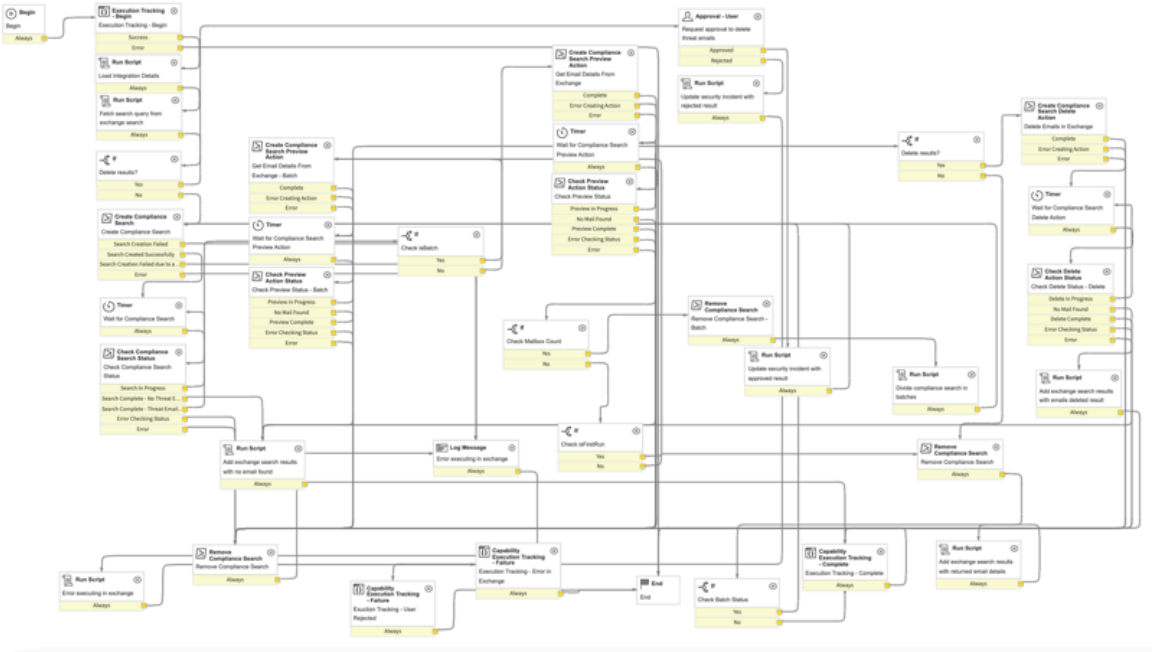
Microsoft Exchange : effectuer un workflow de recherche et de suppression d'e-mails

Lorsque le workflow **Microsoft Exchange - Effectuer une recherche et une suppression d'e-mail** est exécuté, il effectue une recherche dans le serveur Exchange à l'aide de la requête de recherche fournie et renvoie les détails à l'instance locale.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Le workflow **Microsoft Exchange - Effectuer une recherche et une suppression d'e-mail** est exécuté lorsque les recherches d'e-mails sont configurées et que vous appuyez sur le bouton **Supprimer des serveurs de messagerie** ou **Rechercher sur les serveurs de messagerie** .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les activités spécifiques à cette intégration sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Les activités du workflow comprennent :

- Créer une activité de recherche de conformité
- Vérifier l'activité d'état de la recherche de conformité

Créer une activité d'action de prévisualisation de recherche de conformité

L'activité Créer une action de prévisualisation de recherche de conformité crée une action de recherche de conformité de type aperçu sur le serveur Exchange pour la recherche de conformité créée.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
targetId	Champ d'identificateur d'hôte cible obligatoire où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Conditions de sortie

Les conditions de sortie possibles pour cette activité sont les suivantes :

Conditions de sortie

Variable	Description
Terminé	Lorsque l'action de recherche de conformité est créée avec succès.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions de sortie (suite)

Variable	Description
Erreur lors de la création de l'action	Lorsque la création de l'action de recherche de conformité échoue en raison d'une exception dans le serveur Exchange.
Erreur	Lorsqu'une exception se produit dans l'activité du workflow.

Vérifier l'activité du statut de l'action de l'aperçu

L'activité Statut de l'action d'aperçu vérifie l'état de l'action de recherche de conformité de type aperçu et renvoie les informations d'aperçu des e-mails trouvés tels que le destinataire, l'expéditeur, l'objet, la date de réception de l'e-mail.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
targetId	Champ d'identificateur d'hôte cible obligatoire où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
réponse	Contient l'état de l'action de recherche de conformité et les informations d'aperçu de l'e-mail trouvés dans le cadre de la recherche de conformité.

Conditions de sortie

Les conditions de sortie possibles pour cette activité sont les suivantes :

Conditions de sortie

Variable	Description
Aperçu en cours	Lorsque l'état de l'action de recherche de conformité est en cours.
Aucun e-mail trouvé	Lorsque l'état de l'action de recherche de conformité est terminé et qu'aucun e-mail n'est trouvé dans le cadre de la recherche de conformité.
Aperçu terminé	Lorsque l'état de l'action de recherche de conformité est terminé et que des e-mails sont trouvés dans le cadre de la recherche de conformité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions de sortie (suite)

Variable	Description
Erreur lors de la vérification de l'état	Lorsque la vérification de l'état échoue en raison d'une exception dans le serveur Exchange.
Erreur	Lorsqu'une exception se produit dans l'activité du workflow.

Créer une activité d'action de suppression de recherche de conformité

L'activité Créer une action de suppression de recherche de conformité crée une nouvelle action de recherche de conformité de type purge sur le serveur Exchange pour la recherche de conformité créée.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
targetId	Champ d'identificateur d'hôte cible obligatoire où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Conditions de sortie

Les conditions de sortie possibles pour cette activité sont les suivantes :

Conditions de sortie

Variable	Description
Terminé	Lorsque l'action de recherche de conformité est créée avec succès.
Erreur lors de la création de l'action	Lorsque la création de l'action de recherche de conformité échoue en raison d'une exception dans le serveur Exchange.
Erreur	Lorsqu'une exception se produit dans l'activité du workflow.

Vérifier l'activité Supprimer le statut de l'action

L'activité Vérifier le statut de l'action de suppression vérifie le statut de l'action de recherche de conformité de type purge et effectue une opération de suppression réversible sur le serveur Exchange pour les e-mails trouvés dans le cadre de la recherche de conformité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
targetId	Champ d'identificateur d'hôte cible obligatoire où se trouve le serveur Exchange.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
réponse	Contient l'état de l'action de recherche de conformité et le nombre d'e-mails supprimés, qui ont été trouvés dans le cadre de la recherche de conformité.

Conditions de sortie

Les conditions de sortie possibles pour cette activité sont les suivantes :

Conditions de sortie

Variable	Description
Suppression en cours	Lorsque l'état de l'action de recherche de conformité est en cours.
Aucun e-mail trouvé	Lorsque l'état de l'action de recherche de conformité est terminé et qu'aucun e-mail n'est supprimé dans le cadre de la recherche de conformité.
Suppression terminée	Lorsque l'état de l'action de recherche de conformité est terminé et que les e-mails sont supprimés dans le cadre de la recherche de conformité.
Erreur lors de la vérification de l'état	Lorsque la vérification de l'état échoue en raison d'une exception dans le serveur Exchange.
Erreur	Lorsqu'une exception se produit dans l'activité du workflow.

Supprimer l'activité de recherche de conformité

L'activité Supprimer la recherche de conformité supprime la recherche de conformité créée à partir du serveur Exchange.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
targetId	Champ d'identificateur d'hôte cible obligatoire où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration de l'ingestion d'alerte de l'API Microsoft Graph Security

Utilisez l'intégration API de sécurité Microsoft Graph pour ingérer des alertes des fournisseurs de sécurité Microsoft Graph et créer automatiquement des incidents de sécurité.

Vue d'ensemble

Il API de sécurité Microsoft Graph s'agit d'un service intermédiaire (ou courtier) qui fournit une interface de programmation unique pour connecter plusieurs fournisseurs de sécurité (natif de Microsoft ainsi que des partenaires ServiceNow).

L'intégration API de sécurité Microsoft Graph résout ces problèmes en utilisant la pour se connecter à différentes technologies de sécurité Microsoft telles qu'Azure API de sécurité Microsoft Graph Sentinel, Microsoft Defender Advanced Threat Protection et Azure Advanced Threat Protection. Les alertes des fournisseurs de sécurité Microsoft sont ingérées et les incidents de sécurité sont automatiquement créés dans Réponse aux incidents de sécurité.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

- Détection des API de sécurité Microsoft Graph alertes qui sont candidates aux incidents de sécurité et automatiser la création d'incidents de sécurité.
- Mappage des champs d'alerte aux champs d'incident de sécurité.
- Agrégation d'alertes similaires à des incidents de sécurité ouverts existants au lieu de créer des incidents de sécurité en double.
- Prévisualisez les valeurs de champ d'alerte et validez leurs mappages dans l'incident de sécurité.
- Mise à jour automatique de l'état d'alerte pour la création et la fermeture d'incidents de sécurité.
- Configurez l'ingestion planifiée d'alertes pour créer régulièrement des incidents de sécurité.

Configurez votre instance Now Platform pour l'intégration de l'API Microsoft Graph Security

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform® instance avant d'installer l'application à partir du ServiceNow Store.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application pour garantir une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform® AND Réponse aux incidents de sécurité .	Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre Now Platform® instance.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	• Un utilisateur disposant du rôle administrateur Now Platform® (admin) installe l'application à partir de et ServiceNow Store affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Un utilisateur disposant du rôle sn_si.admin supervise les tâches suivantes dans :Now Platform® ◦ Nomme, crée et modifie les profils d'alerte. ◦ Sélectionne et mappe les champs de données d'alerte de l'API Microsoft Graph Security aux champs d'incident de sécurité. ◦ Prévisualise l'exactitude des détails de l'incident de sécurité avant de finaliser la configuration. ◦ Planifie l'ingestion d'alerte en cours. ◦ Active les mises à jour des alertes lorsqu'un Réponse aux incidents de sécurité incident est créé et fermé. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Les utilisateurs avec l'sn_si.analyst travaillent avec des incidents de sécurité. Pour plus d'informations sur les rôles et l'affectation de rôles aux utilisateurs, consultez Rôles sur le site web de la documentation produit ServiceNow .
Enregistrez votre application dans le Microsoft Azure portail.	Avant de pouvoir ingérer des alertes, vous devez configurer votre application dans le Microsoft Azure portail. Consultez Configurer le portail Microsoft Azure pour en savoir plus.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Ingestion d'événements et d'alertes pour Security Operations : Cette application nécessite :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	◦ com.glide.hub.integration.runtime => l'exécution du Centre d'intégration ServiceNow ◦ com.glide.hub.action_step.rest => Étape d'action du Centre d'intégration ServiceNow : REST **Remarque :** Les composants du concentrateur d'intégration sont installés en même temps que le module d'extension d'ingestion d'événements et d'alertes. Si ceux-ci ne sont pas installés, contactez le support client pour obtenir de l'aide. Pour plus d'informations sur l'installation des Opérations de sécurité applications principales, consultez et .

Configurer le portail Microsoft Azure

Pour récupérer les alertes de sécurité pour une application disponible dans le locataire Microsoft Azure à l'aide de , API de sécurité Microsoft Graphvous devez enregistrer l'application dans le Microsoft Azure portail et accorder l'accès en lecture et en écriture aux événements de sécurité à l'application.

Avant de commencer

Rôle requis :

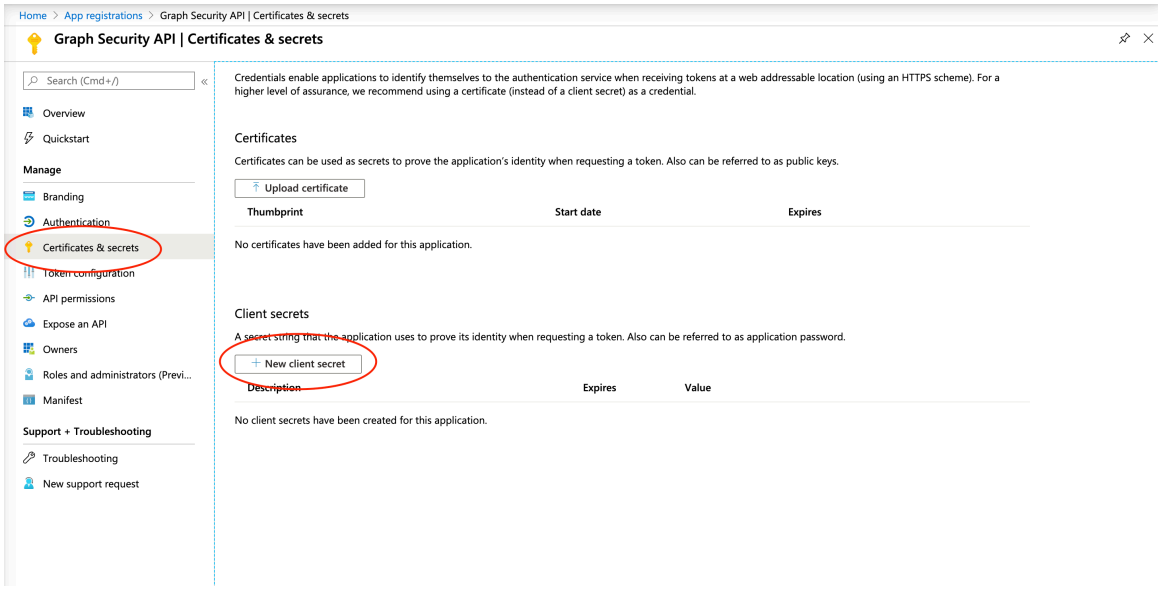
- Développeur d'application : requis pour enregistrer l'application.
- Administrateur locataire : l'administrateur Microsoft Azure locataire doit accorder les autorisations à l'application en appelant le point de terminaison de consentement de l'administrateur.

Procédure

1. Connectez-vous au Microsoft Azure portail.
2. Entrez **les inscriptions d'application** dans la zone **de recherche** .
3. Cliquez sur **Nouvelle inscription**.
4. Entrez un nom pour votre application et l'URI de redirection, par exemple http://localhost et cliquez sur **Enregistrer**.
   L'URI de redirection est utilisé lors de l'octroi du consentement administrateur pour l'application.
5. Sur la page Inscriptions des applications, sélectionnez l'application que vous avez enregistrée, par exemple Démo de sécurité graphique.
6. Sous **Gérer**, sélectionnez **Certificats et secrets**.

Traduction automatique

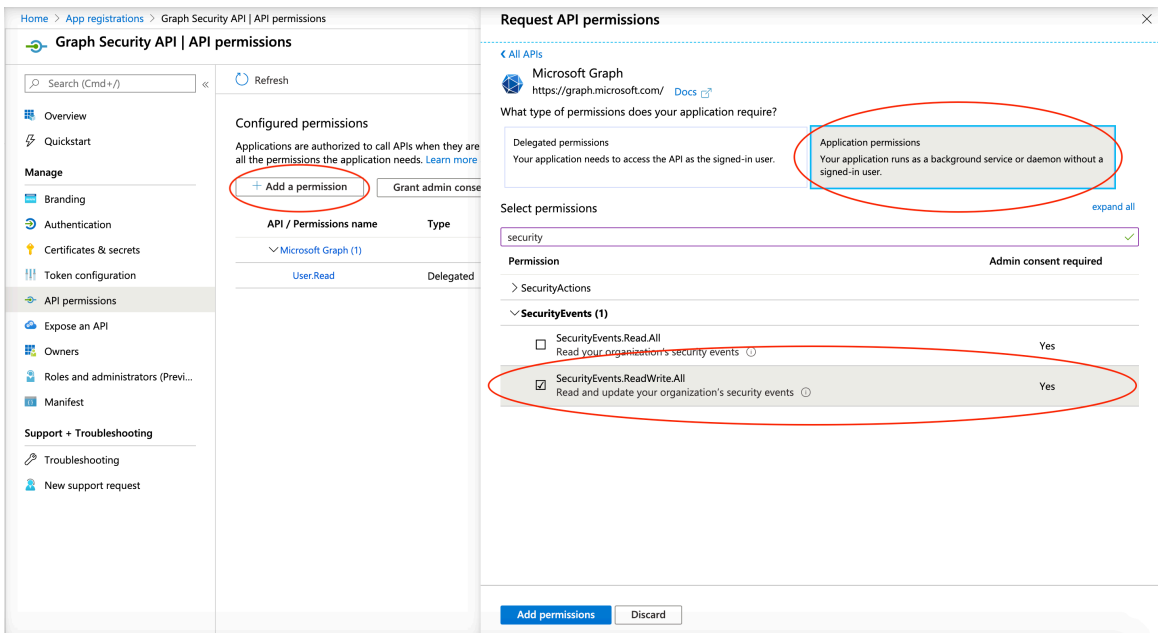
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Sélectionnez **Nouveau secret client** pour créer un secret client.
   Copiez le secret client et enregistrez-le, car il ne sera plus visible ultérieurement. Si vous avez oublié le secret client, vous pouvez générer un nouveau secret client.

   Remarque : Si vous oubliez le secret client, vous pouvez en générer un nouveau en suivant les instructions des étapes 4 et 5.

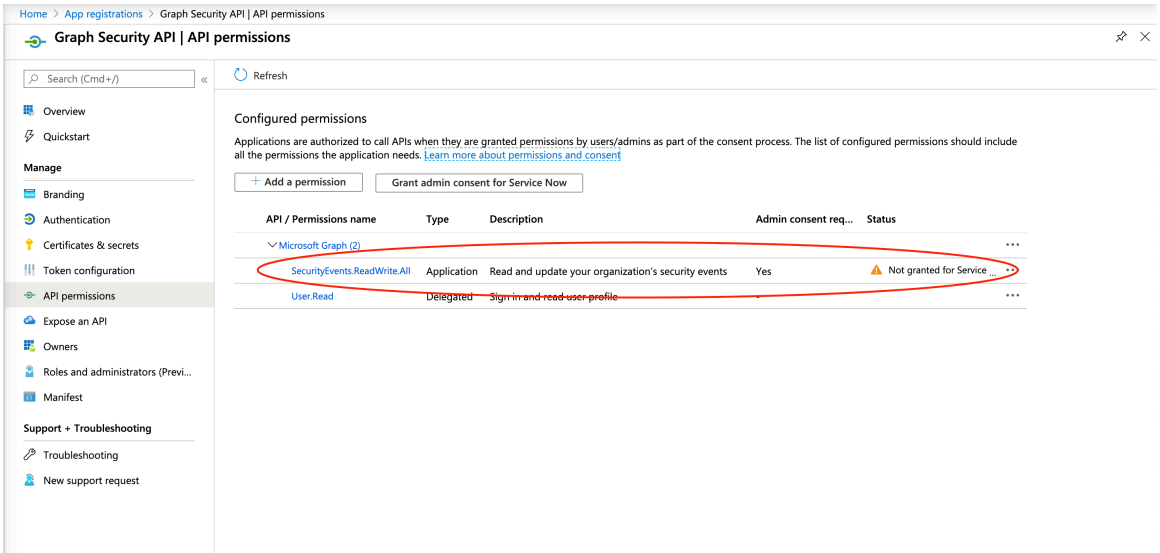
8. Cliquez sur **Afficher les autorisations API** dans la page Vue d'ensemble.
9. Ajoutez de nouvelles autorisations d'API au niveau de l'application pour les événements de sécurité SecurityEvents.ReadWrite.All.



10. Accordez le consentement de l'administrateur pour les autorisations d'API nouvellement ajoutées.
    Pour plus d'informations, consultez le modèle d'autorisation Microsoft Graph de référence des autorisations Microsoft Graph .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



11. Connectez-vous en tant qu'administrateur locataire et donnez votre consentement à l'application.
    Les étapes sont indiquées ci-dessous :

    a. Accédez à l'URL suivante : https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

    Saisissez le APPLICATION_ID de l'application que vous avez enregistrée.

12. Cliquez sur **Accepter** pour accepter les autorisations demandées par l'application créée ci-dessus.
    Vous pouvez ensuite utiliser l'application pour lire les événements de sécurité. Consultez la documentation sur l'autorisation de sécurité Microsoft Graph pour plus d'informations.

Installer et configurer l'application ServiceNow pour l'intégration de l'ingestion d'alerte de l'API Microsoft Graph Security

Avant d'exécuter l'intégration sur votre Now Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre Réponse aux incidents de sécurité correctement aux produits et Opérations de sécurité sur votre Now Platform instance.

Avant de commencer

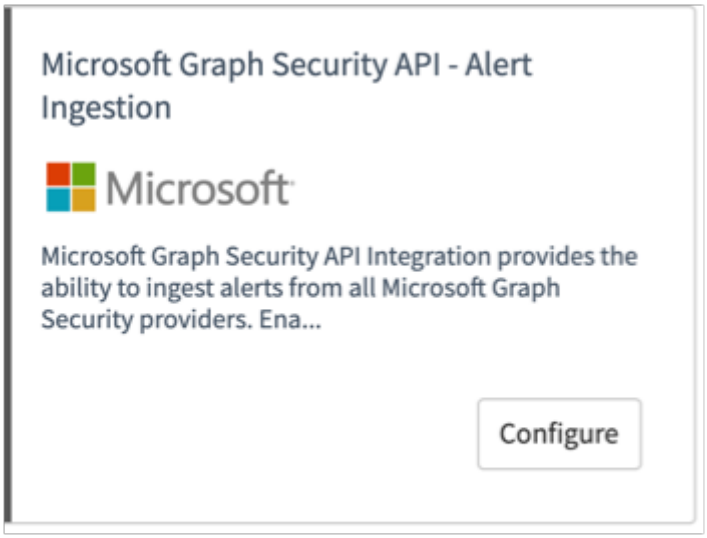
Rôle requis : sn_si.admin

Procédure

1. Si vous n'avez pas installé l'application API de sécurité Microsoft Graph à partir de ServiceNow Store pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette API Microsoft Graph Security - Ingestion d'alerte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

3. Pour configurer l'application, cliquez sur **Configurer**.
4. Renseignez les champs de la boîte de dialogue Configuration des ingestions d'alerte qui s'affiche.

Champ	Description
Nom	Nom de l'instance dans le Microsoft Azure cloud. Vous ne pouvez saisir que des valeurs alphanumériques et des traits d'union (-) dans ce champ.
ID de locataire	ID Microsoft Azure du locataire. Il s'agit de l'instance à partir de laquelle toutes les alertes du portail sont récupérées Microsoft Azure .
ID client	ID client de l'application que vous avez enregistrée dans le Microsoft Azure portail. Consultez Configurer le portail Microsoft Azure pour en savoir plus.
Secret client	Le mot de passe de votre application enregistrée.

5. Cliquez sur **Envoyer**.
   Une fois validée et soumise, chaque configuration du serveur d'ingestions d'alerte est enregistrée sous forme de vignette sur la page Intégrations de sécurité. Si vos vignettes de configuration enregistrées ne s'affichent pas sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste de choix Afficher les configurations, cliquez sur **Oui**.

Que faire ensuite

Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer un profil d'alerte.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un profil pour l'intégration d'ingestion d'alertes de l'API Microsoft Graph Security

En tant qu'utilisateur disposant du rôle sn_si.admin, vous créez un profil d'alerte dans votre Now Platform instance et déterminez quelles alertes créent des incidents de sécurité. Avant que les incidents de sécurité ne soient créés à partir d'alertes ingérées, les valeurs de champ des alertes sont affichées sur la mise en page d'un Now Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera affiché.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

L'intégration vous permet d'ingérer différents types d'alertes, telles que les tentatives d'accès non autorisé et les logiciels malveillants, par exemple. Ces alertes sont ingérées en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance. Toutes les alertes sont initialement ingérées pour un type d'alerte configuré dans un profil. Les alertes ingérées peuvent ensuite être filtrées pour spécifier quelles alertes créent des incidents de sécurité.

Par exemple, vous pouvez préférer les filtres qui créent des incidents de sécurité uniquement pour les alertes identifiées comme présentant un risque élevé. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir d'alertes ingérées, les valeurs de champ individuelles des alertes filtrées sont mappées aux champs correspondants sur une mise en page de l'incident de sécurité pour un aperçu. Toutes les alertes qui répondent aux critères de sélection de votre Microsoft Azure locataire et qui sont disponibles sur le API de sécurité Microsoft Graph sont initialement ingérées dans votre Now Platform instance.

Identifier la source du profil

Spécifiez le nom et la source du profil.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Pour créer un profil pour une alerte dans votre Now Platform instance, accédez à **Intégration de l'API Microsoft Graph Security** > **Profil de l'API Microsoft Graph Security**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs.

   Le tableau ci-dessous un exemple de formulaire rempli.

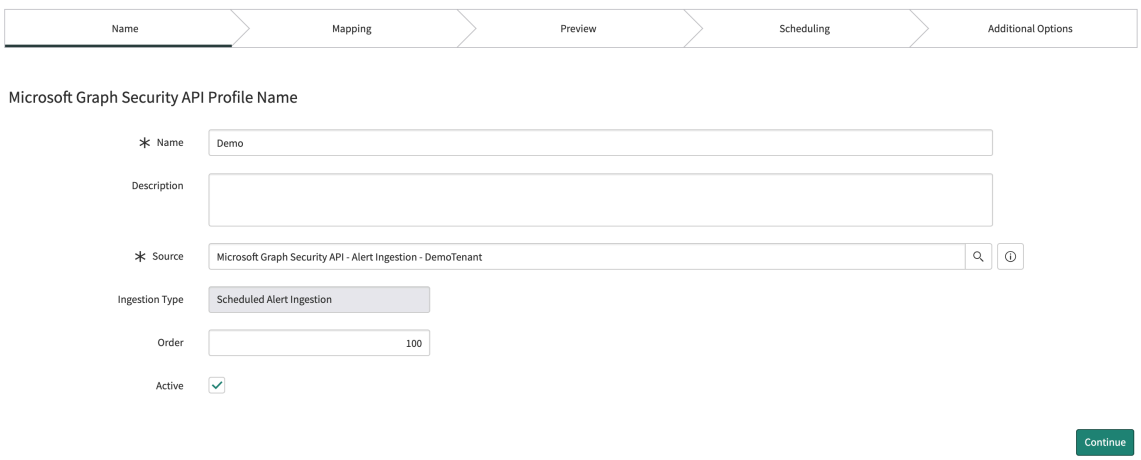
Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre Now Platform instance doivent être uniques.
Actif	La case n'est pas cochée par défaut. Si cette option est désactivée, le profil n'est pas actif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Vous devez remplir toutes les sections du profil avant de l'activer.
Source	Le Microsoft Azure locataire que vous avez configuré pour ingérer des alertes. Si vous avez plusieurs locataires configurés, sélectionnez le locataire approprié pour les types d'alertes que vous prévoyez d'ingérer pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Plus la valeur de l'ordre est faible, plus la priorité est élevée.
(Facultatif) Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

La figure suivante est un exemple de formulaire rempli.



Que faire ensuite

L'étape suivante consiste à mapper les champs d'alerte.

Mappage des champs d'alerte pour l'intégration de l'ingestion d'alerte de l'API Microsoft Graph Security

Une fois que vous avez identifié les sources pour l'ingestion d'alerte planifiée, l'étape suivante consiste à mapper les champs d'alerte individuels aux champs d'un Now Platform SIR incident de sécurité.

Pour l'étape de mappage, vous devez d'abord ingérer des échantillons d'alertes Microsoft Azure du locataire. Ensuite, vous devez vous assurer que toutes les données de champ d'alerte pertinentes sont mappées à l'emplacement approprié sur le formulaire d'incident SIR , puis visualiser l'incident SIR dans la section d'aperçu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le mappage des champs d'alerte d'exemple implique les éléments suivants :

- Ingérer un échantillon d'alertes de l'API Microsoft Graph Security
- Mappage des alertes aux champs de réponse aux incidents de sécurité

Ingérer un échantillon d'alertes de l'API Microsoft Graph Security

Ingérer des échantillons d'alertes de votre Microsoft Azure locataire.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

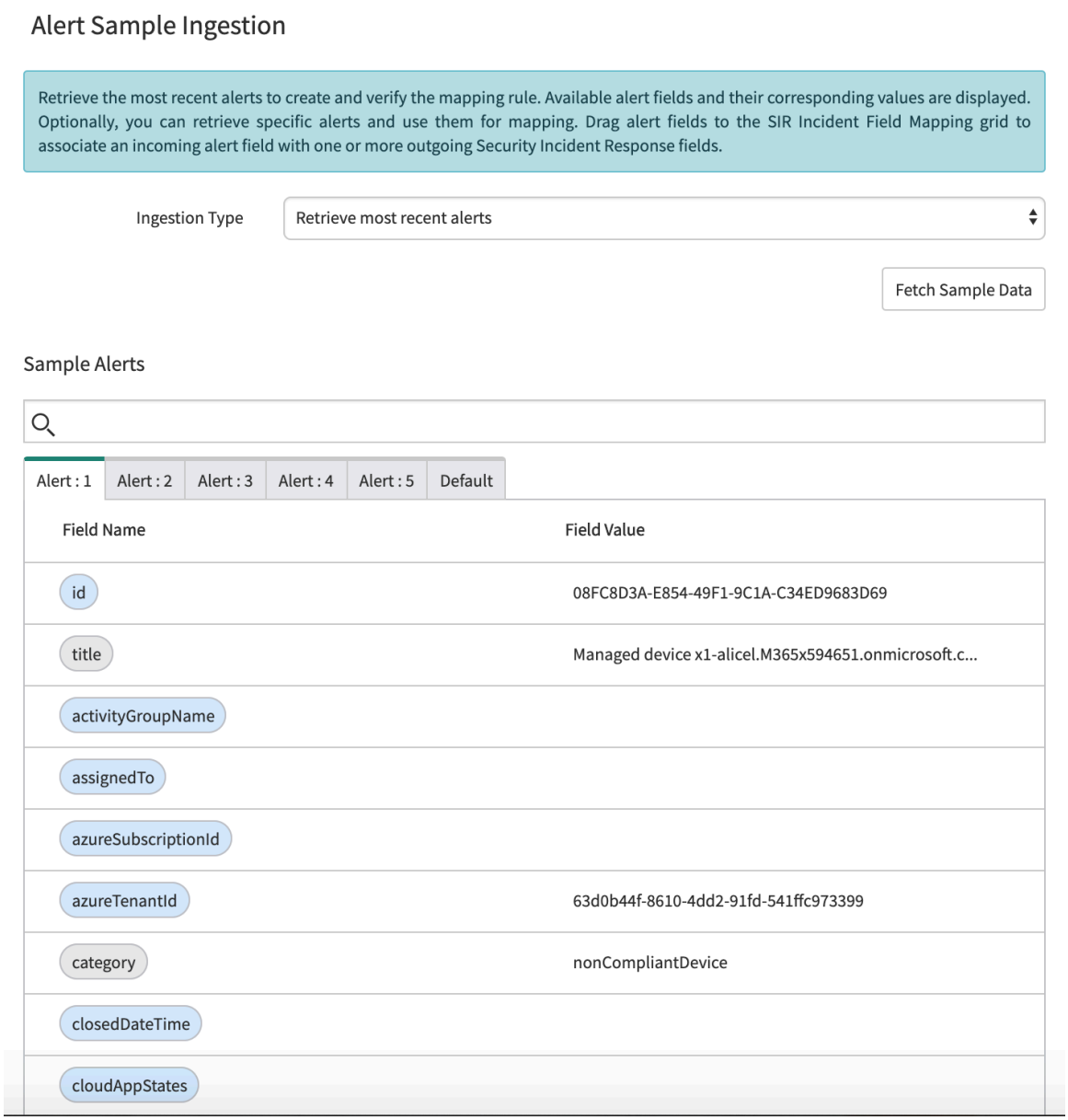
1. Vous pouvez soit extraire les 5 alertes d'échantillon les plus récentes, soit fournir les ID d'alerte uniques pour les alertes spécifiques que vous souhaitez utiliser pour votre expérience de mappage.
   Dans la liste de choix **Préférences d'ingestion** , sélectionnez l'une des options suivantes :
   - Récupérer les alertes les plus récentes : les 5 alertes les plus récentes sont récupérées.
   - Sélectionner les alertes en fonction de l'ID d'alerte : spécifiez l'ID d'alerte pour les alertes à récupérer. Vous pouvez spécifier un maximum de 5 ID d'alertes séparés par des virgules.
2. Cliquez sur **Récupérer les données d'échantillon** pour extraire les dernières données d'alerte d'échantillon Microsoft Azure du locataire.
   L'extraction des échantillons d'alertes peut prendre quelques instants.

   Les valeurs du champ d'alerte d'échantillon sont renseignées sur le côté gauche du formulaire lorsque des alertes d'échantillon sont ingérées par le profil. Il s'agit des alertes

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que vous mappez aux SIR champs d'incident de sécurité. Les champs et les valeurs d'alerte, résultats sont affichés sous forme d'onglets individuels.



Que faire ensuite

Une fois les exemples de données extraits, l'étape suivante consiste à mapper les champs d'alerte à l'incident de sécurité.

Mappage des alertes aux champs de réponse aux incidents de sécurité

Mappez les champs d'alerte individuels des alertes déclenchées aux champs d'un Now Platform incident de sécurité.

Mappage de champs d'alertes

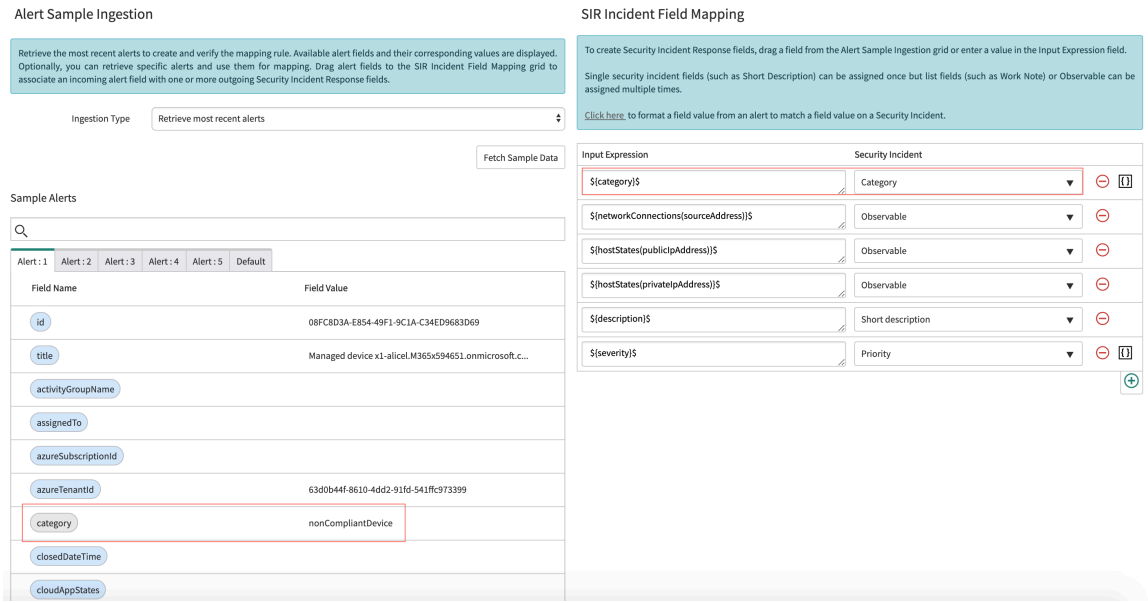
En tant qu'utilisateur disposant du rôle sn_si.admin, utilisez les champs de la section Échantillons d'alertes sur la gauche et mappez-les aux champs d'incident de sécurité dans la colonne Mappage des champs d'incidents SIR du panneau de droite. Modifiez la configuration du mappage en faisant glisser les champs d'alerte depuis le côté gauche et en les déposant dans la section de mappage des SIR incidents située à droite. Le mappage sur la droite associe le champ d'alerte entrante à un champ d'incident de sécurité sortant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Une fois les exemples de données extraits, l'étape suivante consiste à mapper les champs d'alerte à l'incident de sécurité. Pour mapper une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez longuement sur un nom de champ bleu sur le côté gauche du formulaire.
2. Faites glisser le nom du champ, par `exemple catégorie`, et déposez-le sur un champ de la colonne Expression d'entrée en regard d'un nom de champ dans la colonne Incident de sécurité.

   La valeur du champ est affichée dans la colonne Expression d'entrée. Dans l'image suivante, la `catégorie` est mappée au champ `Catégorie` de l'incident de sécurité.



Toutefois, vous pouvez faire correspondre n'importe quelle valeur du côté gauche à un champ de droite. Vérifiez que la valeur est correctement mappée sur l'incident de sécurité pendant l'étape de prévisualisation.

Pour vous assurer qu'aucun champ d'alerte n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par couleur. Le codage couleur des champs d'alerte vous aide à suivre les valeurs d'alerte que vous avez déjà mappées à mesure qu'elles sont grisées tandis que tous les champs non mappés restants apparaissent en bleu. Cela vous aide à mieux visualiser quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si des informations d'alerte importantes restantes restent non mappées.

Les champs bleu clair sur la gauche indiquent qu'un champ d'alerte n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ d'alerte entrante à plusieurs champs sur un incident de sécurité. Un champ gris indique qu'un champ a été sélectionné et mappé à un champ sur l'incident de sécurité. Ce code couleur vous aide à suivre le mappage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

a. Pour saisir manuellement une valeur dans le champ expression d'entrée, saisissez-la au format ${fieldname}$. Le champ d'alerte est mappé au champ d'incident de sécurité.

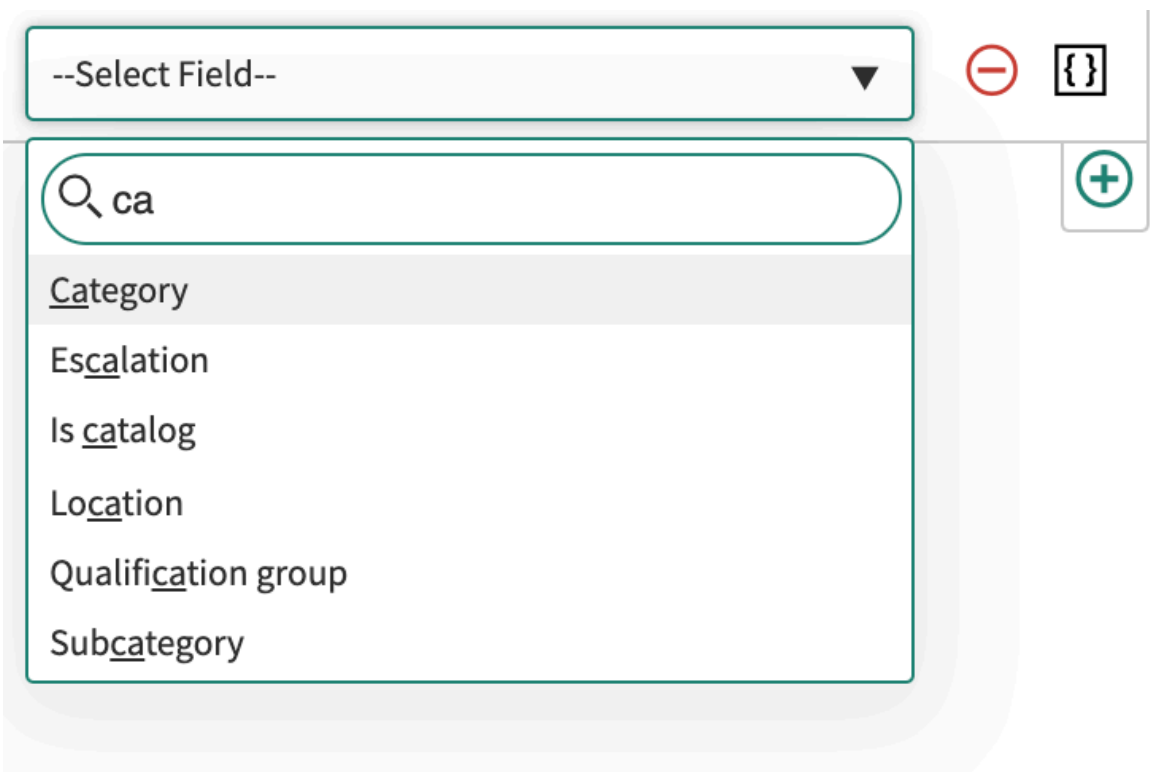
b. Vous ne pouvez pas mapper les alertes ingérées aux MITRE-ATT&CK champs Cadre de travail de la section de mappage des incidents de sécurité. Si vous mappez toujours les champs, les informations ne seront pas disponibles dans le cadre de la section de cadre de travail de la MITRE-ATT&CK carte MITRE-ATT&CK du formulaire d'incident de sécurité. Pour associer les MITRE-ATT&CK techniques, utilisez la fonctionnalité d'extraction automatique disponible dans le MITRE-ATT&CKRenseignements sur les menaces cadre du cadre de travail du module.

3. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit.

a. À droite du formulaire, dans la section Mappage des champs d'incidents SIR , en bas de la grille, cliquez sur l'icône plus (+). Un nouveau champ s'affiche.

b. Dans la colonne Incident de sécurité, développez la liste de choix qui s'affiche, puis sélectionnez un champ.

Dans la liste de choix développée pour le nouveau champ, certains champs sont grisés. Dans la figure suivante, la catégorie a un arrière-plan gris, car elle a été mappée dans l'incident de sécurité. À l'instar du code couleur pour les champs d'alerte sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident déjà mappés SIR .



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Étant donné que plusieurs observables peuvent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité dispose d'une liste de choix dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affiché dans la liste de choix, le champ n'est pas renseigné sur l'incident de sécurité.

c. Vous pouvez également saisir une valeur dans le champ Rechercher pour la nouvelle ligne.

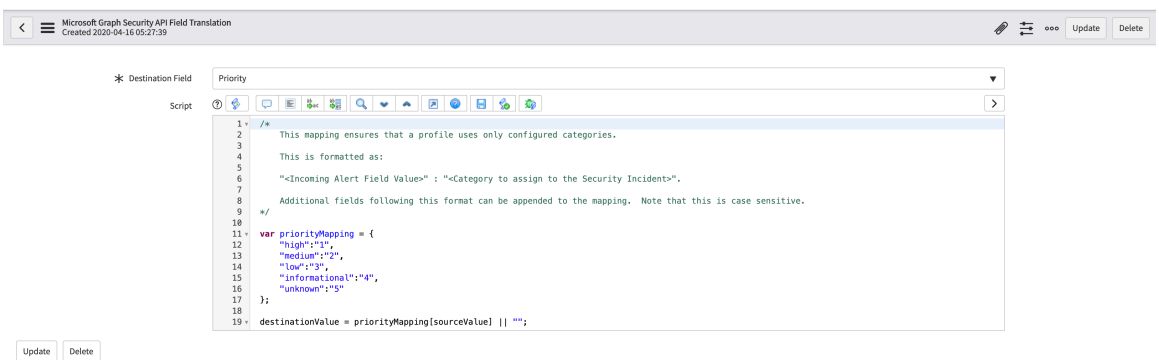
d. Sur le côté gauche du formulaire, cliquez avec le bouton gauche de la souris pour sélectionner l'ID d'alerte souhaité dans le champ expression d'entrée. Grâce à la fonction glisser-déposer, mappez-le à côté de votre nouveau champ.

4. Poursuivez le mappage en ajoutant ou en supprimant des valeurs de champ au mappage.
5. Une fois que vous avez terminé les étapes de mappage de champs précédentes, vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir les critères supplémentaires qu'une alerte entrante doit satisfaire pour créer un incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

Formater la traduction du champ

Dans certains cas, les valeurs de champ d'alerte dans API de sécurité Microsoft Graph peuvent ne pas se traduire directement dans les champs de l'incident de sécurité SIR. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez mettre en forme des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident de sécurité SIR à l'aide de la fonctionnalité Formater la traduction de champ.

Pour utiliser l'éditeur de script, cliquez sur l'icône {}. L'éditeur de script s'affiche.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions de génération d'incidents

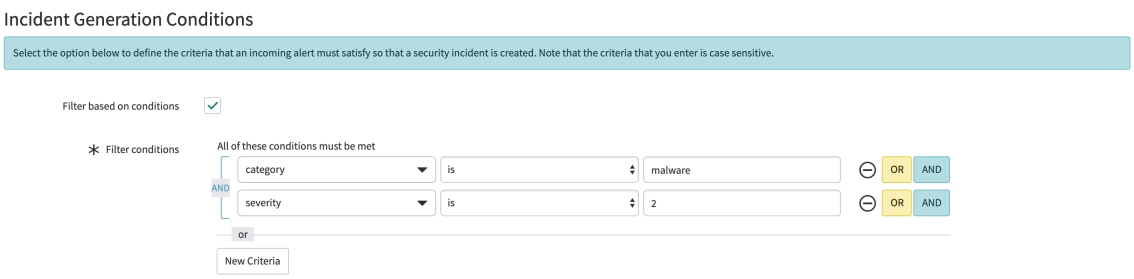
Une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de spécifier quelles alertes doivent créer des incidents de sécurité par rapport à quelles alertes doivent être filtrées (par exemple, les alertes de faible priorité). Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir les critères supplémentaires qu'une alerte entrante doit satisfaire pour créer un incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

1. Faites défiler la page du formulaire jusqu'à la section Conditions de génération d'incidents et sélectionnez l'option Filtrer en fonction des conditions. Le Créateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

   Les options des listes de choix pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Ingestion d'échantillons d'alerte pour l'alerte que vous avez ingérée. Ces champs sont dynamiques et changent en fonction de l'alerte que vous ingérez. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'alerte. Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférez peut-être revenir à votre locataire Microsoft Azure et examiner vos alertes pour les mots clés.

2. À l'aide des listes de choix et des champs du générateur de conditions, définissez des filtres pour la première ligne.
3. Pour ajouter d'autres conditions, à droite des champs, cliquez sur **ET** ou **OU**.
   - Si **ET**est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU**est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. Dans la deuxième ligne, définissez une deuxième condition de filtre

   L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création des incidents de sécurité.



   Vous avez défini les conditions de déclenchement de sorte que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

   Ce type de filtrage vous aide à isoler les alertes de sécurité et limite le nombre d'incidents de sécurité que vous créez. Si des critères de filtrage supplémentaires sont définis, seules les alertes requises sont ingérées sans avoir à modifier la requête ou la configuration des alertes déclenchées.

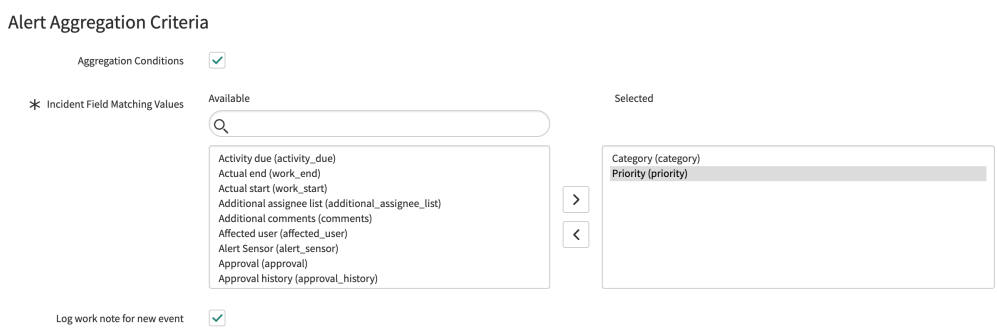
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Critères d'agrégation d'alertes pour gérer des alertes similaires et empêcher les incidents en double

Définissez des critères d'agrégation d'alertes supplémentaires qui regroupent une alerte entrante en un incident de sécurité existant SIR au lieu de créer des incidents similaires potentiellement dupliqués. En utilisant des critères de valeur de correspondance de champ pour chaque profil, cette aptitude d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données d'alerte connexes sur un seul incident de sécurité. Pour définir les critères, procédez comme suit :

1. Faites défiler l'écran jusqu'à la section Critères d'agrégation d'alertes du formulaire et sélectionnez l'option Conditions d'agrégation. Les colonnes Incident Field Matching Values (Valeurs correspondantes du champ d'incident) s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés dans l'incident SIR de sécurité.
2. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre Now Platform et déplacez-les vers la liste Sélectionné. Toutes les valeurs de champ que vous sélectionnez doivent correspondre pour ajouter cette alerte entrante à un incident de sécurité existant. Cela inclut les champs, tels que les observables et les éléments de configuration, qui peuvent avoir plusieurs valeurs de champ d'alerte mappées. Toutes les valeurs doivent correspondre. Si seul un sous-ensemble de valeurs correspond, les conditions d'agrégation d'alertes ne seront pas remplies et un nouvel incident de sécurité sera créé. Voir la capture d'écran ci-dessous pour le mappage de champs à valeurs multiples.



Si une nouvelle alerte correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation de l'étape de mappage, l'alerte est automatiquement ajoutée à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher toutes les alertes agrégées ajoutées dans une liste connexe d'un incident de sécurité. Toutes les alertes agrégées sur un incident de sécurité sont affichées dans la liste connexe Alertes Microsoft Graph agrégées. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi des alertes sont ajoutées aux incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de l'enregistrement sous Liens connexes et cliquez sur le lien **Afficher toutes les listes connexes** .

3. (Facultatif) Pour consigner une note de travail pour une nouvelle alerte récemment ajoutée à l'incident de sécurité, cochez la case pour activer cette option. La note de travail consigne qu'une nouvelle alerte a été ajoutée, ainsi qu'un lien vers les détails de l'alerte et tous les autres détails qui peuvent avoir été ajoutés au champ Note de travail dans votre section de mappage.

Vous avez mappé avec succès les valeurs d'une alerte aux champs d'un SIR incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

création d'incidents de sécurité avec des critères de filtrage. Vous avez également ajouté des alertes ou des événements aux incidents de sécurité existants SIR .

4. Cliquez sur **Continuer** pour poursuivre la configuration du profil. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un incident de sécurité SIR

Prévisualiser l'incident de sécurité pour l'intégration de l'API Microsoft Graph Security

Une fois que vous avez terminé l'étape de mappage, prévisualisez les valeurs que vous avez mappées dans un Now Platform SIR incident de sécurité. Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs d'alerte que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer

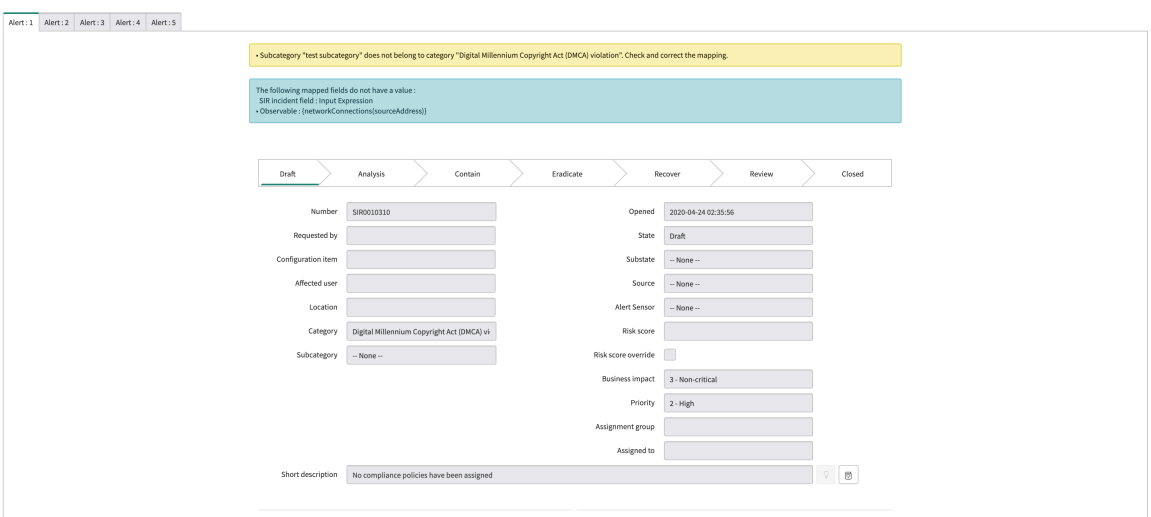
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

En tant qu'utilisateur disposant du rôle sn_si.admin, prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs contenant des erreurs ou pour renseigner les données manquantes. Si l'aperçu n'est pas terminé, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de SIR sécurité ne sont pas enregistrés en tant qu'incidents réels dans le Réponse aux incidents de sécurité produit.

Procédure

1. Si l'aperçu de l'incident de sécurité n'est pas affiché, cliquez sur **Aperçu** dans la barre de progression.
   Toutes les alertes ingérées et les mappages de champs définis dans la page Mappage s'affichent.
2. Cliquez sur un ID d'alerte pour afficher un aperçu de l'incident de sécurité.
   Il s'agit d'une vue en lecture seule et un enregistrement de cet incident de sécurité n'est pas enregistré.
3. Examinez le mappage des champs des valeurs d'alerte sur l'incident de sécurité.



L'image précédente est un exemple d'aperçu avec une erreur de mappage des échantillons qui ont été ingérés.

4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

Que faire ensuite
Si aucun message d'erreur n'est affiché et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à définir le calendrier.

Définir le calendrier pour l'intégration de l'API Microsoft Graph Security

Vérifiez les paramètres par défaut pour la récupération d'alerte ou modifiez la planification selon vos besoins. Cette étape vous permet de filtrer votre récupération d'alerte en fonction d'une plage de dates.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Vous choisissez également la fréquence à laquelle vous procéderez à une interrogation pour les alertes futures qui correspondent à la configuration du profil d'alerte. Pour les profils d'ingestion d'alertes automatisées, avant d'activer le profil, vous vérifiez et modifiez la planification et la récupération des alertes. Cette étape est nécessaire pour les profils d'alerte planifiée.

En tant qu'utilisateur disposant du rôle sn_si.admin, vous configurez ces intervalles d'interrogation pour chaque profil. Les performances de l'intégration de l'ingestion d'alerte API de sécurité Microsoft Graph sont impactées par les différents intervalles d'interrogation. Lors de la planification, vous préférerez peut-être équilibrer la charge du système par rapport à l'urgence de l'incident. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférerez peut-être modifier ce paramètre en fonction de l'urgence de l'incident et de la charge prévue sur votre système.

Procédure
1. Si la page Planification de la barre de progression n'est pas affichée, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment Microsoft Azure et quand les alertes sont extraites du locataire.

Option	Description
Ingestion d'alerte en cours sélectionnée	En fonction du paramètre par défaut, l'instance Now Platform extrait du locataire pour de Microsoft Azure nouvelles alertes toutes les cinq minutes. Les incidents de sécurité sont créés si des alertes déclenchées sont détectées et si les critères de filtrage de génération d'incident sont respectés. Pour équilibrer l'ingestion d'alertes par rapport à la charge du serveur et pour extraire les données les plus récentes, cinq minutes est le paramètre que vous préférez. Toutefois, cette valeur peut être modifiée si nécessaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
◦ Ingestion d'alerte en cours sélectionnée ◦ Définir le délai d'ingestion de l'alerte initiale	Délai d'ingestion initial Si vous souhaitez planifier l'ingestion initiale à une heure précise, procédez comme suit : ◦ Sélectionnez les champs Intégration d'alerte en cours et Définir la durée d'ingestion d'alerte initiale. ◦ Spécifiez l'heure dans le champ Entrer le délai d'ingestion de l'alerte initiale. L'ingestion initiale aura lieu à l'heure spécifiée ici. Les ingestions suivantes seront basées sur le calendrier défini dans le champ Incrémentation de l'interrogation (minutes). Par exemple, pour la planification, si vous avez une tâche d'alerte quotidienne qui s'exécute une fois par jour à 4 h (heure locale), vous pouvez configurer le profil d'alerte correspondant dans votre instance Now Platform pour qu'il s'exécute à 4 h 05 (heure locale) afin de capturer immédiatement l'alerte et créer un incident de sécurité. Entrez 04 05 00 dans le champ Ingestion d'alerte initiale. Dans le champ Incrémentation (minutes), saisissez 1 440 (24 heures) pour planifier la prochaine ingestion d'alerte pendant 24 heures à compter de l'ingestion d'alerte initiale. L'heure d'ingestion d'alerte initiale et l'heure d'ingestion d'alerte suivante sont affichées dans les champs. Pour configurer les paramètres de cet exemple, procédez comme suit : ◦ Sélectionnez l'option **Ingestion d'alerte en cours** . ◦ Dans le champ Incrémentation de l'interrogation (minutes), saisissez 1 440 (24 heures). ◦ Cliquez sur l'option **Définir le délai d'ingestion de l'alerte initiale** pour activer la modification des champs Délai d'ingestion de l'alerte initiale et Délai d'ingestion de l'alerte suivante (estimée). ◦ Dans le champ Délai d'ingestion de l'alerte initiale, saisissez 04 05 00. Le champ Heure d'ingestion (estimée) de la prochaine alerte s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Champ de récupération unique sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhaitez effectuer une extraction unique pour ingérer des alertes historiques. Lorsque ce paramètre est configuré, un profil est utilisé une fois pour récupérer les alertes des événements historiques basés sur une plage de dates. À droite du champ Depuis date, cliquez sur l'icône Calendrier. Dans le calendrier qui s'affiche, sélectionnez la date à laquelle vous souhaitez commencer à extraire les alertes. À partir de la valeur Date de début, les alertes sont récupérées jusqu'à la date actuelle. Notez que vous pouvez remonter jusqu'à sept jours en arrière à partir de la date actuelle. Cette fonctionnalité n'est pas destinée à récupérer des quantités significatives d'alertes historiques, mais plutôt une quantité minimale d'alertes en cours d'utilisation au moment de l'activation du profil. Une fois les alertes extraites, ce paramètre ne récupérera plus d'alertes pour ce profil à partir de la date actuelle. Ce paramètre remplit l'incident de sécurité avec toutes les alertes trouvées pour la plage que vous saisissez.

3. Cliquez sur **Continuer** pour accéder à la page Options supplémentaires.

Automatiser les mises à jour et la fermeture des alertes en fonction de l'état de l'incident SIR

L'intégration API de sécurité Microsoft Graph de l'ingestion d'alerte dispose d'une interface bidirectionnelle qui permet aux alertes de créer des incidents de sécurité et de mettre à jour les alertes une fois l'incident de sécurité créé et/ou fermé avec les détails pertinents de l'incident tels que SIR le numéro d'incident, le groupe d'affectation, SIR l'URL de l'incident, entre autres. T

Avant de commencer

Rôle requis : sn_si.admin

Remarque : Les statuts des alertes initiales et de fermeture ne sont mis à jour que si cette fonctionnalité est prise en charge par le fournisseur de service. Pour en savoir plus, consultez la documentation et celle API de sécurité Microsoft Graph du fournisseur de sécurité.

Procédure

1. Si la page Options supplémentaires de la barre de progression n'est pas affichée, sélectionnez **Options supplémentaires**.
2. Suivez les instructions ci-dessous pour terminer la configuration de mise à jour des alertes lors de la création de l'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
Mettre à jour les alertes lors de la création de l'incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour l'état de l'alerte et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir de l'alerte. Cela peut se produire à la fois pour les alertes initiales qui créent l'incident de sécurité et pour les alertes agrégées.
Mise à jour de l'état de l'alerte initiale	Sélectionnez un état d'alerte initial dans la liste. Cet état sera défini pour toutes les alertes lors de la création d'un incident de sécurité pour une alerte ingérée. Cela inclut les alertes qui créent de nouveaux incidents et les alertes qui sont ingérées et agrégées à un incident ouvert existant. **Remarque :** En fonction de l'état de l'alerte sélectionné ici, l'état de l'alerte utilisé par les fournisseurs de sécurité sera mis à jour en conséquence.
Commentaires initiaux envoyés à l'alerte	En fonction de l'étape que vous avez sélectionnée, des commentaires par défaut s'affichent. Vous pouvez modifier le texte par défaut et utiliser le format ${field name}$ pour ajouter ou modifier les champs disponibles dans le formulaire d'incident de sécurité.
Fermer les alertes lors de la fermeture de l'incident SIR	Sélectionnez cette option si vous souhaitez utiliser l'option de fermeture automatique des alertes. Cela peut se produire à la fois pour les alertes initiales qui créent l'incident de sécurité et pour les alertes agrégées. L'état de l'alerte est mis à jour dans le fournisseur de sécurité avec les commentaires d'état et de fermeture après SIR la fermeture de l'incident dans le Now Platform.
Mise à jour de l'état de l'alerte de fermeture	Sélectionnez un état d'alerte dans la liste. Sélectionnez la valeur d'état à définir pour toutes les alertes lorsqu'un incident de sécurité est fermé pour une alerte ingérée.
Commentaires de fermeture renvoyés à l'alerte	Les commentaires de fermeture par défaut sont affichés ici. Vous pouvez modifier le texte par défaut et utiliser le format ${field name}$ pour ajouter ou modifier des champs disponibles dans le formulaire d'incident de sécurité.

3. Cliquez sur **Terminer** pour terminer la configuration et déplacer le profil vers l'état **En attente** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Activez ce profil pour extraire des alertes du Microsoft Azure locataire en fonction de votre planification. Un maximum de 1 000 incidents de sécurité peut être créé dans un délai de 24 heures.

Paramètres de configuration de l'intégration de l'API Microsoft Graph Security

Utilisez cette option pour modifier les propriétés système par défaut de l'intégration d'ingestion API de sécurité Microsoft Graph .

Avant de commencer

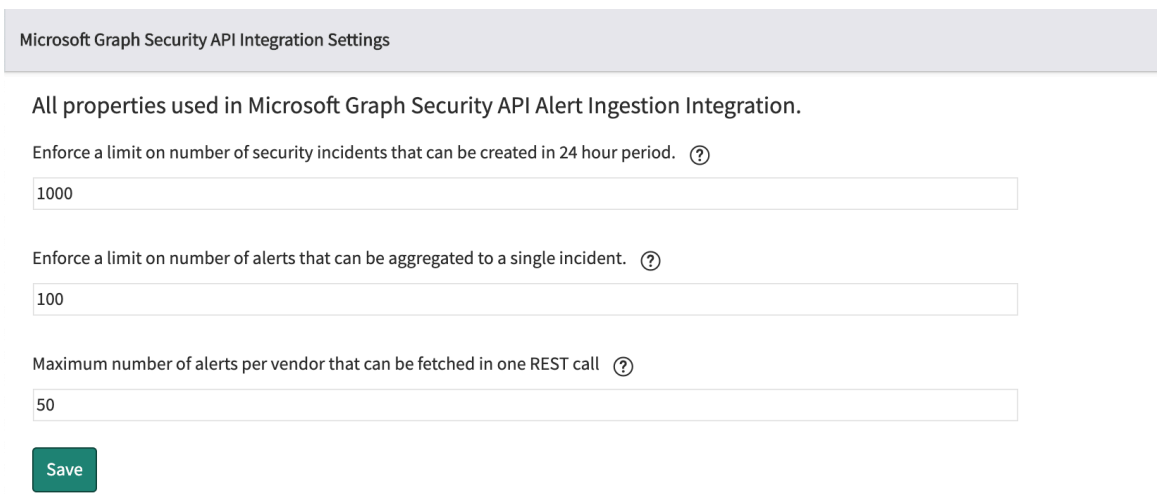
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Modifiez les propriétés de configuration par défaut pour limiter le nombre d'incidents de sécurité qui peuvent être créés au cours d'une période de 24 heures ou le nombre d'alertes qui peuvent être regroupées dans un incident de sécurité.

Pour modifier les propriétés système, connectez-vous en tant qu'utilisateur ayant le rôle *sn_si.admin* et accédez à **Intégration de l'API Microsoft Graph Security** > **Paramètres de l'API de sécurité Microsoft Graph**.

Les paramètres de configuration par défaut s'affichent. Vous pouvez modifier ces paramètres si nécessaire.



Tous les paramètres d'intégration modifiés seront appliqués lors du prochain intervalle d'interrogation, tel que défini dans le profil.

Formulaire de réponse aux incidents de sécurité après l'ingestion d'alerte

Une fois qu'une API de sécurité Microsoft Graph alerte a été ingérée, un incident de sécurité est créé et les mises à jour correspondantes sont apportées à l'enregistrement d'incident de sécurité.

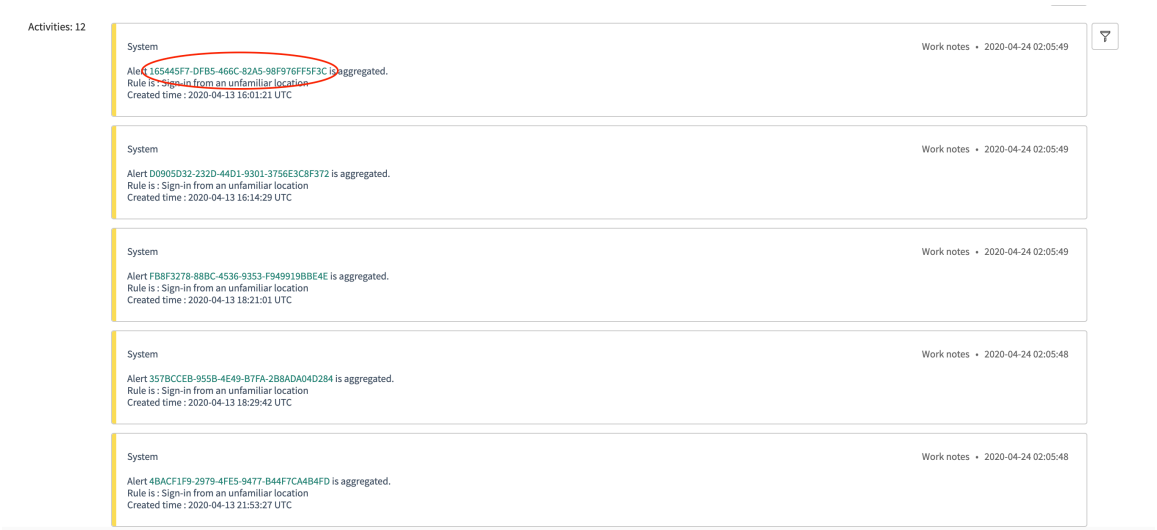
Notes de travail

Si vous aviez sélectionné l'option **Consigner la note de travail pour la nouvelle alerte** dans les critères d'agrégation des alertes, comme décrit dans , une note de Mappage des alertes

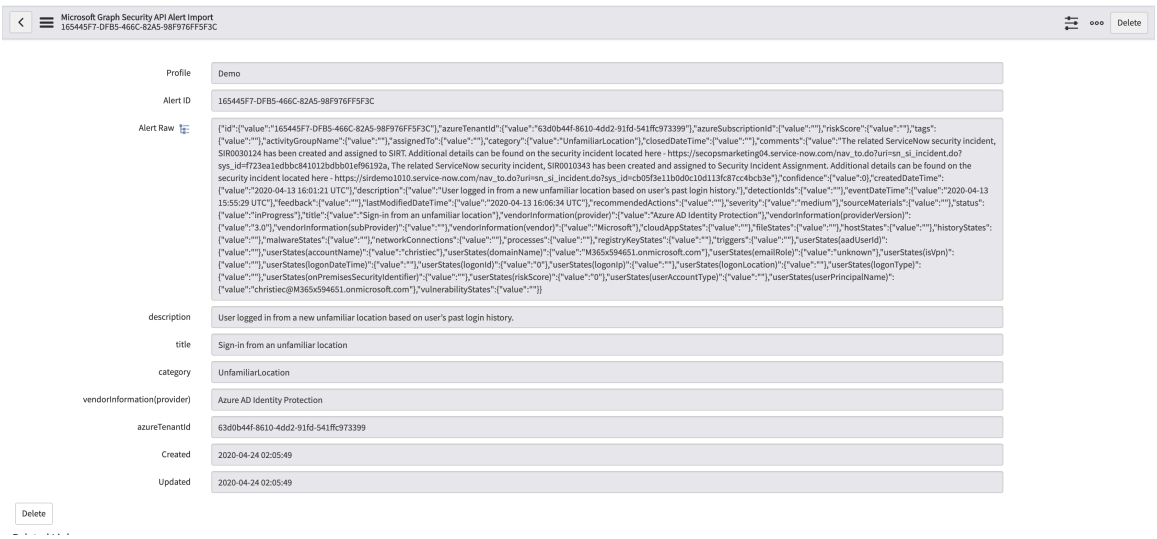
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

aux champs de réponse aux incidents de sécuritétravail est publiée lorsque les alertes sont regroupées.

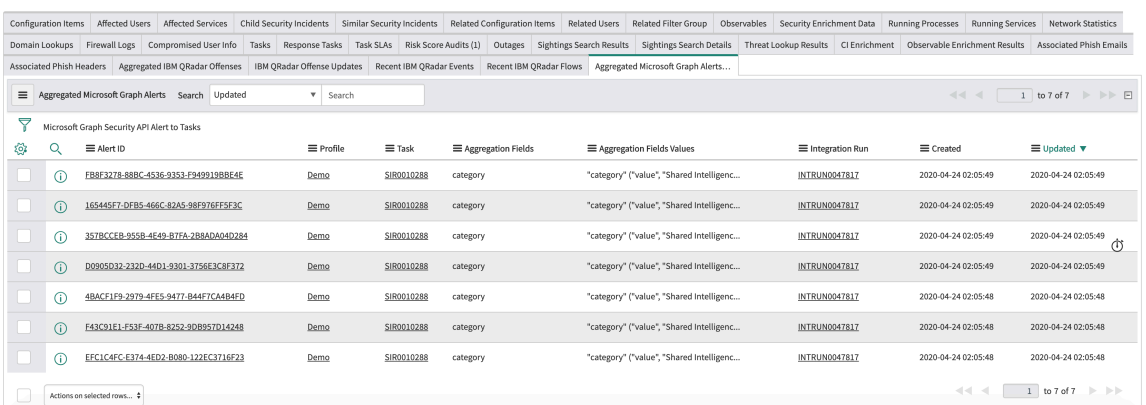


Cliquez sur le lien d'alerte pour accéder à l'enregistrement d'importation d'alerte interne qui contient des données d'alerte brutes.



Alertes agrégées

Cliquer sur **Listes connexes** > **Alertes de sécurité Microsoft Graph agrégées** pour afficher les alertes agrégées à l'incident de sécurité.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Créer un incident de sécurité** : sélectionnez une alerte dans la liste, cliquez sur le menu **Actions** , puis sur **Créer un incident de sécurité**. Cette option crée un nouvel incident de sécurité pour l'alerte et cette alerte est désagrégée de l'incident de sécurité parent.
- **Supprimer l'enregistrement d'alerte** : sélectionnez une alerte dans la liste, cliquez sur le menu **Actions** , puis sur **Supprimer**. Cette option supprime l'enregistrement d'alerte.

Facultatif : copiez un profil d'API Microsoft Graph Security

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils pour gagner du temps.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

En tant qu'utilisateur disposant du rôle sn_si.admin, si vous copiez un profil, le nom du profil est d'abord modifié pour éviter les profils en double. En outre, le profil copié est désactivé (faux) afin qu'il ne soit pas activé accidentellement avant la fin de la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure

1. Accédez à la **Tout** > **Intégration de l'API Microsoft Graph Security** > **Profil de l'API Microsoft Graph Security**.
2. Dans la API de sécurité Microsoft Graph liste Profils qui s'affiche, sélectionnez un profil que vous souhaitez copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier**.
   Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (`vrai`), la copie est désactivée à ce stade (`faux`). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.

   Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. Notez que l'état de la colonne **Actif** est défini sur faux, car le profil doit être activé.

Que faire ensuite

Vous êtes invité à activer le nouveau profil une fois que vous avez terminé les étapes de configuration.

Séparation de domaine et API de sécurité Microsoft Graph ingestion d'alerte

L'application Séparation de domaine est prise en charge. L'intégration API de sécurité Microsoft Graph ingère les alertes des fournisseurs de sécurité Microsoft Graph et crée automatiquement des incidents de sécurité. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : basique

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

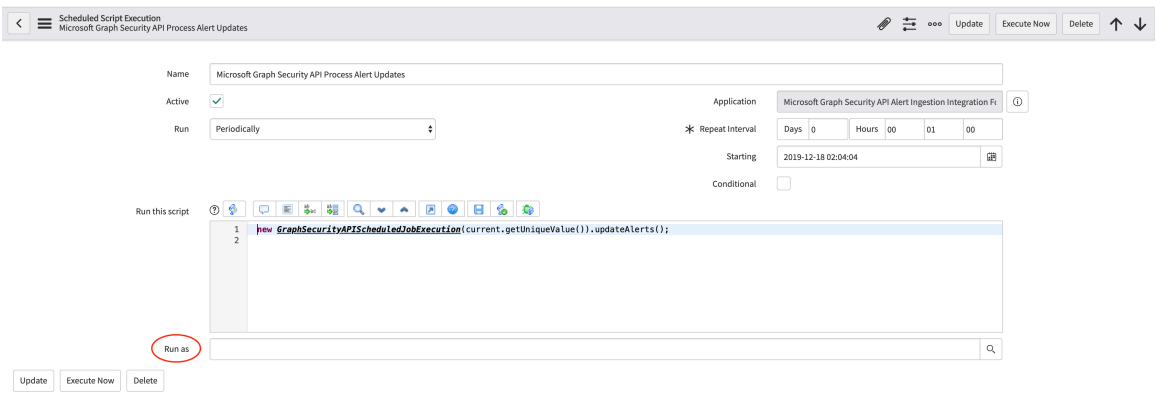
- Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de service de l'application.
- L'application prend en charge Séparation de domaine lors de l'exécution. Séparation de domaine inclut la séparation à partir de l'interface utilisateur, des clés de cache, du reporting, des déploiements et des agrégations.
- Le propriétaire de l'instance doit configurer l'application de sorte qu'elle fonctionne sur plusieurs locataires.

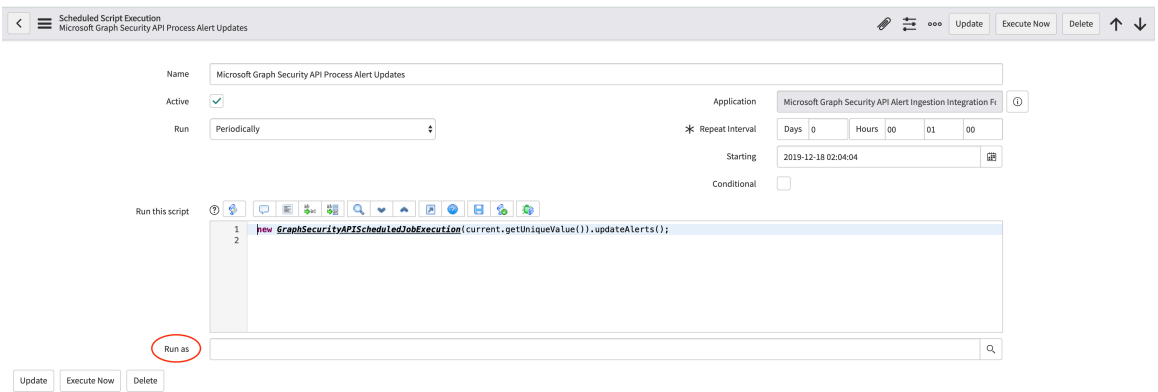
Exemple de cas d'utilisation : lorsqu'un fournisseur de service (SP) utilise la messagerie instantanée pour répondre au message d'un locataire-client, le client doit pouvoir afficher la réponse du SP.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Comment fonctionne Séparation de domaine dans API de sécurité Microsoft Graph

Pour réaliser Séparation de domaine, répliquez les API de sécurité Microsoft Graph travaux planifiés Processus de profil et SIR Alerte de processus Mises à jour et modifiez **l'option Exécuter en tant qu'utilisateurs** . Par défaut, ce sont les utilisateurs système qui exécutent ces travaux planifiés. Modifiez **l'exécution en tant qu'utilisateur** ayant le rôle sn_si.admin dans le domaine respectif et exécutez la tâche planifiée.





Information associée

Séparation de domaine pour les fournisseurs de services

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation de Flow Designer et d'Integration Hub dans l'intégration de l'API Microsoft Graph Security

À l'aide des fonctionnalités de Concepteur de flux et de concentrateur d'intégration, plusieurs flux secondaires et actions ont été créés dans le cadre de l'intégration API de sécurité Microsoft Graph .

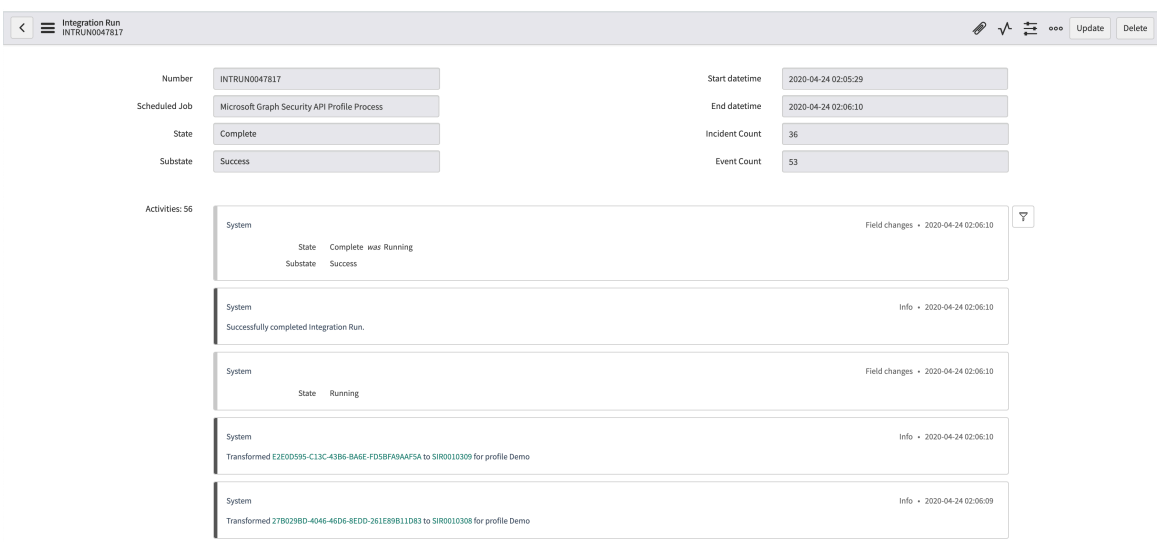
Les flux secondaires suivants sont disponibles :

- API de sécurité Microsoft Graph Validation de la configuration : elle est utilisée dans la vignette de configuration pour valider les informations d'identification lors de la configuration initiale.
- Appel API de sécurité Microsoft GraphREST : utilisé pour toutes les interactions avec l'API de sécurité Microsoft Graph à l'aide d'appels REST.
- Récupérer des échantillons d'alertes : cette option est utilisée dans la section Mappage de la configuration du profil pour extraire des exemples de données. Ce flux secondaire est déclenché de façon asynchrone.

Dépanner l'intégration de l'API Microsoft Graph Security

Cette section couvre des conseils de dépannage importants et les questions fréquemment posées concernant l'intégration de l'ingestion d'alerte API de sécurité Microsoft Graph .

- **Exécution de l'intégration** : lorsqu'une tâche planifiée commence à s'exécuter, un enregistrement d'exécution de l'intégration avec les journaux, les erreurs et les avertissements s'affiche. Le nombre d'alertes extraites et le nombre d'incidents créés dans une exécution de tâche planifiée sont également affichés. Les utilisateurs disposant du rôle `sn_si.analyst` peuvent voir si l'extraction de profils/erreurs a échoué pendant l'exécution de l'intégration. Les utilisateurs disposant du rôle `sn_si.analyst` peuvent vérifier la table `sn_event_ingestion_integration_run` pour voir s'il y a des erreurs qui se sont produites. Pour résoudre tout problème d'intégration, vous devez d'abord vérifier l'exécution de l'intégration. Les erreurs sont enregistrées sous forme de notes de travail dans les enregistrements d'exécution de l'intégration pour chaque exécution de tâche planifiée.



- **Profil incomplet** : lors de la configuration du profil, dans la section Options supplémentaires (Automatiser les mises à jour et la fermeture des alertes en fonction de l'état de l'incident SIR), vous devez cliquer sur le bouton **Terminer** pour vous assurer que le profil passe à l'état En attente, ce qui indique qu'il est en attente d'ingestion.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Valider le profil** : pour valider si l'intégration fonctionne correctement, vérifiez les états du profil, la date de la dernière opération Pull du profil, la table d'importation d'alerte, les enregistrements de la table d'alerte à la tâche.
- **Problèmes SSL** : lors de la connexion via le API de sécurité Microsoft Graph, assurez-vous que l'instance dispose d'un certificat CA valide qui n'a pas expiré. Vous pouvez importer RSA ou vos propres certificats dans la plateforme et vous assurer que le nom commun du certificat correspond au nom d'hôte. Voir KB0778285 pour plus de détails.

Palo Alto Networks - AutoFocus intégration

Le Palo Alto Networks - AutoFocus système de base d'intégration inclut un workflow et une série d'activités de workflow que vous pouvez utiliser pour l'intégration Palo Alto Networks - AutoFocus à votre instance.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

Activer et configurer l'intégration Palo Alto Networks - AutoFocus

Utiliser

- Security Operations Palo Alto Networks : workflow de vérification et de blocage de la valeur
- Obtenir des informations sur la session AutoFocus Workflow d'enrichissement

Développer

- ServiceNow Opérations de sécurité Directives de développement de l'intégration
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté des opérations de sécurité
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Activer et configurer l'intégration Palo Alto Networks - AutoFocus

La fonction de configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, notamment Palo Alto Networks - AutoFocus. Avant de pouvoir utiliser le Palo Alto Networks - AutoFocus, vous devez le télécharger à ServiceNow Storepartir du fichier .

Avant de commencer

Rôle requis : sn_si_admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. .
2. Une fois l'installation terminée, accédez au site d'assistance de Palo Alto Networks et obtenez la clé API.
3. Dans votre instance, accédez à **Security Operations** > **Configuration de l'intégration**.
4. Dans la carte Palo Alto Networks AutoFocus, cliquez sur **Configurer**.
5. Entrez (ou collez) la **clé API** que vous avez acquise sur le site d'assistance de Palo Alto Networks.
6. Cliquez sur **Envoyer**.

Obtenir des informations sur la session AutoFocus Workflow d'enrichissement

Lorsque le workflow **d'enrichissement de Security Operations Palo Alto Networks - Obtenir des informations sur la session AutoFocus** est exécuté, il met en file d'attente une requête de recherche avec AutoFocus pour recueillir des informations sur une adresse IP source spécifiée. Si AutoFocus a connaissance des sessions précédentes provenant de cette adresse IP, un rapport au format JSON est renvoyé.

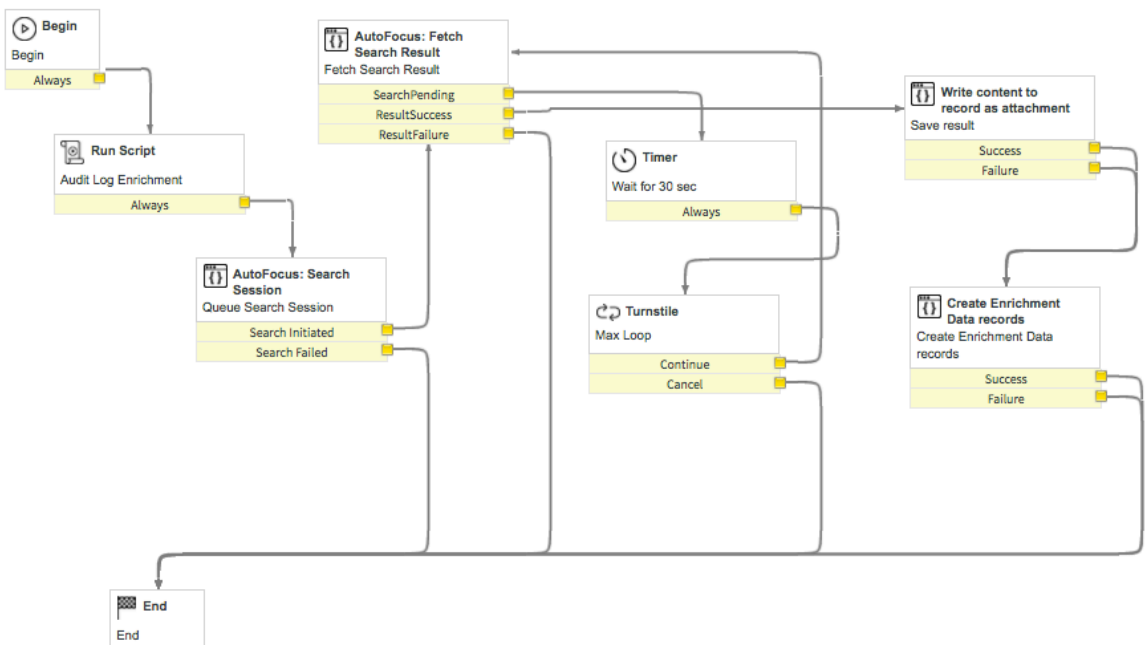
Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Le workflow **d'enrichissement Palo Alto Networks - Obtenir des informations sur la session AutoFocus** pour Security Operations est exécuté lorsque le champ **Adresse IP source** d'un incident de sécurité est modifié et que l'enregistrement est mis à jour. Le workflow récupère l'adresse IP et envoie une demande de requête à AutoFocus. Si AutoFocus a déjà identifié des sessions provenant de l'adresse IP, un rapport au format JSON est renvoyé.

Security Operations Palo Alto Networks - Obtenir le workflow d'enrichissement des données WildFire



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. Cliquez sur **l'onglet Indicators of Compromise (Indicateurs de compromission**) et renseignez le champ **Source IP (IP source**).
3. Cliquez sur **Mettre à jour**.
   AutoFocus analyse les informations à partir de l'adresse IP et un fichier texte au format JSON est joint à l'incident de sécurité.

   Les activités spécifiques à cette intégration sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Recherche de mise au point automatique Activité de la session

L'activité de workflow **Session de recherche AutoFocus** télécharge les informations d'une adresse IP affectée à un incident de sécurité vers AutoFocus et les met en file d'attente pour une requête de recherche.

Variables d'entrée

Remarque :

Lorsque l'activité s'exécute, elle met en file d'attente une requête de recherche avec AutoFocus pour collecter des informations pour une adresse IP source spécifiée. Si AutoFocus a déjà identifié des sessions provenant de cette adresse IP, un rapport au format JSON est renvoyé.

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
searchSessionQuery [chaîne]	Requête de recherche d'informations sur la session.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
requestStatus [booléen]	Vrai si une requête de recherche a été planifiée pour une exécution dans AutoFocus.
erreur [chaîne]	Erreur qui s'est produite, le cas échéant, dans l'activité.
afcookie [chaîne]	Identificateur de la requête de recherche AutoFocus utilisée par le Activité Extraire les résultats de la recherche pour récupérer les résultats de la recherche.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activité Extraire les résultats de la recherche

L'activité de workflow **Extraire les résultats de recherche** extrait les résultats de recherche identifiés par un cookie dans la requête de recherche initiée par l'activité de **session de recherche AutoFocus** .

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
afcookie [chaîne]	Le cookie AutoFocus pour la requête de recherche générée par le Recherche de mise au point automatique Activité de la sessionfichier .

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
searchPending [booléen]	Vrai si la demande de recherche est toujours en cours de traitement dans AutoFocus.
Résultat [chaîne]	Données des résultats de la recherche.
état [booléen]	Vrai si la recherche est terminée et que les résultats ont été générés avec succès.
erreur [chaîne]	Erreur qui s'est produite, le cas échéant, dans l'activité.

Palo Alto Networks - Firewall intégration

Pour effectuer l'intégration Palo Alto Networks - Firewall , assurez-vous d'avoir configuré Serveur MID avec des informations d'identification SSH. Si aucun pare-feu n'est déjà configuré, ajoutez-en un.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

- Activer et configurer l'intégration du pare-feu Palo Alto Networks
- Configurer les informations d'identification SSH sur Serveur MID

Utiliser

Workflow du lanceur de pare-feu Security Operations Integration Palo Alto Networks

Développer

- ServiceNow Opérations de sécurité Directives de développement de l'intégration
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	• Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide • Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service et assistance client	

Configurer les informations d'identification SSH sur Serveur MID

Le pare-feu Palo Alto Networks envoie des appels d'API au MID Server. En tant que tel, assurez-vous que les informations d'identification SSH ont été créées pour le serveur MID.

Avant de commencer

- Le module d'extension Orchestration doit être activé.

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Orchestration** > **Informations d'identification et connexions** > **Informations d'identification**.
2. Cliquez sur **Nouveau**.
3. Dans l'écran Intercepteur, cliquez sur **Informations d'identification SSH**.
4. Renseignez les champs nécessaires.

Informations d'identification SSH

Champ	Description
Nom	Donnez un nom aux informations d'identification.
Actif	Cochez cette case pour activer ces informations d'identification.
Concerne	Sélectionnez **Tous les serveurs MID** ou **Serveurs MID spécifiques**.
Serveurs MID	Si vous avez sélectionné **des MID Servers spécifiques**, cliquez sur l'icône de verrou et sélectionnez les MID Servers auxquels vous souhaitez appliquer ces informations d'identification.
Ordre	Sélectionnez l'ordre dans lequel les informations d'identification sont utilisées par le serveur. Les plus petits nombres sont essayés en premier.
Nom d'utilisateur	Saisissez le nom d'utilisateur de l'utilisateur associé à ces informations d'identification, le cas échéant.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mot de passe	Si vous avez entré un **nom d'utilisateur**, saisissez le mot de passe de l'utilisateur.
Balises	Entrez une balise à utiliser pour les critères de recherche. Le champ **Balise** doit contenir la même valeur que le **nom**.

Activer et configurer l'intégration du pare-feu Palo Alto Networks

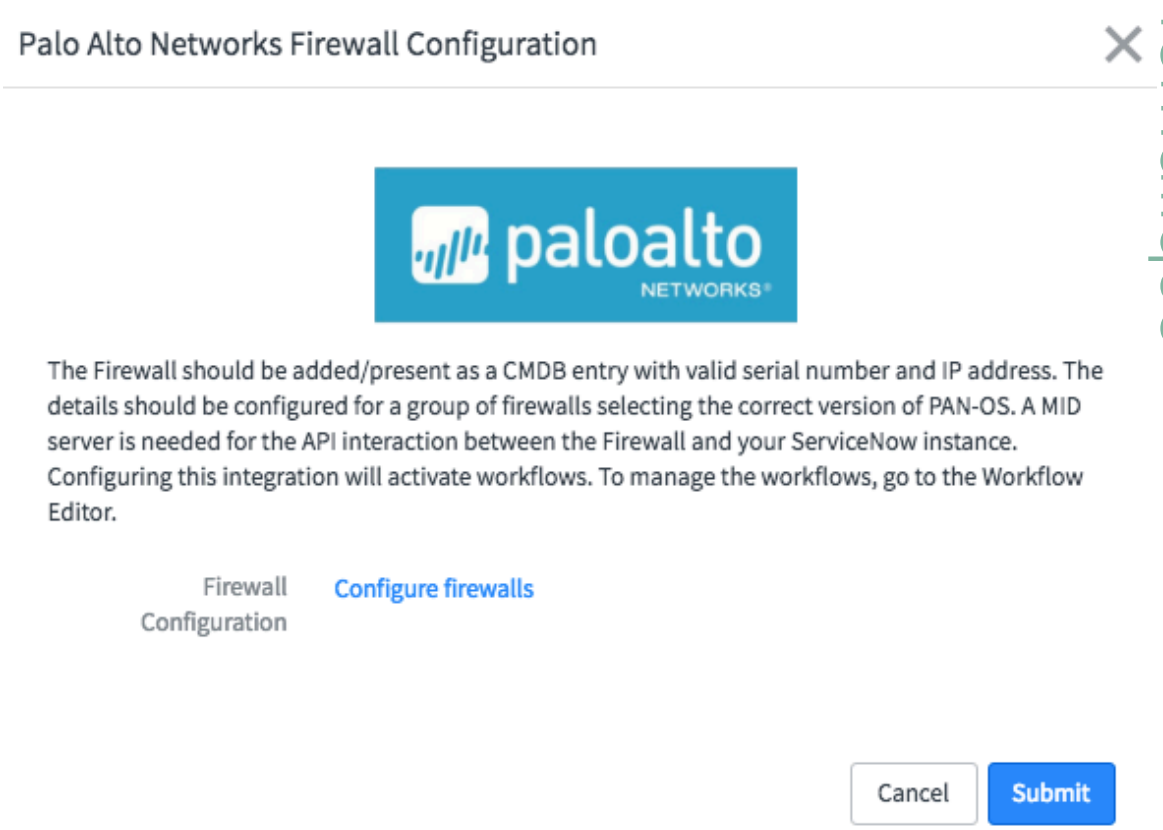
La fonction de configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, notamment Palo Alto Networks - Firewall. Avant de pouvoir utiliser le Palo Alto Networks - Firewall, vous devez le télécharger à ServiceNow Storepartir du fichier .

Avant de commencer

Rôle requis : sn_si_admin

Procédure

1. Avant d'activer et de configurer l'intégration, accédez au tableau de bord du pare-feu Palo Alto Networks.
   Notez les noms de la liste dynamique d'adresses IP, de la liste dynamique d'URL ou de la liste dynamique de domaines que vous utilisez pour bloquer le pare-feu.
2. Téléchargez l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à **Security Operations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la carte Palo Alto Networks Firewall, cliquez sur **Configurer**.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Configurer les pare-feu**.
6. Sur l'écran Configurations du pare-feu, cliquez sur **Nouveau**.
7. Renseignez les champs du formulaire comme il convient.

Champ	Description
Pare-feu	Cliquez sur l'icône de verrouillage et sélectionnez le pare-feu à configurer.
Version de pare-feu	Sélectionnez la version du pare-feu Palo Alto Networks.**PAN-OS-7.1** est la version recommandée. La sélection de versions antérieures peut renvoyer des résultats incohérents.
Nom d'utilisateur	Entrez le nom d'utilisateur à utiliser lors de la connexion au pare-feu via des points de terminaison REST.
Mot de passe	Entrez le mot de passe de l'utilisateur qui se connecte.
Liste dynamique d'adresses IP	Entrez le nom de la liste dynamique externe ou de la liste de blocs dynamiques que vous utilisez pour les adresses IP.
Liste dynamique d'URL	Saisissez le nom de la liste externe dynamique ou de la liste de blocs dynamiques que vous utilisez pour les URL.
Liste dynamique de domaines	Entrez le nom de la liste externe dynamique ou de la liste de blocs dynamiques que vous utilisez pour les domaines.

8. Cliquez sur **Envoyer**.

Workflow du lanceur de pare-feu Security Operations Integration Palo Alto Networks

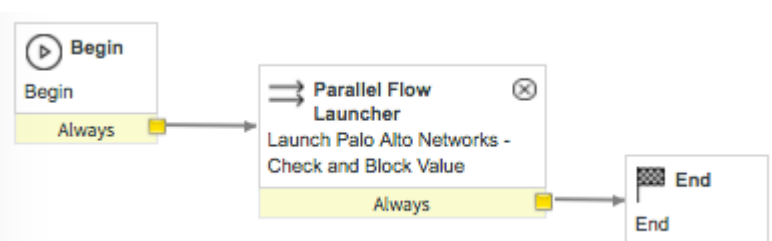
Le workflow Lanceur de pare-feu Palo Alto Networks est l'implémentation du pare-feu Palo Alto Networks lancée par le workflow **d'aptitude Intégration de Security Operations - Demande de bloc** .

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Les activités de processus du workflow incluent :Security Operations Palo Alto Networks : workflow de vérification et de blocage de la valeur



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Operations Palo Alto Networks : workflow de vérification et de blocage de la valeur

Au fur et à mesure que les incidents de sécurité sont créés et triés pour identifier les menaces potentielles, vous pouvez utiliser le workflow **Security Operations Palo Alto Networks - Check and Block Value** pour vérifier et mettre à jour automatiquement les adresses IP, les URL et les domaines à l'aide des listes dynamiques externes définies dans Palo Alto Networks - Firewall.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Le workflow **Security Operations Palo Alto Networks - Vérifier et bloquer la valeur** est exécuté lorsque des demandes de blocage de pare-feu sont soumises. La demande de bloc spécifie le pare-feu à utiliser, le type d'observable à vérifier et à bloquer (si nécessaire) et la valeur du bloc. C'est-à-dire l'adresse IP, l'URL ou le domaine en question.

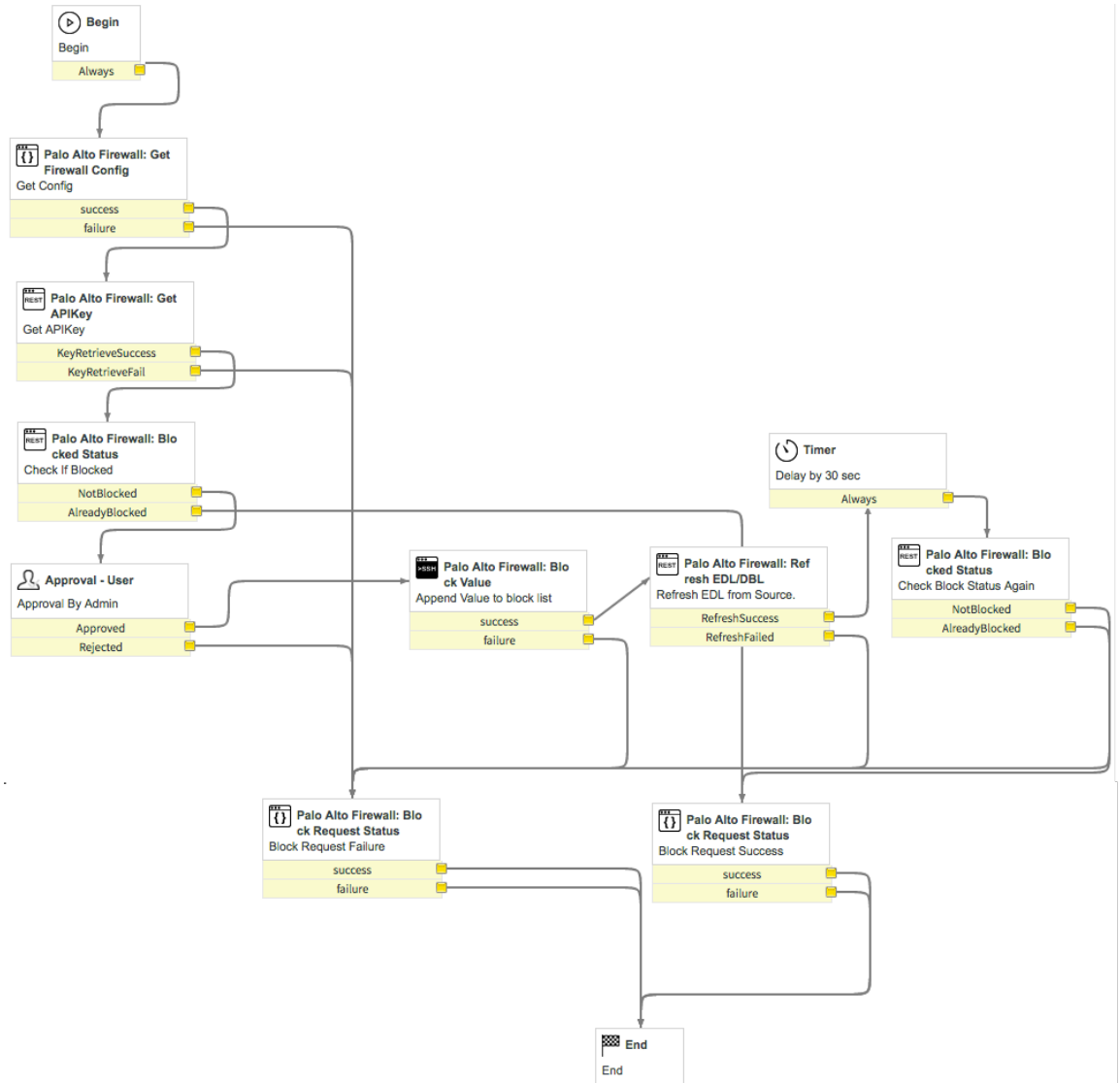
Pendant l'exécution du workflow, les commandes définies sous **Intégration de Palo Alto Networks** > **Pare-feu** > **Commandes** sont exécutés. Les commandes de type Afficher (par exemple, Show-IP-ExternalDynamicList) déterminent si la valeur existe sur le pare-feu. Les commandes de type Actualiser (par exemple, Refresh-IP-ExternalDynamicList) ajoutent à la liste de blocs une valeur qui n'existe pas sur le pare-feu.

Une fois l'activité État bloqué exécutée, l'approbation d'un administrateur système est requise pour que le workflow puisse continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Operations Palo Alto Networks : workflow de vérification et de blocage de la valeur



Procédure

1. Accédez à la **Intégration de Palo Alto Networks** > **Pare-feu** > **Demandes de blocs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Pare-feu	Sélectionnez le pare-feu à utiliser.
Type de bloc	Sélectionnez le type de valeur à vérifier : ◦ IP ◦ URL ◦ DOMAINE
Valeur de bloc	Entrez la valeur du type sélectionné à vérifier sur le pare-feu.

4. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pare-feu Palo Alto : activité d'état des demandes de blocs

Cette activité est appelée par d'autres activités pour définir l'état de la demande de bloc de pare-feu sur réussite ou échec.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
firewallBlockRequestSysid [chaîne]	ID système de la demande de blocage de pare-feu. Cette variable d'entrée est obligatoire.
État [chaîne]	Indique si la tâche d'actualisation a exécuté : réussite ou échec.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
Résultat [chaîne]	Indique si la tâche d'actualisation a réussi ou échoué.

Pare-feu Palo Alto : activité de valeur de bloc

Une fois que le workflow a identifié une valeur qui n'est pas sur le pare-feu, l'enregistrement est acheminé pour approbation. Après approbation, cette activité se connecte au serveur MID via vos informations d'identification SSH et appelle un script qui ajoute la valeur à la liste de blocs externes du pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Remarque : Vous devez saisir manuellement les variables d'entrée pour cette activité, puis publier le workflow. Si le workflow n'est pas publié, les variables d'entrée ne sont pas enregistrées pour les utilisateurs non-administrateurs.

Variables d'entrée

Variable	Description
toBeBlockedValue [chaîne]	Valeur à ajouter à l'EDL si elle n'est pas déjà présente. Cette variable d'entrée est obligatoire.
typeToBeBlocked [chaîne]	Type de valeur à bloquer : IP, URL ou Domaine. Cette variable d'entrée est obligatoire.
targetHost [chaîne]	Serveur MID sur lequel le script est exécuté.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée (suite)

Variable	Description
SSHCredentialTag [chaîne]	La balise d'informations d'identification SSH définie sur le MID Server.
scriptCommand [chaîne]	Script AppendValueToList.sh utilisé pour ajouter la valeur à l'EDL. Il nécessite le chemin d'accès complet au serveur MID.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
Résultat [chaîne]	Le résultat a été transmis à l'EDL.

Pare-feu Palo Alto : activité d'état bloqué

Cette activité vérifie si la valeur (IP, URL ou domaine) est incluse dans sa liste dynamique externe/liste de blocs dynamiques (EDL/DBL) respective sur le pare-feu. Les détails EDL/DBL sont obtenus à partir du pare-feu à l'aide d'une commande opérationnelle, et une routine est exécutée pour vérifier si la valeur est bloquée sur le pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité. Toutes les entrées de variables d'entrée répertoriées sont obligatoires.

Variables d'entrée

Variable	Description
valueToBeChecked [chaîne]	La valeur de la demande de bloc.
showEDLDetailsCommand [chaîne]	Commande Liste dynamique externe utilisée pour déterminer si la valeur existe sur le pare-feu.
FirewallIpAddress [chaîne]	Adresse IP du pare-feu utilisé.
FirewallApiKey [chaîne]	Clé API du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement à l'aide du message d'API Palo Alto Firewall Operational Command.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
commandResult [chaîne]	Résultats du pare-feu pour la commande show EDL Details.
blockedStatus [booléen]	Vrai indique un élément bloqué. Faux indique qu'il n'est pas bloqué.
commandResponse [chaîne]	État de la réponse obtenu à partir du pare-feu pour la commande show EDL Details.

Pare-feu Palo Alto : obtenir l'activité de clé API

Cette activité récupère la clé API du pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité. Toutes les entrées de variables d'entrée répertoriées sont obligatoires.

Variables d'entrée

Variable	Description
Nom d'utilisateur [string]	Nom d'utilisateur de l'administrateur du pare-feu.
Mot de passe [string]	Le mot de passe de l'administrateur du pare-feu.
FirewallIpAddress [chaîne]	Adresse IP du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
APIKey [chaîne]	Clé API du pare-feu.

Pare-feu Palo Alto : obtenir l'activité de configuration du pare-feu

L'activité de workflow Pare-feu Palo Alto : obtenir la configuration du pare-feu accède à toutes les informations de configuration de pare-feu connexes à partir de la base de données et les rend disponibles pour l'activité suivante.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Variable	Description
firewallSysid [chaîne]	ID système du pare-feu. Cette variable d'entrée est obligatoire.
typeOfValueToBeBlocked [chaîne]	Type de valeur à bloquer sur le pare-feu : IP, URL ou Domaine.
pare-feuIPAddress [chaîne]	Adresse IP du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
ipEDLName [chaîne]	Nom de la liste dynamique externe pour les adresses IP.
urlEDLName [chaîne]	Nom de la liste dynamique externe pour les URL.
domainEDLName [chaîne]	Nom de la liste dynamique externe pour les domaines.
firewallVersionSysId [chaîne]	ID système de la version de pare-feu.
refreshEDLCommand [chaîne]	Commande à utiliser pour actualiser l'EDL à partir de la source.
ShowEDLDetailsCommand [chaîne]	Commande à utiliser pour obtenir les détails de l'EDL.
état [booléen]	Vrai indique la réussite. Faux indique un échec.
erreur [chaîne]	Erreur qui s'est produite, le cas échéant, dans l'activité.
point de terminaison [chiffré]	Point de terminaison chiffré de la base de données.

Pare-feu Palo Alto : actualiser l'activité EDL/DBL

Cette activité exécute une commande opérationnelle sur le pare-feu pour actualiser la liste dynamique externe à partir de la source configurée sur le pare-feu. La sortie de cette activité indique si la tâche d'actualisation a été mise en file d'attente.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité. Toutes les entrées de variables d'entrée répertoriées sont obligatoires.

Variables d'entrée

Variable	Description
FirewallIpAddress [chaîne]	Adresse IP du pare-feu en cours d'actualisation.
FirewallApiKey [chaîne]	Clé API de pare-feu actualisée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée (suite)

Variable	Description
Commande de pare-feu [chaîne]	Commande opérationnelle à exécuter pour mettre en file d'attente la tâche d'actualisation.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
activité. Output.result [chaîne]	Chaîne de texte indiquant si la tâche d'actualisation a été mise en file d'attente pour s'exécuter : réussite ou échec.

Obtenir le workflow des données de journal

Si Réponse aux incidents de sécurité, Renseignements sur les menacesPalo Alto Networks - Firewall et sont activés, le workflow **Security Operations Palo Alto Networks - Obtenir les données de journal** s'exécute automatiquement lorsque l'adresse IP source pour les observables dans un incident de sécurité est modifiée.

Avant de commencer

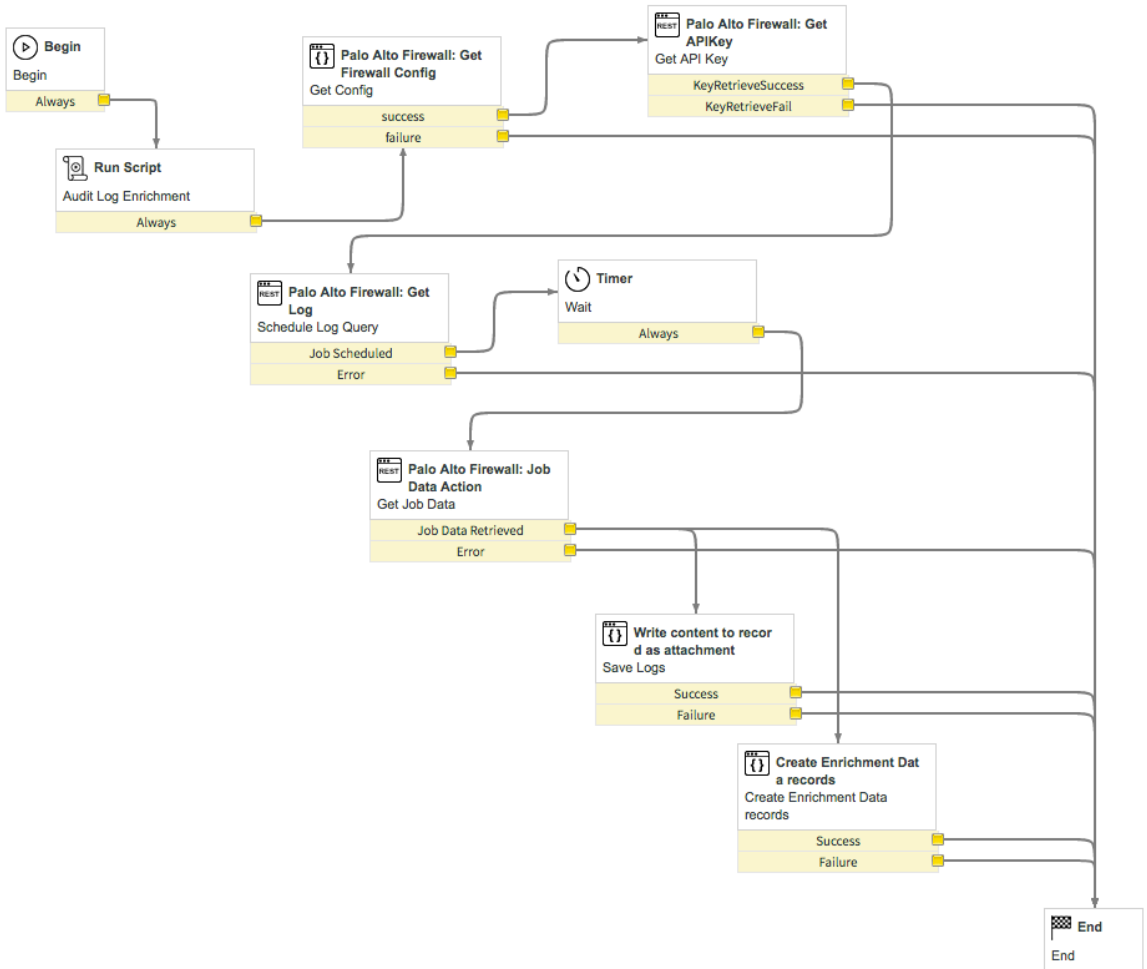
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Lors de l'exécution du workflow, les informations de configuration du pare-feu sont récupérées à partir de la base de données et la clé API est récupérée à partir du pare-feu. L'activité Obtenir le journal met en file d'attente une requête de recherche sur le pare-feu. Lorsque la requête s'exécute, elle renvoie un ID de tâche qui est utilisé pour récupérer les données des journaux de menaces à partir du pare-feu. Il joint les données du journal sous la forme d'un fichier XML à l'incident de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Operations Palo Alto Networks : obtenir le workflow des données de journal



Procédure

1. Accédez à un incident de sécurité qui contient des observables.
2. Cliquez sur l'onglet **Observables d'incident de sécurité** .
3. Dans **Adresse IP source**, ajoutez ou modifiez l'adresse IP.
4. Cliquez sur **Mettre à jour**.
   Le workflow **Palo Alto Networks de Security Operations : obtenir les données de journal** s'exécute et les données de journal des menaces enrichies sont jointes à l'incident de sécurité. Les informations sont également analysées et affichées dans la section **Journaux de pare-feu** sous l'onglet **Données d'enrichissage** .

Pare-feu Palo Alto : obtenir l'activité de clé API

Cette activité récupère la clé API du pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité. Toutes les entrées de variables d'entrée répertoriées sont obligatoires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Variable	Description
Nom d'utilisateur [string]	Nom d'utilisateur de l'administrateur du pare-feu.
Mot de passe [string]	Le mot de passe de l'administrateur du pare-feu.
FirewallIpAddress [chaîne]	Adresse IP du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
APIKey [chaîne]	Clé API du pare-feu.

Pare-feu Palo Alto : obtenir l'activité de configuration du pare-feu

L'activité de workflow Pare-feu Palo Alto : obtenir la configuration du pare-feu accède à toutes les informations de configuration de pare-feu connexes à partir de la base de données et les rend disponibles pour l'activité suivante.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
firewallSysid [chaîne]	ID système du pare-feu. Cette variable d'entrée est obligatoire.
typeOfValueToBeBlocked [chaîne]	Type de valeur à bloquer sur le pare-feu : IP, URL ou Domaine.
pare-feuIPAddress [chaîne]	Adresse IP du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
ipEDLName [chaîne]	Nom de la liste dynamique externe pour les adresses IP.
urlEDLName [chaîne]	Nom de la liste dynamique externe pour les URL.
domainEDLName [chaîne]	Nom de la liste dynamique externe pour les domaines.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
firewallVersionSysId [chaîne]	ID système de la version de pare-feu.
refreshEDLCommand [chaîne]	Commande à utiliser pour actualiser l'EDL à partir de la source.
ShowEDLDetailsCommand [chaîne]	Commande à utiliser pour obtenir les détails de l'EDL.
état [booléen]	Vrai indique la réussite. Faux indique un échec.
erreur [chaîne]	Erreur qui s'est produite, le cas échéant, dans l'activité.
point de terminaison [chiffré]	Point de terminaison chiffré de la base de données.

Pare-feu Palo Alto : obtenir l'activité de journal

L'activité de workflow **Pare-feu Palo Alto : obtenir les journaux** planifie une requête sur le pare-feu pour récupérer les journaux et renvoie un JobID utilisé pour récupérer les données du journal.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
FirewallIpAddress [chaîne]	Adresse IP du pare-feu. Cette variable d'entrée est obligatoire.
FirewallApiKey [chaîne]	Clé d'accès API du pare-feu. Cette variable d'entrée est obligatoire.
FirewallLogType [chaîne]	Type de données de journal à récupérer (défini sur menace). Cette variable d'entrée est obligatoire.
FirewallLogFilterQuery [chaîne]	Requête à exécuter pour rechercher des journaux sur le pare-feu. Cette variable d'entrée est obligatoire.
LogDirection [chaîne]	Spécifie si les journaux sont affichés dans l'ordre le plus ancien (en arrière) ou le plus récent en premier (en avant).
LogNumber [chaîne]	Spécifie le nombre de journaux à récupérer.
LogSkipCount [chaîne]	Spécifie le nombre de journaux à ignorer lors de la récupération d'un journal.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
QueuedJobID [chaîne]	L'ID de tâche renvoyé par le pare-feu.
JobPlanifié [chaîne]	Spécifie (réussite ou échec) si la tâche a été envoyée au pare-feu.
erreur [chaîne]	Toutes les erreurs renvoyées.

Pare-feu Palo Alto : données de tâche Activité d'action

Une fois que **l'activité Palo Alto Firewall : obtenir le journal** met en file d'attente la requête de recherche vers le pare-feu et que la tâche s'exécute, l'activité **Palo Alto Firewall : action de données de tâche** récupère les données du journal des menaces du pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité. Tous les champs d'entrée sont obligatoires.

Variables d'entrée

Variable	Description
FirewallIpAddress [chaîne]	Adresse IP du pare-feu.
FirewallApiKey [chaîne]	Clé d'accès API du pare-feu.
JobID [chaîne]	ID de la tâche en file d'attente.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
commandStatus [chaîne]	Spécifie (réussite ou échec) si les données ont été récupérées à partir du pare-feu.
JobData [chaîne]	Les données collectées à partir du pare-feu.
erreur [chaîne]	Toutes les erreurs renvoyées.

Palo Alto Networks - WildFire intégration

Palo Alto Networks - WildFire est une application basée sur le cloud qui interagit avec le pare-feu de votre système.

Explorer	Configurer
Intégrations de Réponse aux incidents de sécurité	Activez Security Operations Palo Alto Networks - WildFire

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser	Développer
Obtenir le workflow d'enrichissement des données WildFire	• ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide	
• Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service et assistance client	

Activez Security Operations Palo Alto Networks - WildFire

Avant de pouvoir utiliser l'intégration de Security Operations Palo Alto Networks - WildFire, vous devez télécharger l'intégration à partir du ServiceNow Storefichier .

Avant de commencer

Rôle requis : administrateur

Procédure

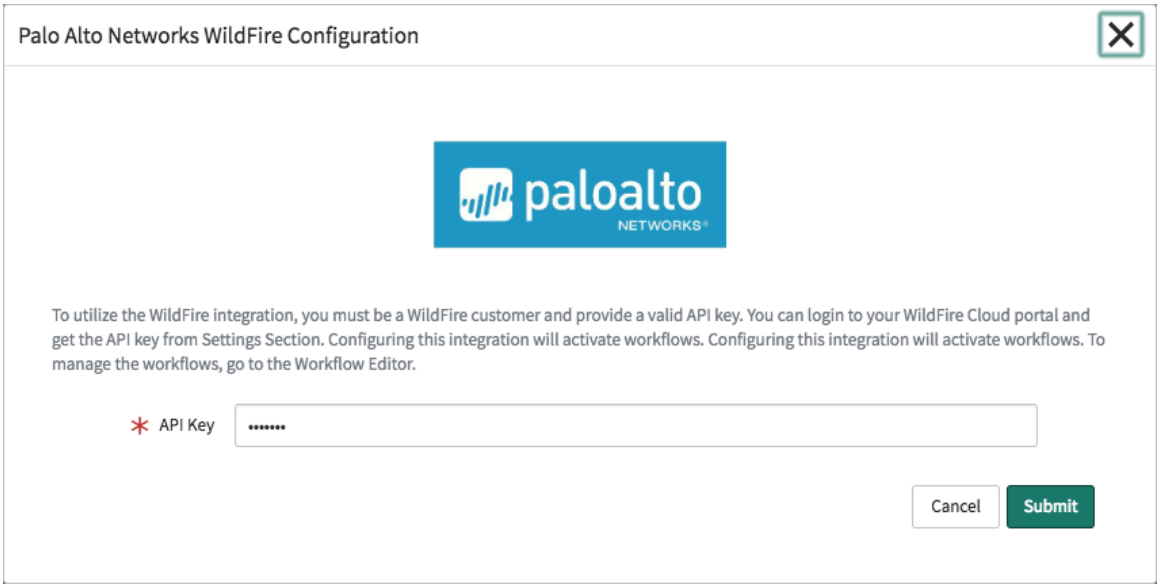
1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.



3. Dans la Carbon Black carte, cliquez sur **Configurer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Saisissez la clé API, puis cliquez sur **Soumettre**.
   La carte de configuration de l'intégration s'affiche.
5. Pour revenir à la liste initiale des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Obtenir le workflow d'enrichissement des données WildFire

Lorsque le workflow **d'enrichissement des données de Security Operations Palo Alto Networks - Get WildFire** est exécuté, un fichier de hachage est téléchargé dans WildFire. Les données sont enrichies et les rapports sont téléchargés sur l'instance pour faciliter le traitement des attaques potentielles de logiciels malveillants.

Avant de commencer

Rôle requis : sn_si.analyst

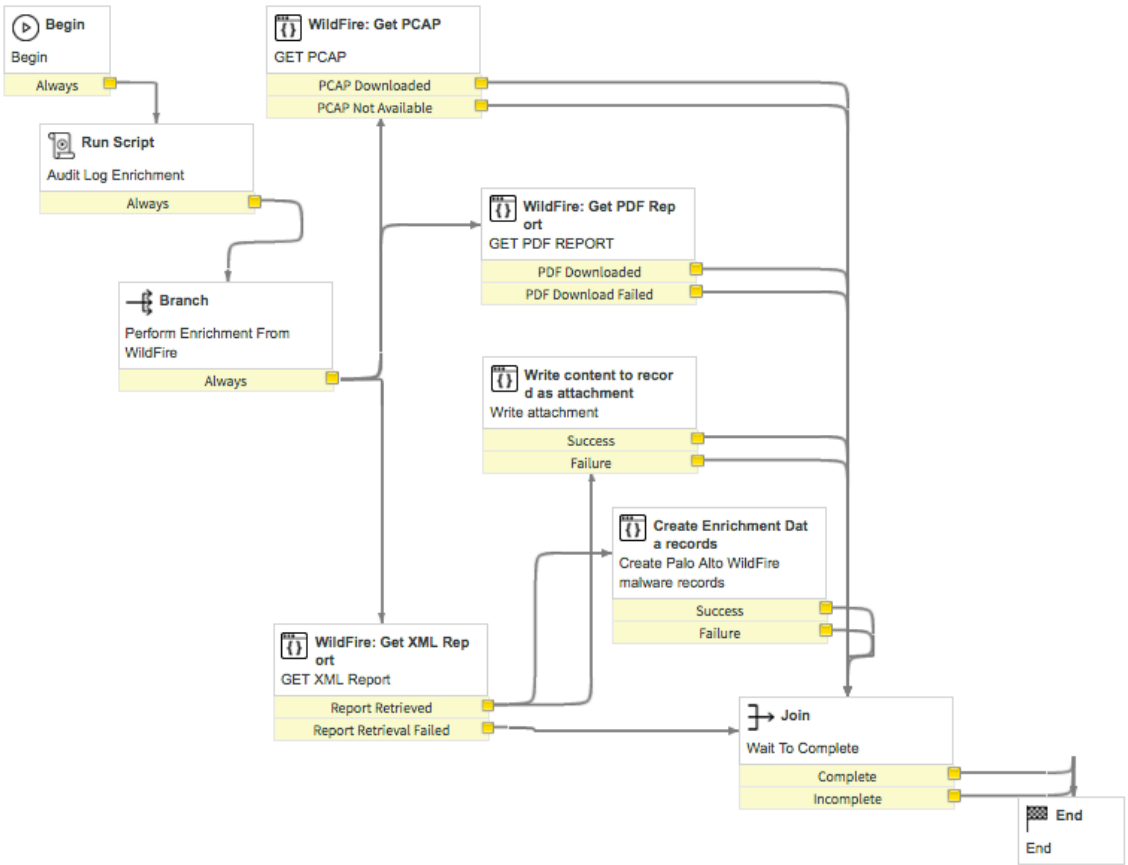
Pourquoi et quand exécuter cette tâche

Le workflow **Security Operations Palo Alto Networks - Get WildFire Data Enrichment** est exécuté lorsqu'un incident de sécurité est créé à partir d'une alerte reçue de l'application Palo Alto Network Firewall. Un hachage de programme malveillant provenant de la notification par e-mail reçue du pare-feu est saisi dans l'onglet **IoC** de l'incident de sécurité et l'enregistrement est mis à jour.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Operations Palo Alto Networks - Obtenir le workflow d'enrichissement des données WildFire



Procédure

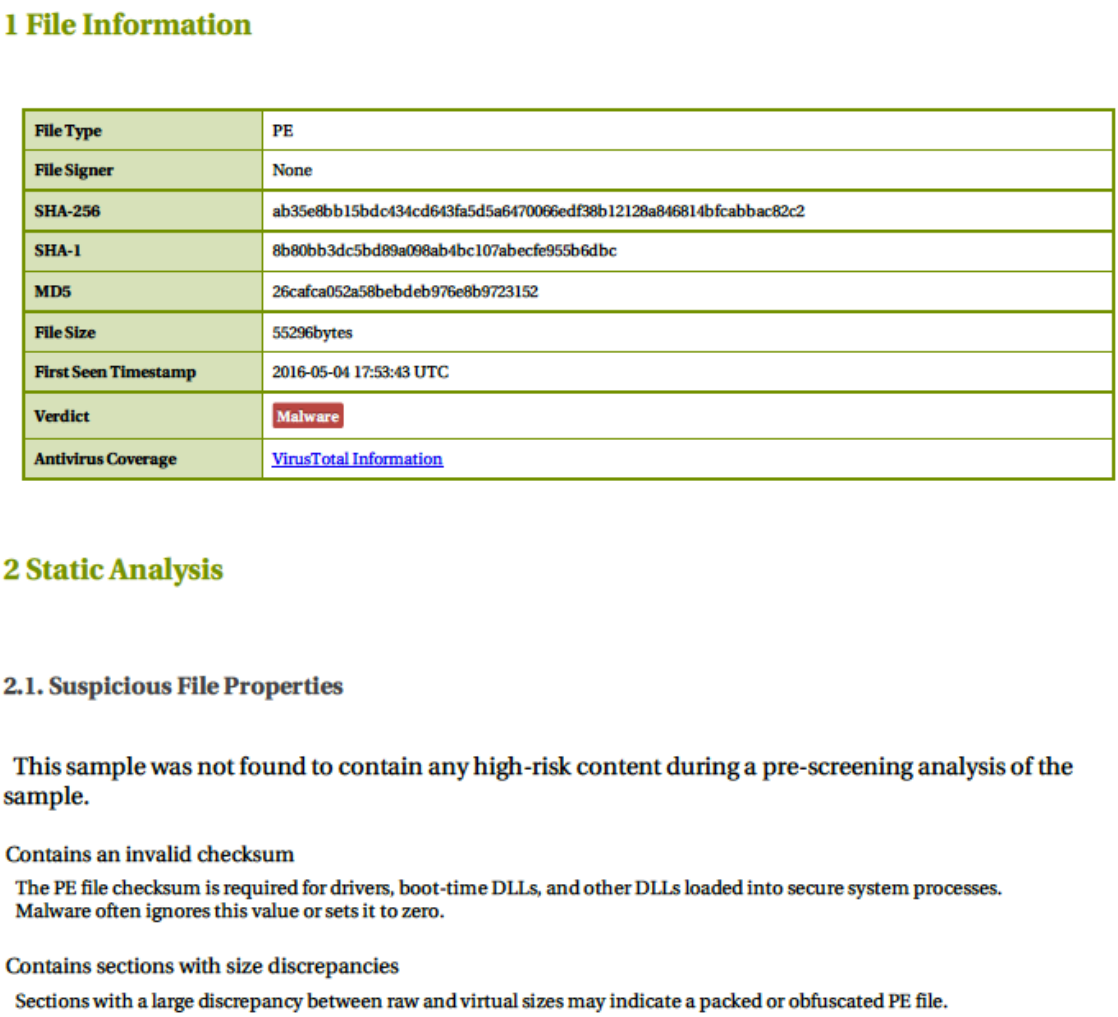
1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. En fonction de la notification par e-mail reçue du pare-feu, localisez et ouvrez l'incident de sécurité qui a été créé.
3. Cliquez sur **l'onglet Indicateurs de compromission** et renseignez le **hachage de programme malveillant** avec le hachage que vous avez reçu dans l'alerte.
4. Cliquez sur **Mettre à jour**.
   Le workflow entraîne le téléchargement du fichier de hachage dans WildFire où les données sont enrichies. Les rapports aux formats PDF et XML sont joints à l'enregistrement (incident de sécurité ou IoC) dans votre instance pour faciliter le traitement des attaques potentielles de logiciels malveillants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si les données enrichies comprennent des informations de capture de paquets, les informations PCAP sont également téléchargées. Les données PCAP capturent les actions effectuées par le fichier. Par exemple, il peut signaler les serveurs contactés par le fichier. Pour afficher les fichiers PCAP, vous avez besoin d'un analyseur de paquets, tel que Wireshark .

Exemple de PDF généré par Wildfire



1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

WildFire : obtenir l'activité PCAP

L'activité de workflow **WildFire : Get PCAP** obtient les informations de capture de paquets (PCAP) générées lors de l'analyse d'un hachage de fichier spécifié sur WildFire. Le résultat de cette activité est joint à un enregistrement spécifique identifié par **TableName** et **RecordId**.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
FileSHA256Hash [chaîne]	Hachage du fichier reçu de l'application Palo Alto Network Firewall.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée (suite)

Variable	Description
Nom de table [chaîne]	Table affectée.
RecordId [chaîne]	L'incident de sécurité ou l'IoC en cours de mise à jour.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
commandStatus [booléen]	Vrai si un résultat est obtenu et joint avec succès.
errorMessage	Erreur qui s'est produite, le cas échéant, dans l'activité.

WildFire : obtenir l'activité du rapport PDF

L'activité de workflow **WildFire : Obtenir un rapport PDF** obtient le rapport généré lors de l'analyse d'un hachage de fichier spécifié sur WildFire au format PDF. Le résultat de cette activité est joint à un enregistrement spécifique identifié par **TableName** et **RecordId**.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
Nom de table [chaîne]	Table affectée.
FileSHA256Hash [chaîne]	Hachage du fichier reçu de l'application Palo Alto Network Firewall.
RecordId [chaîne]	L'incident de sécurité ou l'IoC en cours de mise à jour.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
commandStatus [booléen]	Vrai si un résultat est obtenu et joint avec succès.
errorMessage	Erreur qui s'est produite, le cas échéant, dans l'activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

WildFire : obtenir l'activité du rapport XML

L'activité de workflow **WildFire : Get XML Report** obtient le rapport généré lors de l'analyse d'un hachage de fichier spécifié sur WildFire au format XML. Le résultat de cette activité est joint à un enregistrement spécifique identifié par **TableName** et **RecordId**.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
Nom de table [chaîne]	Table affectée.
FileSHA256Hash [chaîne]	Hachage du fichier reçu de l'application Palo Alto Network Firewall.
RecordId [chaîne]	L'incident de sécurité ou l'IoC en cours de mise à jour.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
commandStatus [booléen]	Vrai si un résultat est obtenu et joint avec succès.
errorMessage	Erreur qui s'est produite, le cas échéant, dans l'activité.

Palo Alto Networks - Next-Generation Firewall intégration

Une fois l'installation et la configuration effectuées, l'analyste des incidents de sécurité utilise cette intégration pour bloquer les adresses IP, les URL et les domaines malveillants à l'aide des options de liste dynamique externe (EDL) avec les ServiceNow Réponse aux incidents de sécurité produits (SIR). L'analyste des incidents de sécurité crée des entrées pour une EDL à partir d'observables identifiés comme malveillants sur ServiceNow SIR les incidents de sécurité.

Un EDL est un fichier texte qui est hébergé sur un serveur Web externe. Pour cette intégration, ce serveur Web est votre Now Platform instance, ce qui vous permet Palo Alto Networks - Next-Generation Firewall d'importer des objets inclus dans la liste, des adresses IP, des URL et des domaines, et d'appliquer la stratégie.

Pour appliquer la politique aux entrées EDL, la liste est référencée dans une règle de politique ou un profil. Au fur et à mesure que les entrées EDL sont modifiées, le pare-feu importe dynamiquement la liste à l'intervalle configuré et applique la politique sans changement de configuration ni validation sur le pare-feu. Pour cette intégration, Now Platform a créé une table contenant les entrées EDL qui sont récupérées par autorisé Palo Alto Networks - Next-Generation Firewall aux intervalles de récupération configurés.

L'intégration comprend les fonctionnalités suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Flexibilité de création de plusieurs EDL qui s'appliquent à différentes stratégies de refus ou d'autorisation de pare-feu.
- Rapports détaillés sur les types de sites bloqués (hameçonnage, logiciels malveillants et sites sur liste d'autorisation).
- Balisage des incidents de Now Platform sécurité avec entrées EDL par type d'observable (URL, domaine, adresse IP).
- Configurer les périodes d'expiration des EDL pour maintenir la taille de la liste EDL en faisant automatiquement expirer ou en supprimant les entrées les plus anciennes.
- Rechercher, supprimer ou migrer les entrées EDL entre les listes EDL.
- Liaison des entrées EDL aux enregistrements d'observables et aux incidents de sécurité qui incluent des résultats de Threat Intelligence et des détails sur les raisons pour lesquelles une entrée est bloquée.

L'intégration nécessite que les modules d'extension (com.snc.security_incident) et (com.snc.secops.orchestration) du Réponse aux incidents de sécurité produit soient activés.

Cette intégration ne prend en charge Palo Alto Networks que (PAN-OS 8.x). Les versions antérieures ne sont pas prises en charge.

Cette intégration est compatible avec les versions Kingston, London, Madrid et New York du Now Platform®fichier .

Remarque : Les sujets suivants sont numérotés. Pour une installation, une configuration et une vérification fluides des résultats attendus, suivez les rubriques dans l'ordre où elles sont présentées.

Créer un profil de certificat pour le Palo Alto Networks - Next-Generation Firewall

L'intégration nécessite un profil de certificat pour valider et authentifier la connexion sécurisée entre le serveur et le Now Platform®Palo Alto Networks - Next-Generation Firewall serveur.

Avant de commencer

Rôle requis : Palo Alto Networks - Next-Generation Firewall administrateur

Pourquoi et quand exécuter cette tâche

A Palo Alto Networks - Next-Generation Firewall s'authentifie auprès d'une Now Platform® instance, récupère les entrées EDL de la table de base de données et incorpore les entrées dans les règles de stratégie de pare-feu correspondantes. Cette récupération nécessite le rôle de compte d'utilisateur de l'API dans l'instance Now Platform®, qui est utilisé par l'administrateur du pare-feu PAN pour accéder à l'API Now Platform® .

L'administrateur Palo Alto Networks - Next-Generation Firewall crée un profil de certificat dans Palo Alto Networks. Ce certificat valide et authentifie la connexion sécurisée entre le serveur et Palo Alto Networks le Now Platform® serveur de pare-feu.

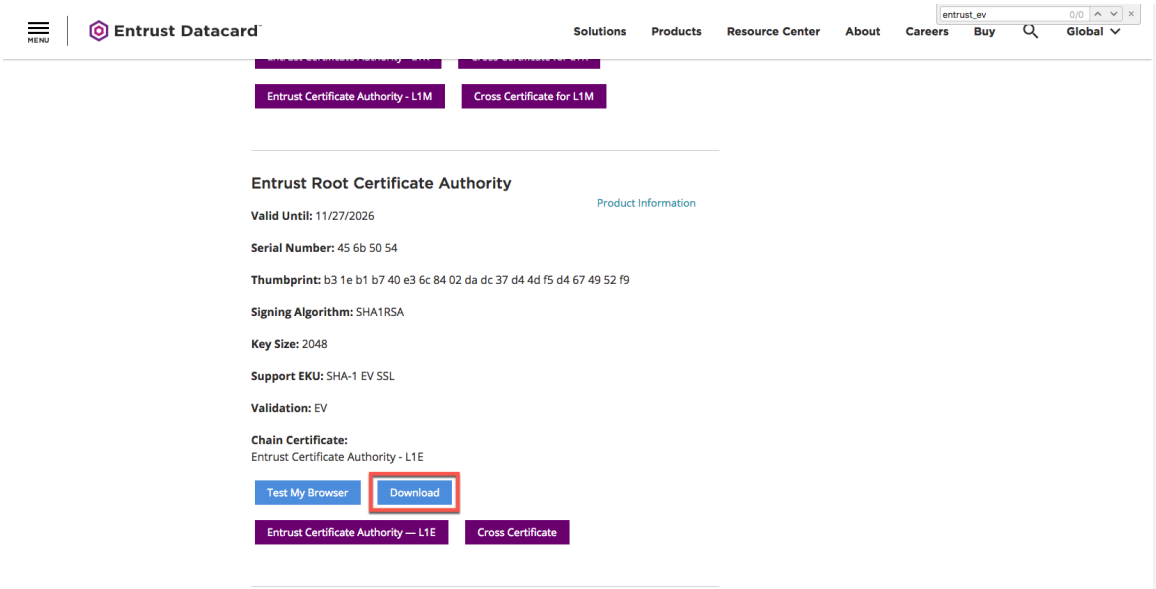
Now Platform® utilise Entrust en tant qu'autorité de certification et le profil de certificat requis est créé à l'aide du certificat `entrust_ev_ca.cer` . Ce certificat peut être téléchargé sur le site de la carte™ EntrustData. Pour vous assurer d'obtenir les versions les plus récentes, téléchargez ces certificats directement à partir du site Web d'Entrust.

Procédure

1. Accédez au téléchargement des certificats racines .
2. Sur le site Web d'Entrust, faites défiler l'écran jusqu'au certificat de **l'autorité de certification racine Entrust** , comme illustré dans la figure suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur **Télécharger**.
   Le nom du fichier téléchargé est **entrust_ev_ca.cer**.
4. Consultez Palo Alto Networks la documentation pour savoir comment configurer le profil de certificat une fois que vous l'avez téléchargé.
   Les exigences peuvent être consultées sur le Palo Alto Networks site Web.

Information associée

« Configurer un profil de certificat » dans le Guide de l'administrateur de PAN-OS 10.0

Configurer et installer Palo Alto Networks - Next-Generation Firewall

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches de configuration sont nécessaires pour une installation en douceur.

Avant de commencer

Rôle requis : (admin)

Tâche de configuration	Description
Vérifiez que les rôles requis Now Platform et Réponse aux incidents de sécurité vous ont été affectés.	Les rôles suivants sont requis : • L'administrateur système (admin) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration et crée, active et supprime les EDL. Ce rôle attribue également le rôle sn_si.analyste. • L'administrateur attribue le rôle de Now Platform® compte API (sn_sec_panfw.api_account_access), qui est utilisé exclusivement pour saisir les informations d'identification requises pour l'authentification afin Palo Alto Networks

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	que les pare-feux puissent récupérer les EDL à partir du Now Platform®. • (sn_si.analyst), ou analyste du centre des opérations de sécurité (SOC), crée les entrées EDL et travaille avec les incidents de sécurité.
Vérifiez que vous utilisez la Palo Alto Networks - Next-Generation Firewall version OS 9.x et 10.x.	Cette intégration ne prend en charge Palo Alto Networks - Next-Generation Firewall que OS 9.0 et versions ultérieures.
Configurez tous les profils EDL, règles de politique de sécurité et profils de certificat comme Palo Alto Networks recommandé dans Palo Alto Networks la documentation.	Reportez-vous à la documentation générale et aux Palo Alto Networks exigences sur le site Web de la documentation de Paloalto Networks .
Vérifiez que vous avez téléchargé et configuré le certificat de l'autorité de certification racine Entrust™.	L'intégration nécessite ce certificat pour valider et authentifier la connexion sécurisée entre le serveur et le Now PlatformPalo Alto Networks - Next-Generation Firewall serveur. Pour plus d'informations sur la configuration du certificat, consultez « Configurer un profil de certificat » dans le Guide de l'administrateur de PAN-OS 10.0 . Pour le téléchargement, consultez Créer un profil de certificat pour le Palo Alto Networks - Next-Generation Firewallet Téléchargement des certificats racines .
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Configuration requise pour la version Madrid et ultérieure Pour la version Madrid et les versions ultérieures de la famille, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Cadre de travail de Security Integration

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	3. Security Support Common **4.** Orchestration de support de sécurité Pour en savoir plus sur la configuration de votre Now Platform instance pour l'intégration, consultez et .
Si votre organisation dispose Now Platform® de processus de gestion des changements et d'approbation pour la suppression des e-mails, vérifiez que l'option d'envoi/réception d'e-mail est activée.	Pour vérifier que l'option d'envoi/réception d'e-mail est activée dans votre Now Platform® instance, accédez à **Propriétés d'e-mail** > **Administration** > **Propriétés d'e-mail**. Dans la configuration des messages sortants, vérifiez que **les options Envoi d'e-mail** et **Réception d'e-mail** sont sélectionnées.

Procédure

Si vous n'avez pas installé l'application pour l'intégration, consultez et suivez les étapes pour l'installer.

Créer le rôle du compte API pour Palo Alto Networks - Next-Generation Firewall

Un rôle de compte API est requis dans votre Now Platform® instance pour cette intégration. Le nom d'utilisateur et le mot de passe associés à ce compte sont créés dans le Now Platform® et saisis afin Palo Alto Networks qu'ils s'authentifient Palo Alto Networks - Next-Generation Firewall auprès de lors Now Platform® de la récupération des entrées EDL.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
L'administrateur Now Platform® crée un rôle de compte API (sn_sec_panfw.api_account_access). Ce compte est utilisé exclusivement pour la saisie des informations d'identification requises pour l'authentification sur Palo Alto Networks afin que les pare-feux puissent récupérer les EDL à partir du Now Platform®. Il s'agit d'un compte d'utilisateur API distinct et unique dans l'instance Now Platform® affecté à l'administrateur Palo Alto Networks - Next-Generation Firewall .

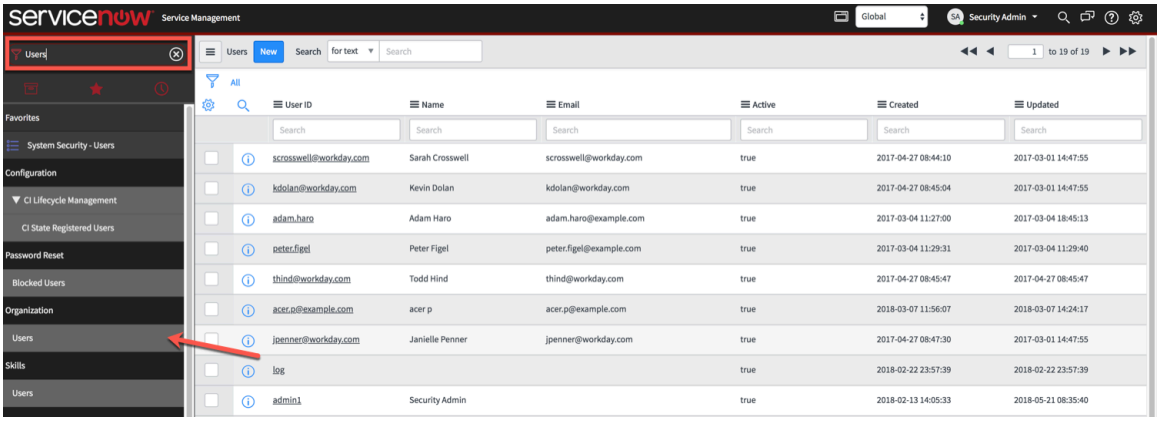
Procédure

1. Accédez à la **Tout** > **Organisation** > **Utilisateurs**.

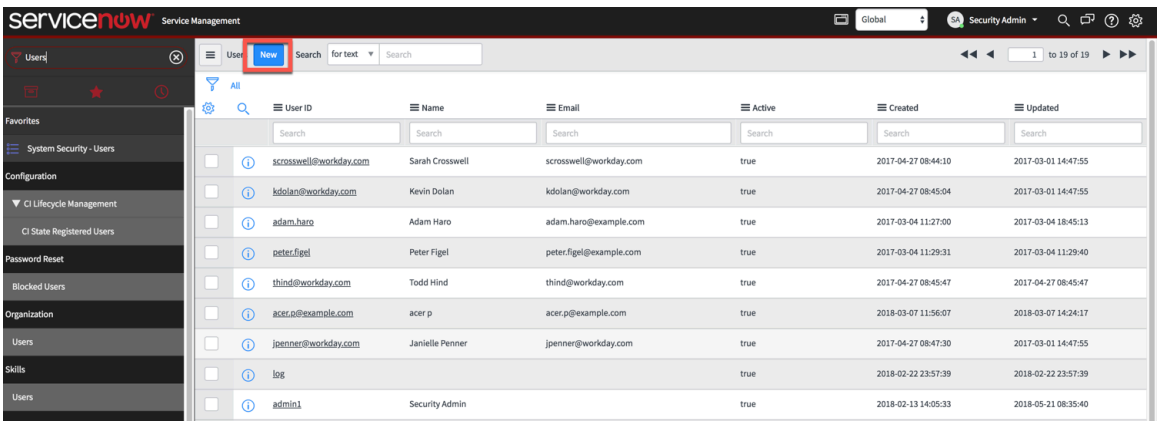
2. Cliquez sur le module **Utilisateurs** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur **Nouveau** dans la liste Utilisateurs qui s'affiche.



Un nouveau formulaire d'utilisateur s'affiche.

4. Remplissez le formulaire.

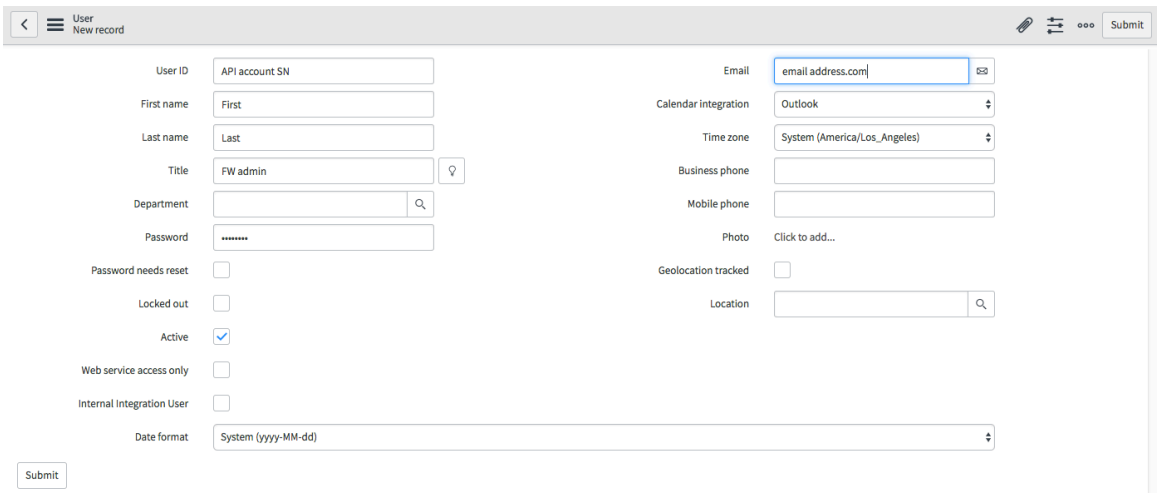
Remarque : Les valeurs d'ID d'utilisateur, de titre et d'adresse e-mail indiquées dans la table et la figure suivantes sont des exemples de valeurs.

Champ	Description
ID d'utilisateur	ID d'utilisateur unique pour le rôle dans votre Now Platform® instance. Cet ID d'utilisateur est entré dans le champ **Nom d'utilisateur** de la section **Authentification client** de la boîte de dialogue Listes dynamiques externes du Palo Alto Networks site. Un exemple est le `compte API SN.`
Prénom	Personne que vous affectez.
Nom de famille	Personne que vous affectez.
Titre	Fonction, par exemple, `FW admin`.
Mot de passe	Mot de passe unique créé pour ce rôle. Ce mot de passe est saisi dans le champ **Mot de passe** de la section **Authentification client** de la boîte de dialogue Listes

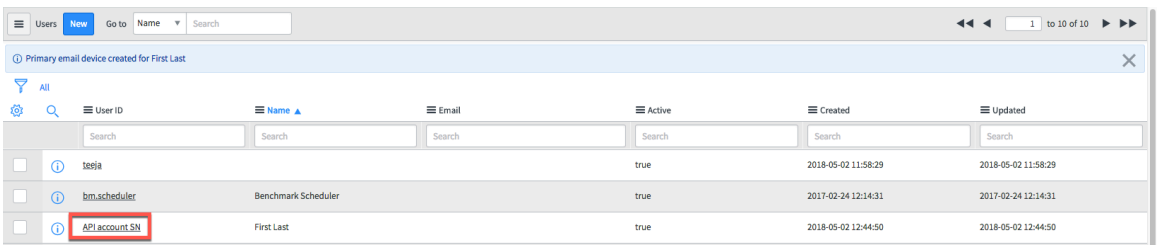
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

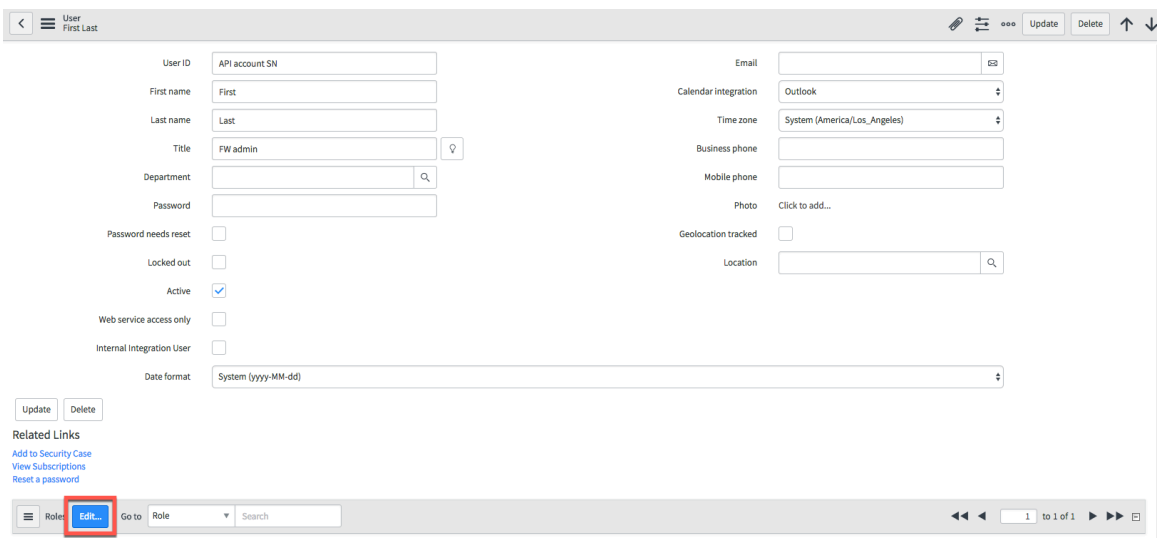
Champ	Description
	dynamiques externes du Palo Alto Networks site.
E-mail	Adresse e-mail unique.



5. Cliquez sur **Envoyer**.
   Une fois soumis, vous pouvez affecter le rôle.
6. Dans la liste Utilisateurs dans la colonne **ID d'utilisateur**, cliquez sur le nom de l'ID d'utilisateur que vous avez saisi, par exemple le `compte d'API SN`.



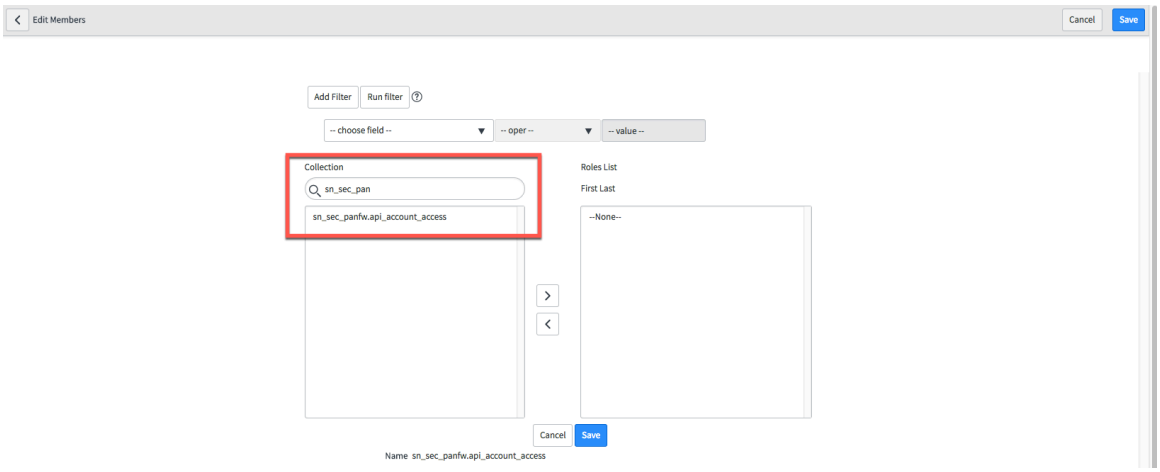
7. Dans l'enregistrement ouvert de la section **Rôles**, cliquez sur Modifier.



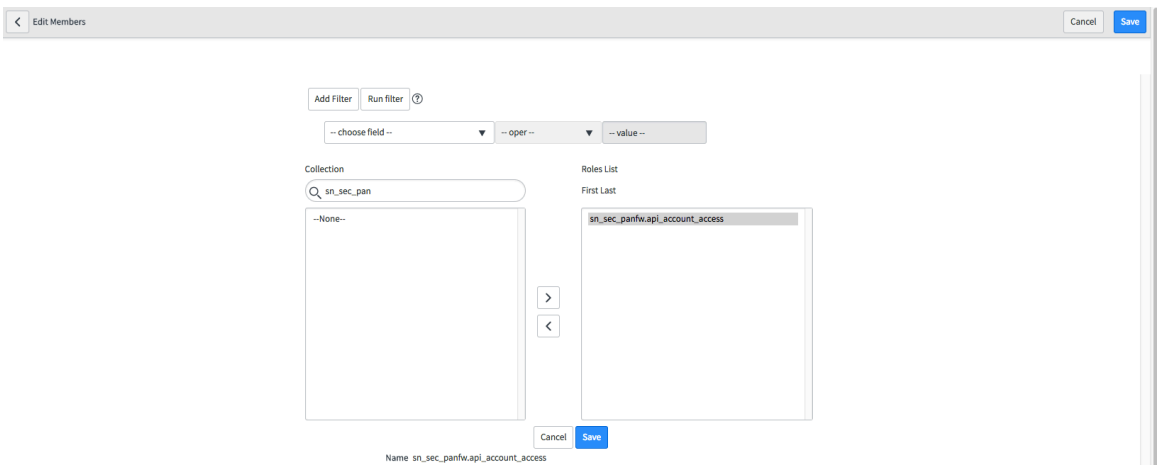
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Sur le formulaire **Modifier les membres**qui s'affiche, saisissez `sn_sec_panfw.api_account_access` dans le champ **Collection** . Sous le champ **Collecte** , le rôle s'affiche dans la colonne.



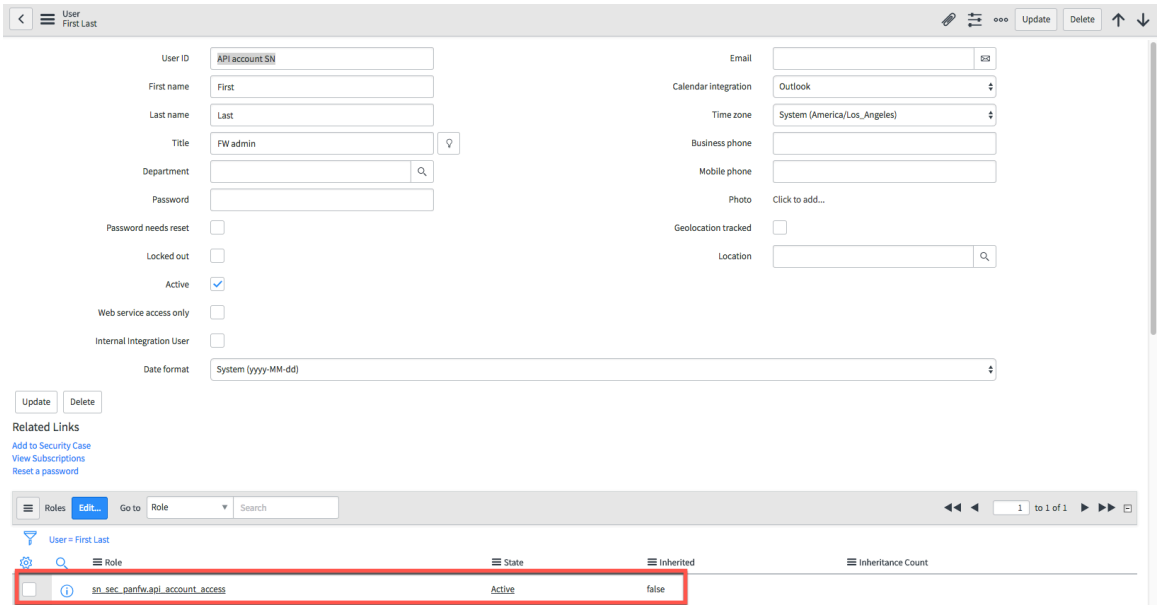
9. Dans la colonne **Collection** , sélectionnez, puis déplacez `sn_sec_panfw.api_account_access` vers la **liste des rôles**.



10. Cliquez sur **Enregistrer**.
11. Accédez à **Utilisateurs** et, dans la colonne **Utilisateur** de la liste, cliquez sur le nom de l'ID que vous avez créé pour le rôle (`compte API SN`) .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'enregistrement utilisateur s'affiche. Cet enregistrement vérifie que le compte d'utilisateur a été affecté. **L'État** est actif et le rôle n'est pas hérité.

Listes dynamiques externes prises en charge pour Palo Alto Networks - Next-Generation Firewall

L'intégration ServiceNow Palo Alto Networks - Next-Generation Firewall prend en charge les listes dynamiques externes (EDL) qui acceptent les observables d'adresse IP, d'URL et de domaine.

Observables et EDL pris en charge

Une liste dynamique externe est un fichier texte hébergé sur un serveur Web externe, qui pour cette intégration est l'instanceNow Platform. Ils Palo Alto Networks - Next-Generation Firewall peuvent ensuite importer des objets (adresses IP, URL, domaines) inclus dans la liste et appliquer la stratégie. Pour appliquer la politique aux entrées EDL, la liste est référencée dans une règle de politique ou un profil.

Cette intégration prend en charge trois types d'EDL :

- IP (cela inclut une seule adresse IP, ainsi que des blocs CIDR (plages) d'adresses).
- URL
- Domaine

La table suivante répertorie les descriptions des observables pris en charge par cette intégration et des exemples de formats pour chaque type.

Observables pris en charge et exemples de formats

Observable	Exemples de formats	Description
Adresse IP	• 95.153.103.54 (IPv4) • (IPv6) : 2001:00B8:130F :FE03:0000:09C0:080F :130B	Représente une adresse d'interface unique et distincte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Observables pris en charge et exemples de formats (suite)

Observable	Exemples de formats	Description
		L'intégration prend en charge les formats IPv4, IPv6 et CIDR. La prise en charge des observables d'adresse IP inclut des plages CIDR (Classless Inter-Domain Routing), par exemple, 95.153.100.0/22. Remarque : Un message d'erreur s'affiche lorsque vous essayez d'associer une seule adresse IP à un EDL que vous avez déjà bloqué dans le cadre d'une plage CIDR. Par exemple, l'adresse unique 95.153.103.54 fait partie de la plage CIDR représentée par 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• www.example.com • www.example.com/article.html • example.com • *.example.com	Les caractères génériques sont pris en charge. Ils Now Platform reforment les entrées d'URL pour se conformer aux exigences de Palo Alto Networks format de l'EDL.
Domaine	• www.example.com • example.com • mail.example.com	Les caractères génériques ne sont pas pris en charge.

Pour plus d'informations sur les directives de formatage et les EDL, consultez « Directives de formatage pour une liste dynamique externe » dans le Guide de l'administrateur de PAN-OS 10.0 sur le Palo Alto Networks site Web.

Créer un EDL pour le pare-feu de nouvelle génération Palo Alto Networks

Créez une liste dynamique externe (EDL) dans votre Now Platform instance. Une fois les incidents approuvés et activés, vous pouvez créer des entrées pour les EDL à partir des observables identifiés comme malveillants sur Now Platform Réponse aux incidents de sécurité les incidents (SIR) et demander l'approbation pour les bloquer.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Créez l'EDL sur votre Now Platform instance afin que le pare-feu puisse importer les objets (adresses IP, URL, domaines) inclus dans la liste et appliquer la stratégie. Pour appliquer la politique aux entrées EDL, la liste est référencée dans une règle de politique ou un profil.

Les figures de la section suivante sont affichées lorsque **les formulaires à onglets** sont désactivés dans les paramètres système. Pour plus d'informations sur la sélection et l'effacement des formulaires à onglets, reportez-vous à la section « Affichage des formulaires à onglets » dans .Configurer la mise en page du formulaire

Procédure

1. Une fois l'installation de l'application terminée, accédez à **Intégrations** > **Configurations d'intégration**.
2. Localisez la Palo Alto Networks - Next-Generation Firewall vignette et cliquez sur **Configurer**.



3. Cliquez sur **Créer une nouvelle liste d'EDL**.



4. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Palo Alto Networks Formulaire de liste dynamique externe de pare-feu

Champ	Description
Nom	Palo Alto Networks Nom de la liste dynamique de pare-feu. Incluez le type d'observable (URL, IP, domaine) dans ce champ afin que l'analyste de sécurité puisse facilement reconnaître l'intention de l'EDL par son nom. Le nom doit également indiquer clairement à quelle stratégie de pare-feu ces objets EDL sont mappés. Voici quelques exemples de noms EDL : adresse IP de programme malveillant sortante ou URL d'hameçonnage sortante.
Actifs	Cette case est décochée par défaut pour indiquer que l'EDL est inactif. Lorsqu'elle est inactive, l'EDL ne peut pas recevoir d'entrées supplémentaires. Lorsque la case est cochée, l'EDL est activée et disponible pour les entrées EDL.
Balise d'affichage	La case à cocher est sélectionnée par défaut pour baliser automatiquement l'observable et l'enregistrement d'incident de sécurité associé si l'observable est bloqué sur un EDL. Lorsque cette option est sélectionnée, les champs Type de balise et Balise EDL pour les observables sont disponibles sur le formulaire. **Remarque :** Un nom de balise est créé par défaut à partir de la valeur que vous saisissez dans le champ **Nom** avec un préfixe EDL, par exemple, EDL-Malware OutBound IP. Vous pouvez modifier le nom et la couleur de la balise. Voir : (Facultatif) Modifier le nom de la balise de sécurité pour Palo Alto Networks - Next-Generation Firewall. Le nom de la balise s'affiche dans le champ Balise EDL pour les observables une fois l'EDL enregistrée. Lorsque la case est décochée, aucune balise n'est créée, et les champs Type de balise et Balise EDL pour les observables ne sont pas disponibles sur le formulaire.
Type d'observable	Sélectionnez un type d'observable que cette EDL accepte dans la liste de choix : IP (y compris CIDR), URL ou domaine.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

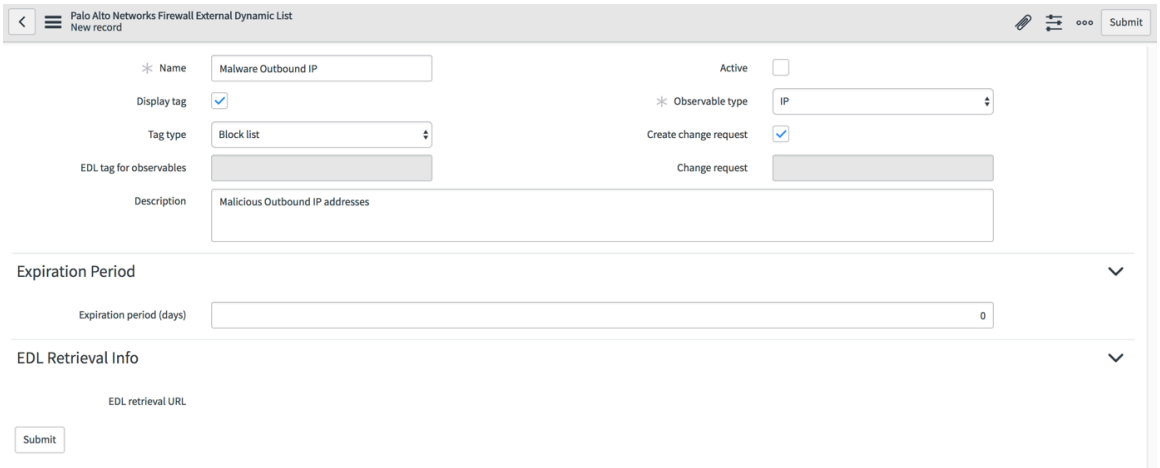
Champ	Description
Type de balise	Balises disponibles dans la liste de choix. Une liste de blocs est une liste d'observables que vous souhaitez Palo Alto Networks - Next-Generation Firewall bloquer. Une liste d'autorisation est une liste d'observables que vous souhaitez autoriser Palo Alto Networks - Next-Generation Firewall . Par défaut, la couleur de la balise de la liste de blocs est le noir et la couleur de la balise de la liste d'autorisation est le gris. Vous pouvez changer la couleur. Voir : (Facultatif) Modifier le nom de la balise de sécurité pour Palo Alto Networks - Next-Generation Firewall.
Création d'une demande de changement	Cette case à cocher est sélectionnée par défaut pour créer automatiquement une demande de changement et des tâches de changement dans votre Now Platform instance, qui sont jointes à l'enregistrement EDL. La demande de changement est utilisée pour configurer l'URL de récupération de la liste EDL dans le Palo Alto Networks - Next-Generation Firewall serveur. Cette option est recommandée si votre administrateur de pare-feu utilise également le pour les modifications de politique ou de règle de Now Platform pare-feu. Si vous créez une demande, une fois qu'elle est fermée, la liste EDL est automatiquement activée. Décochez la case pour activer manuellement l'EDL après avoir reçu une notification par e-mail de l'administrateur du pare-feu indiquant que la configuration est terminée Palo Alto Networks . Lorsque la case à cocher Créer une demande de changement est désactivée, le champ Demande de changement n'est plus disponible.
Balise de l'EDL pour les observables	Ce champ n'est affiché que si la case Balise d'affichage est cochée. Le champ est automatiquement renseigné après l'enregistrement de l'EDL avec une valeur par défaut dans le champ Nom.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

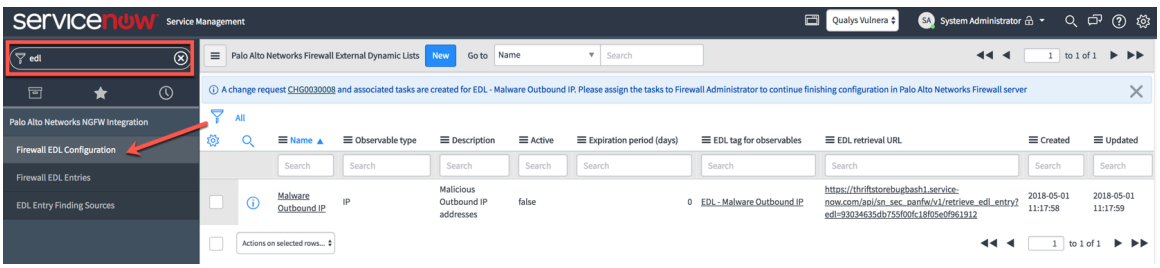
Champ	Description
	Pour plus d'informations sur la modification du nom et de la couleur de la balise par défaut, consultez (Facultatif) Modifier le nom de la balise de sécurité pour Palo Alto Networks - Next-Generation Firewall
Demande de changement	Lorsque la case à cocher Créer une demande de changement est sélectionnée, le numéro de la demande de changement s'affiche sur l'instance Now Platform une fois l'EDL enregistrée. Lorsque la case à cocher Créer une demande de changement est désactivée, ce champ n'est pas affiché.
Description	Description de la liste dynamique du pare-feu Palo Alto Networks. Le nom contient généralement les types de sites et d'observables que vous vous attendez à voir sur cette EDL, et vous pouvez utiliser ce champ pour plus de détails.
Période d'expiration (jours)	Période d'expiration de l'EDL. 0 (valeur par défaut) indique que l'entrée EDL n'expire jamais. Si vous modifiez cette valeur, cette entrée est active pendant le nombre de jours que vous entrez. Vous pouvez entrer une valeur minimale de 1, mais il n'y a pas de valeur maximale. Par exemple, si vous entrez `30` jours à 14 h 01 le 1er mai, l'EDL expirera à 14 h 01 le 31 mai. Toutes les entrées de cet EDL héritent alors de cette valeur par défaut, à moins que vous ne remplaciez la valeur sur la base d'une entrée individuelle.

Traduction automatique

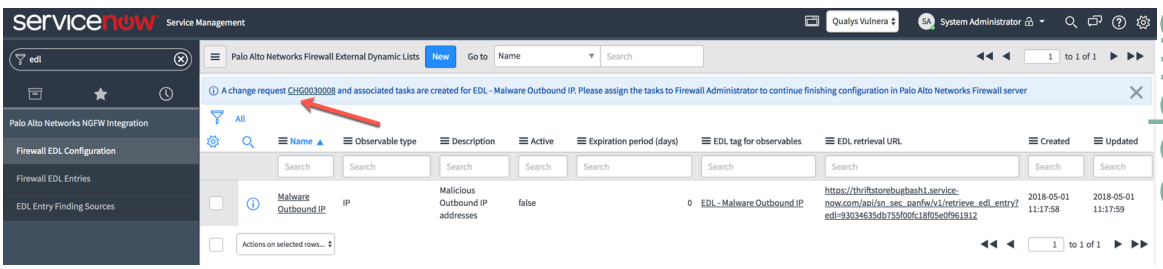
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
6. Si la liste des listes dynamiques externes du pare-feu Palo Alto Networks n'est pas affichée, accédez à **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu** et cliquez sur **Configuration de l'EDL du pare-feu**.



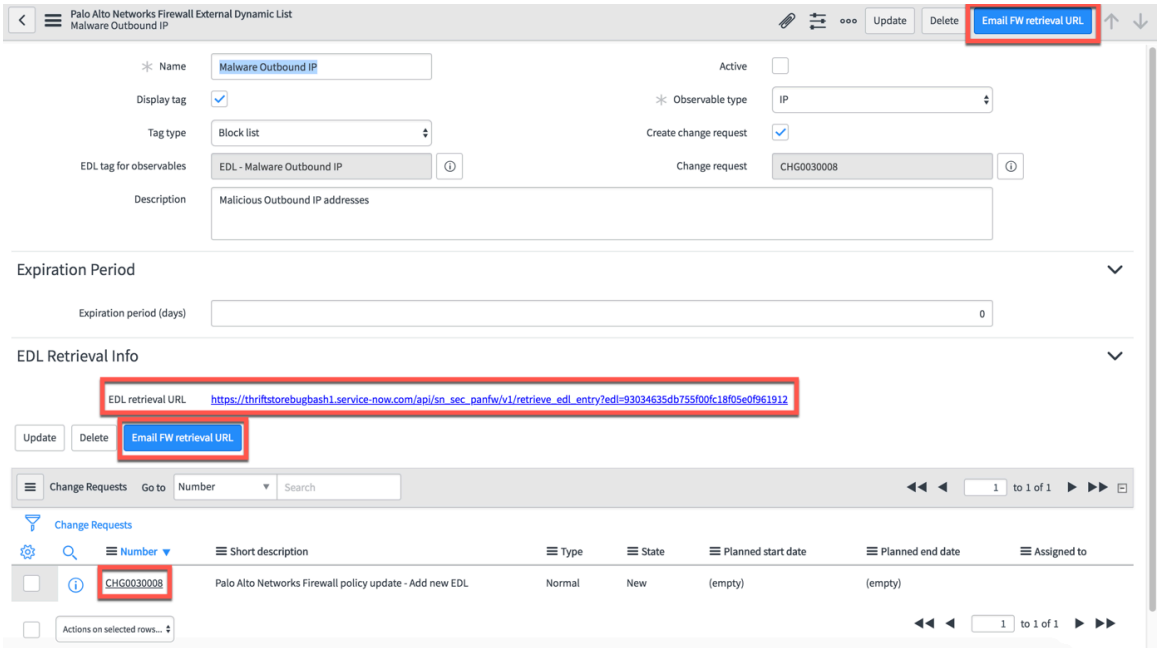
Le nouvel EDL s'affiche. Le statut de l'EDL est toujours inactif (`faux`), ce qui signifie que l'EDL n'est pas disponible pour accepter les entrées. Si **l'option Créer une demande de changement** a été configurée, un message s'affiche indiquant qu'une demande de changement et que des tâches ont été créées dans votre Now Platform instance.



7. Dans la colonne **Nom** , cliquez sur un élément pour ouvrir l'enregistrement. L'enregistrement EDL s'affiche. Cet exemple montre une EDL IP sortante de programme malveillant. Les champs, options et liens suivants sont affichés dans le nouvel enregistrement après soumission et décrits dans la table suivante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



URL de récupération et liens de demande de changement sur l'enregistrement EDL

Option	Description
URL de récupération des TR e-mails	Envoie par e-mail à l'administrateur Palo Alto Networks de pare-feu un avis indiquant que le lien EDL est disponible pour configuration.
URL de récupération de l'EDL	Cette URL est placée dans le champ **Source** de la boîte de dialogue d'authentification des listes dynamiques externes de l'onglet **Créer** une Palo Alto Networks liste du site Web. Le lien URL utilisé par l'administrateur Palo Alto Networks de pare-feu pour la configuration dans le Palo Alto Networks pare-feu est automatiquement généré et affiché. **Remarque :** Si vos paramètres système sont définis sur **Formulaires à onglets**, ce lien s'affiche dans l'onglet Informations sur la **récupération de l'EDL** au bas de l'enregistrement.
Now Platform Demande de changement	Un lien vers l'enregistrement de demande de changement s'affiche dans la section Demandes de changement lorsqu'elle est configurée, et le numéro de la demande s'affiche dans le champ Demande de changement.
Mettre à jour	Modifiez les données et mettez à jour les champs modifiables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Supprimer	Supprimer l'enregistrement.

8. Créez et ajoutez d'autres EDL selon vos besoins.
   Les EDL sont affichées dans la Palo Alto Networks liste des listes dynamiques externes.

Que faire ensuite
Activer un EDL manuellement ou avec une demande de Now Platform changement.

Activer un EDL pour Palo Alto Networks - Next-Generation Firewall

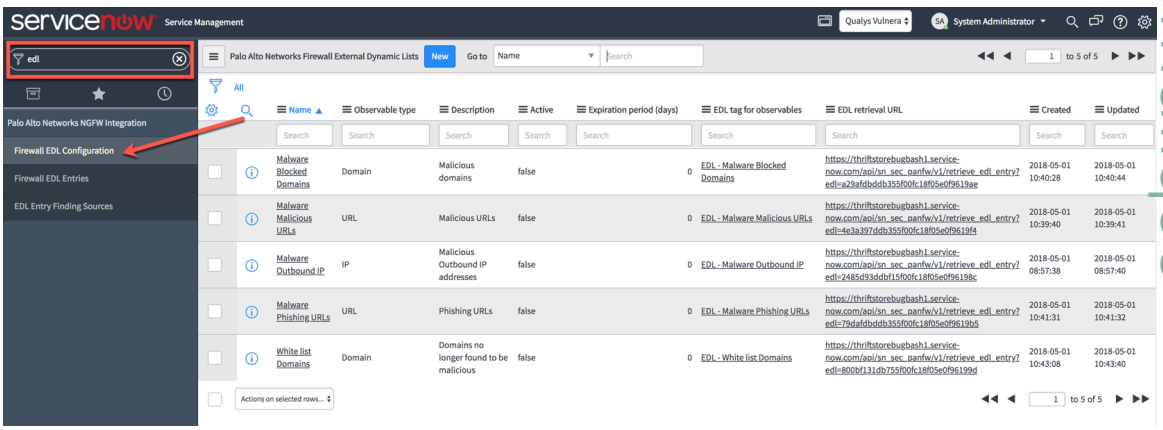
Une fois que la liste dynamique externe (EDL) a été créée dans Ur Now Platform® et que l'URL est disponible, l'administrateur Palo Alto Networks de pare-feu configure l'EDL dans le Palo Alto Networks - Next-Generation Firewallfichier . L'URL de récupération est utilisée par l'administrateur de pare-feu Palo Alto Networks pour configurer l'EDL dans le Palo Alto Networks - Next-Generation Firewall serveur. Avant de pouvoir accepter les entrées EDL, celle-ci doit être configurée et activée dans Palo Alto Networks le Now Platform®fichier .

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Une fois l'EDL configuré, en tant qu'administrateur des incidents de sécurité, vous pouvez activer l'EDL manuellement ou l'EDL est automatiquement activée lorsqu'une Now Platform® demande de changement est terminée. L'EDL doit être approuvée et passée de l'état inactif à l'état actif avant de pouvoir accepter les entrées EDL.

Procédure

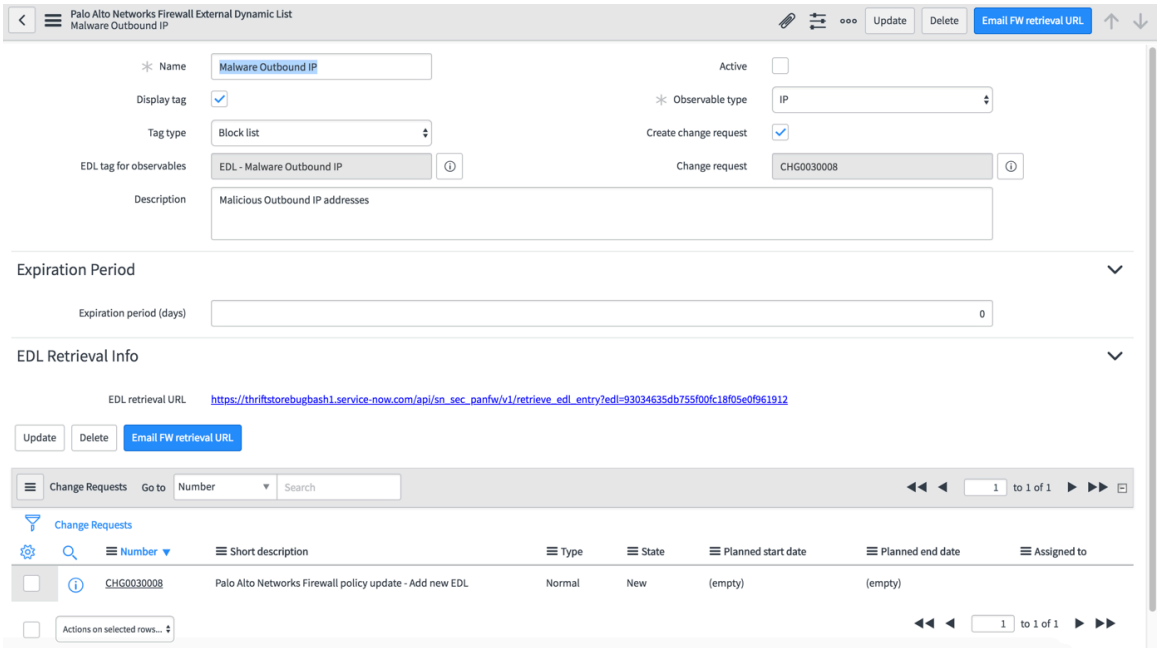
1. Accédez à la **Tout** > **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu** et sélectionnez le module **Configuration de l'EDL du pare-feu** .



2. Dans la liste des listes dynamiques du pare-feu Palo Alto Networks qui s'affiche, sélectionnez votre nouvel EDL dans la colonne Nom.
3. Sur l'enregistrement qui s'affiche, notez les boutons **d'URL de récupération des TR par e-mail** , le lien d'URL de récupération EDL actif et, s'il est configuré, la demande de Now Platform® changement dans la section Demandes de changement.
   Assurez-vous que la case **Actif** n'est pas cochée.

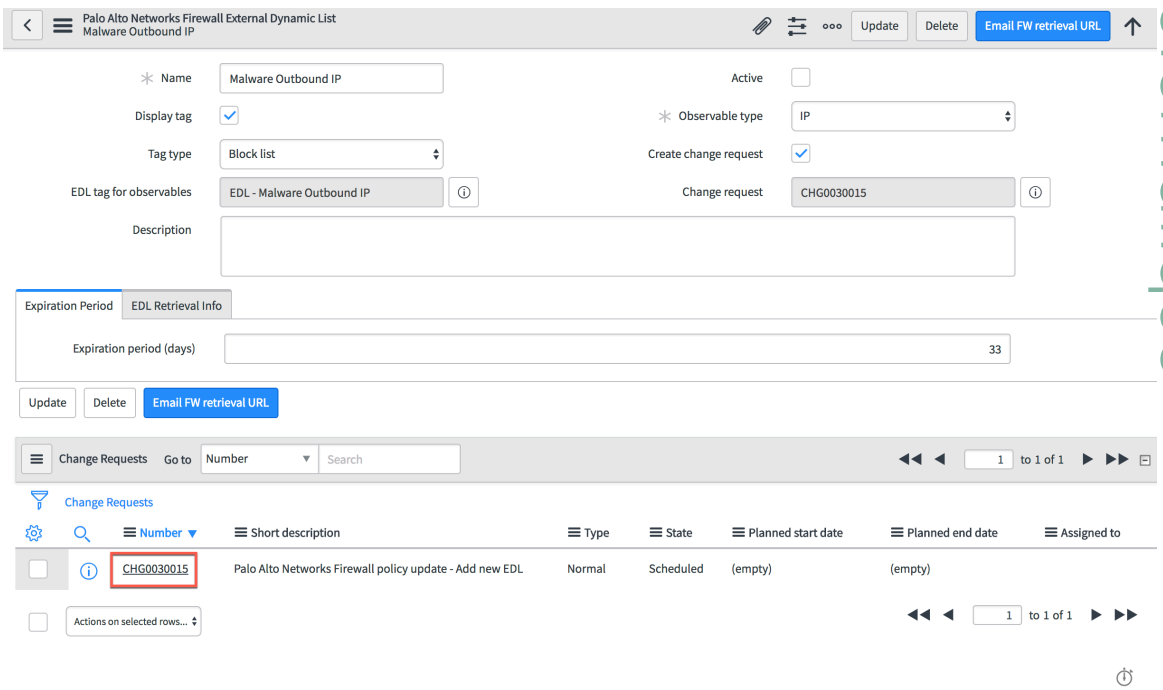
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Lorsque **les formulaires à onglets** sont désactivés dans les paramètres système, l'URL de récupération de l'EDL apparaît dans la section **Informations sur la récupération de l'EDL** , comme illustré dans la figure précédente.

La figure suivante montre les **informations de récupération de l'EDL** affichées sous la forme d'un onglet avec des **formulaires à onglets** sélectionnés dans les paramètres de votre système. Cliquez sur l'onglet **Informations de récupération EDL** pour afficher l'URL de récupération. Le lien vers la demande de changement (**CH0030015**) s'affiche également.



4. Pour terminer la configuration et déplacer l'EDL d'inactif à actif, vous devez choisir l'une des options suivantes pour avertir l'administrateur de pare-feu que l'URL de récupération est disponible.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Cliquez sur **URL de récupération des TR envoyés par e-mail**.	Envoyez l'URL de récupération de l'EDL par e-mail directement à l'administrateur du pare-feu. Cette option permet à l'administrateur du pare-feu de terminer la configuration sur la Palo Alto Networks plateforme. Choisissez cette option si l'administrateur du pare-feu n'utilise pas le Now Platform® fichier . **Remarque :** L'administrateur d'incident de sécurité active manuellement l'EDL dès réception de Now Platform® l'avis indiquant que la Palo Alto Networks - Next-Generation Firewall configuration est terminée. Voir : Activer manuellement un EDL pour Palo Alto Networks - Next-Generation Firewall.
Terminez la demande de Now Platform® changement et affectez les tâches de configuration à l'administrateur de pare-feu.	Cette option n'est disponible que si l'administrateur Palo Alto Networks de pare-feu utilise également le , et que Now Platform®les Now Platform® processus de gestion et d'approbation des changements sont configurés. **Remarque :** Les utilisateurs disposant du rôle sn_si.admin peuvent approuver la demande de Now Platform® changement. Une fois les tâches de configuration terminées et la demande de changement fermée, l'EDL est activé automatiquement. Voir : Activer un EDL pour Palo Alto Networks - Next-Generation Firewall avec une demande de changement.

Après avoir notifié l'administrateur de pare-feu que l'URL de récupération est disponible et confirmé que l'EDL a été configurée dans Palo Alto Networks, en tant qu'administrateur des incidents de sécurité, l'étape suivante consiste à activer l'EDL. Soit vous activez l'EDL manuellement, soit, si la configuration est configurée, vous utilisez le formulaire de Now Platform demande de changement pour activer l'EDL.

Information associée

Configurer un EDL dans Palo Alto Networks - Next-Generation Firewall

Activer manuellement un EDL pour Palo Alto Networks - Next-Generation Firewall

Si l'administrateur du pare-feu Palo Alto Networks n'utilise pas le Now Platform, et que vous êtes directement informé que le Palo Alto Networks - Next-Generation Firewall est configuré, vous pouvez activer manuellement la liste dynamique externe (EDL).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Dans Palo Alto Networks, affectez un objet EDL, une politique et l'URL source à l'EDL que vous avez créée. Pour plus d'informations sur la configuration de l'EDL dans Palo Alto Networks, Palo Alto Networks - Next-Generation Firewall reportez-vous à la section Configurer un EDL dans Palo Alto Networks - Next-Generation Firewall.

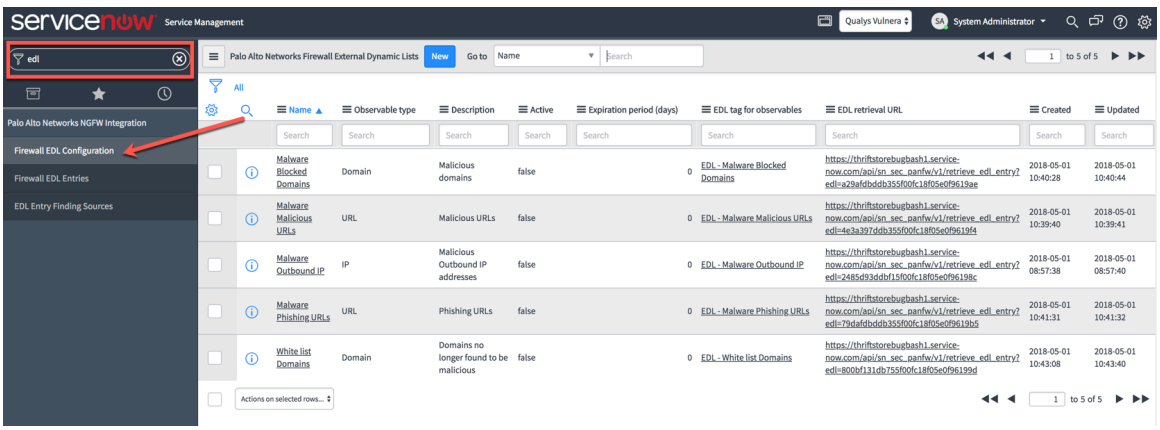
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

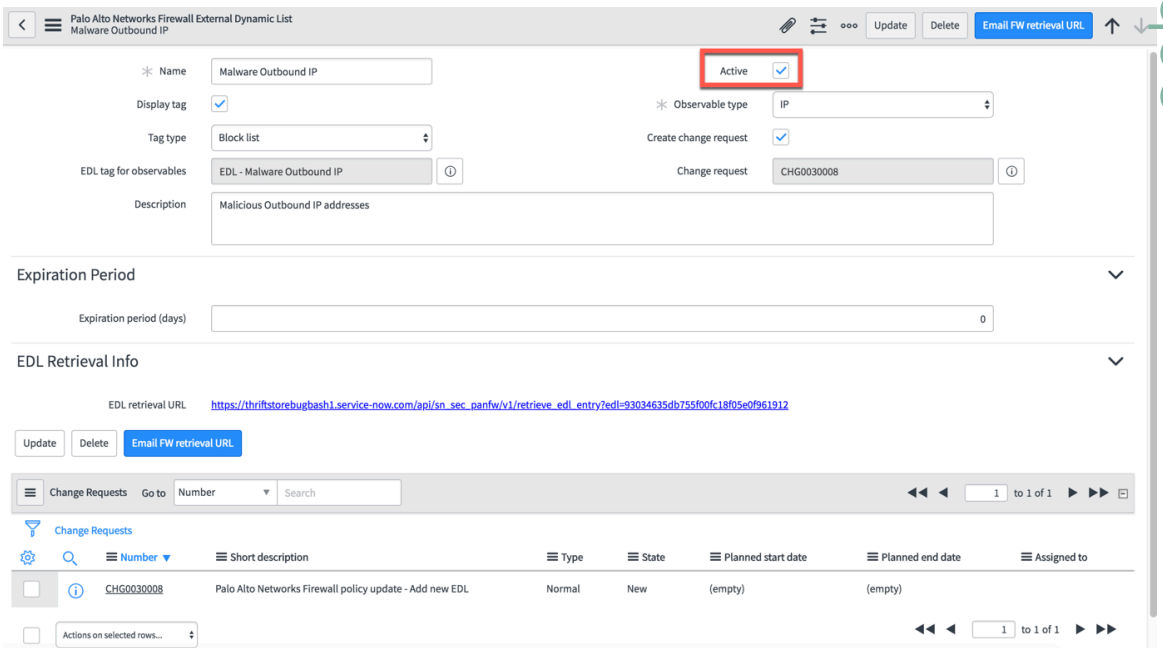
En tant qu'administrateur d'incident Now Platform de sécurité, vous êtes notifié par l'administrateur de Palo Alto Networks pare-feu lorsque la configuration de l'EDL est terminée dans le Palo Alto Networks - Next-Generation Firewall.

Procédure

1. Accédez à la **Tout** > **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu**.



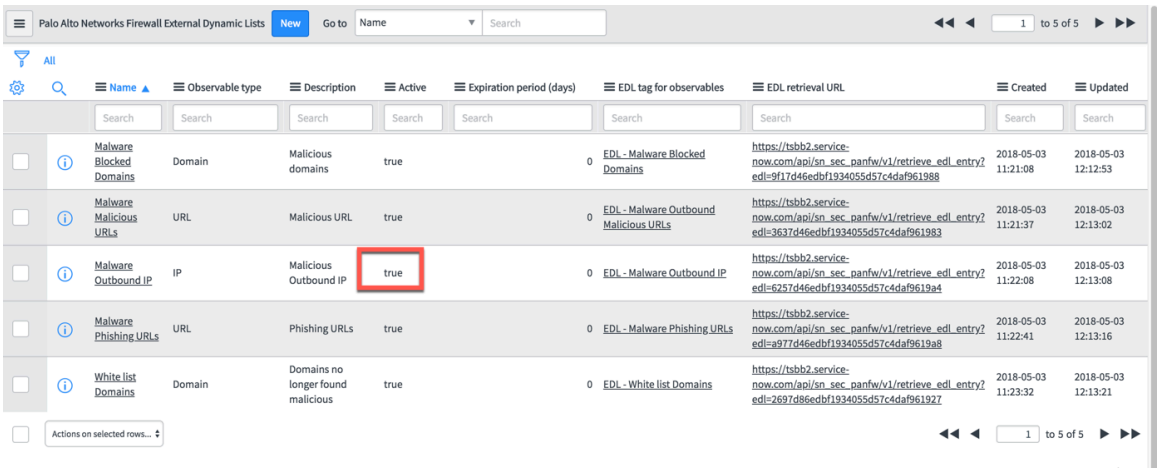
2. Sélectionnez le module **Configuration de l'EDL du pare-feu** .
3. Dans la liste des listes dynamiques externes du pare-feu Palo Alto Networks, cliquez sur un élément dans la colonne **Nom** pour l'ouvrir.
4. Sur l'enregistrement qui s'ouvre, cochez la case **Actif** .



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Mettre à jour**.
   Dans la colonne **Active** de la liste Listes dynamiques externes du pare-feu Palo Alto Networks, le `vrai` s'affiche pour l'état de l'EDL.



Résultats
L'EDL est activée et prête à recevoir les entrées EDL

Que faire ensuite
Soumettre des entrées EDL à partir d'un incident de sécurité ou de la liste de blocage.

Configurer un EDL dans Palo Alto Networks - Next-Generation Firewall

L'administrateur Palo Alto Networks de pare-feu configure un EDL sur le Palo Alto Networks - Next-Generation Firewall Une fois l'URL de récupération notifiée, elle est disponible dans le Now Platform. Avant de pouvoir accepter les entrées EDL, l'EDL doit être configurée dans Palo Alto Networkset activée dans le Now Platform® fichier .

Avant de commencer
Rôle requis : Palo Alto Networks administrateur de pare-feu

Pourquoi et quand exécuter cette tâche
L'administrateur Palo Alto Networks - Next-Generation Firewall crée un objet EDL et affecte l'URL source (récupération) et la politique à l'EDL. Ces tâches sont effectuées avant Palo Alto Networks l'activation de l'EDL dans le Now Platform.

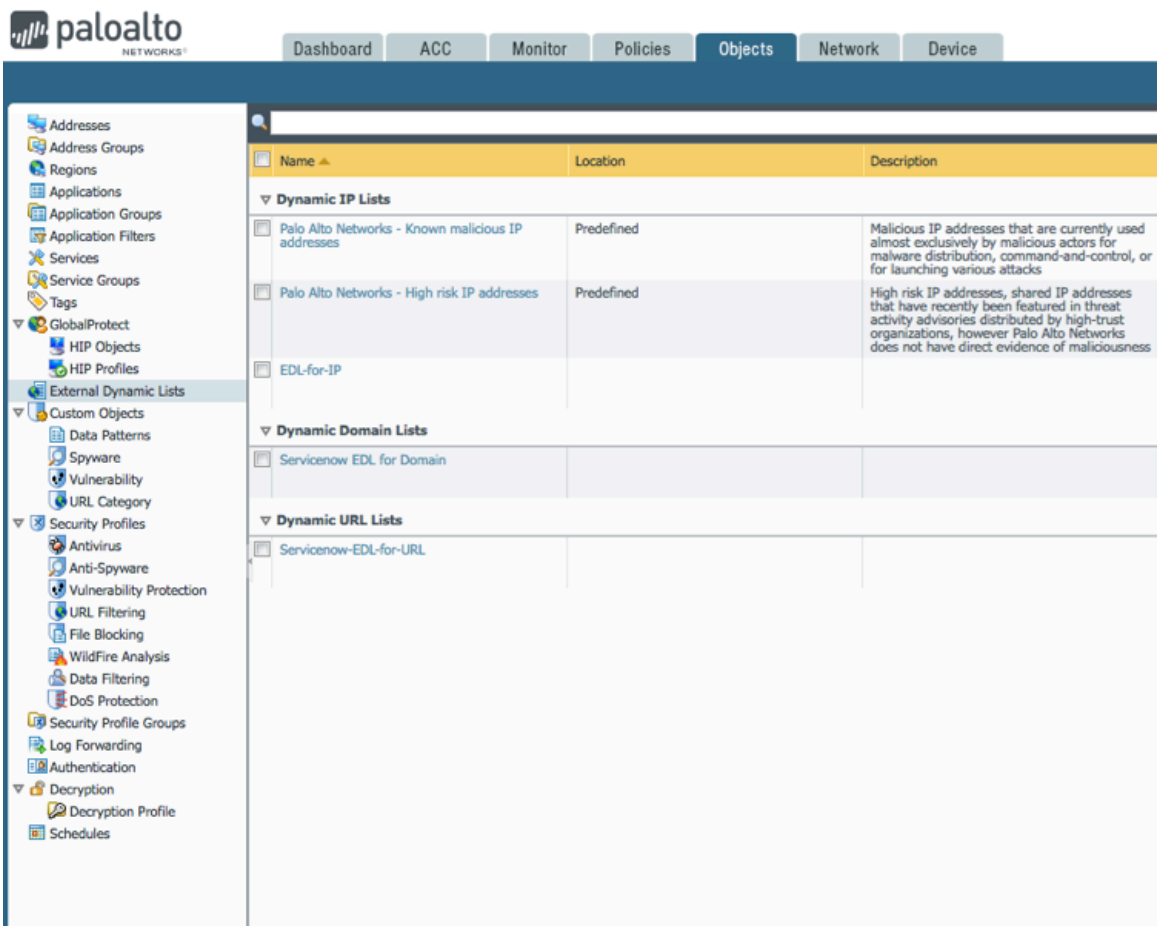
Les images de la section suivante sont utilisées avec permission et sont PRIVILÉGIÉES et PROPRIÉTAIRES.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

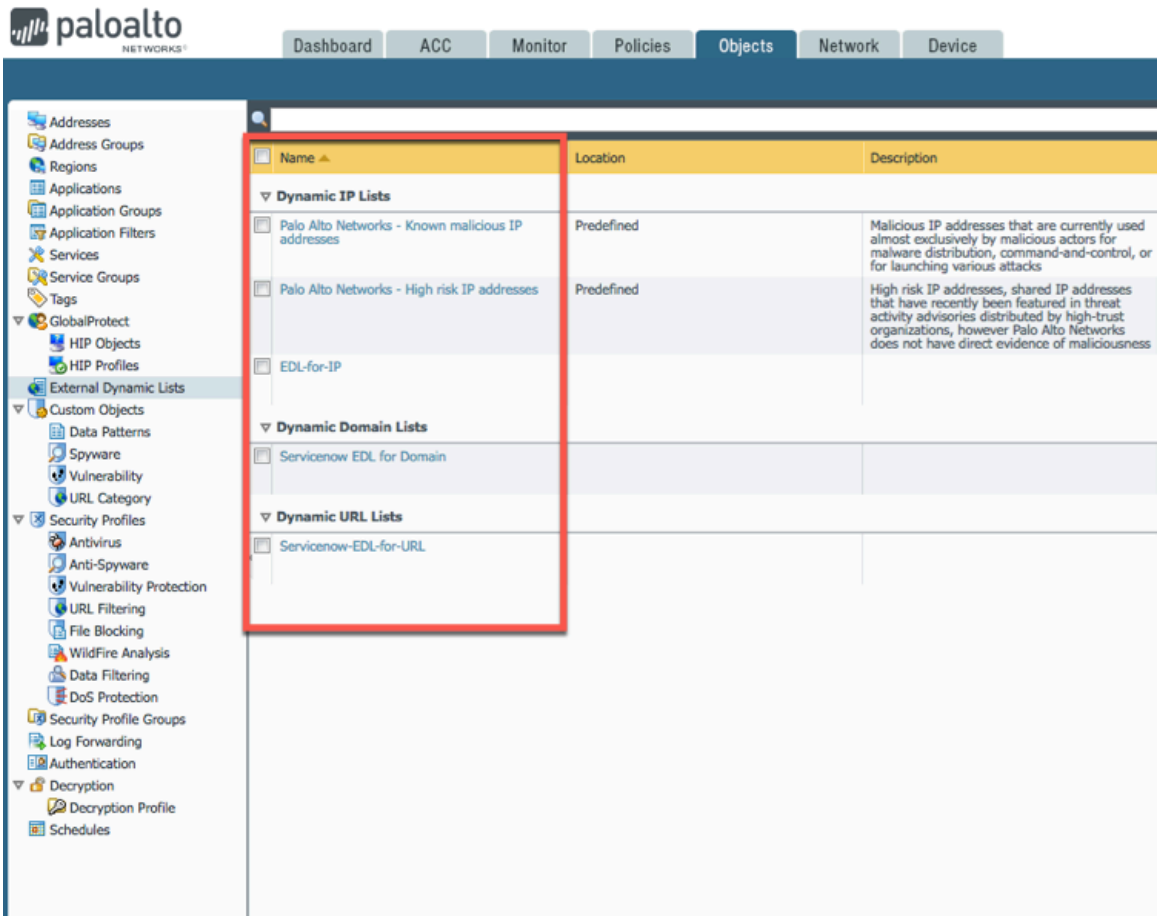
1. Si vous n'avez pas configuré l'EDL sur le pare-feu, accédez à **Listes externes dynamiques** > **Objets** in Palo Alto Networks.



2. Dans la colonne **Nom**, sélectionnez l'EDL ServiceNow que vous souhaitez configurer dans la liste, par exemple, **EDL ServiceNow pour l'URL.**

Traduction automatique

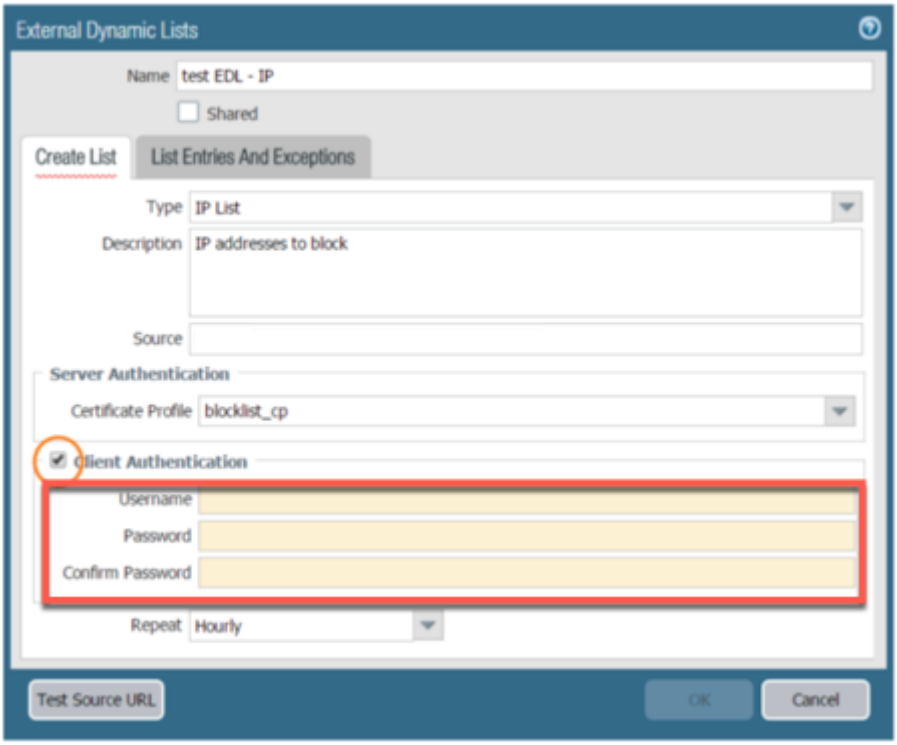
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



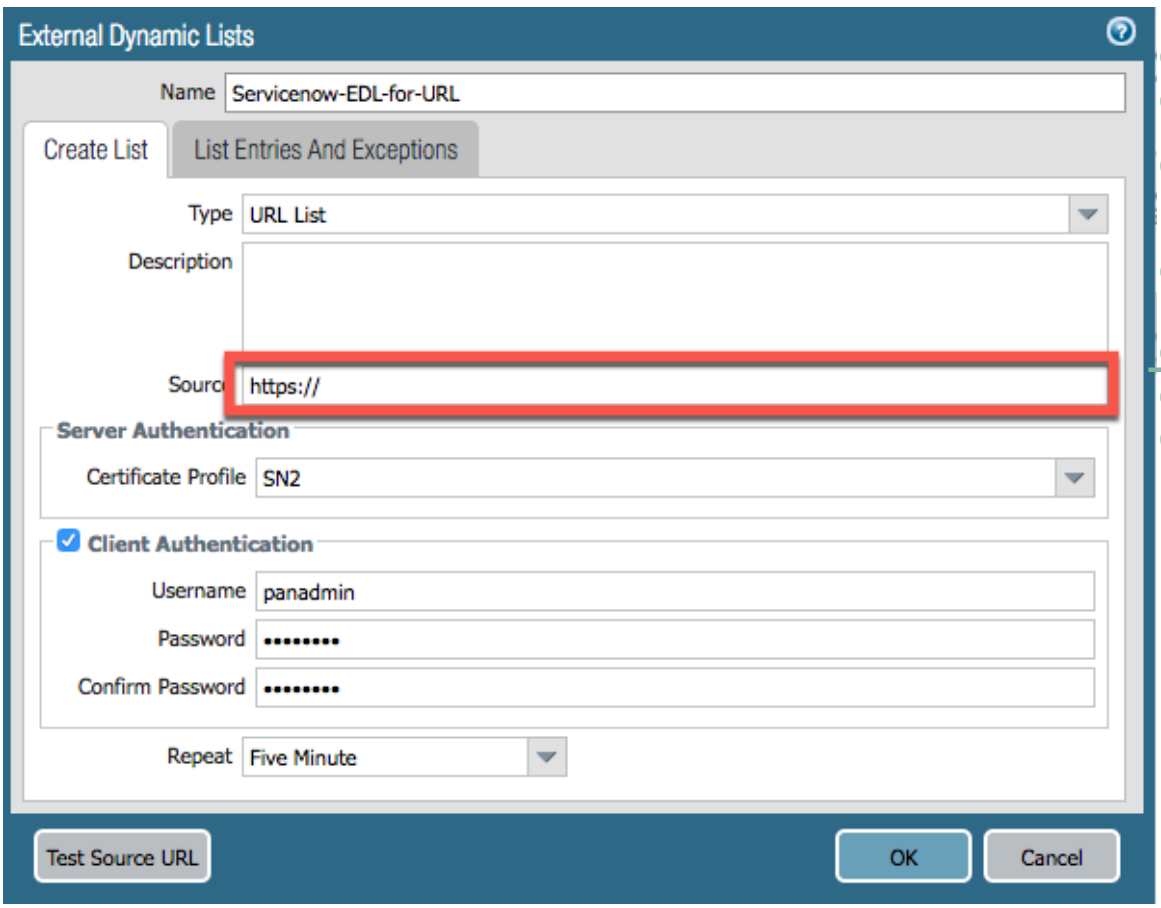
3. Dans la boîte de dialogue Listes dynamiques externes, entrez le nom d'utilisateur et le mot de passe à authentifier avec le Now Platform®.
Ces informations d'identification correspondent au nom d'utilisateur et au mot de passe que vous avez créés pour le rôle de compte API (sn_sec_panfw.api_account_access) dans votre ServiceNow instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans le champ Source, entrez l'URL qui a été générée sur la liste EDL de votre ServiceNow instance.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez un profil de certificat dans la liste de choix, `SN2`, par exemple.
6. Cliquez sur OK.

Activer un EDL pour Palo Alto Networks - Next-Generation Firewall avec une demande de changement

S'il est configuré, le formulaire de demande de ServiceNow changement est utilisé pour activer la liste dynamique externe (EDL). Cette option est recommandée si votre administrateur de pare-feu utilise également le pour les modifications de politique ou de règle de Now Platform pare-feu. L'EDL est activé automatiquement et prêt à recevoir des entrées EDL lors de la fermeture de la Now Platform demande de changement.

Avant de commencer

Remarque : Les figures de la section suivante sont affichées avec **les formulaires à onglets** sélectionnés dans les paramètres du système. Pour plus d'informations sur la sélection et l'effacement des formulaires à onglets, consultez la section intitulée Afficher les formulaires à onglets dans Configuration de la mise en page du formulaire sur le site web de la documentation du produit ServiceNow .

Rôle requis : sn_si.admin pour approuver la demande de changement et les tâches de changement

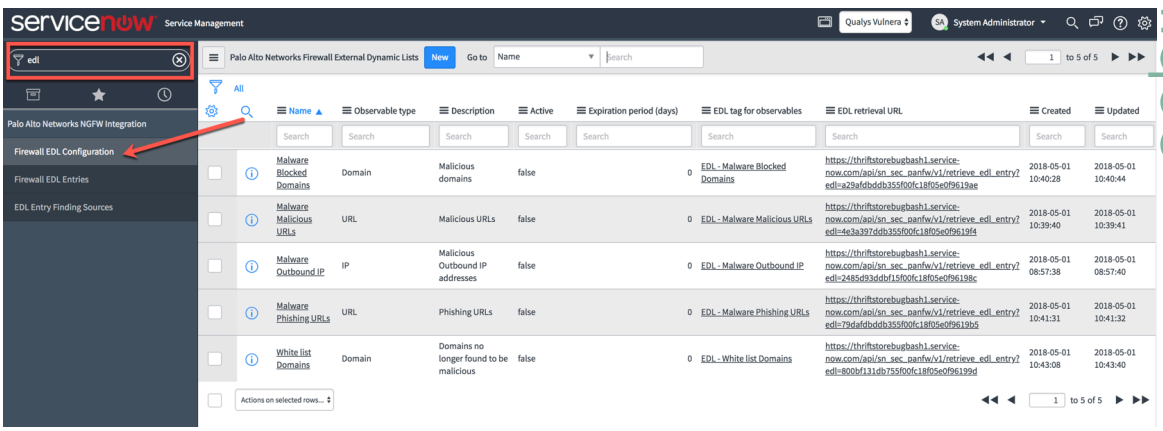
Palo Alto Networks administrateur de pare-feu pour l'exécution des tâches de configuration dans Palo Alto Networks

Pourquoi et quand exécuter cette tâche

Si elle est configurée, surveillez votre Now Platform demande de changement et affectez-lui toutes les tâches requises pour configurer le Palo Alto Networks - Next-Generation Firewall. Une fois ces tâches terminées, fermez la Now Platform demande de changement pour activer automatiquement l'EDL.

Procédure

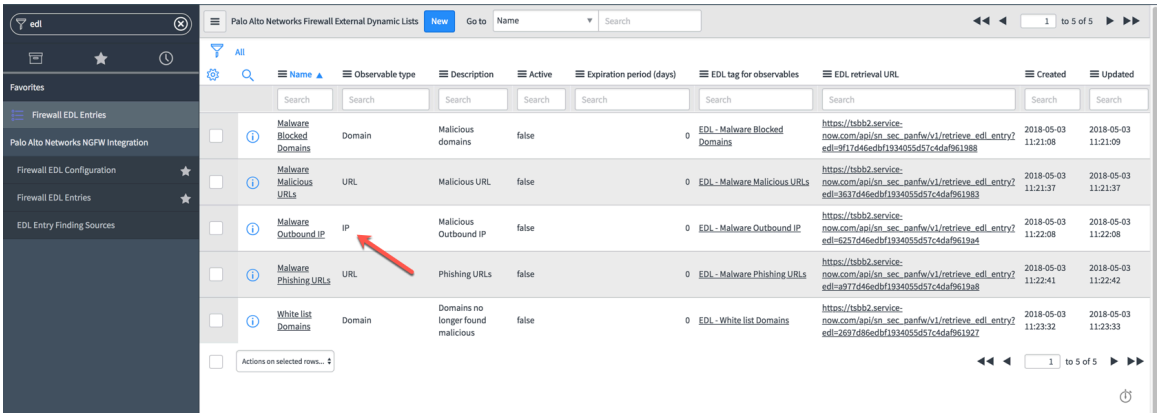
1. Accédez à la **Tout** > **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu**.



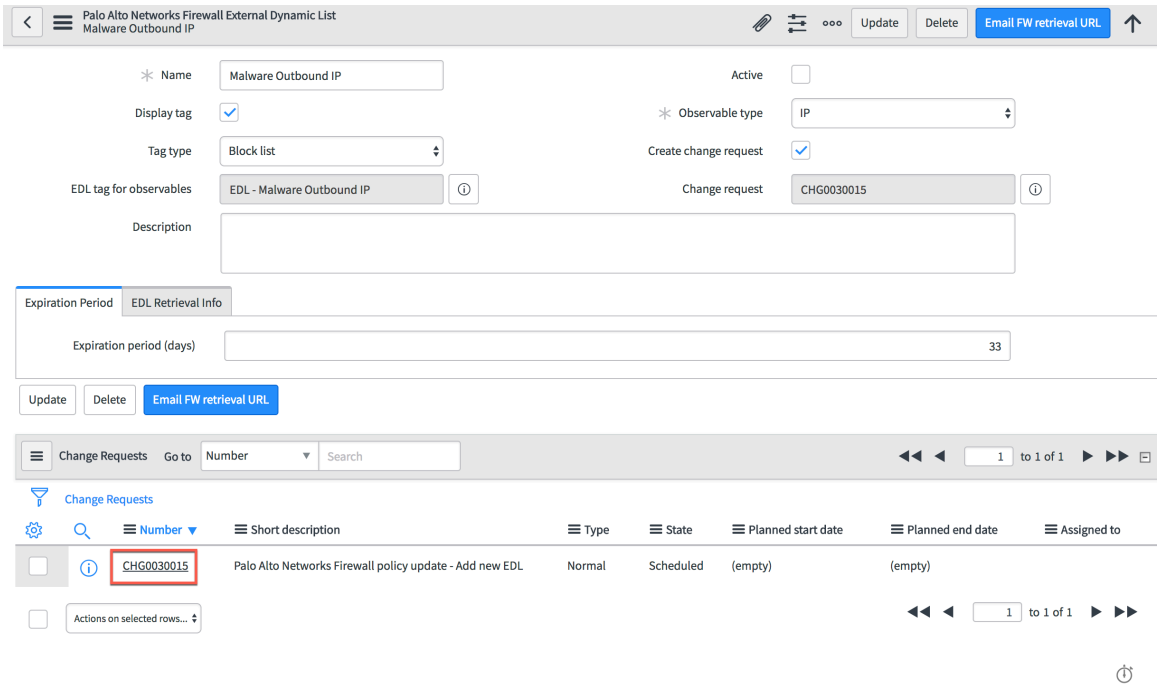
2. Sélectionnez le module EDL et cliquez sur un EDL dans la colonne **Nom** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



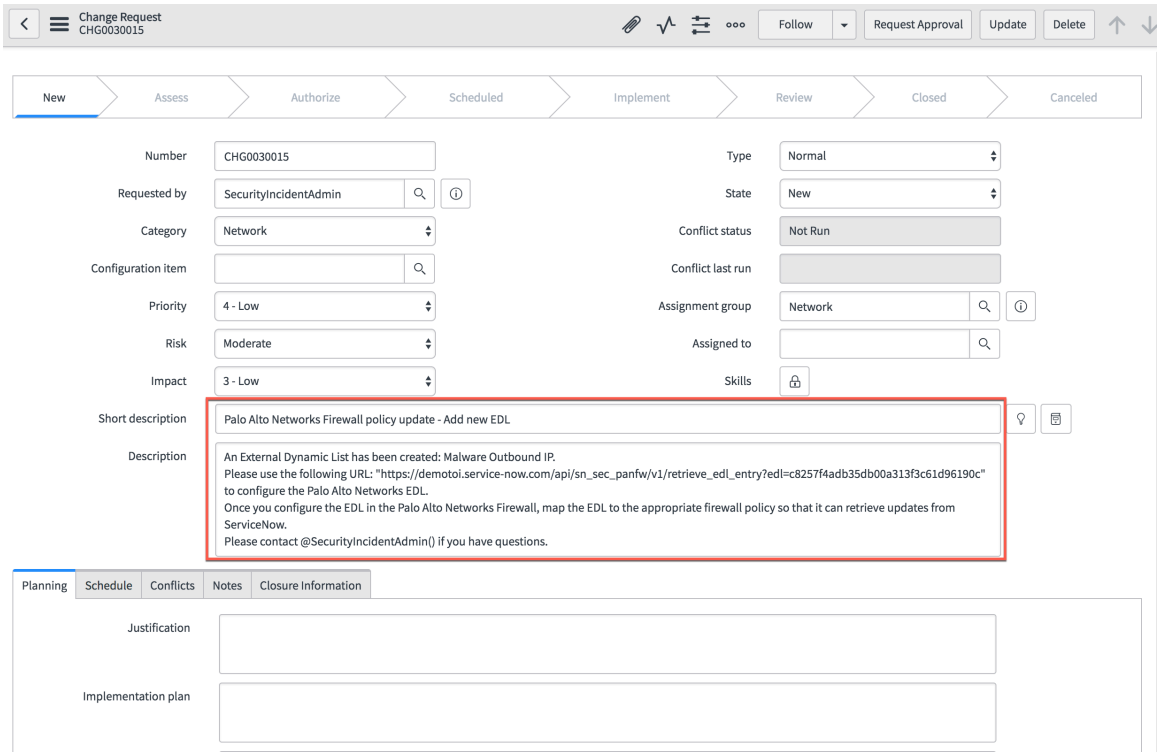
3. Dans l'enregistrement EDL ouvert, cliquez sur le numéro de la demande de changement dans la liste connexe Demandes de changement.



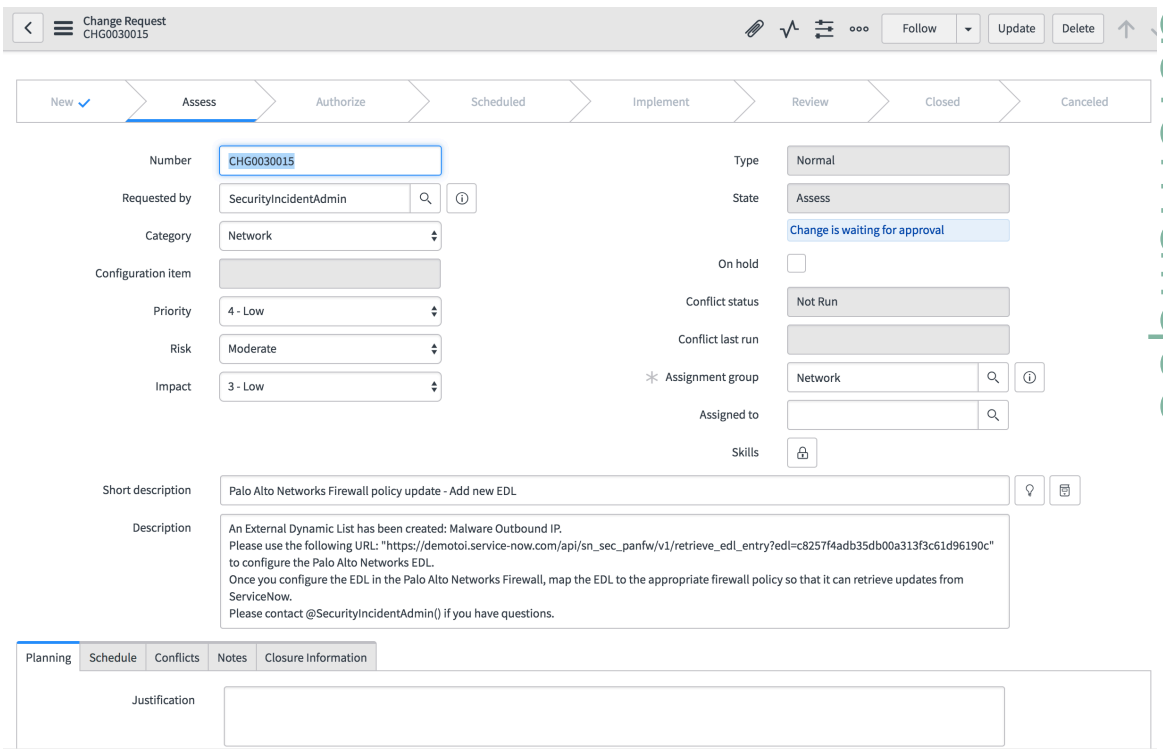
L'enregistrement de la demande de changement s'affiche. Le champ **Description** répertorie l'URL de récupération utilisée pour configurer l'EDL Palo Alto Networks . Des détails sur la mise en correspondance de l'EDEL avec la politique appropriée Palo Alto Networks - Next-Generation Firewall sont également inclus. Dans le champ **Brève description**, un commentaire indique qu'il existe une demande d'ajout d'un nouvel EDL.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans le coin supérieur droit de l'enregistrement, cliquez sur **Demander l'approbation**. L'état passe à Évaluer et un message s'affiche indiquant que la demande de changement est en attente d'approbation.

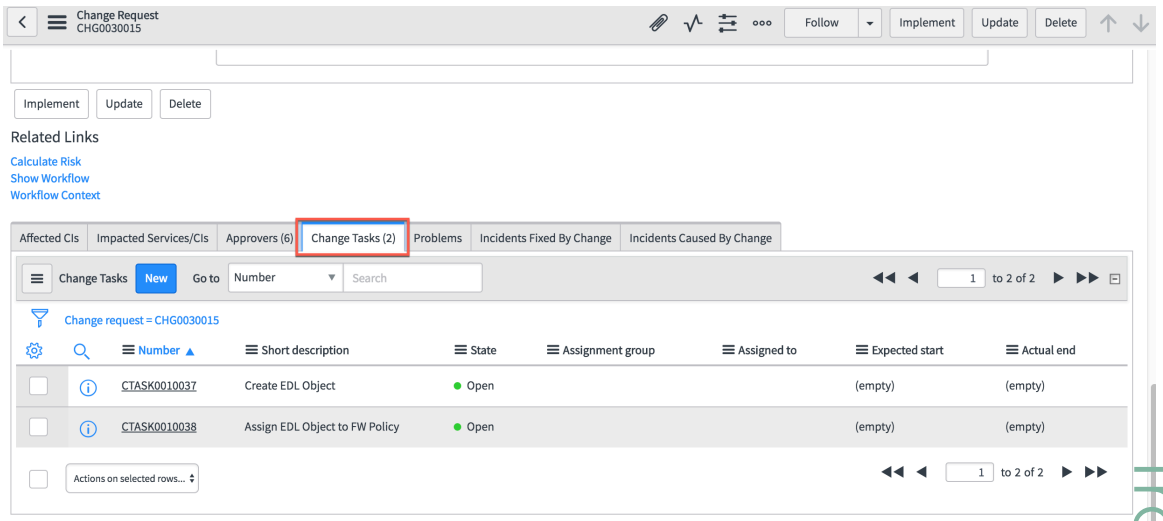


5. Pour terminer la demande de changement et activer l'EDL, procédez comme suit pour affecter les tâches et fermer la demande de changement.

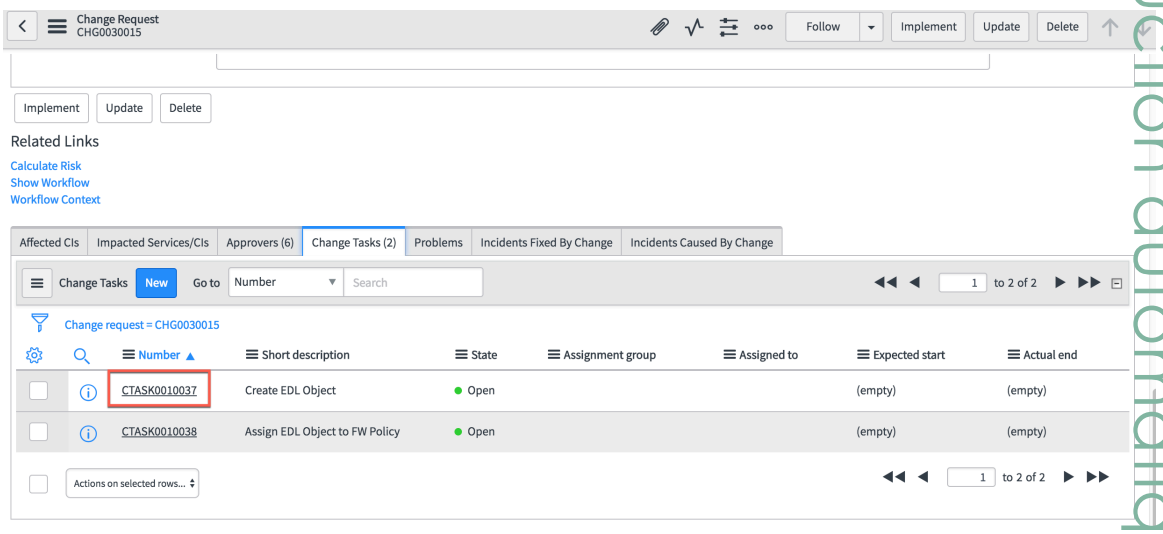
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Si elle n'est pas affichée, ouvrez la demande de changement et sélectionnez l'onglet **Tâches de changement** .



b. Cliquez sur la tâche associée à la création de l'objet EDL pour l'ouvrir.

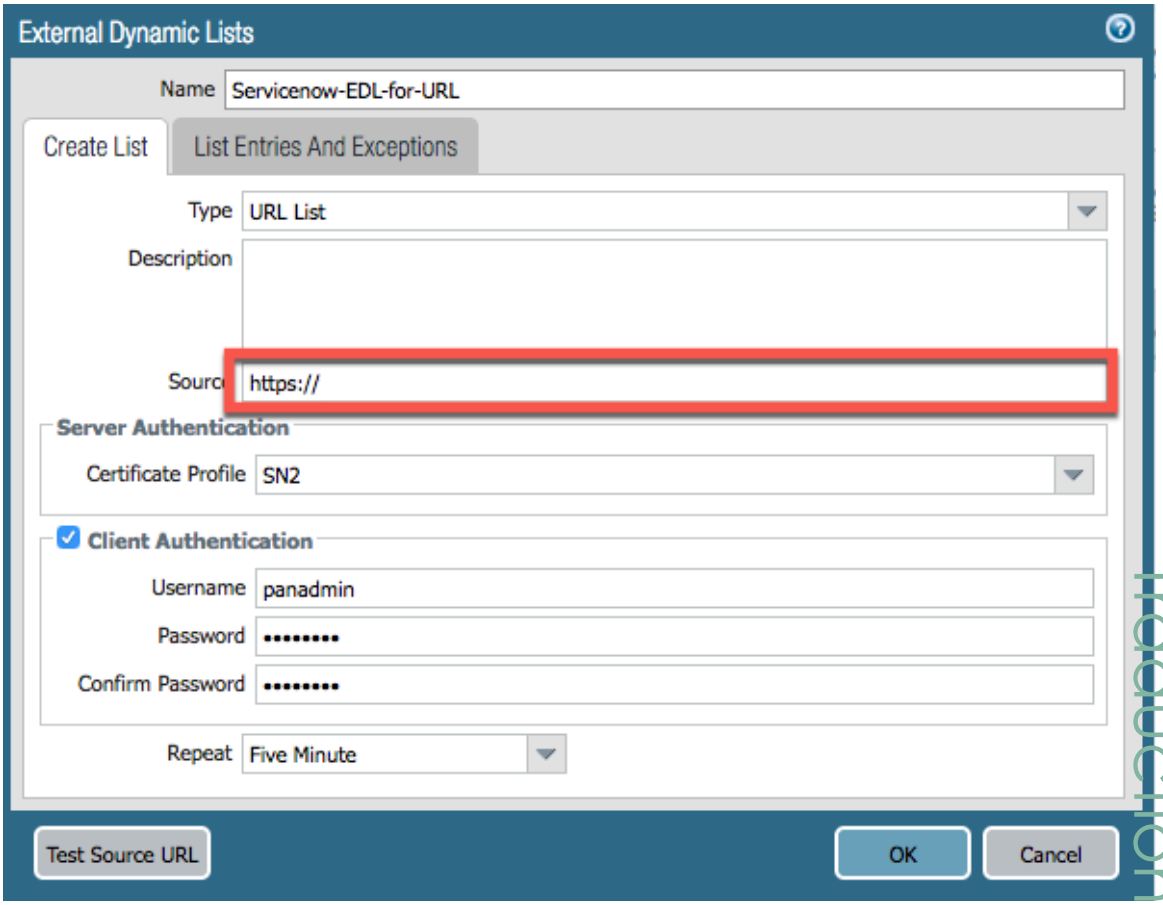


c. Sur l'enregistrement qui s'affiche, affectez la tâche à l'administrateur de pare-feu Palo Alto Networks , puis cliquez sur **Mettre à jour**.
L'administrateur du pare-feu est averti et crée l'objet EDL dans le Palo Alto Networks - Next-Generation Firewallfichier .

Pour créer l'objet EDL, l'URL Now Platform de récupération est copiée à Palo Alto Networks l'adresse **Listes externes dynamiques** > **Créer des listes** > **Source**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

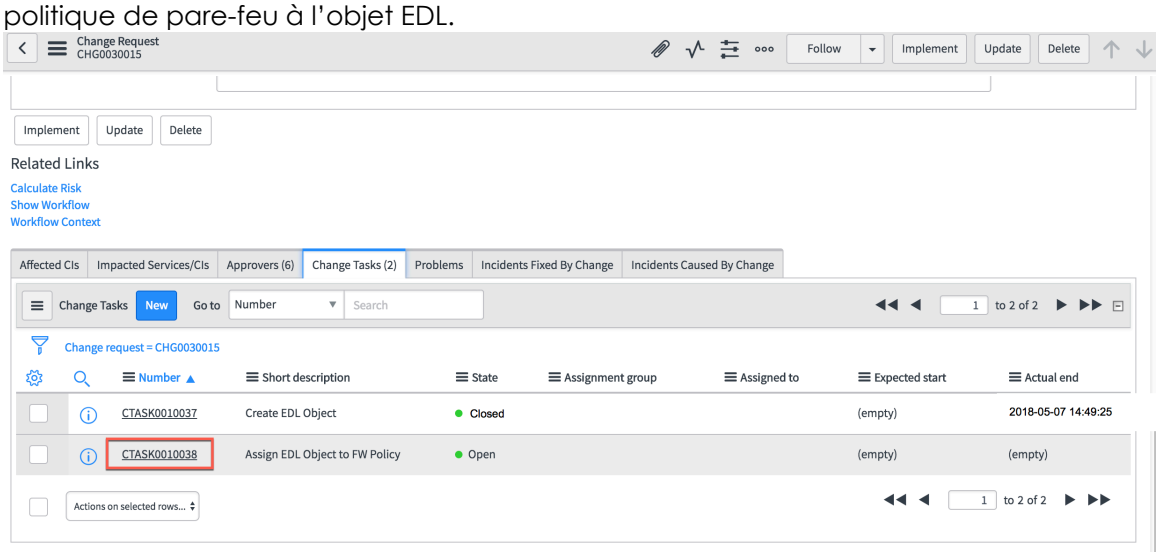


L'image est utilisée avec permission et est PRIVILÉGIÉE et PROPRIÉTAIRE.

d. Après avoir vérifié que l'objet EDL a été créé dans Palo Alto Networks, dans le Now Platform, accédez à la demande de changement associée à la création de l'objet EDL et cliquez sur **Fermer la tâche**.

Sur l'enregistrement de tâche de cet exemple, `CTASK0010037` a été fermée pour cette tâche.

e. Accédez à l'onglet Tâches de changement et cliquez sur la tâche d'affectation d'une politique de pare-feu à l'objet EDL.



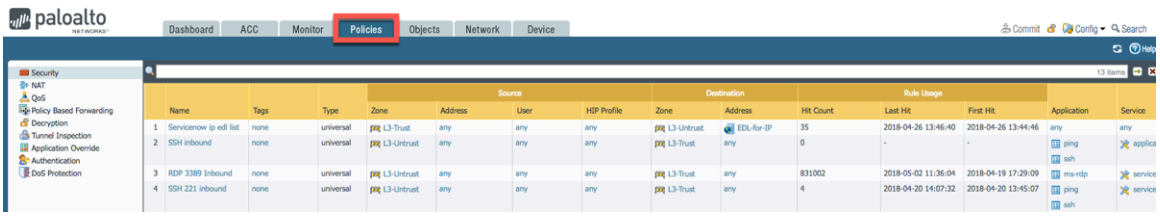
`L'état de CTASK0010037` est `Fermé`.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

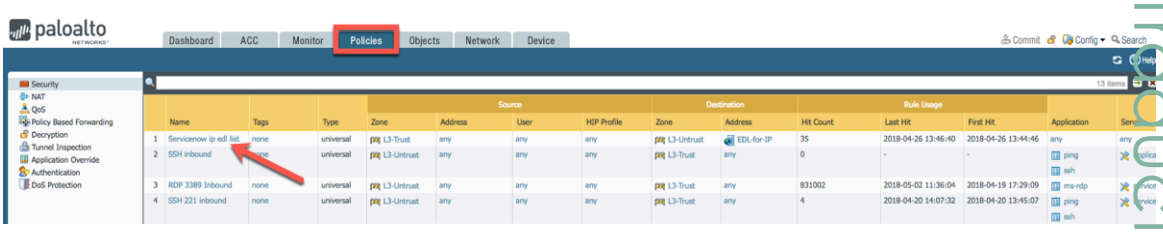
f. Ouvrez l'enregistrement et affectez la tâche suivante.

Une fois la tâche affectée, dans Palo Alto Networks, l'administrateur de pare-feu accède à l'onglet **Politiques** pour affecter la politique.



L'image est utilisée avec permission et est PRIVILÉGIÉE et PROPRIÉTAIRE.

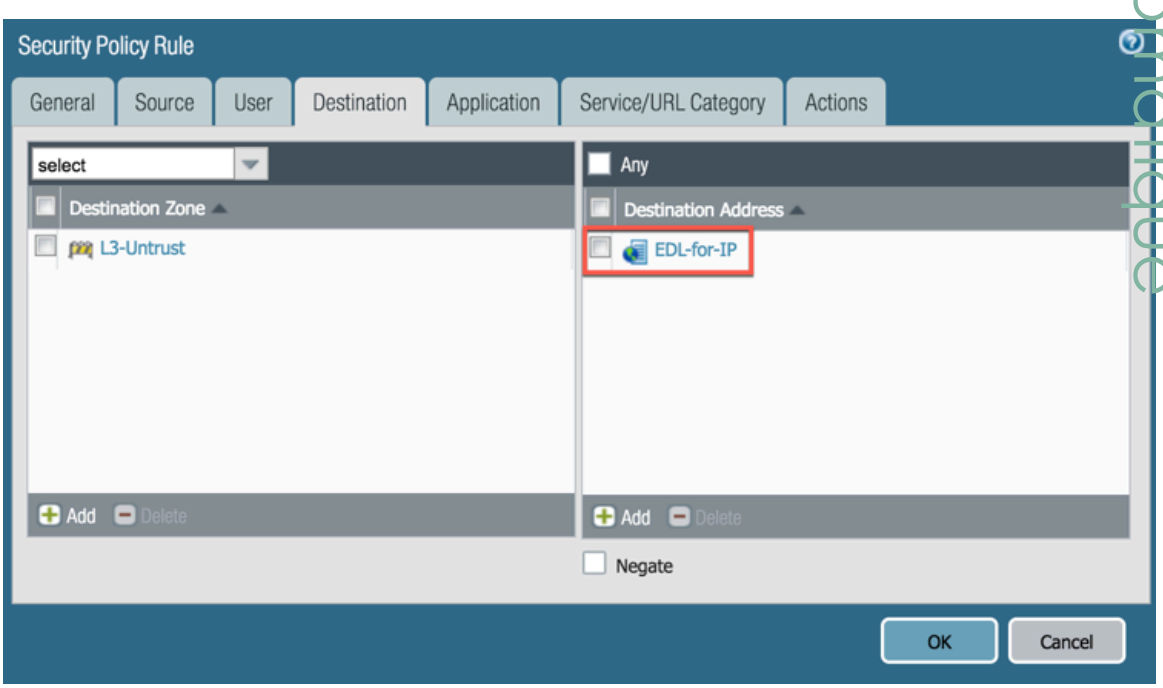
g. Dans la colonne **Nom** , recherchez et cliquez sur la règle de politique de sécurité à laquelle vous souhaitez ajouter l'EDL, par exemple, **Liste d'EDL IP ServiceNow**.



L'image est utilisée avec permission et est PRIVILÉGIÉE et PROPRIÉTAIRE.

h. Dans la boîte de dialogue Règle de politique de sécurité, sélectionnez l'onglet **Destination** pour ajouter une EDL dans le champ **Adresse de destination** .

i. Pour afficher tous les EDL disponibles, cliquez sur l'icône **Ajouter** .



L'image est utilisée avec permission et est PRIVILÉGIÉE et PROPRIÉTAIRE.

j. Cliquez sur **OK**.

Traduction automatique

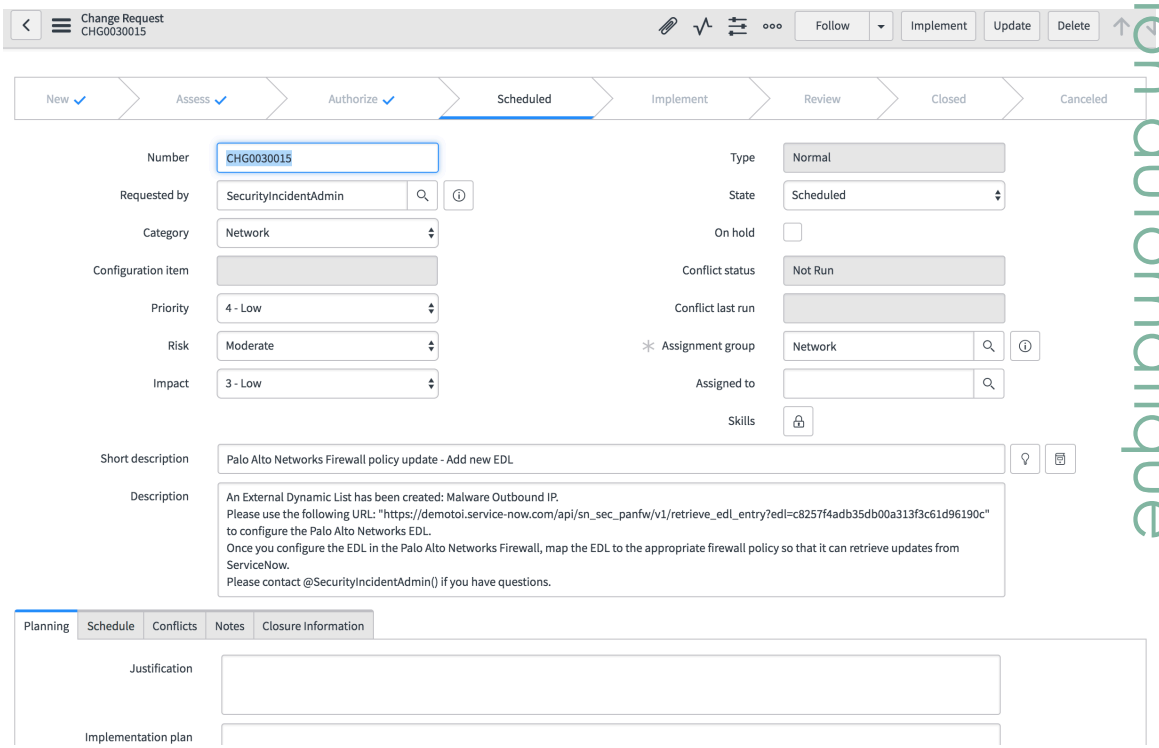
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

k. Une fois que vous avez vérifié que l'objet EDL a été affecté à une politique de sécurité, accédez à la demande de changement dans le Now Platform, ouvrez la tâche associée à l'affectation de l'objet EDL et cliquez sur **Fermer la tâche**.
Une fois les deux tâches fermées, la demande de changement est prête à être approuvée.

l. Dans l'enregistrement de demande de changement, cliquez sur la liste connexe **Approbateurs** , puis sélectionnez un élément dans la colonne **État** pour ouvrir la demande utilisée pour créer l'EDL.



m. Cliquez sur **Approuver** dans le formulaire de demande d'approbation ouvert.
L'état de la demande de changement passe à Planifié.



n. Cliquez **sur Implémenter**.

o. Cliquez sur l'onglet **connexe Informations** sur la fermeture et saisissez des notes pour fermer la demande.

Une entrée dans ce champ est requise pour fermer la demande de changement.

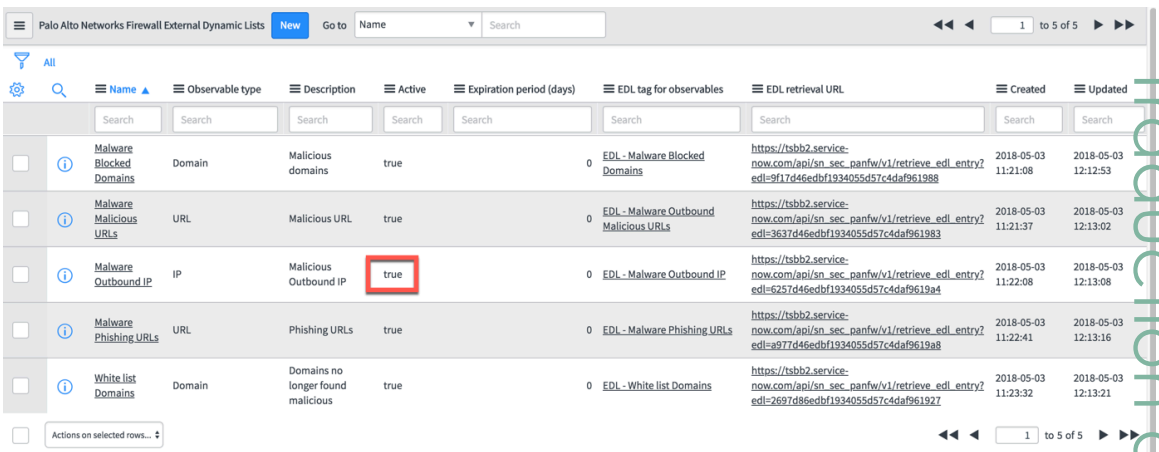
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

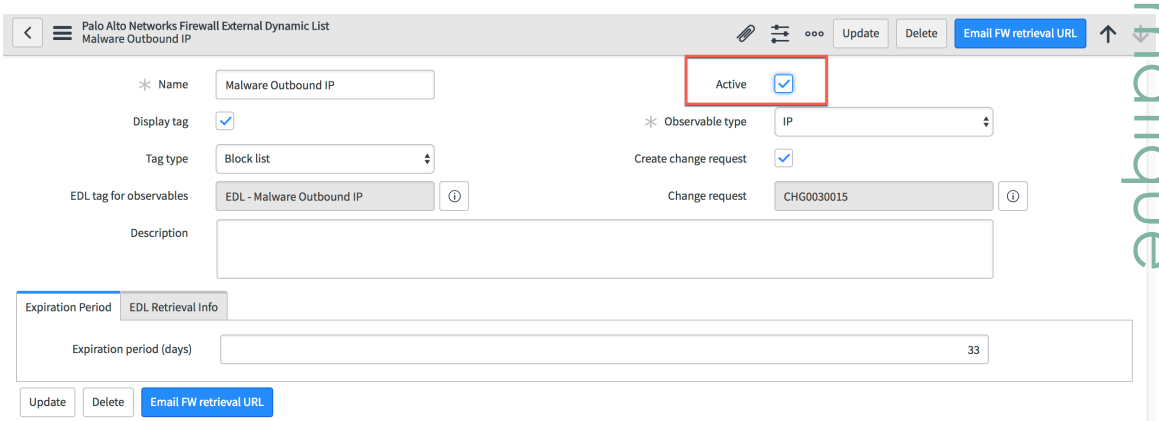


Une fois la demande de changement fermée, l'EDL est activé automatiquement. Si vous n'avez pas vérifié que l'EDL est activé, accédez à **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu**.

Dans la colonne Actif de la liste, notez que l'état de l'EDL est (`vrai`).



Dans la colonne Nom, cliquez sur le nom de l'EDL et, dans l'enregistrement ouvert, notez que la case **Actif** est également cochée.



L'EDL est maintenant prêt à accepter les entrées EDL.

Que faire ensuite

Soumettre des entrées EDL à partir d'un incident de sécurité ou de la liste de blocage.

Soumettre des entrées EDL à partir d'un enregistrement d'incident de sécurité pour Palo Alto Networks - Next-Generation Firewall

Les observables joints à un enregistrement d'incident de sécurité sont soumis pour approbation en tant qu'entrées de liste dynamique externe (EDL) aux EDL. Un processus

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'approbation des entrées EDL fait partie du workflow préconfiguré. Le pare-feu importe les entrées EDL (adresses IP, URL, domaines) qui sont incluses dans les listes d'EDL et applique la stratégie.

Avant de commencer

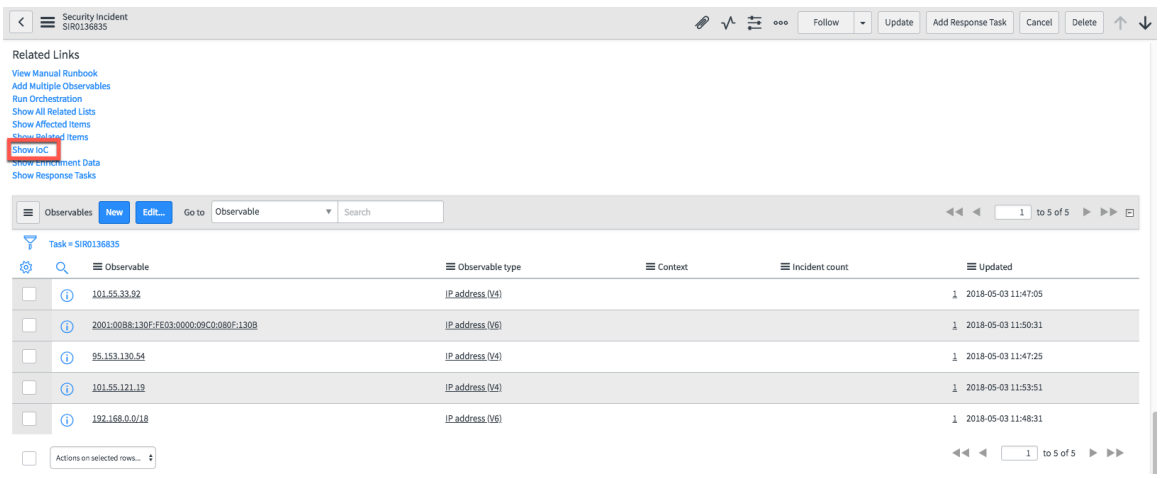
Rôle requis : sn_si.analyst pour la soumission des entrées EDL. Pour approuver les entrées EDL : l'approbation est attribuée à sn_si.admin par défaut, mais cette autorisation peut être attribuée selon les besoins de votre organisation.

Pourquoi et quand exécuter cette tâche

Les utilisateurs ayant le rôle sn_si.analyst soumettent des entrées EDL en demandant un blocage des observables joints à un enregistrement d'incident de sécurité. Une fois soumise, une entrée EDL avec l'état En attente est générée et envoyée pour approbation. L'exemple suivant montre une demande de bloc pour un observable d'URL.

Procédure

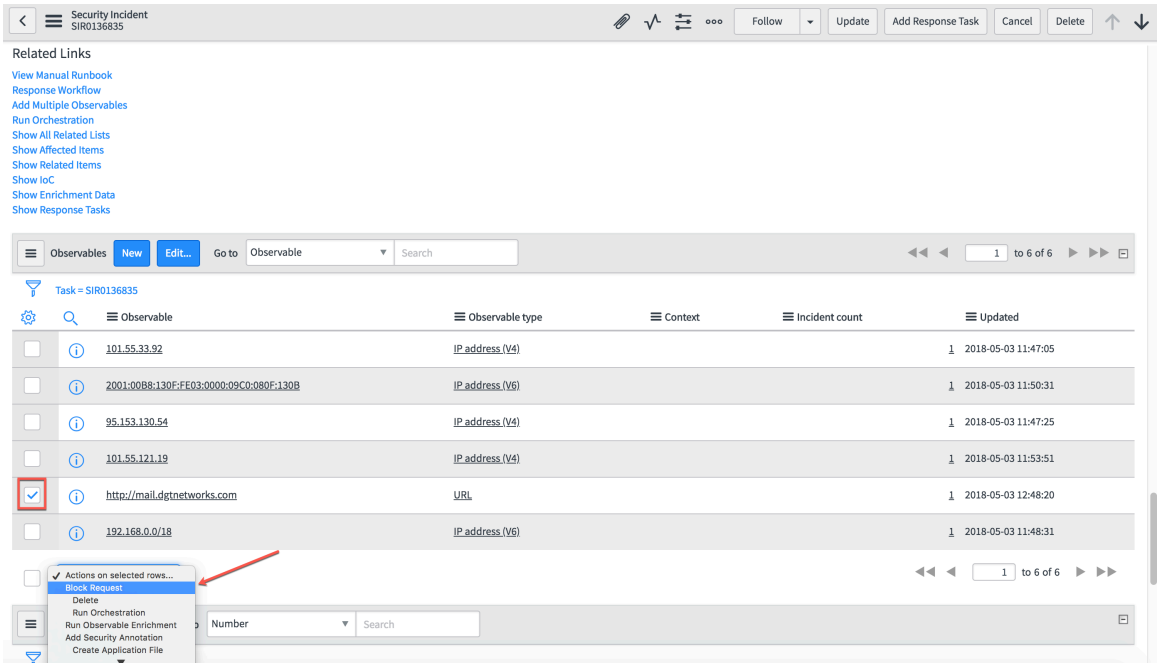
1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**et cliquez sur un enregistrement d'incident de sécurité pour l'ouvrir.
2. Cliquez sur le lien connexe **Afficher IoC** .



3. Dans la liste connexe Observables, sélectionnez les observables que vous souhaitez bloquer et, dans la liste **Actions sur les lignes sélectionnées** , sélectionnez **Bloquer la demande**.

Traduction automatique

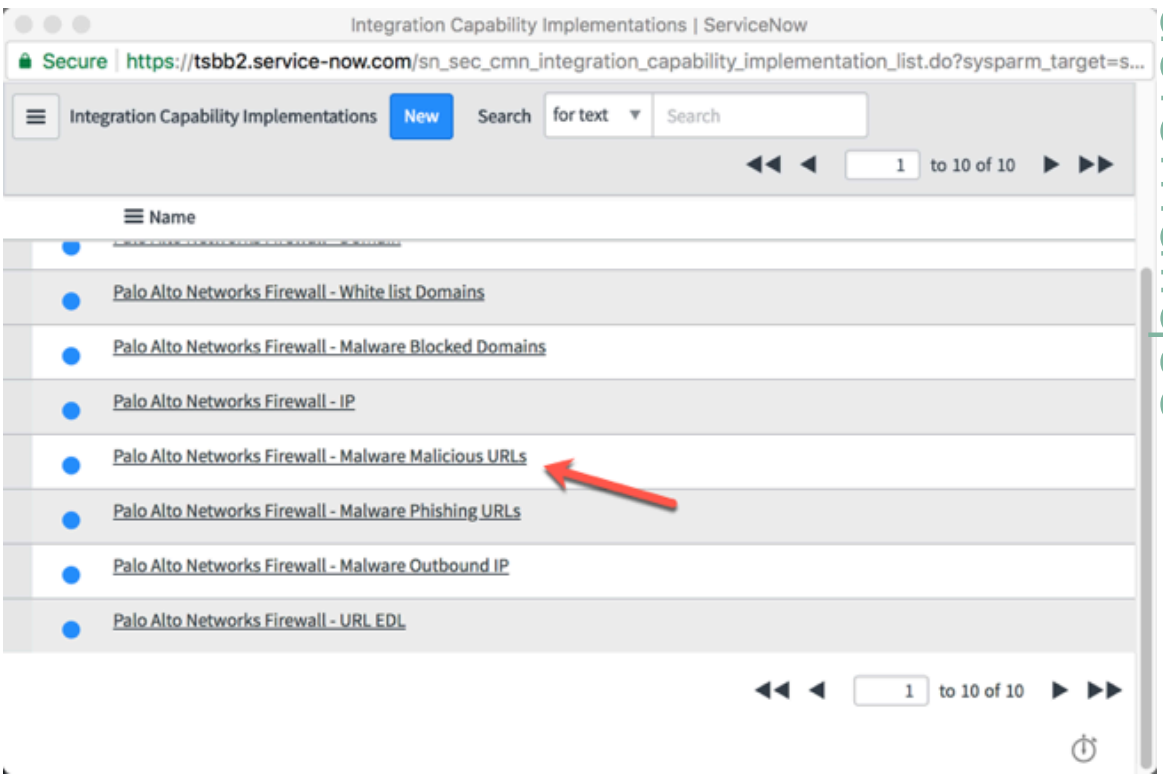
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans la boîte de dialogue qui s'affiche, cliquez sur l'icône de recherche ( ).

5. Dans la liste qui s'affiche, sélectionnez l'EDL auquel vous souhaitez joindre cette entrée.

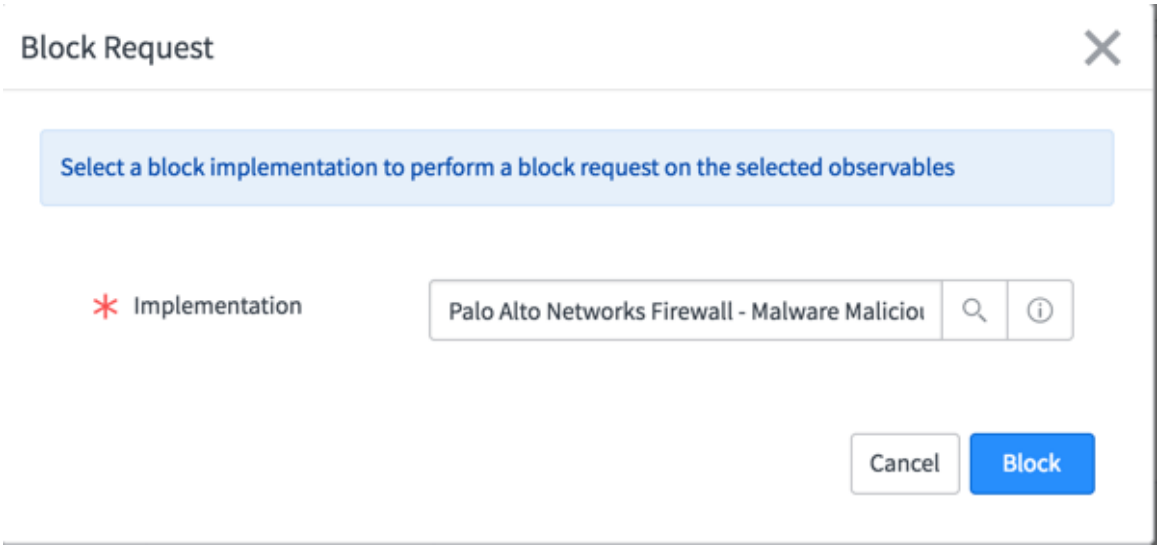
Remarque : Pour cet exemple, le type d'observable d'entrée (URL) doit correspondre au type d'observable de l'EDL (URL).



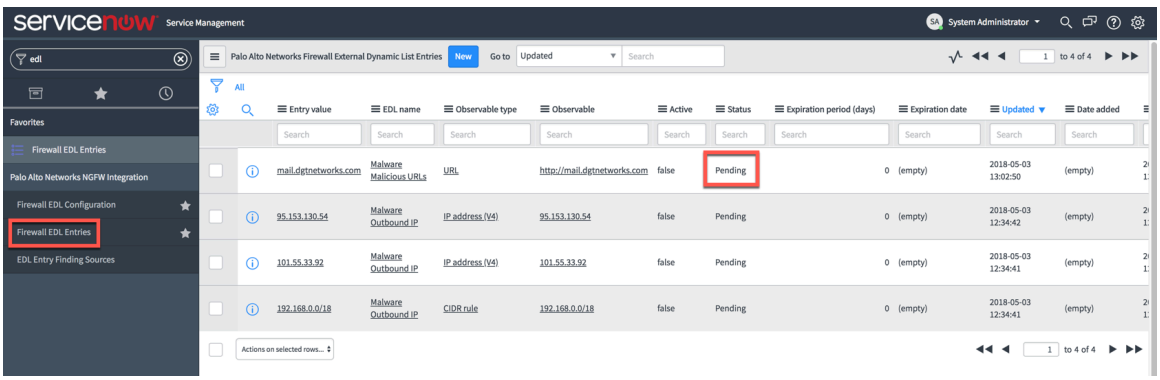
6. Dans la boîte de dialogue Demande de bloc avec le nom de l'EDL affiché dans le champ **Implémentation** , cliquez sur **Bloquer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

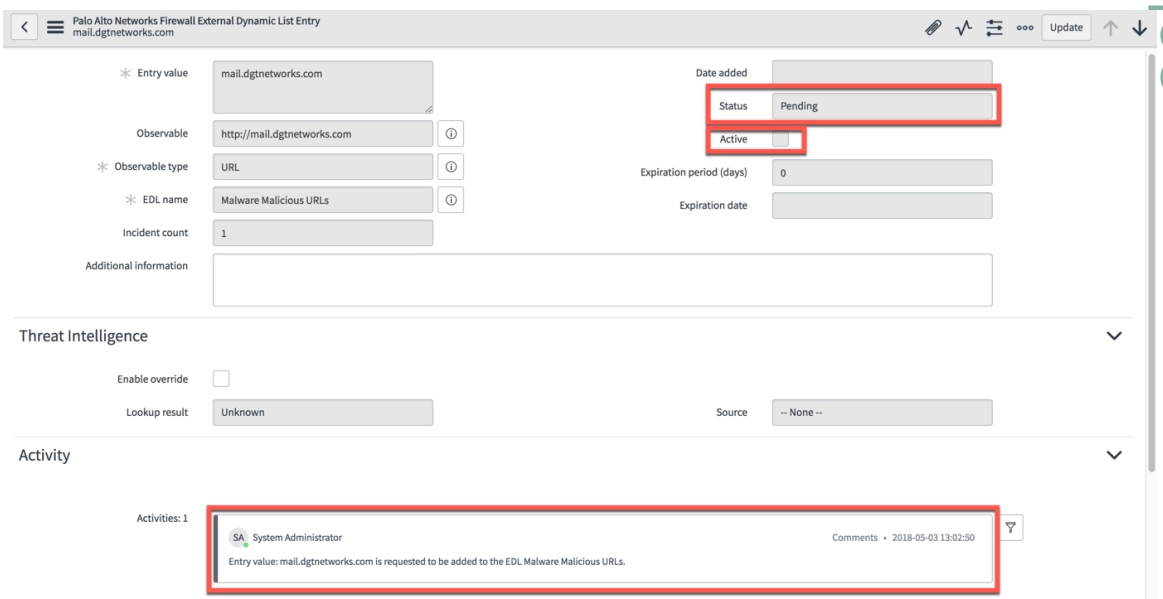


7. Accédez à la **Intégration de Palo Alto Networks NGFW** > **Entrées de l'EDL du pare-feu** et cliquez sur **Entrées EDL du pare-feu**.



8. Dans la liste des entrées de la liste dynamique externe du pare-feu Palo Alto Networks, cliquez sur votre observable dans la colonne **Valeur d'entrée** pour ouvrir l'enregistrement.

Pour cet exemple, l'enregistrement **de mail.dgtnetworks.com** s'affiche.

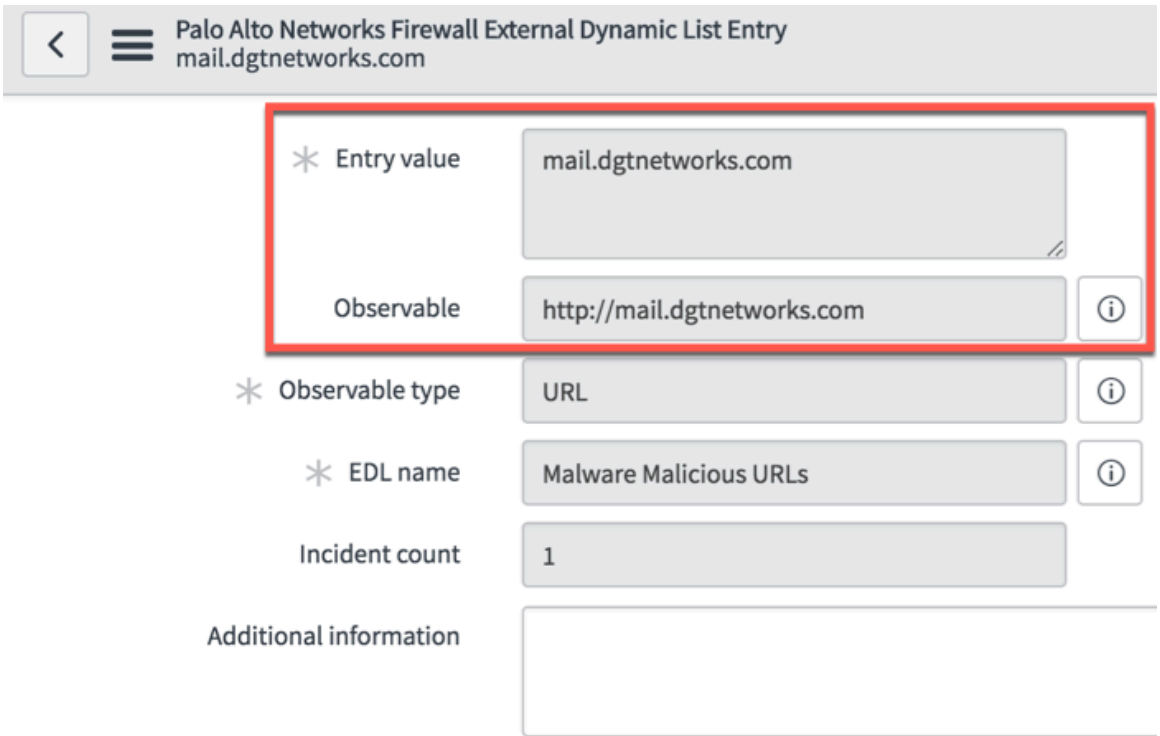


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'état est En attente, la case Actif est décochée et les notes de travail indiquent qu'il existe une demande d'ajout de l'observable. Cette demande d'entrée EDL est prête à être approuvée.

Les champs Valeur d'entrée et Observable présentent des formats différents pour l'observable d'URL.



L'icône en regard du champ `Observable` est un lien vers la Now Platform® table Observable.

La valeur du champ `Observable` (`http://mail.dgtnetworks.com`) est liée à la table Observable et correspond au format qui a été apporté à partir de l'événement déclenchant l'incident Réponse aux incidents de sécurité .

Ils Now Platform® peuvent modifier automatiquement les entrées de l'EDL afin qu'elles soient compatibles avec le format de l'URL de l'EDL Palo Alto Networks .

Dans cet exemple, l'observable a été créé avec le protocole http:// (`http://mail.dgtnetworks.com`), et ce format est affiché dans le champ Observable. Le protocole http:// est automatiquement supprimé de l'observable par le Now Platform® afin qu'il soit compatible Palo Alto Networks et puisse être récupéré. Par conséquent, `mail.dgtnetworks.com s'affiche` dans le champ `Valeur d'entrée` .

Que faire ensuite
Approuvez les entrées EDL.

Information associée

Exceptions d'entrée de l'EDL pour Palo Alto Networks - Next-Generation Firewall

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Soumettre des entrées EDL à partir de la liste de blocs pour Palo Alto Networks - Next-Generation Firewall

Pour les observables déterminés comme malveillants et non associés à un incident de sécurité spécifique Now Platform , vous soumettez des entrées de liste dynamique externe (EDL) à partir de la liste de blocs.

Avant de commencer

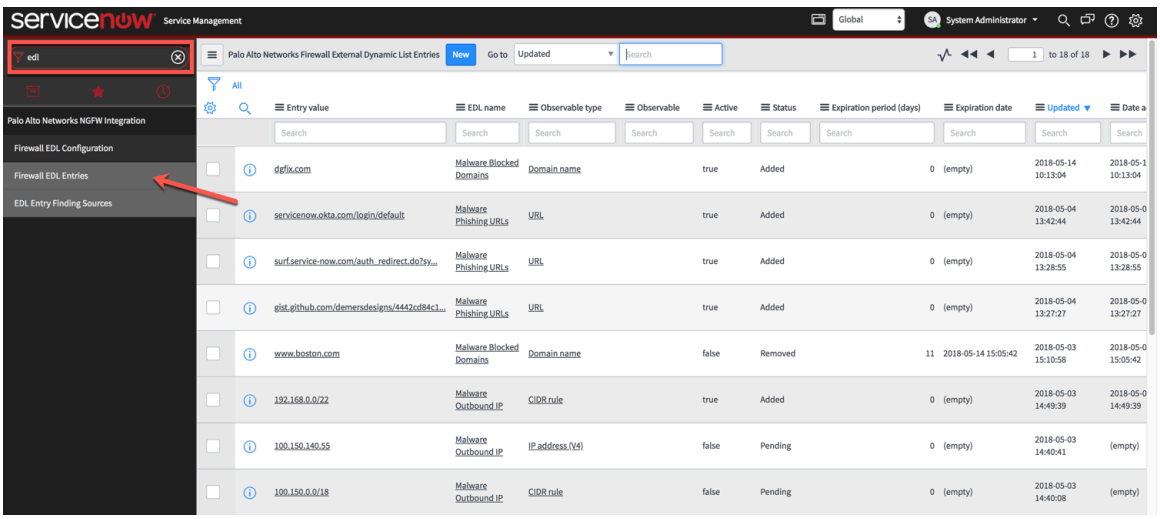
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Lorsque vous souhaitez bloquer un observable que vous avez déterminé comme malveillant ou autoriser un observable que vous avez déterminé comme non malveillant et que l'observable n'est pas associé à un enregistrement d'incident de sécurité spécifique Now Platform , vous soumettez les entrées EDL directement à partir de la liste de blocs. Des exemples de ces types d'entrées EDL peuvent être des URL ou des domaines pour des sites spécifiques.

Procédure

1. Accédez à la **Tout** > **Intégration de Palo Alto Networks NGFW** > **Entrées de l'EDL du pare-feu**.



2. Cliquez sur le module **Entrées de l'EDL du pare-feu** .
3. Dans la liste des entrées de la liste dynamique externe du pare-feu Palo Alto Networks, cliquez sur **Nouveau**.
4. Dans le nouvel enregistrement qui s'affiche, saisissez une valeur pour votre observable dans le champ **Valeur d'entrée** .
   Les deux résultats possibles de cette entrée :

   Les champs restants du formulaire sont remplis automatiquement.

   Un observable correspondant est trouvé et un message s'affiche indiquant qu'un observable correspondant existe. Sélectionnez l'EDL à laquelle vous souhaitez joindre cette entrée et cliquez sur **Soumettre**. Sélectionnez l'EDL auquel vous souhaitez joindre cette entrée avant de définir la période d'expiration.

   Un message s'affiche pour vous demander de remplir le formulaire.

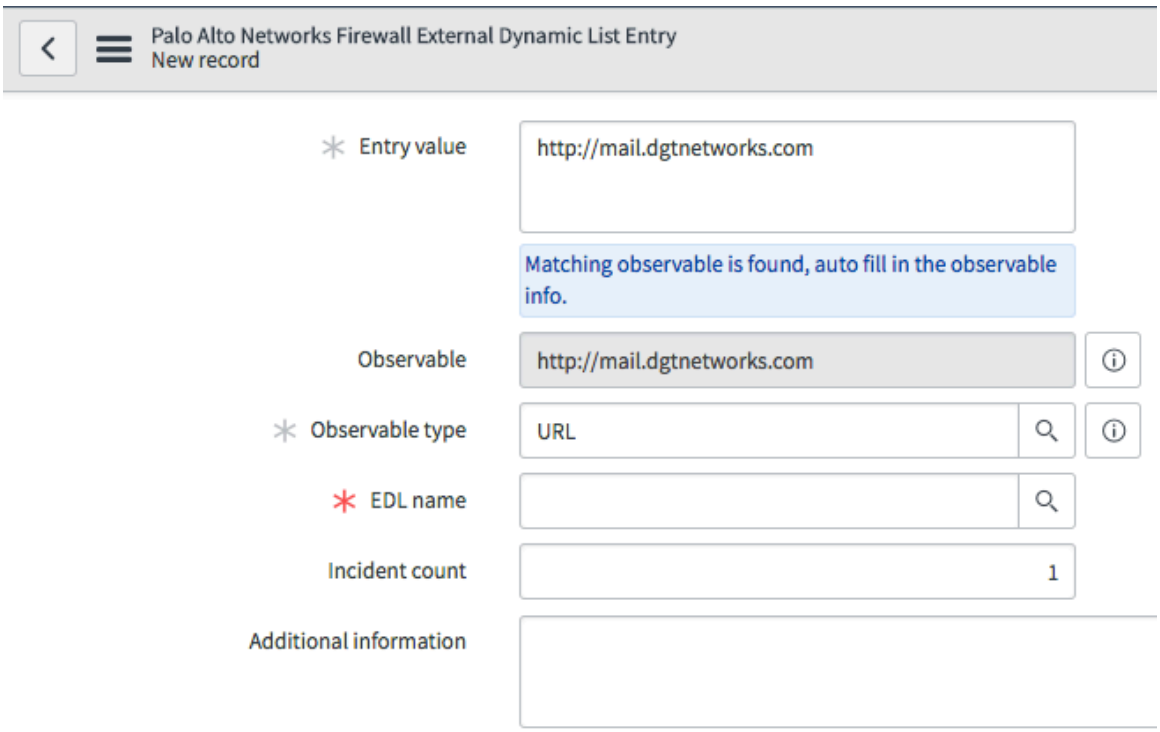
   Aucun observable correspondant n'a été trouvé et vous devez remplir le formulaire. Une fois que vous l'avez terminé, sélectionnez l'EDL auquel vous

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

souhaitez joindre l'observable et cliquez sur **Envoyer**. Un enregistrement d'observable est créé.

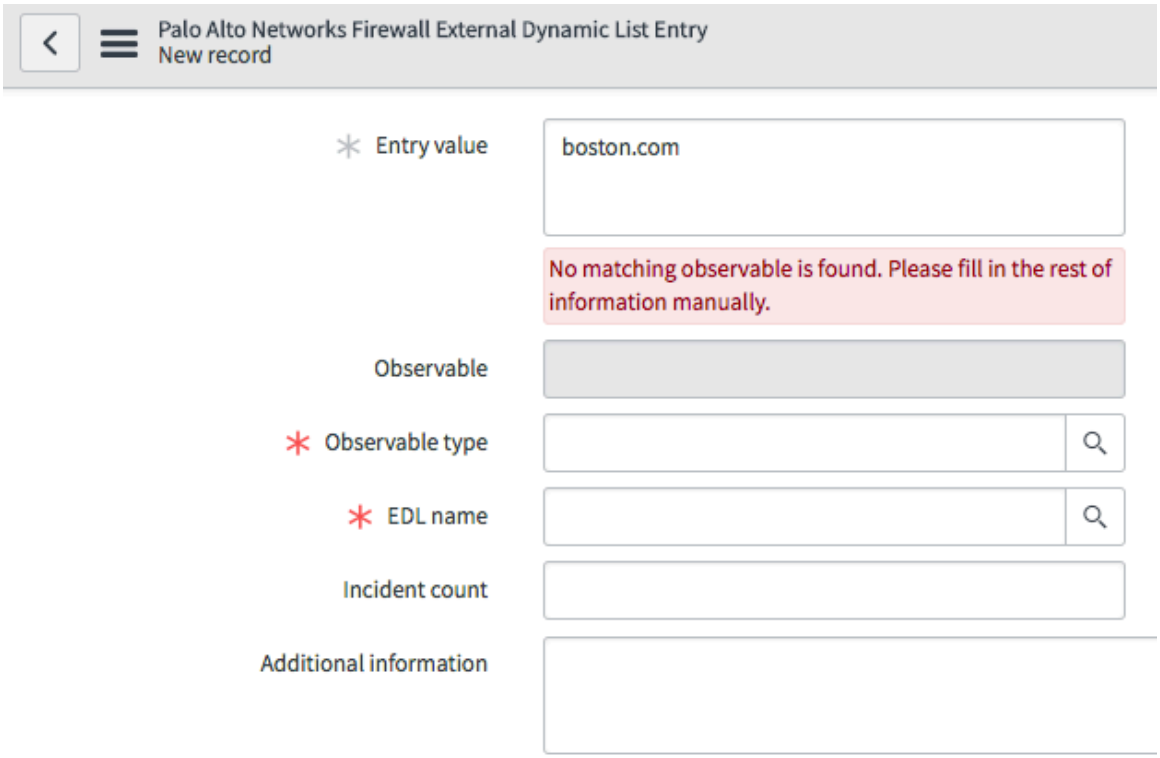
La figure suivante montre un exemple d'observable de domaine existant et comment les champs sont remplis automatiquement.



5. Cliquez sur l'icône de recherche pour sélectionner l'EDL à laquelle vous souhaitez joindre l'entrée.
6. Cliquez sur **Envoyer**.
   Si vous avez configuré une approbation par e-mail dans votre workflow, une demande d'approbation par e-mail est envoyée.
7. Si un message s'affiche vous demandant de remplir manuellement le reste des informations, renseignez les champs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



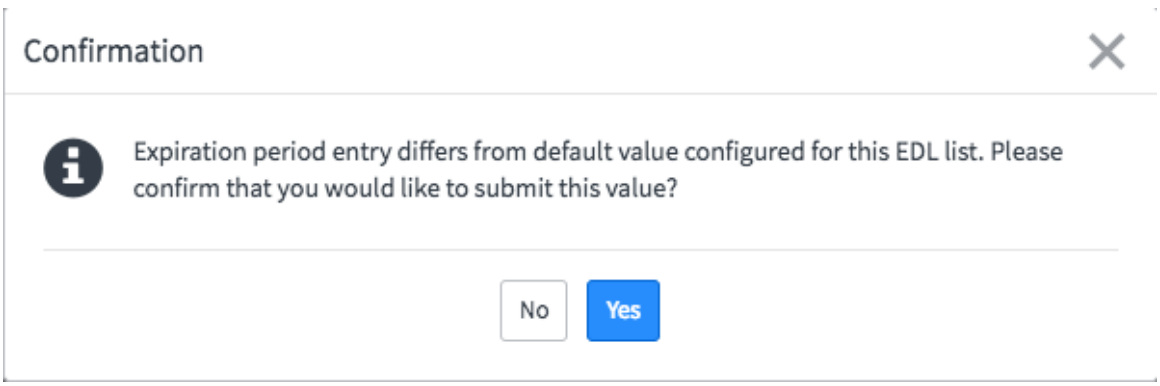
Champ	Description
Type d'observable	Type d'observable pris en charge à partir de la boîte de dialogue.
Nom de l'EDL	EDL auquel vous souhaitez joindre l'entrée. **Remarque :** Sélectionnez l'EDL à laquelle vous souhaitez joindre l'entrée avant de définir la période d'expiration.
Activer le remplacement (sélectionné par défaut)	Rechercher un résultat ou une source. Une fois configuré, elle vous permet **d'entrer un résultat de recherche** et la source utilisée pour trouver les résultats. Ces champs sont généralement renseignés lors de la création d'un enregistrement d'incident de sécurité. Dans ce cas, il n'y a pas de recherche de résultat ou de source, et vous renseignez ces champs manuellement.
Rechercher un résultat	Sélectionnez **Inconnu** ou **Malicieuse**.
Source	Source qui effectue une recherche de menace sur l'entrée EDL, par exemple, ThreatCrowd...
Période d'expiration	Période d'expiration héritée de l'EDL par défaut. Vous pouvez remplacer cette valeur, mais uniquement lors de la création de l'entrée. `0` indique que l'entrée EDL n'expire jamais.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si vous modifiez cette valeur, cette entrée est active pendant le nombre de jours que vous entrez. Vous pouvez entrer une valeur minimale de `1`, mais il n'y a pas de valeur maximale. Par exemple, si vous saisissez `30` jours à 14 h 01 le 1er mai, l'entrée EDL expirera à 14 h 01 le 31 mai.

8. Cliquez sur **Envoyer**.
   Si vous avez modifié la période d'expiration par défaut de l'entrée EDL, une boîte de dialogue de confirmation d'avertissement s'affiche indiquant que la période diffère de l'EDL sélectionnée.



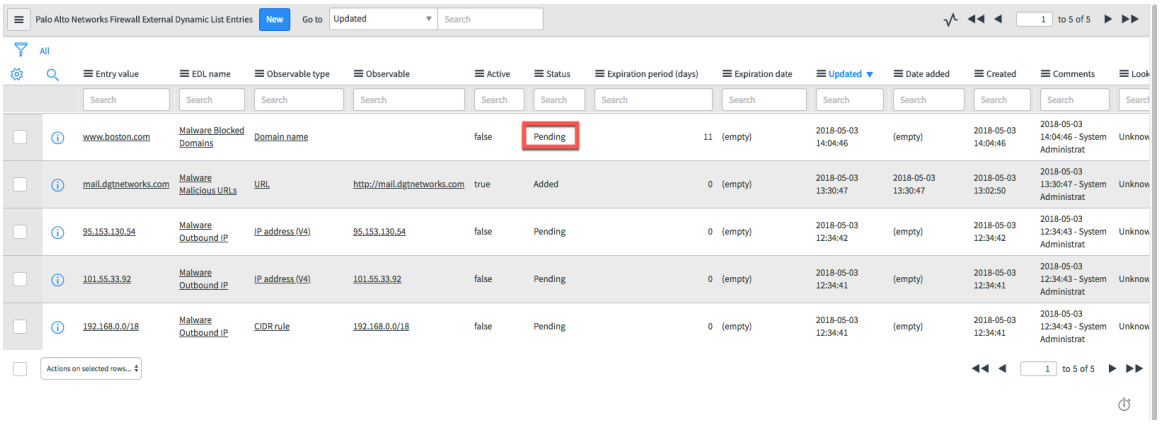
9. Choisissez une option pour configurer la période d'expiration.

Option	Description
Oui	Confirme votre remplacement d'expiration, enregistre l'enregistrement et vous renvoie à la liste des entrées de la **liste dynamique externe du pare-feu Palo Alto Networks** . Si vous avez configuré une approbation par e-mail dans votre workflow, une demande d'approbation par e-mail est envoyée.
Non	Annule le remplacement. À ce stade, vous pouvez modifier la valeur de la **période d'expiration**. Après avoir modifié la valeur, cliquez sur **Envoyer** pour revenir à la liste des entrées de la **liste dynamique externe du pare-feu Palo Alto Networks** .

10. Si ce n'est pas le cas, accédez à la liste Entrées de la **liste dynamique externe du pare-feu Palo Alto Networks** et notez que l'état de l'entrée est En attente.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'entrée est maintenant prête pour approbation.

Que faire ensuite
Approuvez les entrées EDL.

Information associée

Exceptions d'entrée de l'EDL pour Palo Alto Networks - Next-Generation Firewall

Approuver les entrées EDL pour Palo Alto Networks - Next-Generation Firewall

Un processus d'approbation des entrées de liste dynamique externe (EDL) fait partie du workflow préconfiguré. Vous approuvez les entrées EDL avant qu'elles ne soient activées dans les EDL. Une fois que vous approuvez l'entrée EDL, le pare-feu récupère l'entrée et votre observable est bloqué à partir de ce moment-là.

Avant de commencer
Rôle requis : l'approbation des entrées EDL est affectée à sn_si.admin par défaut, mais cette autorisation peut être attribuée selon les besoins de votre organisation. Dans l'exemple suivant, l'administrateur dispose d'une Now Platform autorité d'approbation.

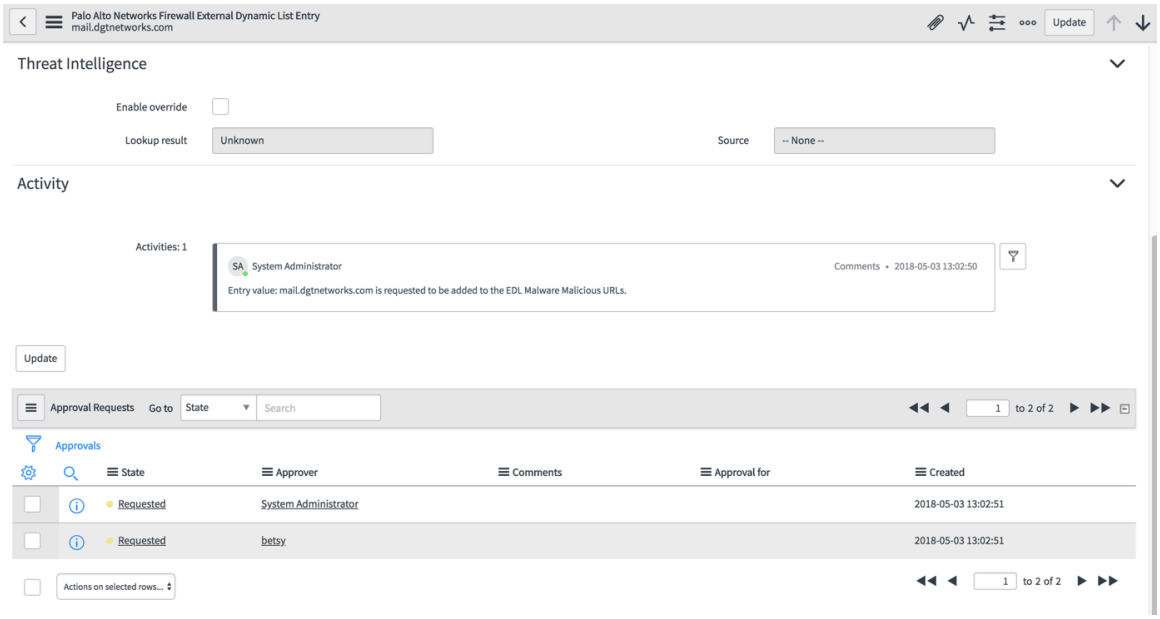
Pourquoi et quand exécuter cette tâche
Lorsque le processus d'approbation est activé, une entrée EDL n'est pas activée ou désactivée sur l'EDL tant qu'elle n'est pas approuvée.

Procédure
1. Accédez à la **Tout** > **Intégration de Palo Alto Networks NGFW** > **Entrées de l'EDL du pare-feu** et ouvrez l'enregistrement EDL.
2. Dans l'enregistrement EDL, faites défiler jusqu'à la section Demandes d'approbation.

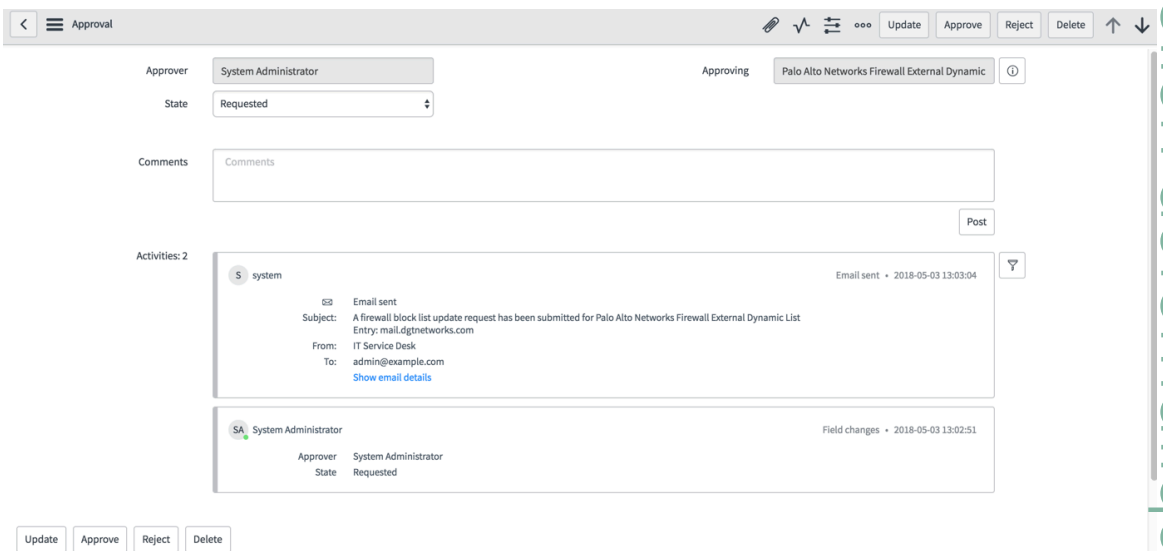
> **Remarque :** Si vous avez sélectionné des formulaires à onglets dans les paramètres du système, la section apparaît sous forme d'onglet sur l'enregistrement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans Demandes d'approbation, cliquez sur un élément de la colonne **État** pour l'ouvrir. L'enregistrement de l'approbation s'affiche.



4. Choisissez une option pour approuver l'entrée EDL.

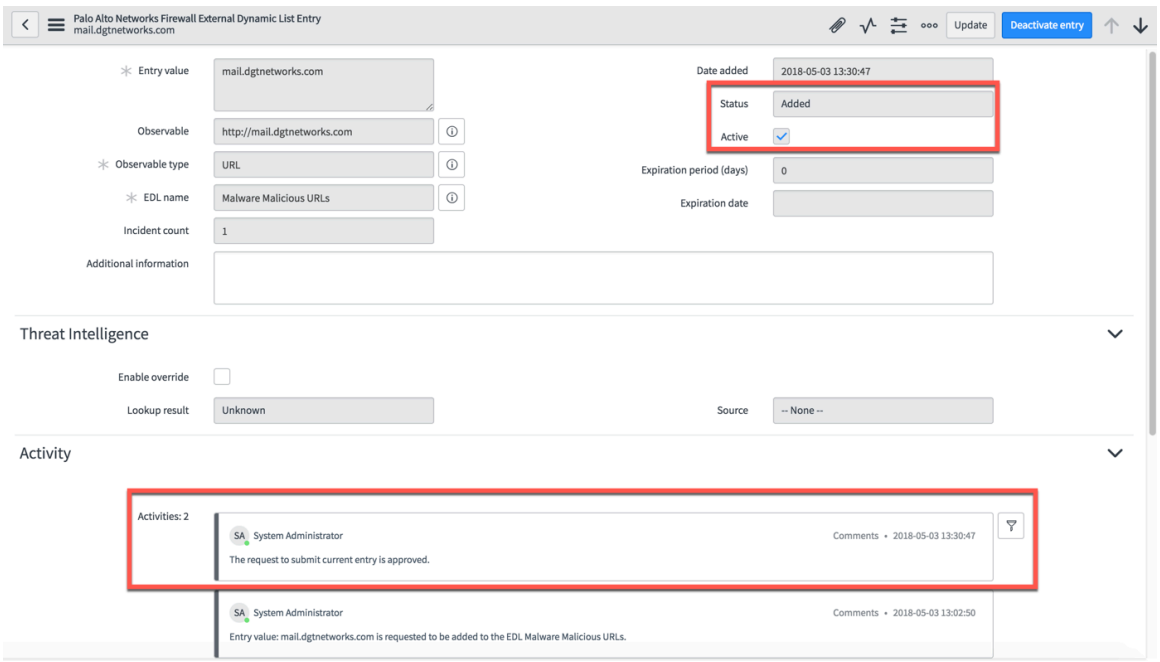
Option	Description
Approuver	Sur l'enregistrement d'entrée, le champ **État**devient `Ajouté` et la case **Actif** est cochée. Le bouton **Désactiver**est affiché et actif. Les notes de travail montrent que la demande d'entrée EDL a été approuvée.
Refuser	Sur l'enregistrement d'entrée, le champ État bascule sur **Rejeté** et la case **Actif** n'est

Traduction automatique

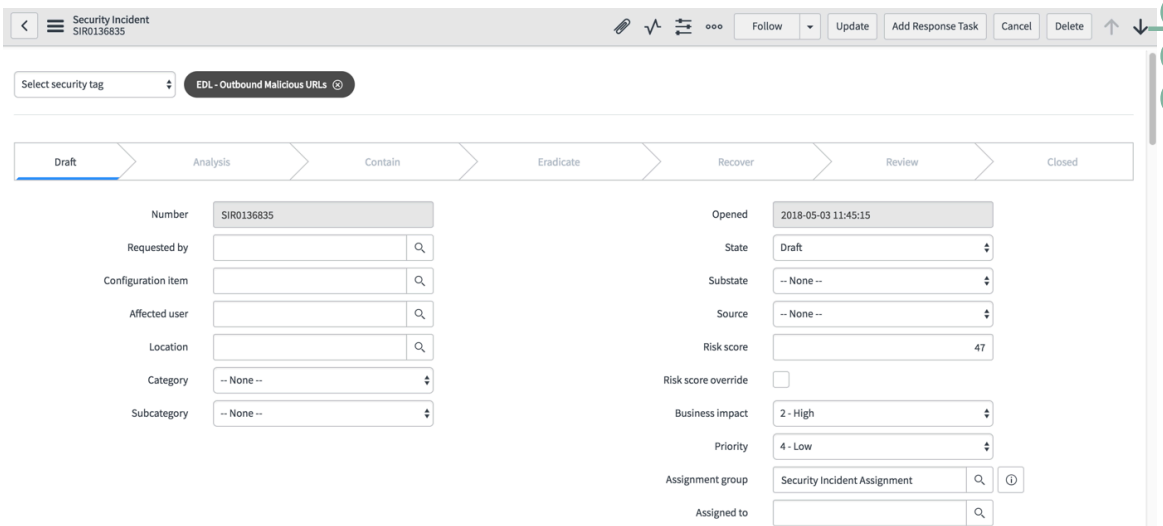
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	pas cochée, ce qui indique que l'entrée n'est pas bloquée sur le pare-feu. Les notes de travail indiquent que la demande d'entrée EDL a été rejetée.

Une fois que vous avez approuvé l'entrée EDL et qu'elle est activée, le Palo Alto Networks - Next-Generation Firewall récupère l'entrée EDL après l'intervalle de récupération suivant. Une fois l'entrée récupérée, l'observable est bloqué à partir de ce moment-là. Dans la figure suivante, notez que la case Actif est cochée, que l'état est Ajouté et que les notes de travail indiquent que la demande a été approuvée.



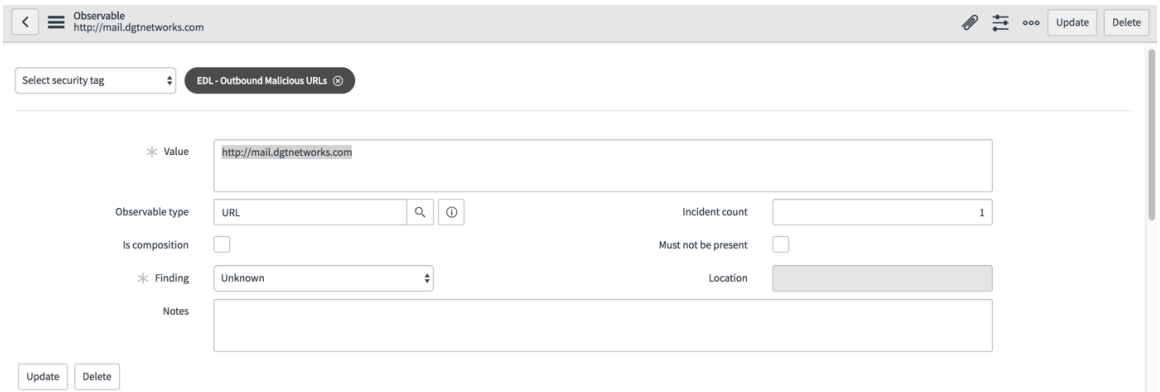
Une fois l'entrée EDL approuvée et activée, l'enregistrement d'incident de sécurité est marqué d'une balise de sécurité. La balise s'affiche en haut de l'enregistrement.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La balise de sécurité est également affichée sur l'enregistrement de l'observable.



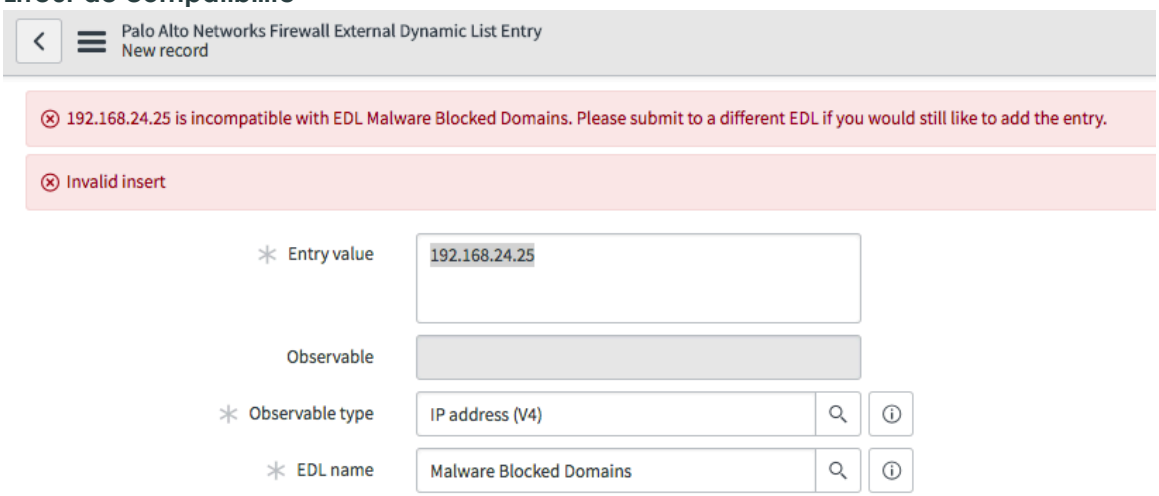
Exceptions d'entrée de l'EDL pour Palo Alto Networks - Next-Generation Firewall

Il existe des restrictions quant à l'ajout d'entrées de liste dynamique externe (EDL) aux EDL. En cas de conflit de doublons, de compatibilité ou CIDR (routage inter-domaine sans classe) lorsque vous essayez d'ajouter des entrées EDL aux EDL, des messages d'erreur s'affichent pour vous aider à résoudre ces erreurs.

Exception de compatibilité

Chaque EDL n'accepte que les entrées qui sont compatibles avec son type d'observable. Si vous créez un EDL de domaine et que vous essayez de lui attacher un observable d'adresse IP, un message d'erreur incompatible s'affiche. Par exemple, une EDL de domaine ne peut accepter que les observables de domaine, comme illustré dans la figure suivante.

Erreur de compatibilité



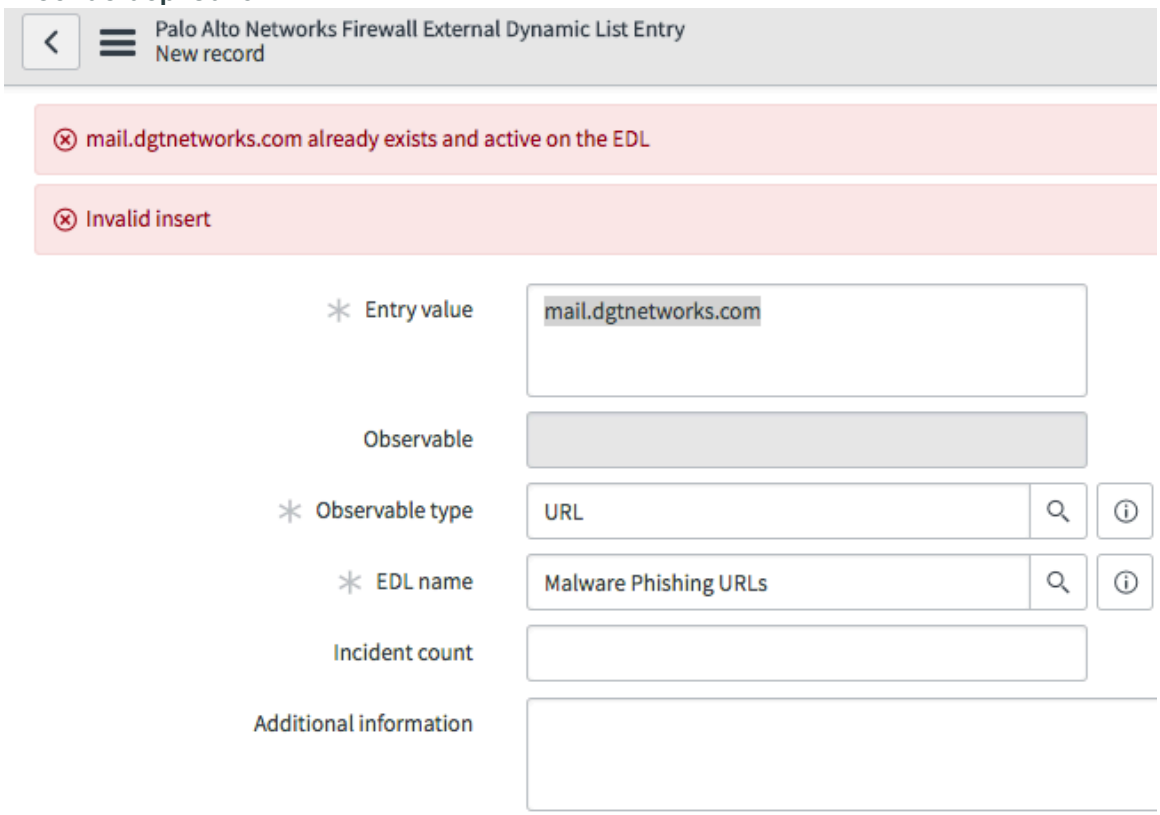
Exception de duplication

Un observable ne peut pas être activé sur plusieurs EDL du même type d'observable. Si un observable d'URL est déjà activé sur une EDL d'URL et que vous essayez d'activer le même observable sur une EDL d'URL d'hameçonnage, un message d'erreur de duplication s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreur de duplication



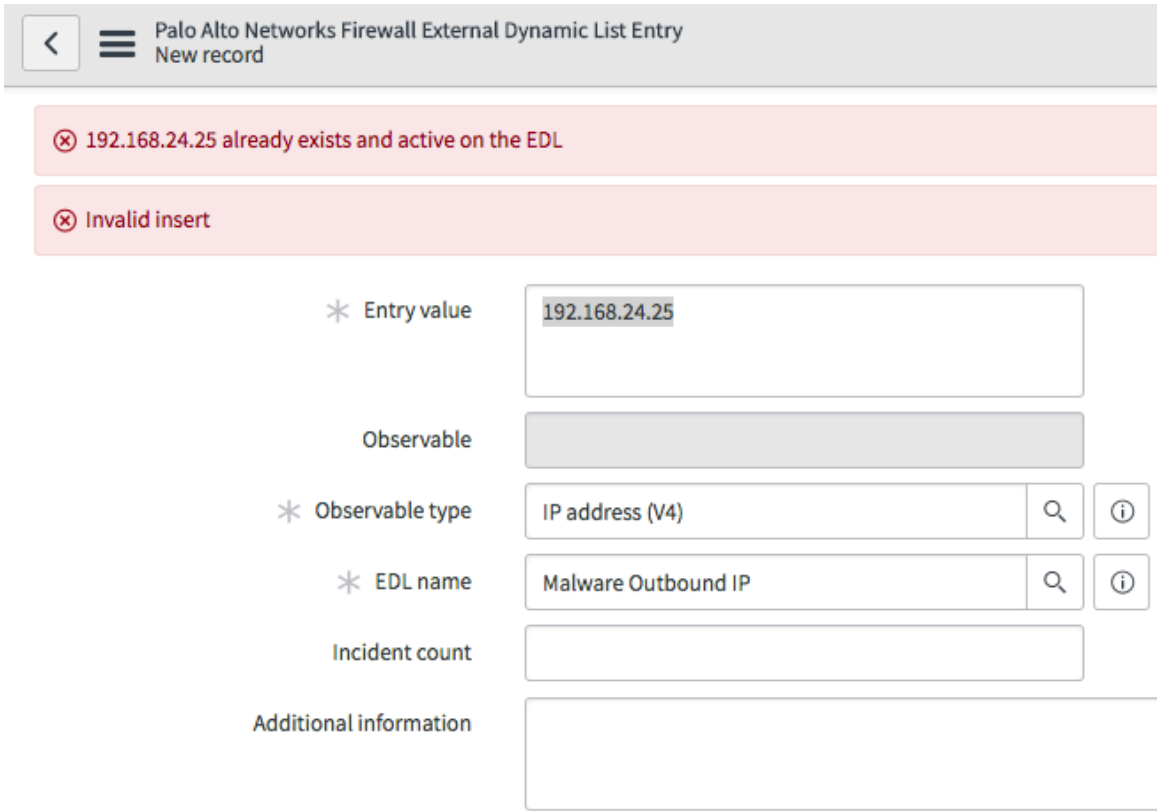
Exception CIDR (Classless Inter-Domain Routing)

Si vous tentez d'attacher une seule adresse IP à un EDL et que cette adresse IP fait partie d'un observable CIDR déjà présent sur un EDL, une erreur de conflit CIDR s'affiche. Cette erreur indique que l'adresse IP unique est déjà incluse dans l'EDL dans le cadre de l'observable CIDR. Par exemple, `192.168.24.25` fait partie du bloc CIDR `192.168.0.0/22`.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conflit CIDR



(Facultatif) Modifier le nom de la balise de sécurité pour Palo Alto Networks - Next-Generation Firewall

Si la case **Afficher la balise** est cochée lors de la création de l'enregistrement de la liste dynamique externe (EDL), vous pouvez modifier les noms des balises et les couleurs des balises de sécurité. Les balises de sécurité vous aident à suivre les observables qui sont déjà bloqués.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

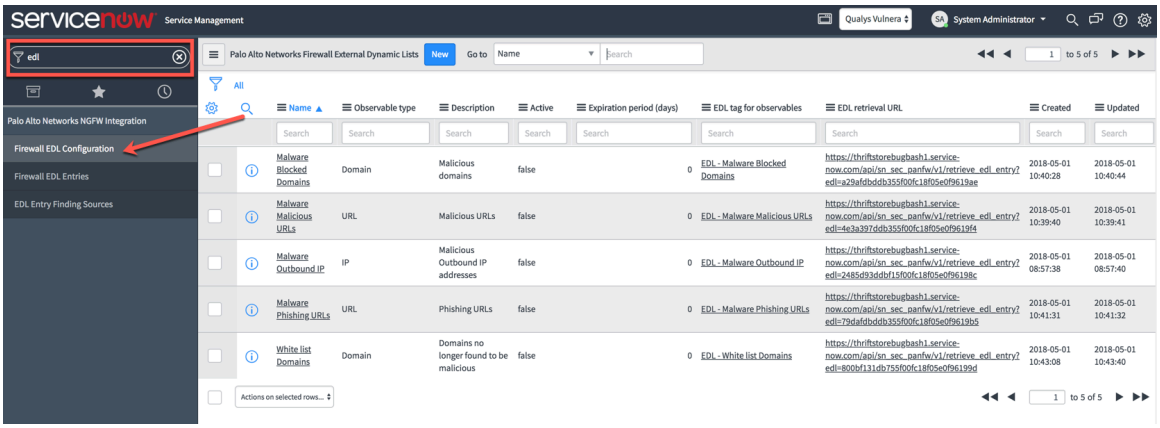
Les balises de sécurité vous aident à identifier rapidement quels incidents de sécurité ont des observables sur une liste de bloc. Les balises vous aident également à identifier si un observable est déjà bloqué ou s'il a été supprimé d'un EDL. Par défaut, la couleur de la balise de sécurité est noire pour les entrées de la liste de blocs et grise pour les entrées de la liste d'autorisation. Vous pouvez modifier les noms et les couleurs des balises pour vous aider à reconnaître plus facilement certaines balises.

Traduction automatique

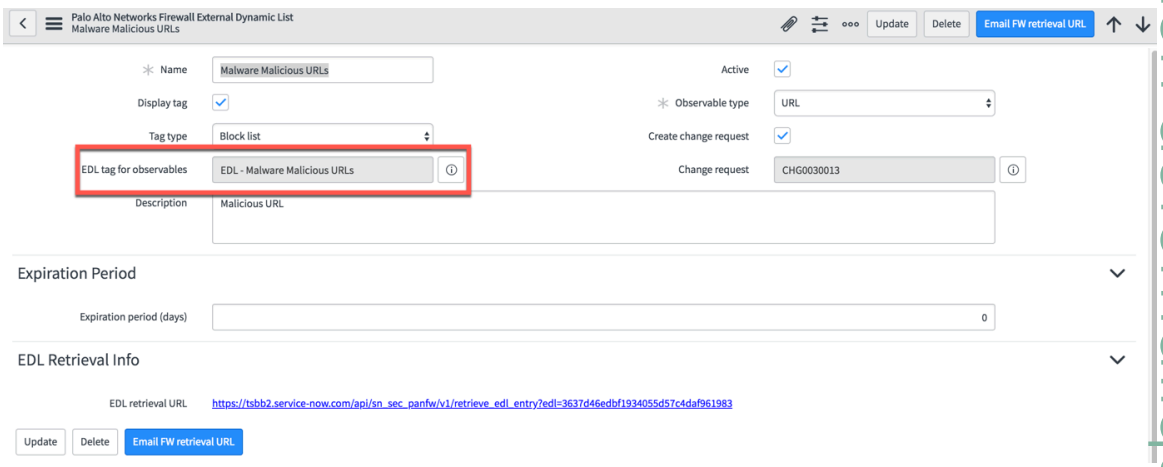
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

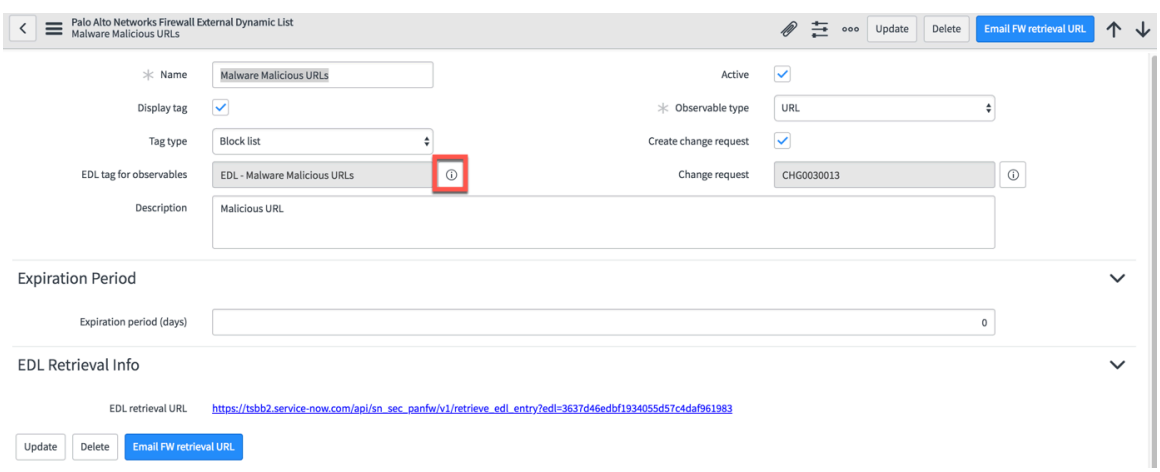
1. Accédez à la **Tout** > **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu**.



2. Cliquez sur un élément dans la colonne **Nom** pour l'ouvrir L'enregistrement EDL s'affiche. Par défaut, le nom de la balise de sécurité est la même que celle que vous avez saisie dans le champ **Nom** de l'EDL lorsque vous l'avez créée. Par défaut, le nom inclut également un préfixe EDL , par exemple, EDL – Malware Malicious URLs.



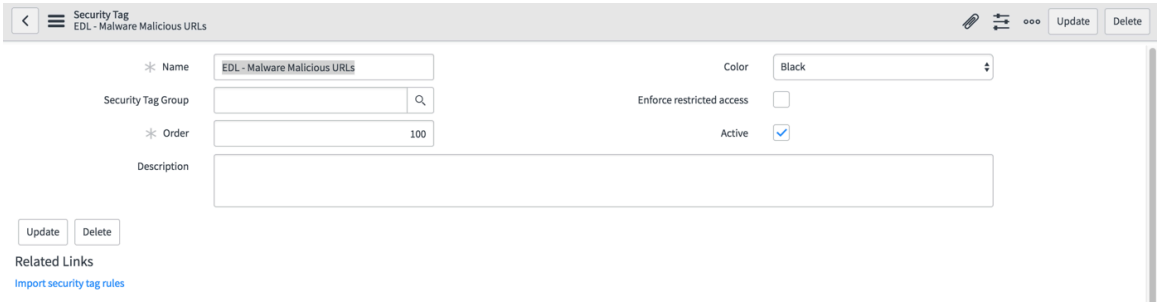
3. Cliquez sur l'icône d'informations (ⓘ) en regard de **Balise EDL pour les observables** , puis **Ouvrir l'enregistrement**.



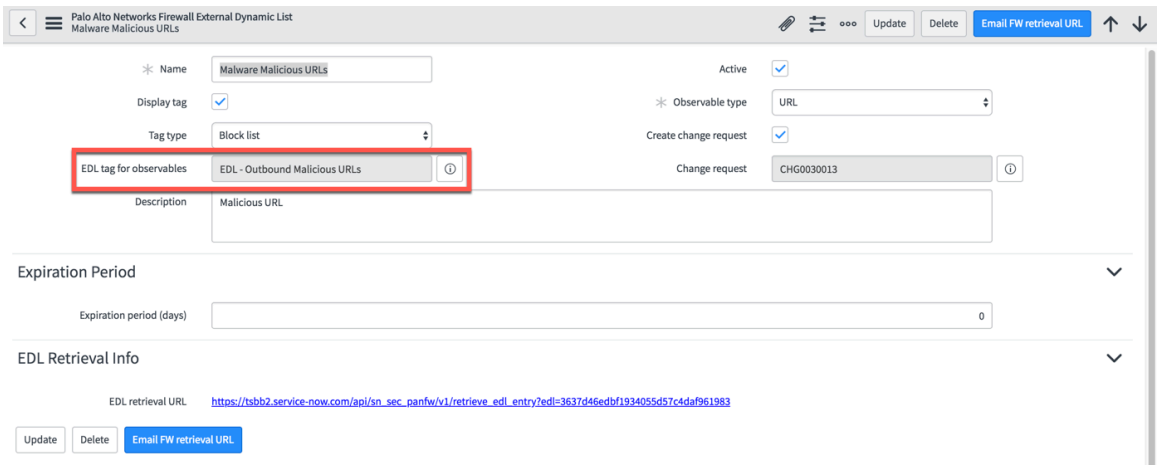
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

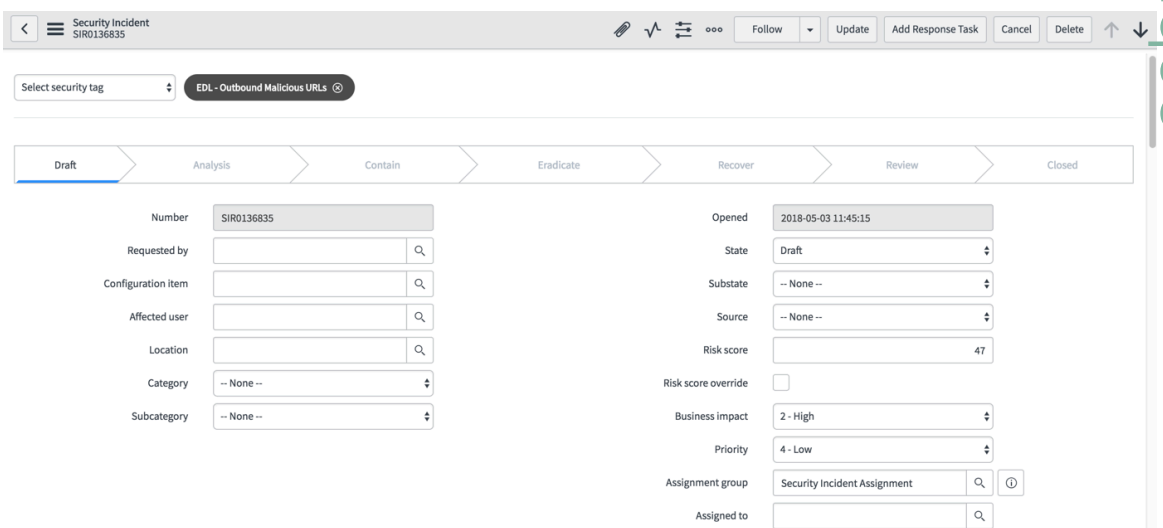
Le formulaire de balise de sécurité s'affiche.



4. Dans le champ **Nom** , modifiez le nom de la balise de sécurité et cliquez sur **Mettre à jour**. L'enregistrement EDL mis à jour s'affiche avec le nom de balise modifié. Dans l'exemple suivant, `Sortant` a été ajouté au nom de la balise. Conservez le préfixe `EDL` dans le nom de votre nouvelle balise pour vous aider à identifier qu'elle est associée à l'intégration Palo Alto Networks - Next-Generation Firewall .



Les balises de sécurité sont affichées pour chaque type d'observable (IP, URL, domaine) sur l'enregistrement d'incident de sécurité et l'enregistrement d'observable chaque fois que l'observable est ajouté à un EDL.



Si un observable a déjà été ajouté à un EDL et qu'une balise de sécurité est affichée sur un incident de sécurité pour cet observable, la balise de sécurité de l'EDL s'affiche

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

automatiquement sur tous les enregistrements d'incident de sécurité ultérieurs qui sont créés. Cette duplication vous indique que l'observable figure déjà sur une liste de blocs. Vous n'avez pas besoin d'ajouter cet observable et de le bloquer à nouveau.

Lorsqu'un observable n'est plus bloqué, une balise de sécurité n'est pas affichée sur l'enregistrement d'incident de sécurité ou l'enregistrement de l'observable. Dans ce cas, aucune balise de sécurité n'indique que la date d'expiration de l'observable est dépassée ou que l'observable a été désactivé à partir d'un EDL.

Désinstaller Palo Alto Networks - Next-Generation Firewall

Si vous souhaitez désinstaller Palo Alto Networks - Next-Generation Firewall de votre Now Platform instance et supprimer tous les éléments restants de l'intégration, consultez le site de documentation pour obtenir des instructions sur la ServiceNow désinstallation d'applications.

Avant de commencer

Rôle requis : Administrateur système (admin)
Reportez-vous à la section Désinstaller des applications sur le site web de la documentation produit ServiceNow .

PhishTank intégration

PhishTank est un système de vérification d'hameçonnage communautaire dans lequel les utilisateurs soumettent des menaces suspectes et les autres utilisateurs du système votent pour déterminer si les menaces d'hameçonnage sont légitimes. Lorsqu'ils sont intégrés au Now Platform Opérations de sécurité produit, les résultats de Threat Intelligence fournissent aux analystes des informations supplémentaires sur les incidents de sécurité ou les enquêtes liés au phishing.

L'intégration PhishTank effectue des recherches sur les URL de sites d'hameçonnage potentiels.

Le workflow recherche les nouveaux observables au fur et à mesure qu'ils arrivent dans les incidents de sécurité. Si les observables sont d'un type reconnu par l'intégration de l'API, les observables sont évalués. Les observables jugés malveillants sont étiquetés.

Installer et configurer PhishTank

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration pour que l'application s'intègre PhishTank correctement à Now Platform Opérations de sécurité.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâches de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform à votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (admin) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	et vérifie les résultats attendus. Ce rôle a également accès au Opérations de sécurité module.
Procurez-vous une clé API.	Visitez le site Web pour plus d'informations sur les PhishTank clés API et pour créer un compte : site Web PhishTank .
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Configuration requise pour la version Madrid et ultérieure Pour la version Madrid et les versions ultérieures de la famille, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Orchestration de support de sécurité Pour en savoir plus sur la configuration de votre Now Platform instance pour l'intégration, consultez et .

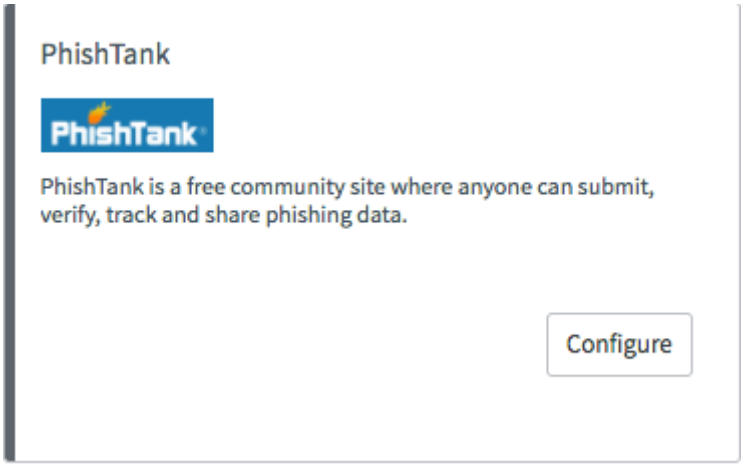
Rôle requis : administrateur

Procédure

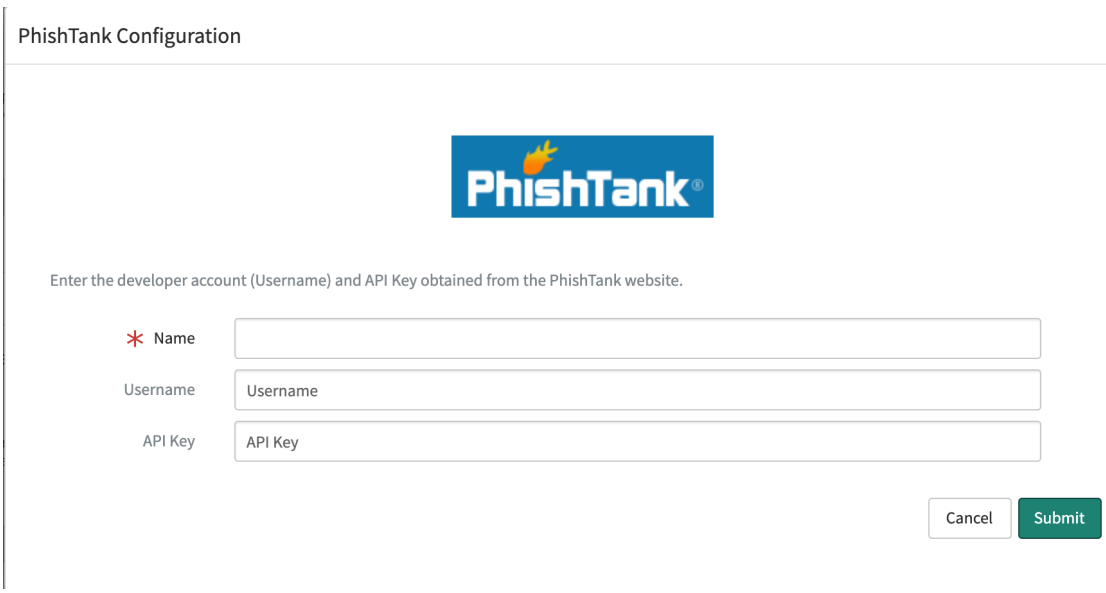
1. Si vous n'avez pas installé l'application pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la PhishTank tuile.
3. Cliquez sur **Configurer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans la boîte de dialogue **Configuration de PhishTank** , saisissez le nom de la configuration, le nom d'utilisateur (compte développeur créé dans PhishTank) et la clé API que vous avez obtenus à partir du PhishTank site web, puis cliquez sur **Envoyer**.



5. Vérifiez que la configuration est correcte.
   La configuration est terminée avec succès, sauf si un message d'erreur s'affiche.

   Trouble?

   Si un message d'erreur s'affiche lors de la configuration, la clé API n'est PhishTank peut-être pas valide.

Vérifier les résultats attendus pour PhishTank

Les observables sont générés automatiquement par un incident de sécurité et analysés par l'application. Les résultats de la recherche sont affichés dans l'onglet Résultats de la recherche de menace en bas de l'enregistrement d'incident de sécurité.

Avant de commencer

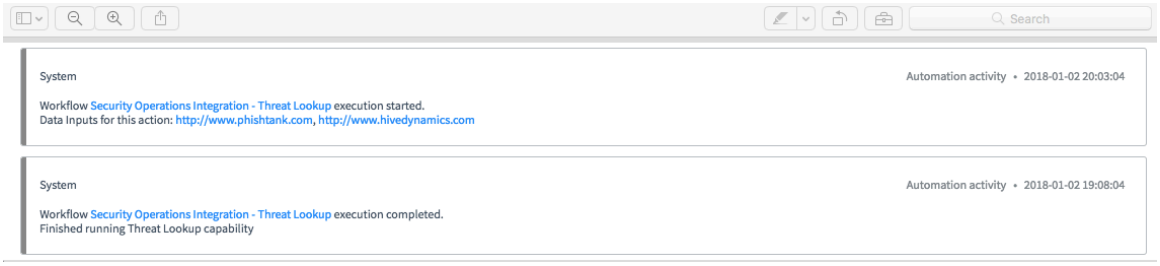
Rôle requis : sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez le formulaire d'incident de sécurité que vous utilisez et vérifiez que la recherche a été exécutée correctement.

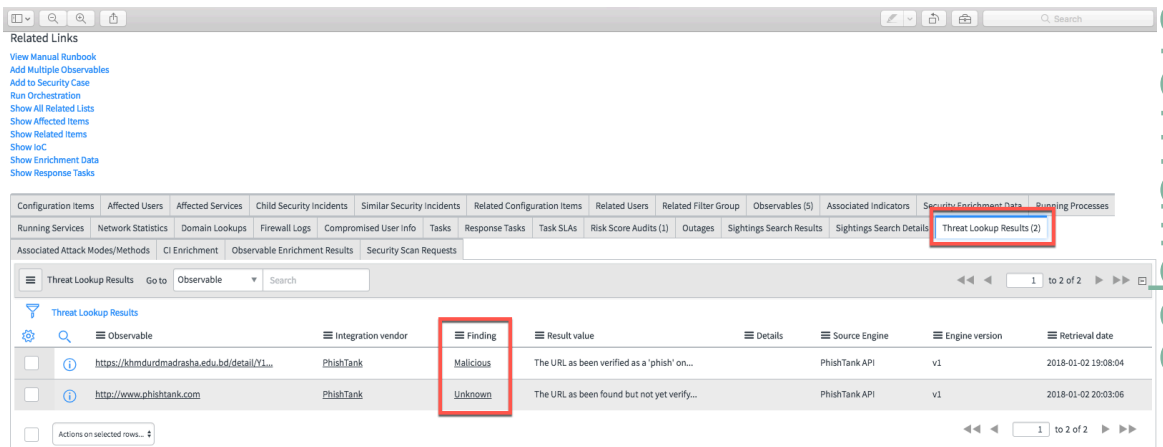


   Une fois l'application configurée, le flux se lance automatiquement lors de la création de l'incident. L'état d'exécution et d'achèvement de la recherche est ensuite affiché dans les notes de travail de l'enregistrement d'incident de sécurité.

2. Consultez les notes de travail pour plus d'informations et pour savoir comment procéder si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.

3. Accédez au bas de l'incident de sécurité et cliquez sur le lien connexe **Afficher toutes les listes connexes** .

   Remarque : Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres du système. Si les formulaires à onglets ne sont pas affichés, cliquez sur l'icône d'engrenage Paramètres dans le coin supérieur droit de la bannière. Dans la boîte de dialogue **Paramètres du système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que les **champs Formulaires à onglets** et **Avec formulaire** sont sélectionnés.



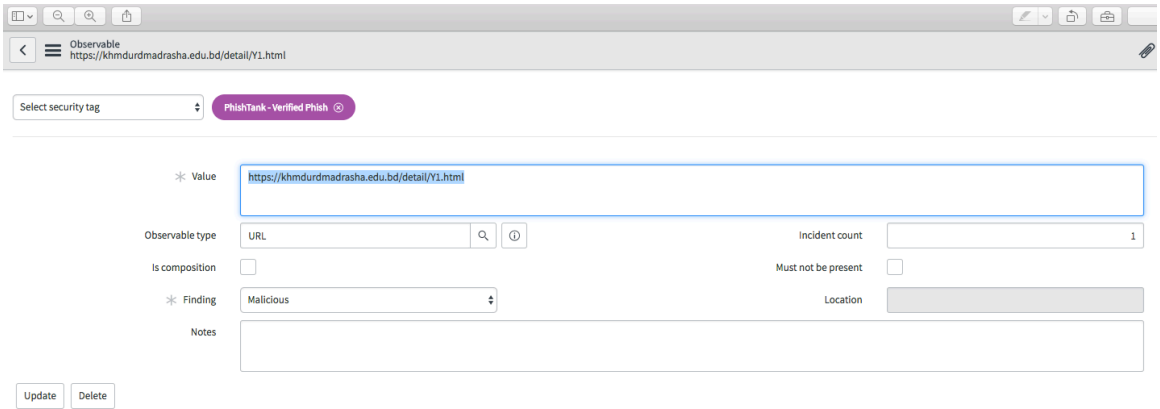
   L'onglet Résultats de la recherche de menaces au bas de l'enregistrement d'incident de sécurité affiche les résultats de la recherche.

   La colonne **Résultat** affiche `Inconnu` pour les enregistrements qui n'ont pas été déterminés comme malveillants. Pour les résultats correspondant à malveillants, `Malveillant` s'affiche dans la colonne **Résultat** .

4. Dans la colonne **Observable** , cliquez sur un observable pour ouvrir un enregistrement et afficher plus d'informations.

Traduction automatique

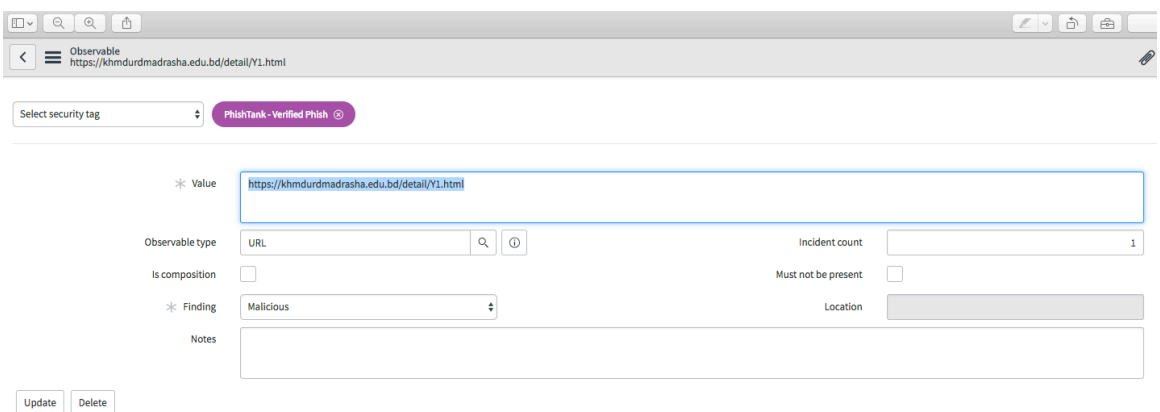
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Dans l'enregistrement de l'observable, pour les recherches correspondant à malveillant, `le` champ **Résultat** s'affiche. L'observable est étiqueté avec la source qui l'a trouvé malveillant, dans ce Renseignements sur les menaces cas, l'application PhishTank .

5. Pour afficher les données brutes, revenez à l'incident de sécurité et cliquez sur l'icône d'informations bleue en regard d'un observable.

6. Dans la fenêtre qui s'affiche, cliquez sur **Ouvrir l'enregistrement**.



Le lien créé par l'API et le champ **Résultat** affiché avec les résultats.

Trouble?
Si vous ne voyez pas de résultats sous l'onglet **Résultats de la recherche de menace** , vérifiez que l'observable est d'un type pris en charge pour la recherche par l'intégration.

(Facultatif) Joindre manuellement un observable pour PhishTank

Vous pouvez joindre manuellement des observables à un incident de sécurité. Vous joignez manuellement les observables lorsque vous souhaitez effectuer des recherches de menaces sur des observables qui ne sont pas joints à un incident de sécurité sur le déclencheur d'événement initial. Vous pouvez également effectuer cette tâche lorsque vous souhaitez plus d'informations sur un observable associé.

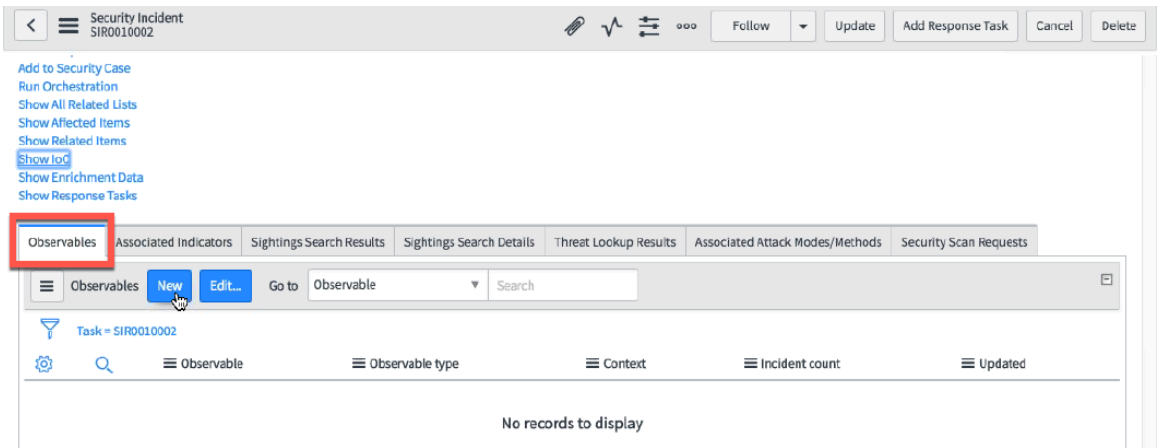
Avant de commencer
Rôle requis : sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

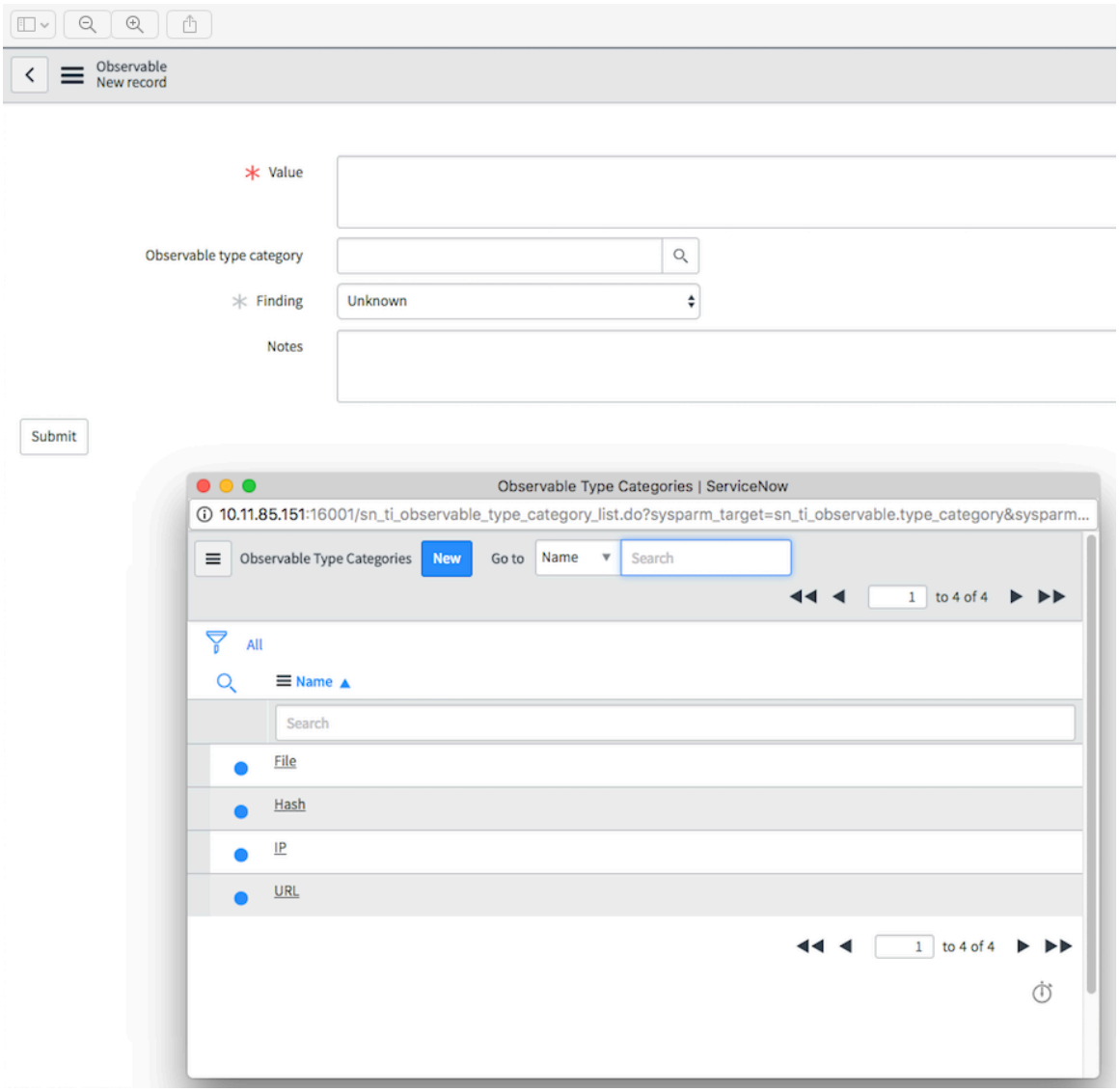
1. Accédez à votre incident de sécurité ouvert.
2. Dans l'enregistrement d'incident de sécurité ouvert, cliquez sur le lien **Afficher IoC**dans **Liens connexes** pour afficher l'onglet **Observables** .



3. Cliquez sur **Nouveau**.
   Le formulaire Observable s'affiche.
4. Dans le champ **Valeur** , saisissez une URL.
5. Cliquez sur l'icône de recherche puis, dans la boîte de dialogue **Catégories de types d'observables** , cliquez sur **URL** dans la liste pour remplir le champ.

Traduction automatique

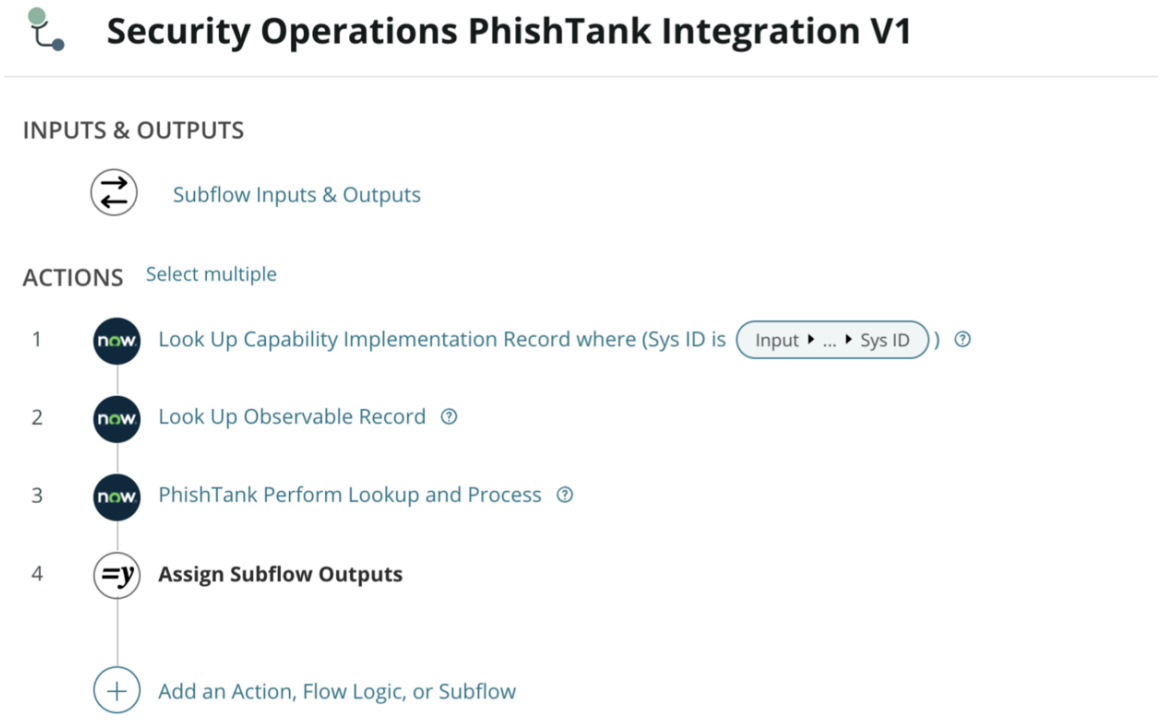
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



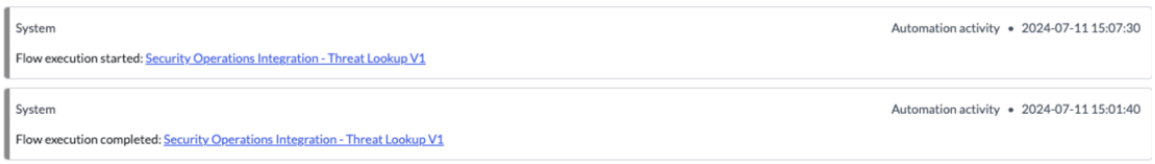
6. Cliquez sur **Envoyer**.
   Le flux lance et vérifie le nouvel observable. L'état d'exécution et d'achèvement est affiché dans la section des notes de travail de l'enregistrement d'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

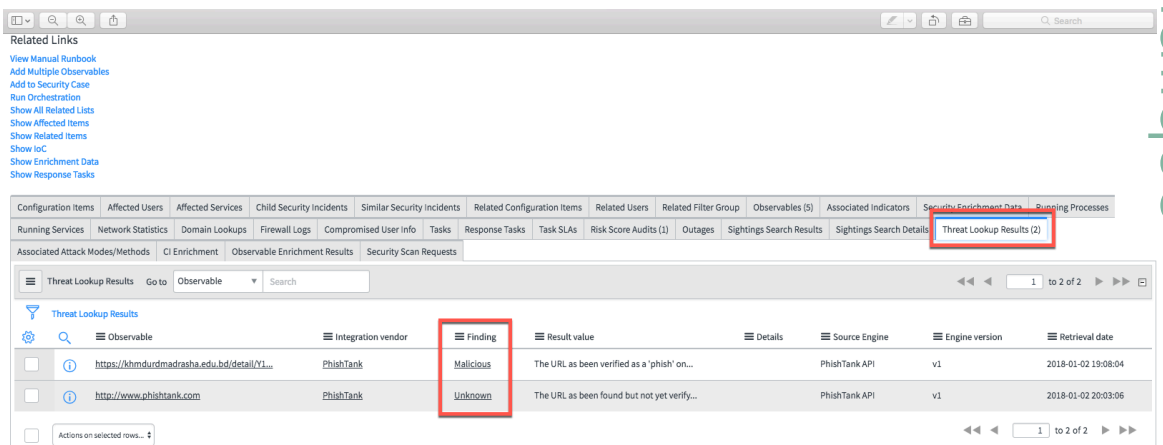


7. Accédez à votre incident de sécurité et passez en revue les notes de travail.



8. Cliquez sur le lien connexe **Afficher toutes les listes connexes** en bas de l'incident de sécurité.

9. Cliquez sur l'onglet **Résultats de la recherche de menaces** pour afficher les résultats.



10. Dans la colonne **Observable** , cliquez sur l'icône d'information bleue en regard d'un observable donné pour plus d'informations et de données brutes.

11. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Trouble?
Consultez les notes de travail pour plus d'informations et pour savoir comment procéder si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.

Reverse Whois intégration

Reverse Whois est un service qui effectue des recherches sur des noms de domaine enregistrés par des individus ou des organisations.

Effectuez des recherches de domaine à l'aide de termes de recherche dans les observables que vous joignez à un incident de sécurité. L'API Reverse Whois recherche les enregistrements de domaine en fonction des termes de recherche que vous saisissez et renvoie tous les enregistrements qui correspondent à ces termes.

Les analystes utilisent parfois cette intégration en même temps que l'intégration pour la recherche d'incidents Whois de sécurité. L'intégration Whois fournit des informations d'enrichissement supplémentaires en fonction des recherches de domaine issues de l'intégration Reverse Whois .

Installer et configurer Reverse Whois

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que l'application Reverse Whois s'intègre correctement au Opérations de sécurité produit.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow .	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (admin) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration. L'administrateur d'incident de sécurité affecte également le rôle d'analyste des incidents de sécurité (sn_si.analyst). • L'analyste des incidents de sécurité (sn_si.analyst) effectue des recherches de domaine avec Reverse Whois , analyse et travaille avec les incidents de sécurité.
Procurez-vous une clé API.	Visitez le site Web de l'API WhoisXML pour plus d'informations sur les clés API et pour créer un compte : site Web de l'API WhoisXML . La configuration nécessite que vous saisissiez les clés API.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Configuration requise pour la version Madrid et ultérieure Pour la version Madrid et les versions ultérieures de la famille, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Orchestration de support de sécurité Pour en savoir plus sur la configuration de votre Now Platform instance pour l'intégration, consultez et .

Rôle requis : administrateur

Procédure

1. Si vous avez déjà installé et configuré l'application Reverse Whois , procédez comme suit :

   a. Supprimez la configuration existante.

   b. Installez et créez une nouvelle configuration à l'aide de la clé API que vous avez obtenue.

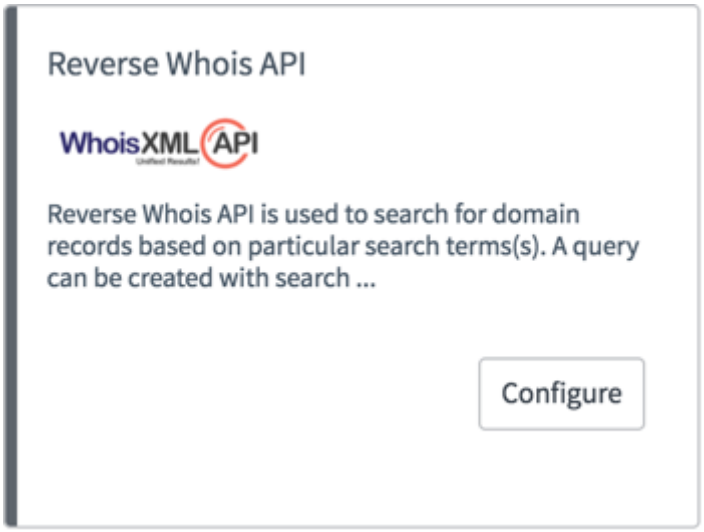
2. Si vous n'avez pas installé l'application pour l'intégration, consultez et suivez les étapes pour l'installer.

3. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette de l'API Reverse Whois .

4. Cliquez sur **Configurer**.

Traduction automatique

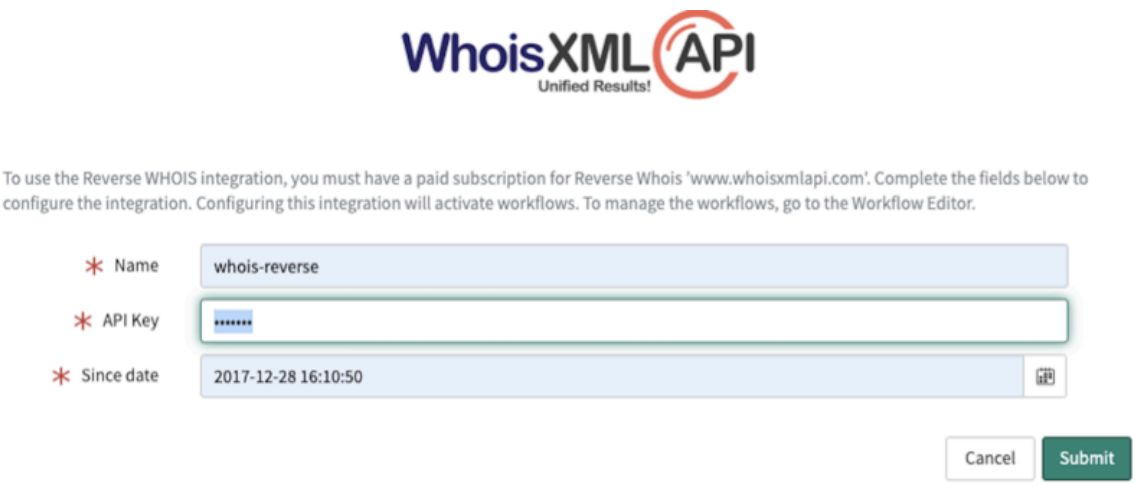
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Dans la boîte de dialogue **Configuration de l'API Reverse Whois** , entrez la clé API que vous avez obtenue à partir du site Web de l'API XML Whois .
6. Choisissez une option dans le tableau suivant pour filtrer les recherches de domaine pour vos termes de recherche.

Description	Paramètre
Votre recherche inclut tous les domaines, actifs et expirés, qui ont été enregistrés après la date Depuis pour les termes de recherche que vous saisissez. Il s'agit du paramètre recommandé.	**Depuis date** : date saisie au format aaaa-mm-jj. Par exemple, `1991-06-01` pour le 1er juin 1991.
Votre recherche inclut tous les domaines actifs pour les termes de recherche que vous saisissez.	**Depuis la date** : Champ effacé.

Ces paramètres de configuration restent enregistrés jusqu'à ce que vous les changiez et que vous les appliquiez à toutes les Reverse Whois recherches d'API.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Envoyer**.
   La configuration est terminée avec succès, sauf si un message d'erreur s'affiche.

Trouble?
Si un message d'erreur s'affiche, la clé API n'est peut-être pas valide.

Message d'erreur

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

(Facultatif) Installer et configurer Whois

Installez le module d'extension Whois pour fournir des informations d'enrichissement supplémentaires sur vos recherches de domaines à partir de l'API Reverse Whois . Cette recherche fournit des données d'enrichissement supplémentaires sur le domaine, telles que la date d'enregistrement, le nom du bureau d'enregistrement et le pays d'origine.

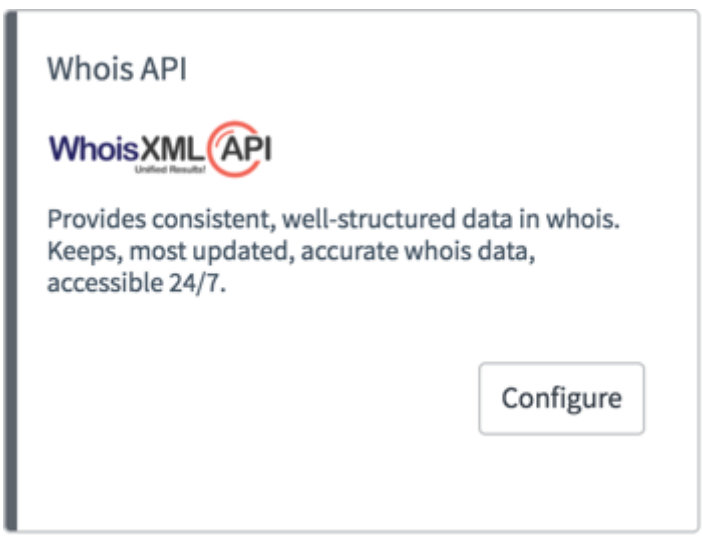
Avant de commencer

1. Si vous n'avez pas demandé d'autorisation pour l'application, consultez l'application Whois à partir de ServiceNow Store.
2. Obtenez les informations d'identification pour la Whois clé API à partir du site Web du produit : site Web de l'API WHOIS .

Rôle requis : administrateur

Procédure

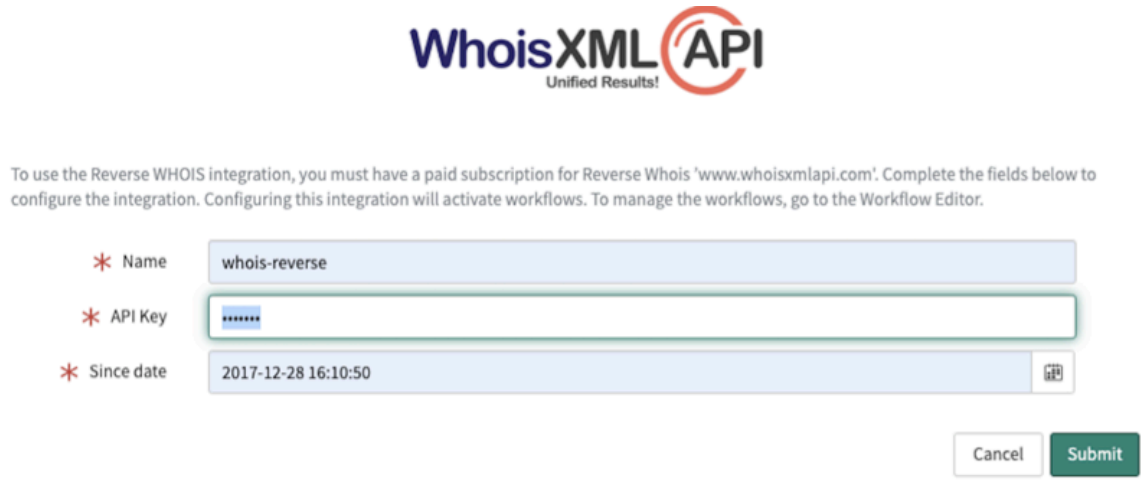
1. Si vous n'avez pas installé l'application, consultez et suivez les étapes pour l'installer.
2. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette de l'API Whois .
3. Cliquez sur **Configurer**.



4. Dans la boîte de dialogue **Configuration de l'API Whois** , saisissez la clé API que vous avez obtenue sur le site Web du produit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
   La configuration est terminée avec succès, sauf si un message d'erreur s'affiche. Vous pouvez maintenant exécuter des recherches d'enrichissement sur les domaines renvoyés par l'intégration Reverse Whois .

Trouble?
Si un message d'erreur s'affiche, la clé API n'est peut-être pas valide.

Dépannage

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

Lancer la recherche de Reverse Whois

Lancez des recherches de domaines à l'aide de termes de recherche dans les observables que vous joignez manuellement à un enregistrement d'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

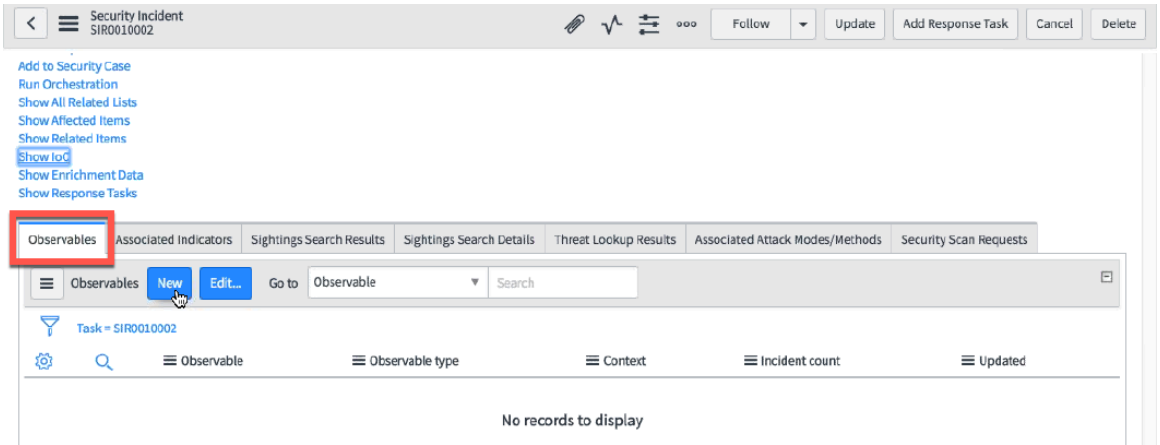
Procédure

1. Si ce n'est pas ouvert, accédez à **Incident de sécurité** > **Incidents** > **Afficher les incidents** et ouvrez l'incident de sécurité sur lequel vous travaillez.
2. En bas de l'enregistrement, cliquez sur le lien connexe **Afficher IoC** pour afficher l'onglet Observables.

> **Remarque :** Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres du système. Si vous ne voyez pas d'onglets sur l'incident de sécurité, dans le coin supérieur droit de la bannière, cliquez sur l'icône d'engrenage **Paramètres** . Dans la boîte de dialogue **Paramètres du système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que les **champs Formulaires à onglets** et **Avec formulaire** sont sélectionnés.

Traduction automatique

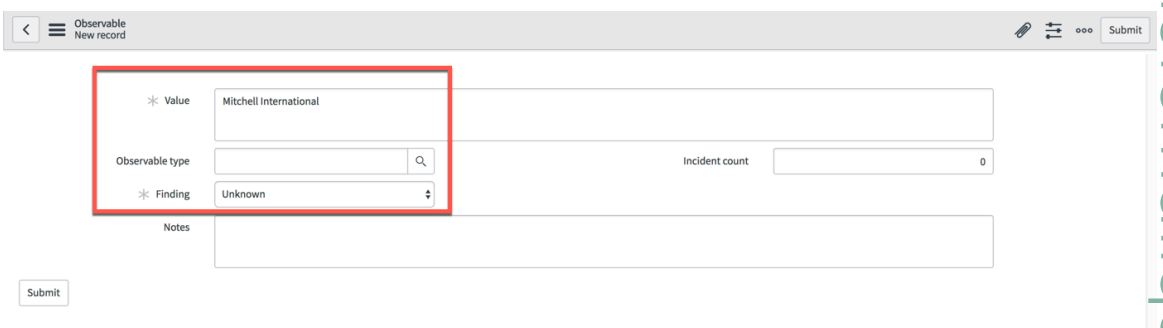
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans l'onglet Observables, cliquez sur **Nouveau**.
4. Renseignez les champs.

Champs obligatoires du nouvel enregistrement

Champ	Description
Valeur	Terme de recherche unique pour un domaine.
Type d'observable	Ce champ est automatiquement effacé.
Résultat	Ce champ est automatiquement défini sur **Inconnu**.



5. Cliquez sur **Envoyer**.
   Vous êtes renvoyé à l'enregistrement d'incident de sécurité et le flux lance la recherche.

Que faire ensuite

Vérifiez les résultats de la recherche sur l'incident de sécurité. Consultez Vérifier les résultats attendus pour Reverse Whois.

Vérifier les résultats attendus pour Reverse Whois

Les résultats de l'enrichissement sont affichés dans l'onglet **Domaines ReverseWhois** en bas de l'enregistrement d'incident de sécurité. Localisez les résultats de la recherche pour vérifier que la recherche s'est correctement exécutée.

Avant de commencer

Rôle requis : sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si ce n'est pas déjà fait, accédez à **Incidents de sécurité** > **Incidents** > **Afficher les incidents** et localisez l'incident de sécurité sur lequel vous travaillez.



Une fois l'application configurée et que vous avez joint un observable, le flux se lance automatiquement. Les notes de travail sur l'enregistrement d'incident de sécurité affichent l'état d'exécution et d'achèvement de la recherche.

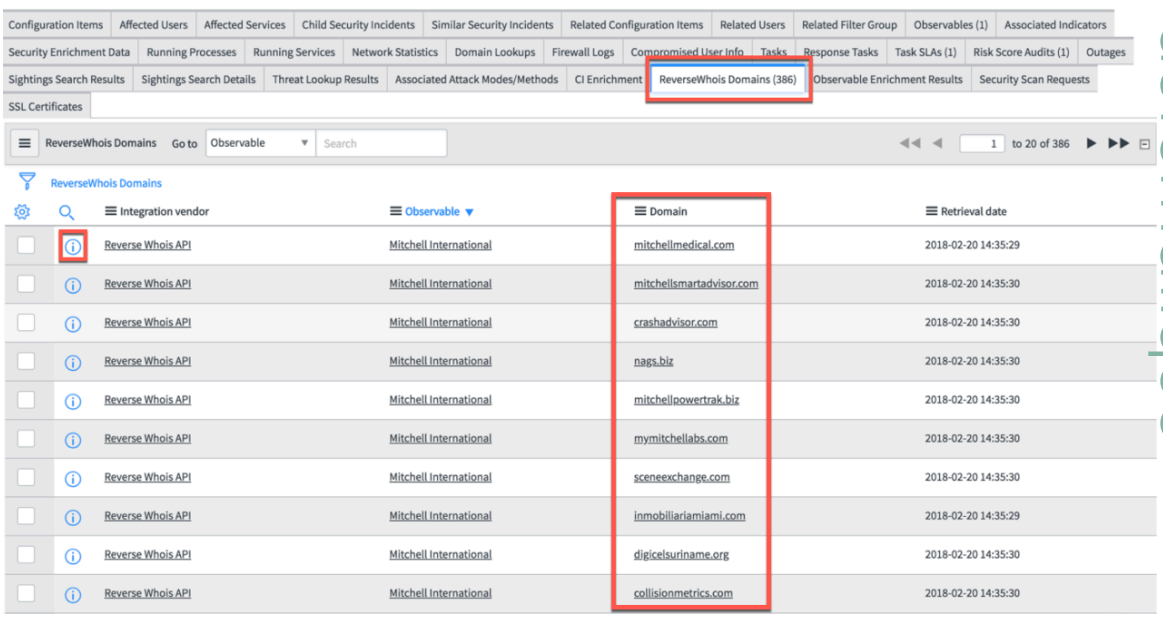


2. Si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée, consultez les notes de travail pour plus d'informations sur la façon de procéder.



3. Accédez au bas de l'incident de sécurité et cliquez sur le lien connexe **Afficher toutes les listes connexes** .

Remarque : Pour les résultats de recherche filtrés présentés dans la figure suivante, les paramètres de configuration dans la vignette de configuration de l'API Reverse Whois ont été enregistrés avec **1991-06-01** saisi dans le champ **Depuis date** .

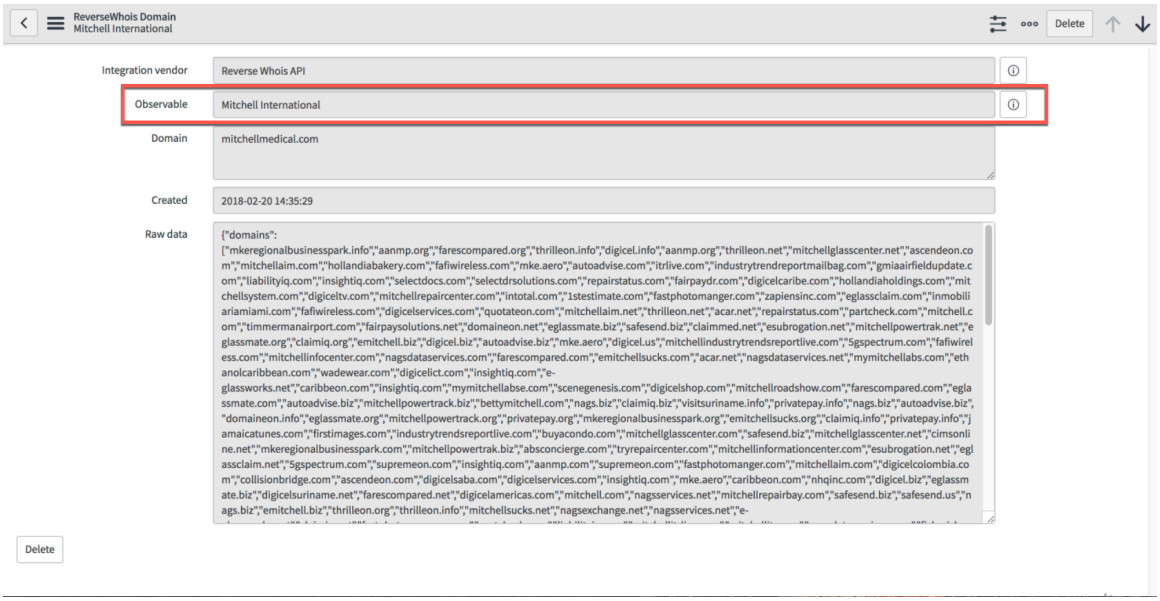


Les résultats de l'enrichissement sont affichés dans l'onglet **Domaines ReverseWhois** . Les domaines actifs de cet observable sont affichés dans la colonne **Domaine** .

4. Cliquez sur l'icône d'information bleue en regard d'un élément, puis cliquez sur **Ouvrir l'enregistrement** dans la boîte de dialogue qui s'affiche.

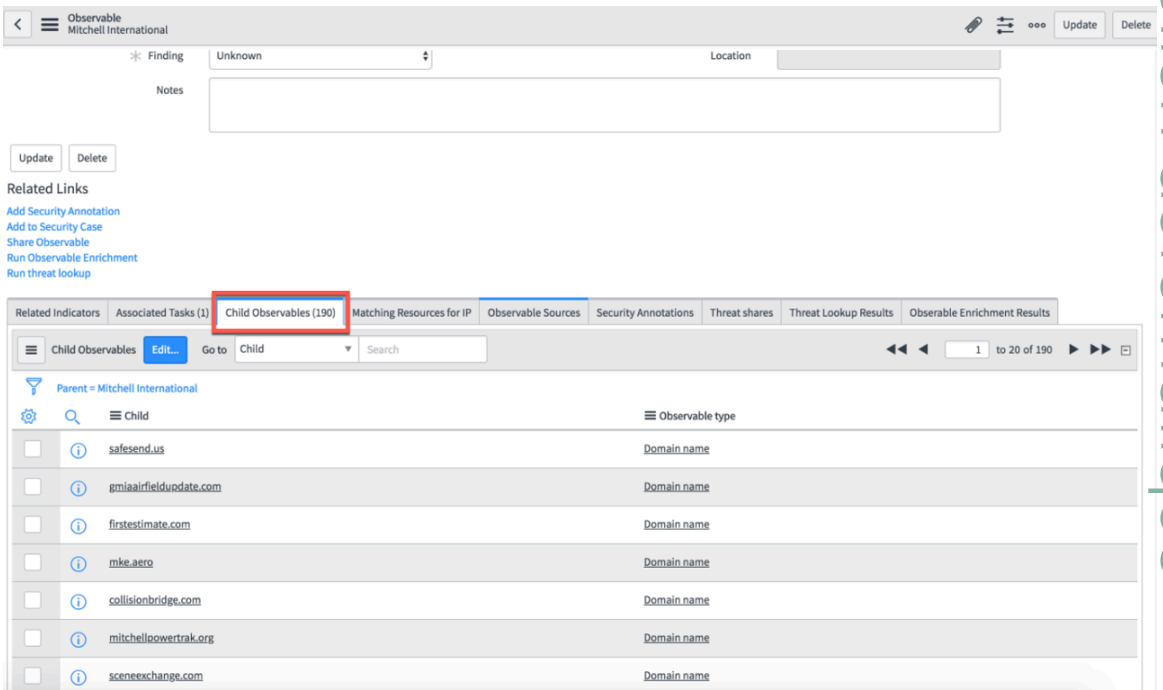
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'enregistrement s'affiche avec les détails d'enrichissement, y compris les données brutes.

5. Revenez à l'incident de sécurité et, avec l'onglet **ReverseWhois Domains** sélectionné, cliquez sur un observable dans la colonne **Observable** pour ouvrir un enregistrement.



Les observables enfants sont affichés dans l'onglet **Observables enfants** de l'enregistrement Observable. Les observables enfants sont générés uniquement si l'application Reverse Whois a renvoyé des domaines.

Trouble?
Si la recherche échoue, vérifiez que les termes de recherche que vous avez saisis sont pris en charge par l'intégration. Passez en revue les notes de travail pour plus d'informations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Pour obtenir plus de données d'enrichissement sur les résultats de la recherche de domaine, vous pouvez exécuter l'intégration Whois pour effectuer des recherches d'enrichissement sur les observables enfants retournés par l'intégration Reverse Whois . Ces données d'enrichissement sur les observables enfants comprennent des informations sur la date d'enregistrement, le nom du bureau d'enregistrement et le pays d'origine.

(Facultatif) Exécuter la recherche d'enrichissement et vérifier les résultats attendus pour Whois

Exécutez l'intégration Whois pour effectuer des recherches d'enrichissement sur les domaines renvoyés par l'intégration Reverse Whois .

Avant de commencer

Vérifiez que vous avez installé et configuré les modules d'extension Reverse Whois and Whois . Effectuez ces étapes uniquement après avoir exécuté avec succès la recherche de domaine avec le module d'extension Reverse Whois .

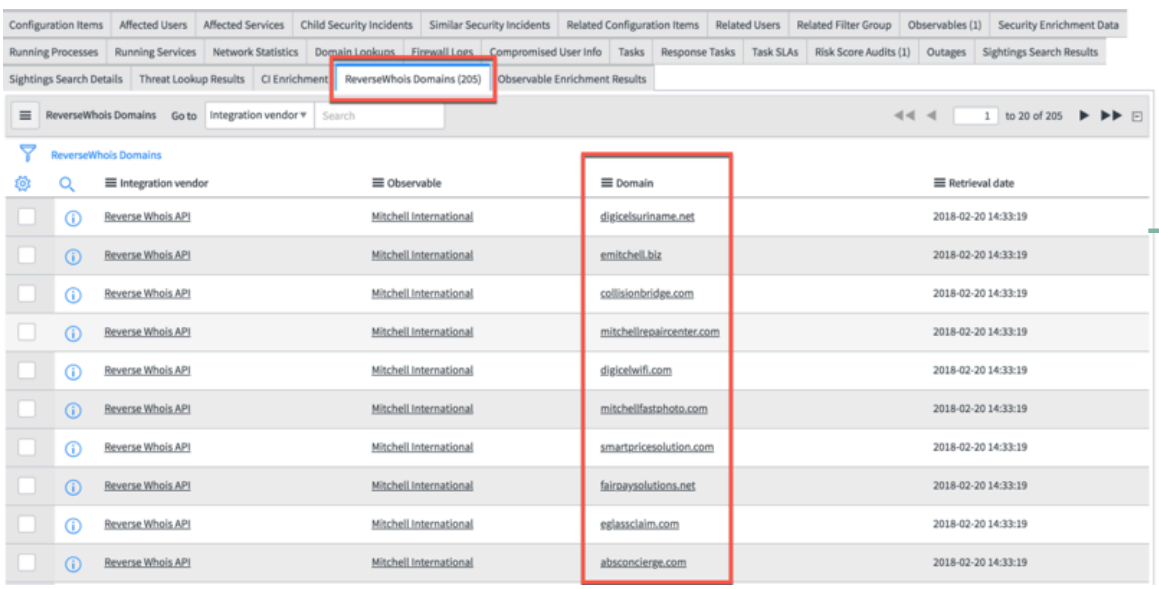
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Les résultats sont affichés dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement Observable.

Procédure

1. Accédez à la **Tout** > **Incidents de sécurité** > **Incidents** > **Afficher les incidents** et localisez l'incident de sécurité sur lequel vous travaillez et qui a exécuté la recherche de domaine avec succès.
2. Ouvrez l'enregistrement et cliquez sur le lien connexe **Afficher toutes les listes connexes** .
3. Sélectionnez l'onglet **Inverser les domaines d'identification** en bas de l'enregistrement.

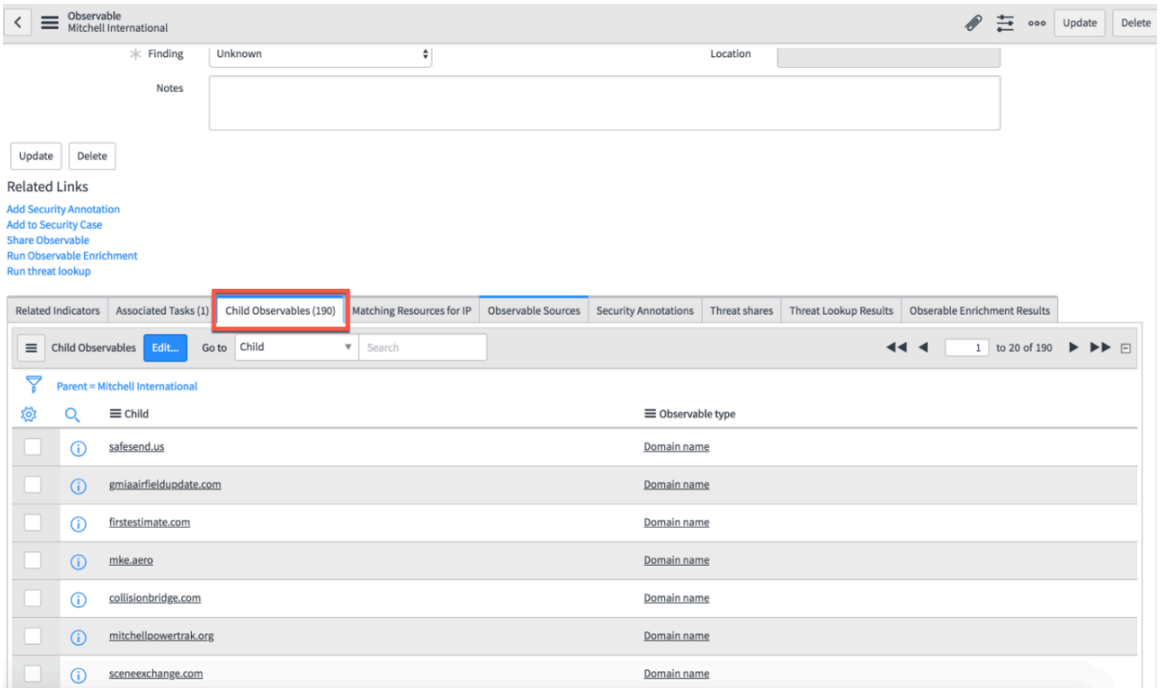


Dans la colonne Domaines, la liste **des** domaines renvoyés s'affiche.

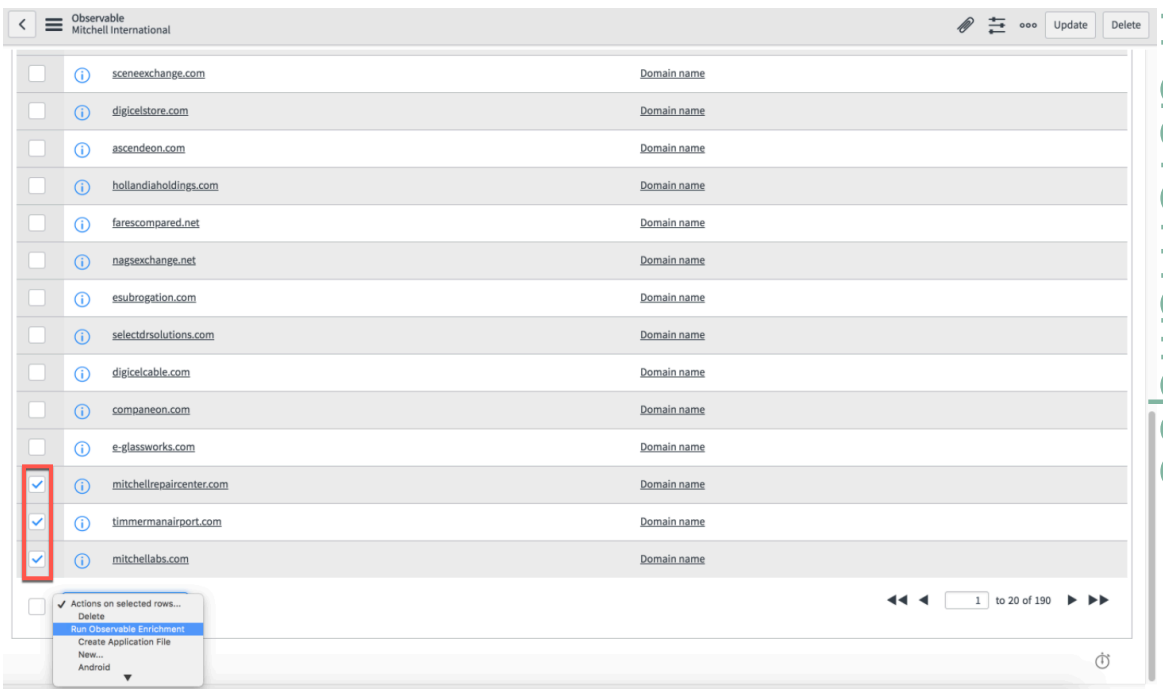
4. Dans la colonne **Observable** , cliquez sur un observable.
   Les observables enfants s'affichent dans l'onglet **Observables enfants** . Les observables enfants sont générés uniquement si l'analyse initiale de l'observable par l'application Reverse Whois a renvoyé des domaines.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Sélectionnez les observables enfants sur lesquels vous souhaitez exécuter l'enrichissement des observables et, dans la liste **de choix Action sur les lignes sélectionnées** , sélectionnez **Exécuter l'enrichissement des observables**.

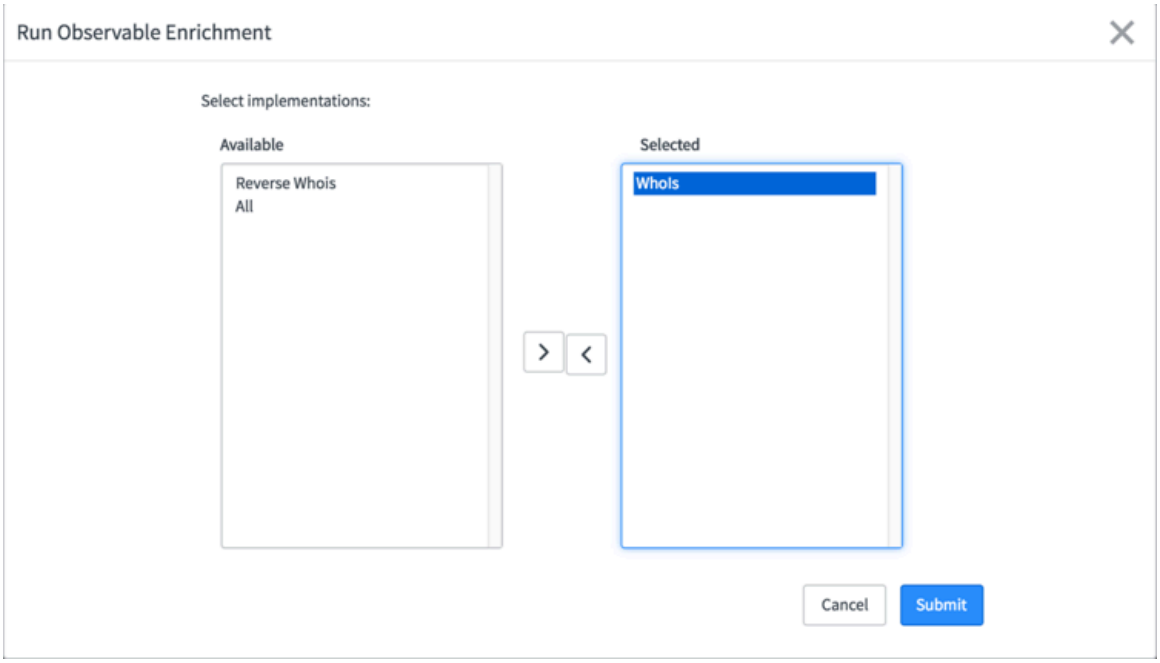


La boîte **de dialogue Exécuter l'enrichissement de l'observable** s'affiche.

6. Déplacez l'intégration Whois de **Disponible** à **Sélectionné,** puis cliquez sur **Soumettre**.

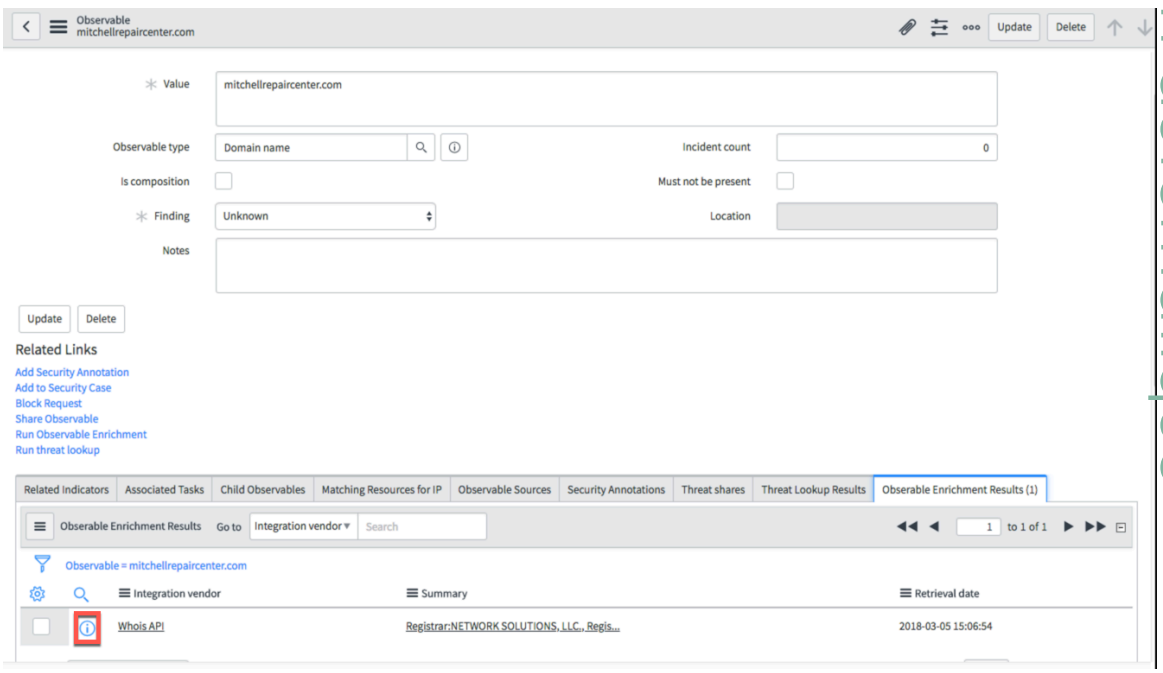
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les résultats sont affichés dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement de l'observable.

7. Cliquez sur l'icône d'information bleue, puis cliquez sur **Ouvrir l'enregistrement** dans la boîte de dialogue qui s'affiche.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Plus d'informations et de données brutes relatives à la recherche de domaine d'origine s'affichent, telles que la date d'enregistrement, le nom du bureau d'enregistrement et le pays d'origine.

Trouble?
Si vous ne pouvez pas localiser les observables enfants ou les résultats d'enrichissement, vérifiez que l'intégration s'est exécutée Reverse Whois avec succès et a renvoyé des domaines. Consultez également les notes de travail figurant dans le dossier pour plus d'informations.

Information associée

Installer et configurer Reverse Whois

Vérifier les résultats attendus pour Reverse Whois

RISKIQ et WHOISIQ l'intégration

Grâce à l'intégration des RISKIQWHOISIQ API dans le produit, les Now Platform® Opérations de sécurité analystes de la sécurité disposent de données d'enrichissement supplémentaires et d'informations sur la validité des sites Web.

L'API RISKIQ Certificats SSL effectue des recherches sur les certificats SSL, qui incluent des détails sur l'autorité de certification émettrice, les organisations qui demandent les certificats, l'entité à laquelle les certificats sont émis et le domaine. Les recherches de certificats SSL sont effectuées automatiquement lorsque des incidents de sécurité sont créés.

L'API RISKIQ WHOISIQ effectue des recherches sur d'autres types d'observables, tels que le domaine, l'e-mail, le serveur de noms, l'organisation, l'adresse et le numéro de téléphone. Les observables d'URL et de domaine sont enrichis automatiquement lors de la création d'incidents de sécurité.

L'intégration nécessite les Réponse aux incidents de sécurité produits and Renseignements sur les menaces .

Observables pris en charge pour RISKIQ et RISKIQ WHOISIQ

L'API RISKIQ prend en charge les recherches automatiques de certificats SSL sur les observables d'adresse IP, de hachage de fichier, de numéro de série de certificat, de domaine et d'URL. Les observables d'URL et de domaine sont enrichis automatiquement avec l'API WHOISIQ . Pour l'enrichissement des observables sur d'autres types d'observables avec l'API WHOISIQ , créez des observables et exécutez des recherches manuellement à partir de la table Observables.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Observables pris en charge

Le tableau suivant répertorie le type d'API utilisées dans cette intégration et les observables pris en charge par chaque API. La table indique également si une recherche a lieu automatiquement lorsque des incidents de sécurité sont créés ou si la recherche est exécutée manuellement à partir de la table Observables.

Observables et recherche pris en charge

API	Observables pris en charge	Recherche (automatisée ou manuelle)
RISKIQ API de certificat SSL	• Adresse IP • Hachage de fichier (empreinte digitale du certificat). Voir la figure suivante pour un exemple de hachage de fichier. • Numéro de série ou numéro de série du certificat. Cette chaîne est un ID unique pour l'entité. Consultez la figure suivante pour obtenir un exemple de numéro de série de certificat. • Domaine (`www.site.com` ou `site.com`) • URL **Remarque :** les analyses automatiques sont exécutées pour le format URL à l'aide du protocole `https://` , par exemple, `https://example.com/index.html`	Recherche automatisée lorsque des incidents sont créés. Les résultats sont affichés dans l'onglet **Certificats SSL** de l'enregistrement d'incident de sécurité.
RISKIQ WHOISIQ API	• Domaine • URL	Recherche automatisée lorsque des incidents sont créés. Les résultats sont affichés dans l'onglet **Résultats de l'enrichissement de l'observable** de l'enregistrement d'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Observables et recherche pris en charge (suite)

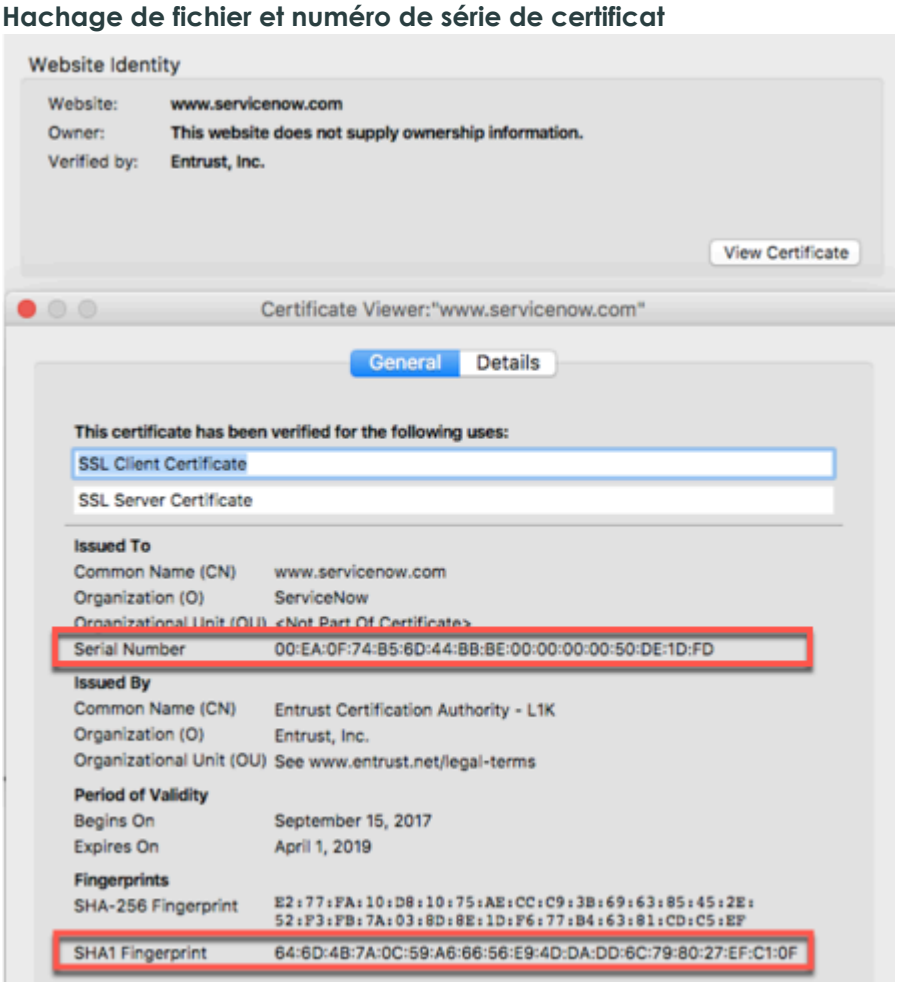
API	Observables pris en charge	Recherche (automatisée ou manuelle)
RISKIQ WHOISIQ API	• Adresse e-mail • Nom de l'organisation • Numéro de téléphone • Adresse postale	La recherche manuelle est exécutée à partir de la table Observables. Les résultats sont affichés dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement Observable.

Exemple de hachage de fichier et de numéro de série de certificat

Cette figure montre un exemple d'observables de hachage de fichier et de numéro de série de certificat utilisés pour les recherches de certificats SSL pour cette intégration. Le hachage de fichier fait référence à une empreinte digitale SHA-1. Cette valeur s'affiche dans votre Now Platform instance sans les séparateurs deux-points. Par exemple, `646D4B7A0C59A66656E94DDADD6C798027EFC10F`.

L'observable de numéro de série du certificat fait référence à l'ID unique ou au numéro de série de l'entité. Cette valeur est également affichée sans les séparateurs deux-points. Par exemple, `00EA0F74B56D44BBBE0000000050DE1DFD`.

Hachage de fichier et numéro de série de certificat



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer et configurer RISKIQ et WHOISIQ

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que les applications and s'intègrent RISKIQ correctement à Now Platform Opérations de sécurité.WHOISIQ

Avant de commencer

Rôle requis : admin RISKIQ et WHOISIQ admin.

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (admin) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration et vérifie les résultats attendus. Ce rôle a également accès au Opérations de sécurité module et affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). • L'analyste des incidents de sécurité (sn_si.analyst) travaille avec les enregistrements d'incidents de sécurité.
Obtenez un nom d'utilisateur et une clé API.	Visitez le site Web pour plus d'informations sur la clé API et comment créer un compte : site Web de RISKIQ . La configuration nécessite que vous saisissiez la clé API.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Configuration requise pour la version Madrid et ultérieure Pour la version Madrid et les versions ultérieures de la famille, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et

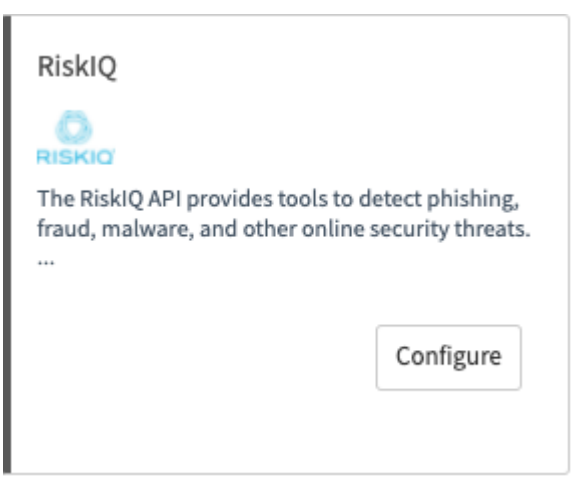
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Orchestration de support de sécurité Pour en savoir plus sur la configuration de votre Now Platform instance pour l'intégration, consultez et .

Procédure

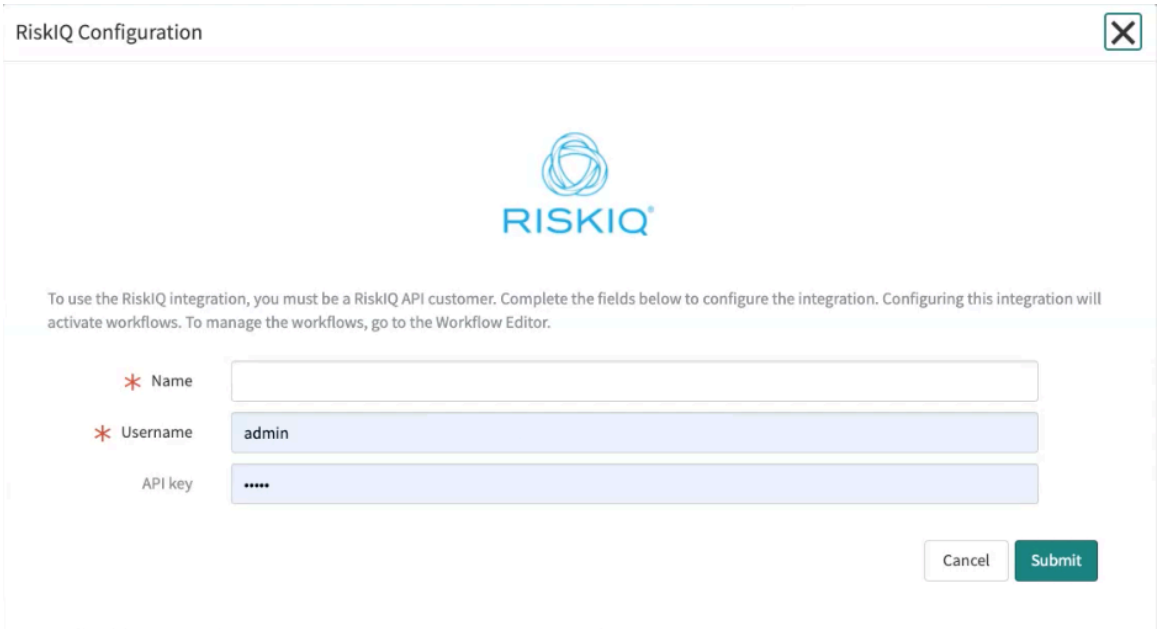
1. Si vous n'avez pas installé l'application pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Intégrations** > **Configurations des intégrations** et localisez la vignette de l'API.
3. Cliquez sur **Configurer**.



4. Dans la boîte de dialogue Configuration de RiskIQ qui s'affiche, entrez le **nom d'utilisateur** et la **clé API**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
6. Vérifiez que la configuration est correcte.
   Lorsque la configuration est terminée avec succès, la page Intégrations de sécurité avec les vignettes d'intégration s'affiche.

Trouble?
Si un message d'erreur s'affiche, le nom d'utilisateur ou la clé API n'est peut-être pas valide. Vérifiez que votre nom d'utilisateur et votre clé API sont corrects :

Dépannage

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

Vérifier les résultats attendus pour RISKIQ les recherches de certificats SSL

Lorsqu'un incident de sécurité génère des observables pour les URL, les domaines, les adresses IP, les hachages de fichiers de certificat (empreinte digitale SHA-1) et les numéros de série des certificats, les analystes des incidents de sécurité utilisent les résultats de la recherche de certificats SSL pour vérifier que les sites disposent de certificats émis par une autorité de certification (CA) publique approuvée.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Pour les observables pris en charge, l'analyse Now Platform de l'occurrence la plus récente des URL, des domaines, des adresses IP, des hachages de fichier de certificat (empreinte digitale SHA-1) et des numéros de série de certificat. Voici les résultats possibles de l'analyse :

Une correspondance exacte a été trouvée

Un émetteur valide d'un certificat SSL est répertorié dans l'enregistrement d'incident de sécurité.

Aucun résultat de certificat n'a été trouvé

Aucun résultat n'est répertorié dans l'enregistrement d'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une correspondance exacte a été trouvée pour un certificat autosigné ou généré en interne

Les résultats d'un certificat SSL généré en interne sont affichés dans l'enregistrement d'incident de sécurité.

Aucune correspondance exacte n'a été trouvée pour un certificat SSL principal

Une valeur de recherche renvoie plusieurs entrées et un certificat primaire ne peut pas être identifié. Un message récapitulatif s'affiche sur l'enregistrement d'incident de sécurité.

Procédure

1. Pour afficher les observables et vérifier les résultats de la recherche, ouvrez l'enregistrement d'incident de sécurité avec lequel vous travaillez et localisez les notes de travail.

Example
Pour illustrer des exemples de résultats de recherche possibles pour cette intégration, supposons qu'un incident de sécurité ait été généré avec les observables suivants :

- community.servicenow.com
- invalidsubdomain.servicenow.com
- mail.dgnetworks.com
- servicenow.com

Observables et emplacement des résultats de la recherche

Observable (exemple)	Résultats de l'analyse	Description et emplacement
community.servicenow.com	Certificat trouvé avec un hachage SHA1.	Une correspondance exacte est trouvée et un émetteur valide d'un certificat SSL est répertorié. Les résultats de la correspondance exacte sont affichés dans l'onglet **Certificats SSL** de l'enregistrement d'incident de sécurité.
invalidsubdomain.servicenow.com	Aucun certificat n'a été trouvé.	Un résumé indiquant qu'aucun résultat de certificat n'a été trouvé s'affiche dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement d'incident de sécurité.
mail.dgnetworks.com	Certificat trouvé avec hachage SHA1.	Une correspondance exacte est répertoriée pour un certificat autosigné ou généré en interne. Les résultats sont affichés dans l'onglet **Certificats SSL** de l'enregistrement d'incident de sécurité.

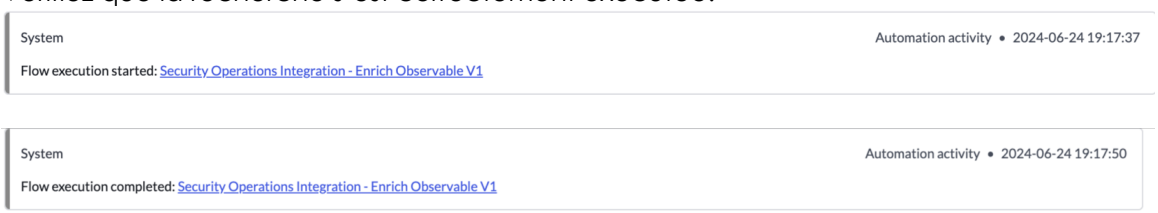
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Observable (exemple)	Résultats de l'analyse	Description et emplacement
servicenow.com	La recherche a renvoyé 138 certificats, et un seul certificat primaire n'a pas pu être identifié.	Aucune correspondance exacte n'est trouvée pour un certificat SSL principal, car une valeur de recherche renvoie plusieurs certificats. Un résumé indiquant qu'aucun certificat primaire n'a été trouvé s'affiche dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement d'incident de sécurité.

Une fois l'application configurée, le flux se lance automatiquement. L'état de la recherche et les observables sont affichés dans les notes de travail.

2. Vérifiez que la recherche s'est correctement exécutée.



Trouble?
Si vous ne pouvez pas afficher les résultats attendus, vérifiez que l'observable est pris en charge par la recherche de certificat SSL pour l'intégration.

Information associée

Observables pris en charge pour RISKIQ et RISKIQ WHOISIQ

RISKIQ Recherches de certificats SSL qui renvoient une correspondance exacte

RISKIQ Les résultats de la recherche de certificats SSL pour une correspondance exacte sont **affichés** dans l'onglet Certificats SSL de l'enregistrement d'incident de sécurité. Une correspondance exacte fournit un nom d'autorité de certification valide, ce qui aide un analyste des incidents de sécurité à déterminer la validité d'un site Web.

Example: Correspondance exacte pour un certificat SSL valide

L'exemple suivant montre un émetteur valide d'un certificat SSL à partir d'une correspondance exacte dans les résultats de la recherche. Suivez les étapes pour afficher les résultats et les données brutes.

Remarque : Les figures des exemples suivants sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres système. Si votre écran ne correspond pas à la vue affichée ci-dessous, suivez les étapes pour définir les formulaires à onglets.

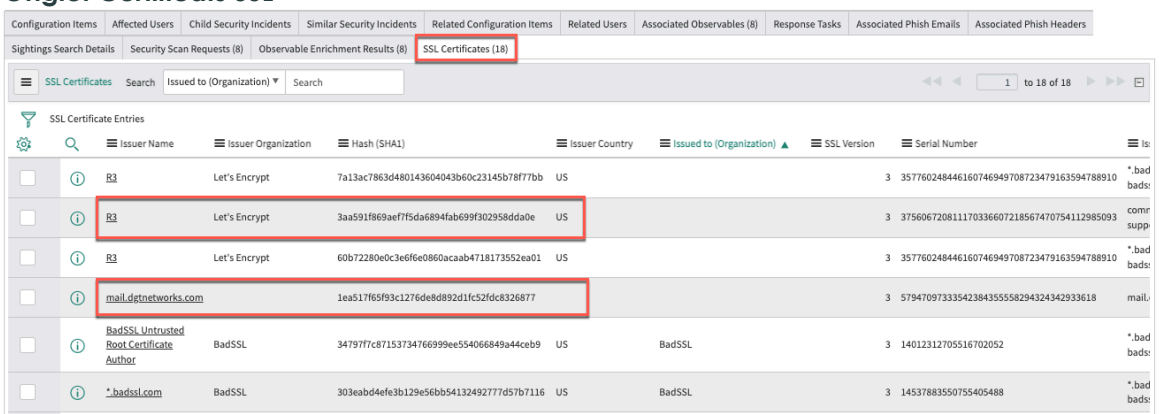
1. Dans le coin supérieur droit de la bannière, cliquez sur l'icône Paramètres.
2. Dans la boîte de dialogue **Paramètres du système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que les **champs Formulaires à onglets** et **Avec formulaire** sont sélectionnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Dans l'enregistrement de l'incident de sécurité, cliquez sur l'onglet **Certificats SSL** .

Onglet Certificats SSL



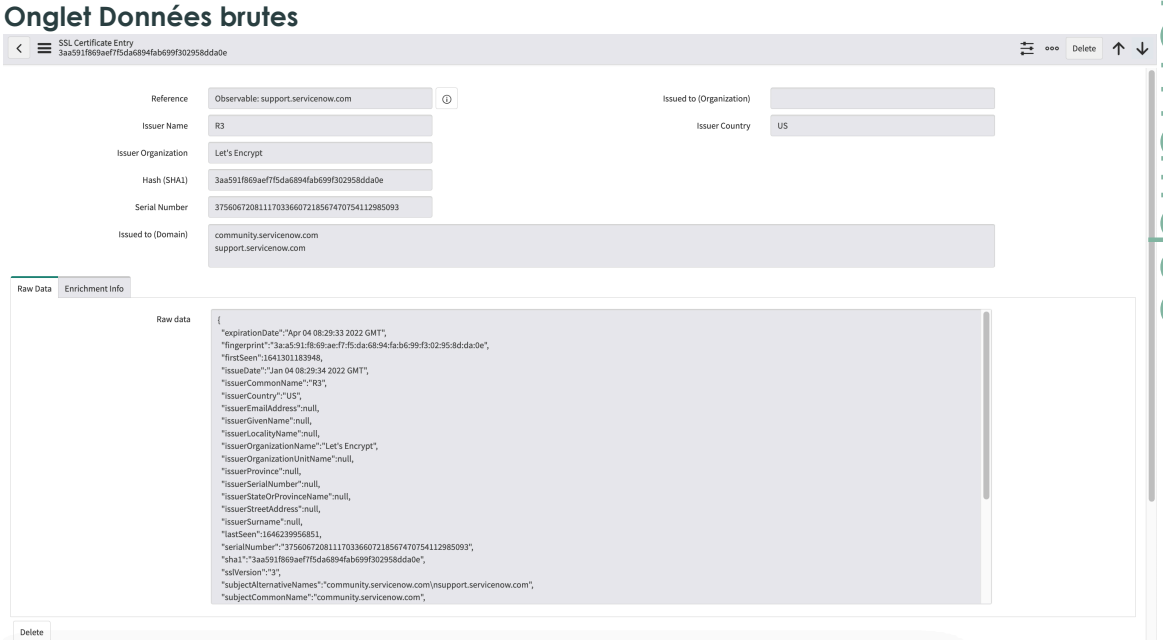
Des informations sur le nom de l'émetteur du certificat, l'organisation de l'émetteur et le destinataire du certificat (Organisation) s'affichent avec d'autres données.

18 éléments sont affichés dans la colonne **Nom de l'émetteur** . Le deuxième élément (`R3`) fournit un nom `d'autorité de certification valide (Let's Encrypt)` dans la colonne **Organisation de l'émetteur** .

Aucune information dans les colonnes **Organisation de l'émetteur** et **Émis à** ne s'affiche pour le deuxième élément (`mail.dgtnetworks.com`).

2. Cliquez sur le deuxième élément de la colonne **Nom de l'émetteur**, qui est (**R3**) pour ouvrir l'enregistrement d'entrée. Vous pouvez également cliquer sur l'icône d'information en regard de l'élément, suivie de **Ouvrir l'enregistrement**.
3. Sélectionnez l'onglet **Données brutes** .

Onglet Données brutes



L'enregistrement d'entrée de certificat SSL inclut l'observable dans l'onglet **Données brutes** sous la colonne **Nom de l'entité** , ainsi que d'autres données.

Remarque : dans la colonne **Catégorie** , `l'objet` et `l'émetteur` correspondent à des entités reconnaissables dans la colonne Nom de **l'entité** . L'émetteur de ce certificat est très probablement valide et provient d'une autorité de certification publique de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

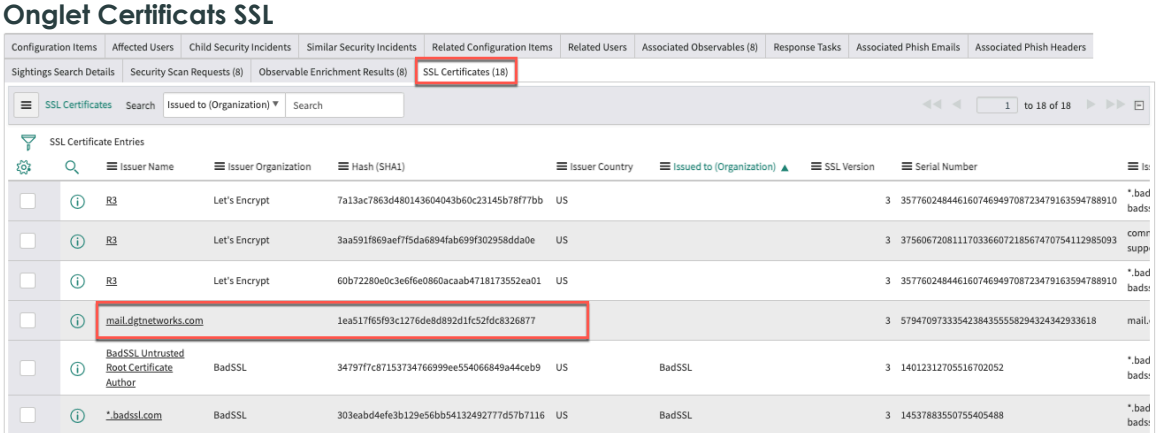
confiance. Notez également que `l'objet` et `l'émetteur` sont des entités différentes. Ces entités distinctes indiquent que le certificat n'est pas un certificat signé en interne et émis par une autorité de certification inconnue.

Example: Correspondance exacte pour un certificat SSL auto-signé

L'exemple suivant montre les résultats de la recherche pour un certificat SSL auto-signé. Suivez les étapes pour afficher les résultats et les données brutes.

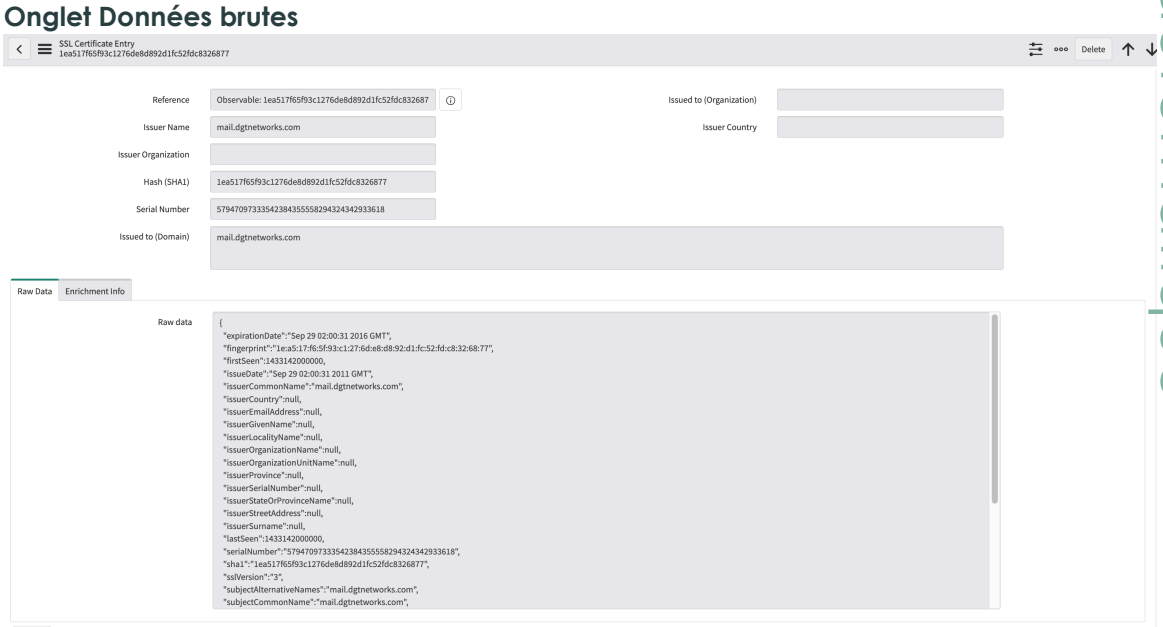
1. Revenez à l'enregistrement de l'incident de sécurité. Dans la colonne **Nom de l'émetteur** , cliquez sur l'autre élément (**mail.dgtnetworks.com**).

Onglet Certificats SSL



2. Dans l'enregistrement ouvert, sélectionnez l'onglet **Données brutes** .

Onglet Données brutes



La colonne **Catégorie** indique `l'émetteur` (`mail.dgtnetworks.com` et `dgtsbs.DGTNetworks.local`) ne sont pas des autorités de certification publiques de confiance. Notez également que `l'émetteur` et `l'objet` sont la même entité (`dgtsbs.DGTNetworks.local`), et chacun contient le nom de l'observable (`dgtsbs`). Il s'agit éventuellement d'un certificat auto-signé. Les certificats autosignés peuvent justifier une enquête plus approfondie, car ces certificats ne sont pas délivrés par une autorité de certification connue.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

RISKIQ Recherches de certificats SSL qui renvoient plusieurs certificats ou aucun certificat

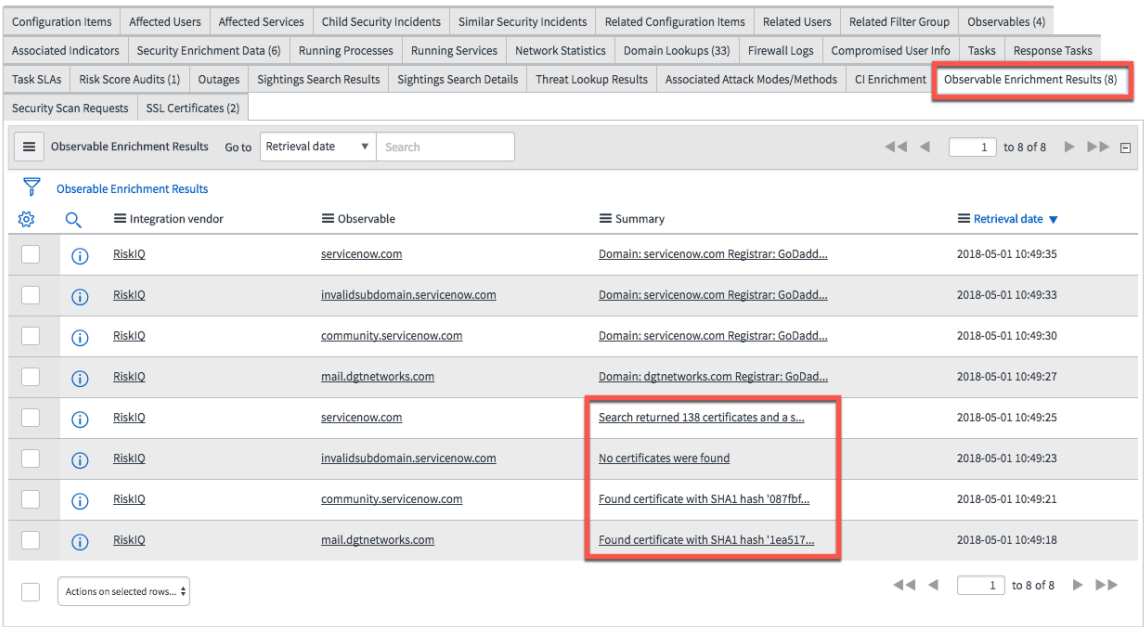
Un analyste des incidents de sécurité peut utiliser plusieurs résultats de certificats SSL pour déterminer si un site fait partie d'une entité commune et reconnaissable. Aucun résultat de certificat SSL peut indiquer que les sites avec des noms obscurs ou suspects n'ont pas de certificats fiables. Les résultats de la recherche des observables qui ne renvoient pas de certificats SSL ou qui renvoient plusieurs certificats SSL sont affichés dans l'onglet Résultats de l'enrichissement des observables de l'enregistrement d'incident de sécurité.

Example: Aucun résultat de certificat SSL ou plusieurs résultats de certificat SSL

Suivez les étapes pour afficher les résultats pour les observables qui ne renvoient pas de certificats SSL ou qui renvoient plusieurs certificats.

1. Dans l'enregistrement d'incident de sécurité, cliquez sur **l'onglet Résultats de l'enrichissement des observables** .

Onglet Résultats de l'enrichissement de l'observable



Les résultats de l'enrichissement des observables pour la recherche et WHOISIQ sont RISKIQ affichés.

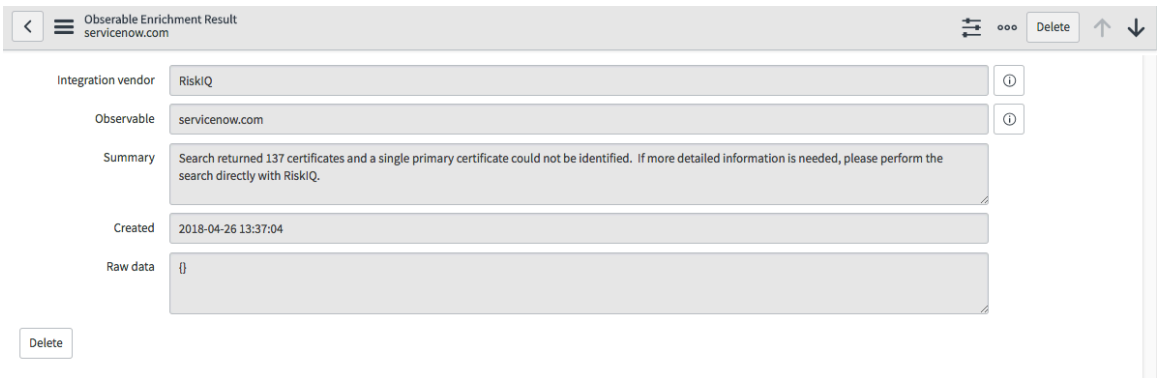
Dans la colonne **Observable** , `servicenow.com` correspond au message `Search returned 138 certificates (La recherche a renvoyé 138 certificats )` dans la colonne **Summary (Résumé**). De même, `invalidsubdomain.servicenow.com` correspond à `Aucun certificat n'a été trouvé` dans la colonne **Résumé**. Ces résumés indiquent que plusieurs certificats SSL ont été trouvés et qu'aucune correspondance exacte pour les certificats SSL n'a été trouvée, respectivement.

2. Dans la colonne **Observable** , cliquez sur **servicenow.com**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Plusieurs certificats SSL



Le message récapitulatif affiché dans l'enregistrement indique que plusieurs résultats pour les certificats SSL ont été renvoyés pour `servicenow.com` et qu'un certificat SSL principal n'a pas pu être mis en correspondance. Ce message est souvent renvoyé lors des recherches qui incluent des noms de domaine courants, tels que `servicenow.com`.

Si vous avez besoin de plus d'informations sur un domaine commun, vous pouvez effectuer la recherche directement avec l'API RISKIQ .

3. Revenez à l'onglet **Résultats de l'enrichissement des observables** et, dans la colonne **Observable** , cliquez sur **invalidsubdomain.servicenow.com**.

Aucun certificat SSL



Remarque :

- Si aucun certificat SSL n'est trouvé pour l'observable actuel, le champ Résumé affiche le message Aucun `certificat n'a été trouvé.`
- Si aucun certificat SSL actif n'est trouvé pour l'observable actuel, le champ Résumé affiche le message Aucun `certificat actif n'a été trouvé.`

Vérifier les résultats attendus pour WHOISIQ les recherches d'URL

Lorsqu'un incident de sécurité génère des observables pour les URL ou les domaines, l'API WHOISIQ procède automatiquement à l'enrichissement des observables lors de la création de l'incident de sécurité. Les résultats de la recherche sont affichés dans les onglets **Résultats de l'enrichissement de l'observable** et **Certificats SSL** de l'enregistrement d'incident de sécurité.

Avant de commencer

Remarque : Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres du système.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

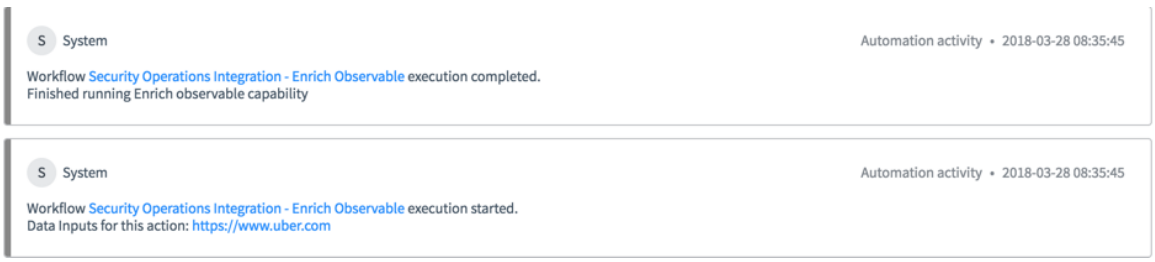
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Les résultats de l'enrichissement des observables sont affichés dans l'onglet **Résultats de l'enrichissement des observables** en bas de l'enregistrement d'incident de sécurité. Pour les observables pris en charge, une recherche de certificats SSL est également exécutée et les résultats sont **affichés dans l'onglet Certificats SSL**.

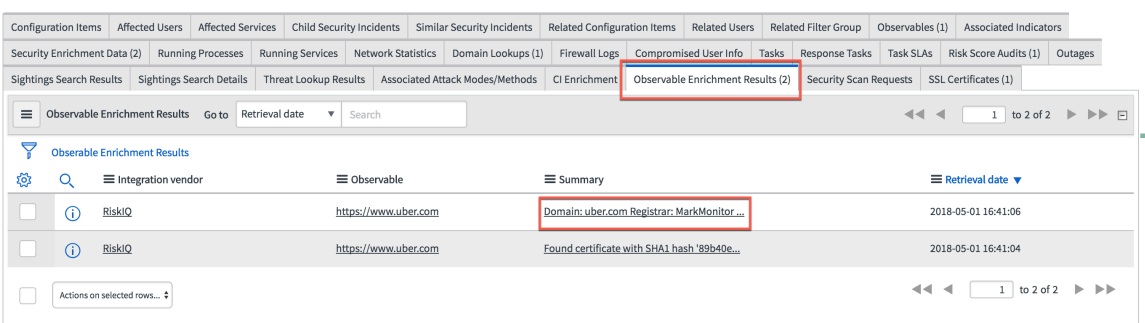
Procédure

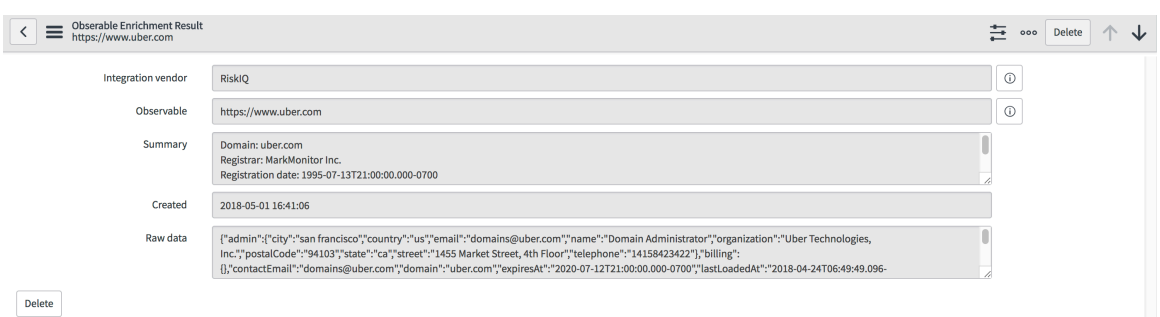
1. Ouvrez l'enregistrement d'incident de sécurité avec lequel vous travaillez et vérifiez que la recherche a été exécutée avec succès dans les notes de travail.



   Une fois l'application configurée, le flux se lance automatiquement lors de la création de l'incident. L'état d'exécution et d'achèvement de la recherche est affiché dans les notes de travail de l'enregistrement d'incident de sécurité.

2. Si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée, consultez les notes de travail pour plus d'informations sur la façon de procéder.
3. Sur l'incident de sécurité ouvert, cliquez sur le lien connexe **Afficher toutes les listes connexes** .
4. Cliquez sur l'onglet **Résultats de l'enrichissement de l'observable** pour le sélectionner.
5. Dans la colonne **Résumé**, cliquez sur le premier élément, **Domaine : uber.com Bureau d'enregistrement : Markmonitor...**





   L'enregistrement qui s'affiche contient des informations sur le domaine.

Traduction automatique

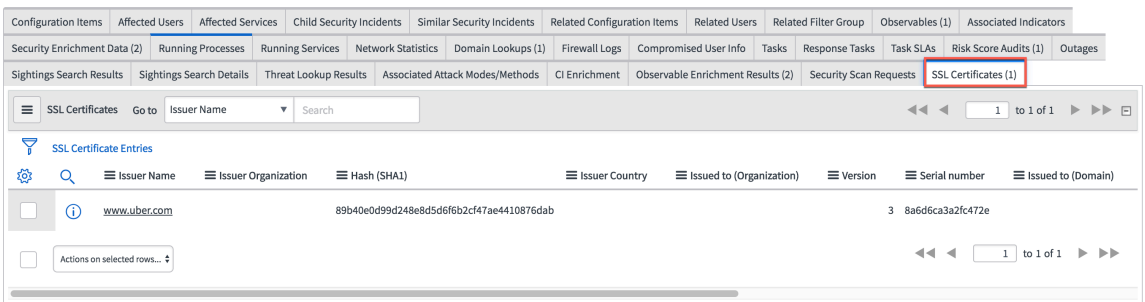
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Revenez à l'onglet **Résultats de l'enrichissement des observables** et, dans la colonne **Résumé** , cliquez sur le deuxième élément, **Certificat trouvé avec hachage SHA1...**.



Cet enregistrement indique qu'un certificat SSL avec un hachage de fichier a été trouvé.

7. Revenez à l'enregistrement d'incident de sécurité et cliquez sur l'onglet **Certificats SSL** .



Les résultats du certificat SSL pour le hachage de fichier sont également affichés ici.

Trouble?
Si vous ne pouvez pas afficher les résultats attendus, passez en revue les notes de travail. Vérifiez également que l'observable est pris en charge pour la recherche par l'intégration.

Information associée

Observables pris en charge pour RISKIQ et RISKIQ WHOISIQ

Créer un observable pour les recherches manuelles WHOISIQ

Les analystes d'incidents de sécurité utilisent les informations issues de l'enrichissement des observables avec l'API WHOISIQ pour en savoir plus sur les adresses e-mail, les noms et les numéros de téléphone des organisations.

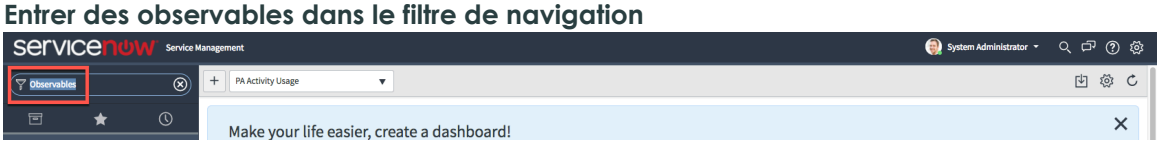
Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tout** > **Référentiel IoC** > **Observables**.

Entrer des observables dans le filtre de navigation

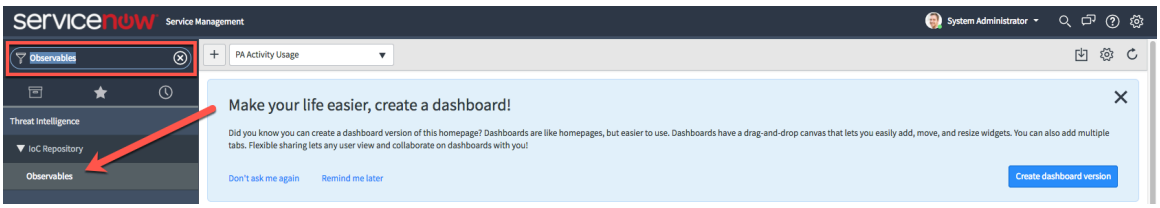


Le module Observables s'affiche sous le panneau de navigation.

Traduction automatique

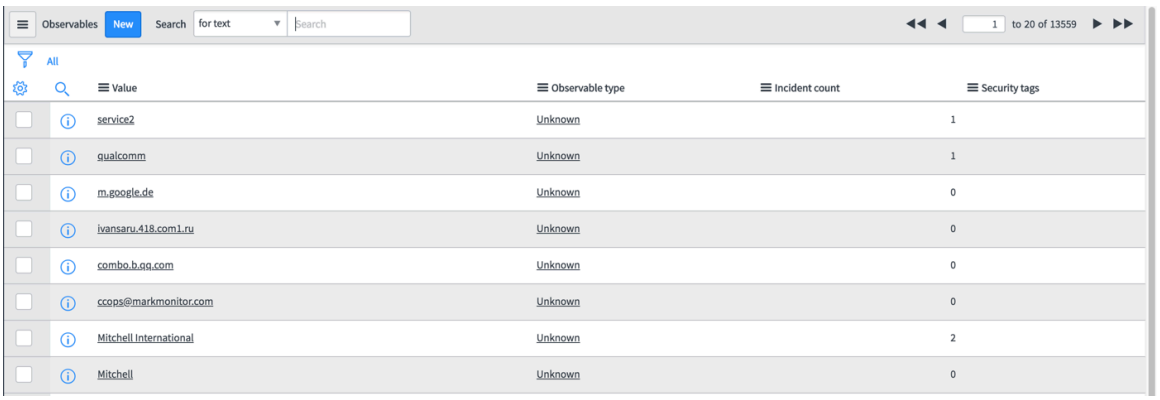
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Module Observables



2. Cliquez sur le module **Observables** pour afficher la liste des observables.

Liste des éléments observables

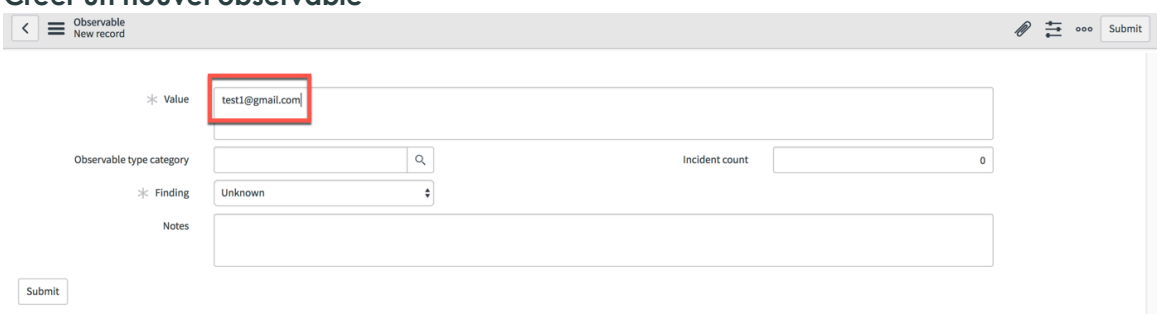


3. Cliquez sur **Nouveau** pour créer un observable.

4. Renseignez les champs du formulaire Observable.

Champ	Description
Valeur	Adresse e-mail, nom de l'organisation, numéro de téléphone ou adresse postale. Par exemple, `test1gmail.com`
Type d'observable	Le champ est automatiquement effacé.
Résultat	Ce champ est automatiquement défini sur **Inconnu**.

Créer un nouvel observable



5. Cliquez sur **Envoyer**.
Vous êtes renvoyé à la liste des observables. Dans la colonne **Valeur** , votre nouvel observable s'affiche.

Remarque : Si vous ne parvenez pas à localiser votre observable sur la partie de la liste qui est affichée, utilisez la fonctionnalité de recherche pour le trouver.

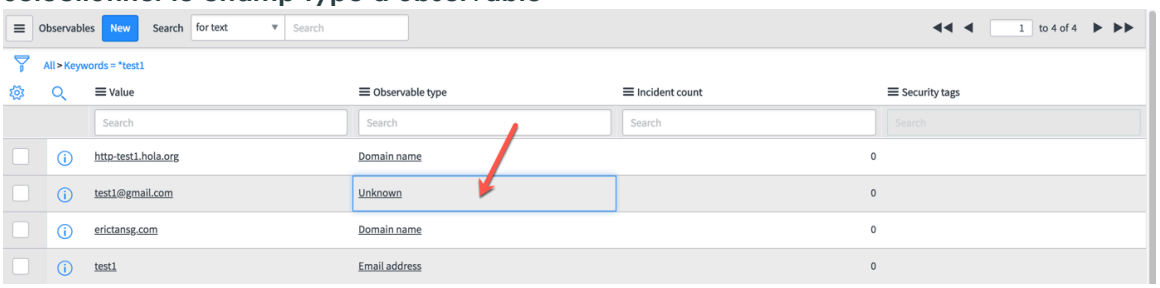
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Modifiez le champ **Type d'observable** pour modifier le type de **Inconnu** en **Adresse e-mail** pour qu'il corresponde à votre observable.

   a. Dans la colonne **Type d'observable** , cliquez une fois à droite du texte **inconnu** pour le sélectionner.

Sélectionner le champ Type d'observable

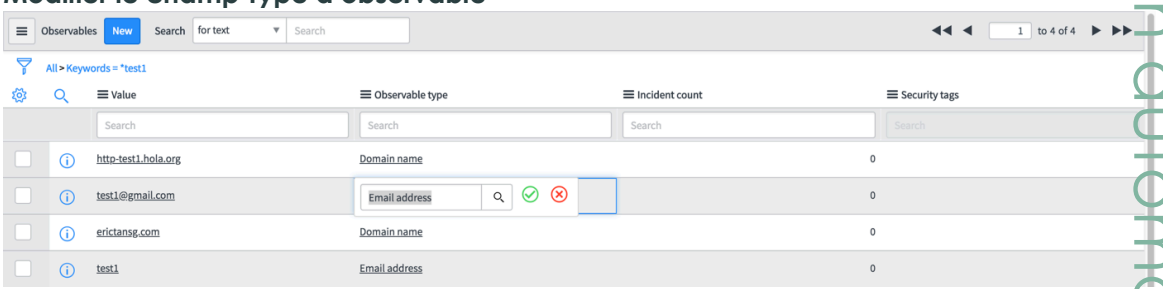


   Le champ sélectionné est entouré en bleu.

   b. Avec le champ délimité en bleu, double-cliquez n'importe où à l'intérieur du champ en surbrillance pour ouvrir l'éditeur.

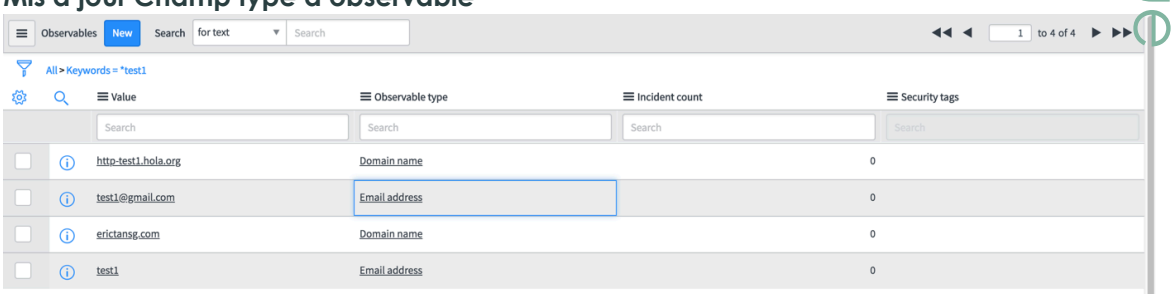
   c. Dans le champ qui s'affiche, saisissez le type d'observable (`adresse e-mail`) et cliquez sur la coche verte pour enregistrer la valeur.

Modifier le champ Type d'observable



   Dans la colonne **Type d'observable** de la liste, `l'adresse e-mail` est affichée pour votre nouvel observable.

Mis à jour Champ type d'observable



Que faire ensuite

Si vous avez créé et modifié un observable pour la recherche, exécutez la recherche d'enrichissement d'observable à partir de l'enregistrement d'observable avec l'API WHOISIQ .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vérifier les résultats attendus pour les recherches manuelles WHOISIQ

Exécutez une recherche manuelle sur un observable lorsqu'il ne génère pas automatiquement un incident de sécurité. Pour les recherches d'enrichissement d'observables à l'aide de l'API pour les adresses e-mail, les noms d'organisation WHOISIQ , les numéros de téléphone ou les adresses postales, lancez la recherche manuellement à partir de la table Observables.

Avant de commencer

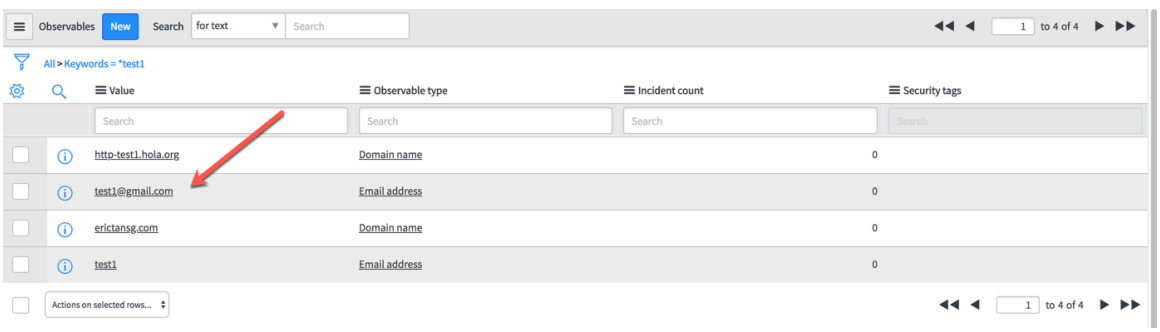
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

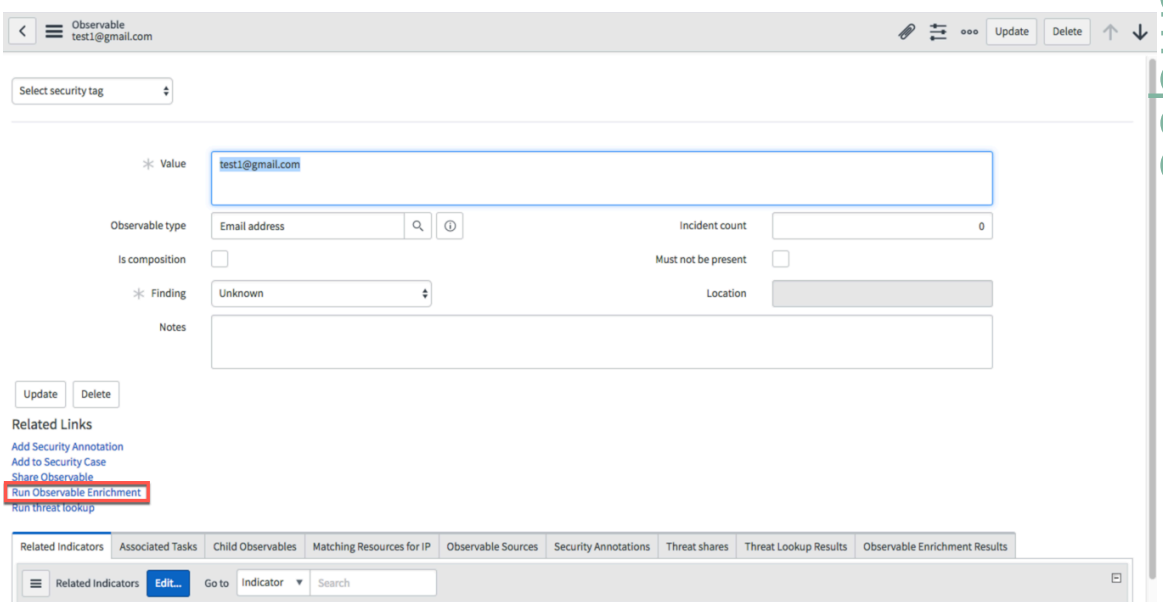
Créez un observable pour une recherche manuelle à l'aide de l'API WHOISIQ . Pour en savoir plus sur la création et la modification d'un observable, reportez-vous à Créer un observable pour les recherches manuelles WHOISIQ.

Procédure

1. Accédez à la **Tout** > **Référentiel IoC** > **Observables** et localisez l'observable dans la liste sur laquelle vous travaillez.
2. Cliquez sur votre observable dans la colonne **Valeur** pour ouvrir l'enregistrement.



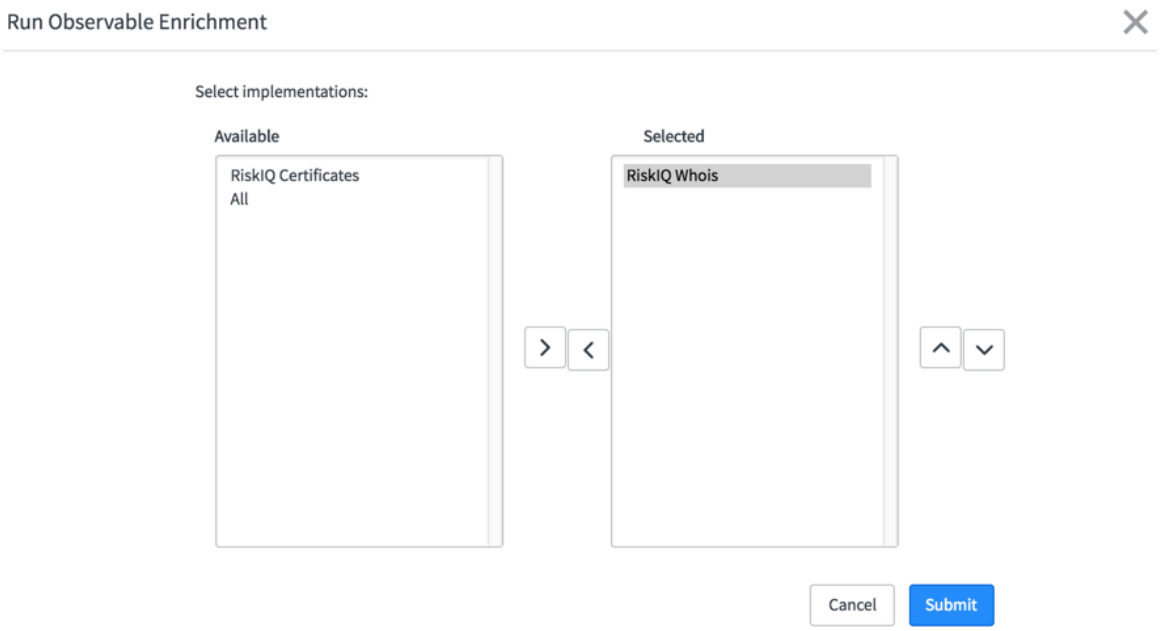
3. Cliquez sur le lien connexe **Exécuter l'enrichissement des observables** pour exécuter la recherche.



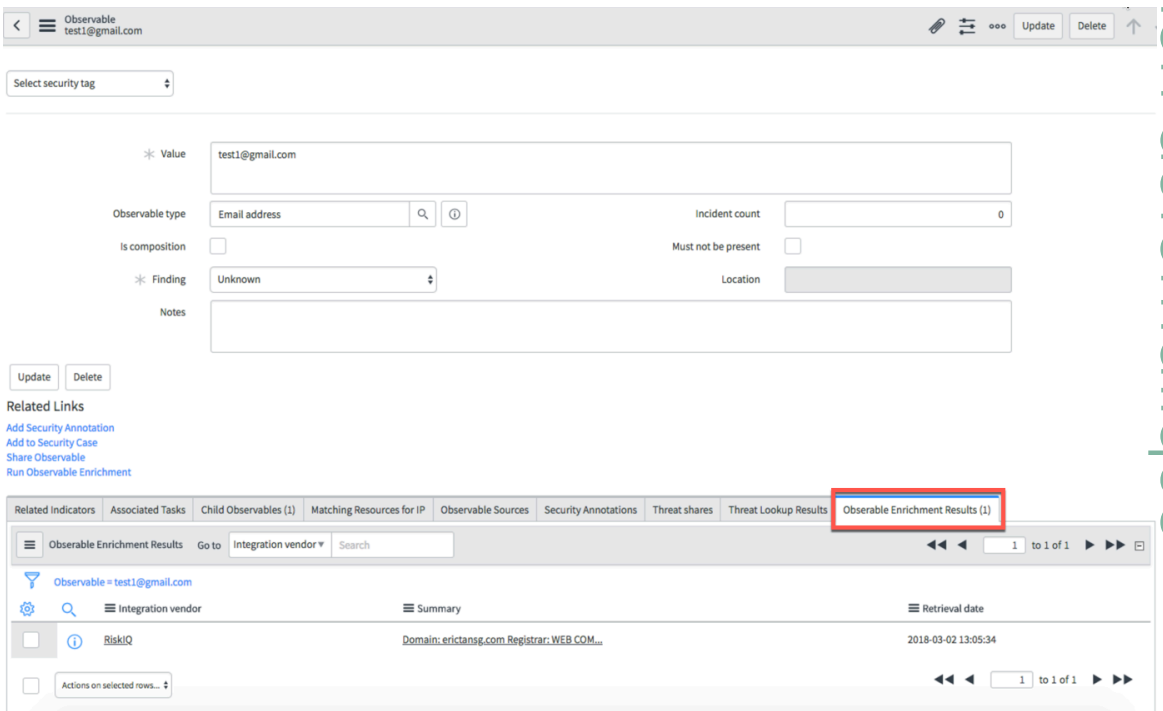
4. Dans la fenêtre **Exécuter l'enrichissement des observables** , déplacez **RiskIQ Whois** vers la liste sélectionnée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
Les résultats de la recherche sont affichés dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement de l'observable.



Trouble?
Si aucun résultat n'est renvoyé pour l'observable, un message s'affiche dans la colonne **Résumé** . Si vous ne voyez pas de résultats, vérifiez que l'observable est pris en charge par l'API.

Information associée

Observables pris en charge pour RISKIQ et RISKIQ WHOISIQ

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Shodan intégration

Shodan est un moteur de recherche qui analyse les informations des bannières de service à partir d'appareils connectés dans le monde entier. Les bannières de service comprennent des informations sur un système informatique, telles que le nom d'hôte, le type d'appareil, le système d'exploitation, l'emplacement géographique et le FAI connecté. Lorsqu'elles sont intégrées au Now Platform Opérations de sécurité produit, ces informations de bannière de service fournissent aux analystes des données d'enrichissement et des informations supplémentaires pour les incidents de sécurité ou les enquêtes.

L'intégration nécessite les modules d'extension Réponse aux incidents de sécurité and Renseignements sur les menaces .

L'intégration Shodan effectue un enrichissement sur les observables suivants :

- Adresses IP
- URL

L'application recherche de nouveaux observables toutes les cinq minutes. Si les observables sont d'un type reconnu par l'intégration Shodan , les observables sont enrichis.

Installer et configurer Shodan

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration pour que l'application s'intègre Shodan correctement à Now Platform Opérations de sécurité.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâches de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform à votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (admin) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration et vérifie les résultats attendus. Ce rôle a également accès au Opérations de sécurité module.
Procurez-vous la Shodan clé API.	Créez un compte et obtenez la clé API à partir du Shodan site web : Shodan website .
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Pour la version Madrid et les versions ultérieures de la famille, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances

Traduction automatique

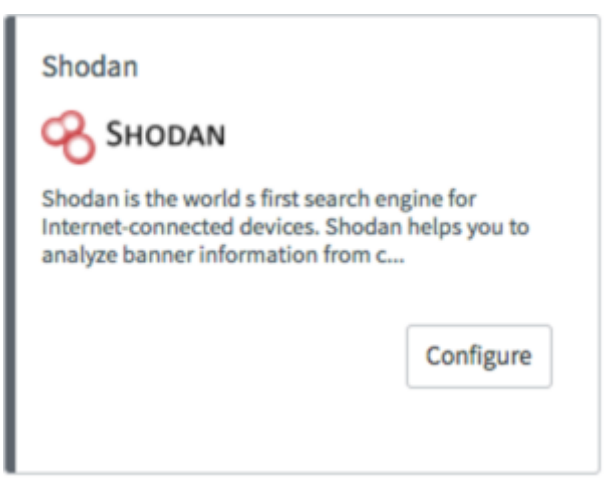
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Orchestration de support de sécurité Pour en savoir plus sur la configuration de votre Now Platform instance pour l'intégration, consultez et .

Rôle requis : administrateur

Procédure

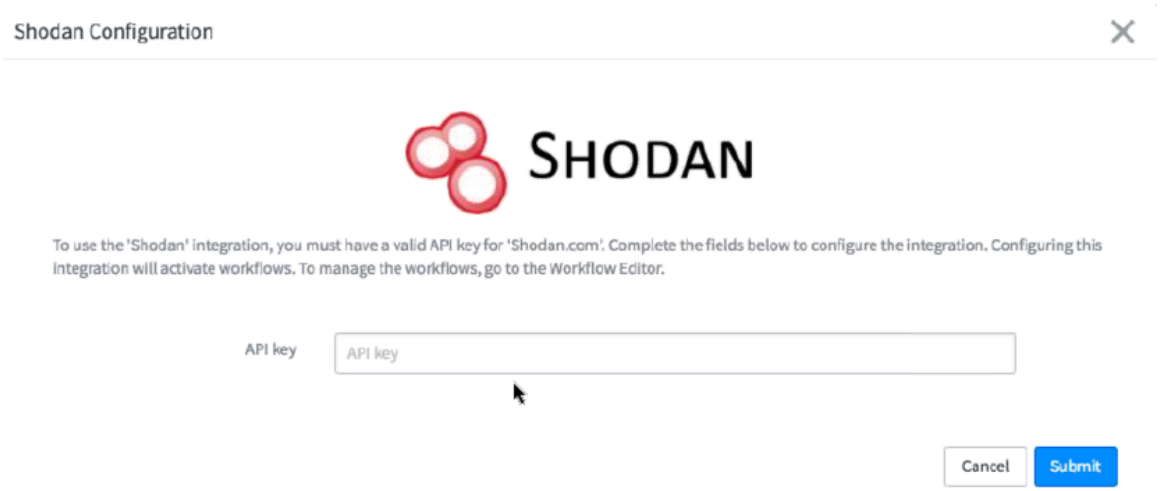
1. Si vous n'avez pas installé l'application pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la Shodan tuile.



3. Cliquez sur **Configurer**.
4. Dans la boîte de dialogue **Configuration Shodan** , saisissez la clé API que vous avez obtenue à partir du Shodan site Web et cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Vérifiez que la configuration est correcte.
   La configuration est terminée avec succès, sauf si un message d'erreur s'affiche.

   Trouble?

   Si un message d'erreur s'affiche lors de la configuration, la clé API n'est Shodan peut-être pas valide.

Vérifier les résultats attendus pour Shodan

Les observables sont générés automatiquement par un incident de sécurité et analysés par l'application. Les résultats de l'enrichissement sont affichés dans les onglets **Résultats de l'enrichissement de l'observable** et **Bannières réseau** .

Avant de commencer

Rôle requis : sn_si.analyst.

Procédure

1. Ouvrez l'incident de sécurité sur lequel vous travaillez et vérifiez que la recherche a été exécutée avec succès.



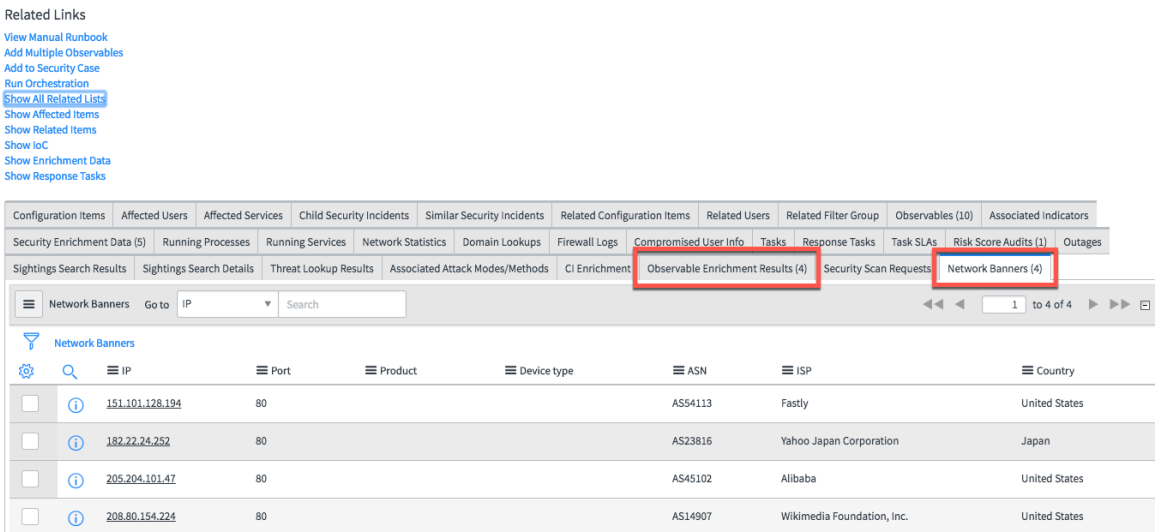
   Une fois l'application configurée, le workflow se lance automatiquement lors de la création de l'incident. L'état d'exécution et d'achèvement de la recherche est affiché dans les notes de travail de l'incident de sécurité.

2. Consultez les notes de travail pour plus d'informations et pour savoir comment procéder si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.
3. Accédez au bas de l'incident de sécurité et cliquez sur le lien **Afficher toutes les listes connexes** dans **Liens connexes**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres du système. Si les formulaires à onglets ne sont pas affichés, cliquez sur l'icône d'engrenage Paramètres dans le coin supérieur droit de la bannière. Dans la boîte de dialogue **Paramètres du système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que les **champs Formulaires à onglets** et **Avec formulaire** sont sélectionnés.



Les résultats sont affichés dans les **onglets Résultats de l'enrichissement de l'observable** et **Bannières réseau** en bas de l'incident de sécurité.

4. Après avoir sélectionné **l'onglet Bannières réseau** , cliquez sur l'icône d'information bleue en regard d'un observable.

5. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement** pour afficher les données brutes et plus de détails.

Trouble?
Si vous ne voyez pas de résultats sous les onglets **Résultats de l'enrichissement de l'observable** et **Bannières réseau** , vérifiez que l'observable est d'un type pris en charge pour la recherche par l'intégration.

(Facultatif) Joindre manuellement un observable pour Shodan

Vous pouvez joindre manuellement des observables à un incident de sécurité. Vous joignez manuellement les observables lorsque vous souhaitez effectuer des recherches de menaces sur des observables qui ne sont pas joints à un incident de sécurité sur le déclencheur d'événement initial. Vous pouvez également effectuer cette tâche lorsque vous souhaitez plus d'informations sur un observable associé.

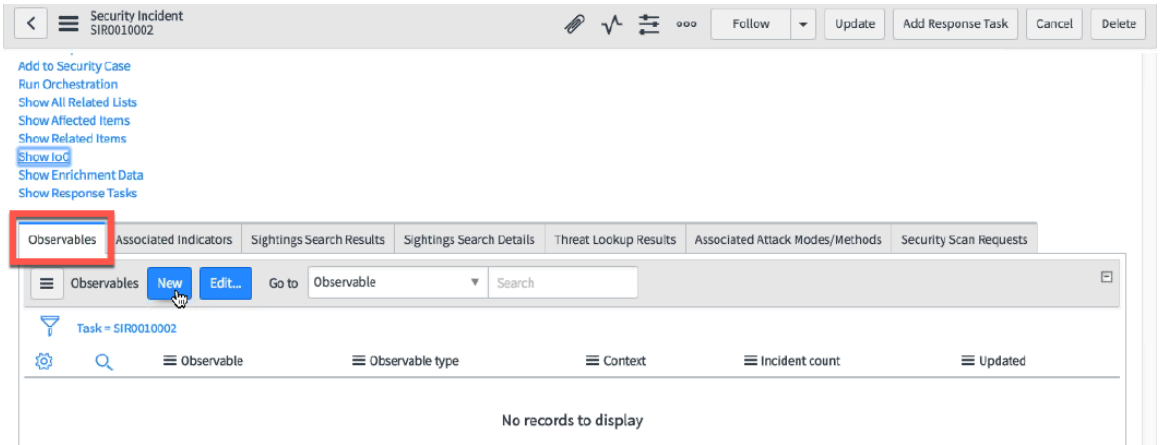
Avant de commencer
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents** et ouvrez un incident de sécurité auquel vous souhaitez joindre l'observable.
2. Au bas de l'enregistrement, cliquez sur le lien **Afficher IoC**dans **Liens connexes**.

Traduction automatique

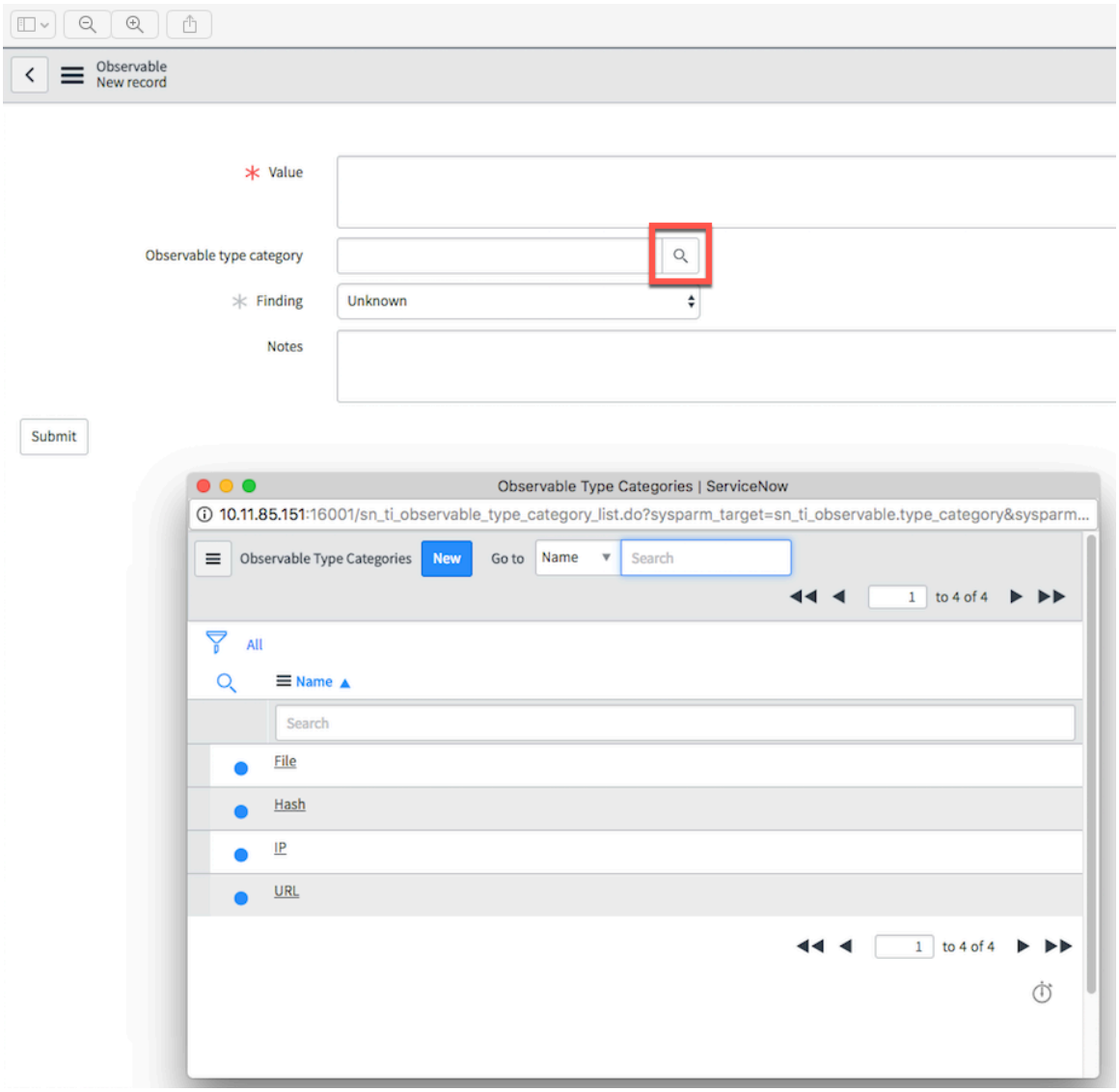
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans l'onglet **Observables** , cliquez sur **Nouveau**.
   Le formulaire Observable s'affiche.
4. Dans le champ **Valeur** , entrez un observable (adresse IP ou URL).
5. Cliquez sur l'icône de recherche puis, dans la boîte de dialogue **Catégories de types d'observables** , cliquez sur le type d'observable souhaité dans la liste pour remplir le champ.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



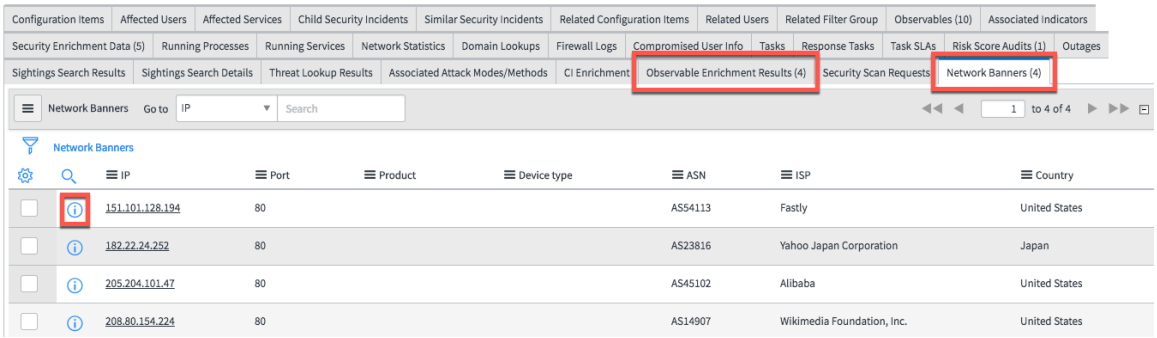
6. Cliquez sur **Envoyer**.
   Le workflow lance et vérifie le nouvel observable. L'état d'exécution et d'achèvement est affiché dans la section Notes de travail de l'enregistrement d'incident de sécurité.
7. Accédez à votre incident de sécurité et passez en revue les notes de travail.



8. Au bas de l'enregistrement, cliquez sur le lien connexe **Afficher toutes les listes connexes** .
9. Cliquez sur les **onglets Résultats de l'enrichissement des observables** ou **Bannières réseau** pour obtenir des résultats, puis cliquez sur l'icône d'informations bleue en regard d'un observable pour obtenir plus d'informations sur un élément spécifique.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement** pour afficher les données brutes et plus de détails.
11. Facultatif : Cliquez sur l'icône bleue des paramètres près de l'icône de recherche pour personnaliser la sortie et l'ordre des colonnes.
12. Dans **l'onglet Personnaliser les colonnes de la liste**, sélectionnez les paramètres disponibles, déplacez-les vers la colonne **Sélectionné** , puis cliquez sur **OK**.

Trouble?
Examinez les **notes de travail** pour plus d'informations et savoir comment procéder si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.

Secureworks CTP Intégration de l'ingestion de tickets

L'intégration Secureworks Counter Threat Platform de l'ingestion de tickets vous permet de récupérer Secureworks CTP automatiquement les tickets, de les convertir en incidents de sécurité et d'effectuer des actions de réponse automatisées.

Les principales fonctionnalités de cette intégration sont les suivantes :

- Ingestion automatique des tickets sélectionnés (y compris les pièces jointes) en fonction d'un calendrier prédéfini.
- Mappage des champs de ticket et d'événement aux Réponse aux incidents de sécurité champs.
- Aperçu des incidents de sécurité mappés aux champs de ticket.
- Filtrage et agrégation des tickets.
- Récupération sur demande des événements associés à un ticket.
- Suivi périodique des principales mises à jour des tickets.
- Automatisation des mises à jour et des fermetures de tickets en fonction de l'état de l'incident SIR
- Mise à jour du ticket principal.
- Synchronisation des journaux de travail Secureworks avec Réponse aux incidents de sécurité les notes de travail.

Configurer votre Now Platform instance pour l'intégration de l'ingestion Secureworks CTP de tickets

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform instance avant d'installer l'application à partir du ServiceNow Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application pour garantir une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform AND Réponse aux incidents de sécurité .	Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre Now Platform instance. • Un utilisateur disposant du Now Platform rôle administrateur (admin) installe l'application à partir du rôle administrateur ServiceNow Store (sn_si.admin) et lui attribue le SIR rôle. • Un utilisateur disposant du rôle sn_si.admin supervise les tâches suivantes dans :Now Platform ◦ Nomme, crée et modifie les profils. ◦ Sélectionne et mappe Secureworks CTP les champs de ticket aux champs d'incident de sécurité. ◦ Prévisualise l'exactitude des détails de l'incident de sécurité avant de finaliser la configuration. ◦ Planifie l'ingestion de ticket en cours. ◦ Active les mises à jour des tickets lorsqu'un incident SIR SIR est créé et fermé. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Les utilisateurs avec l'sn_si.analyst travaillent avec des incidents de sécurité. Pour plus d'informations sur les rôles et l'affectation de rôles aux utilisateurs, consultez Gestion des rôles
Vérifiez que vous utilisez les versions suivantes : • API de ticket SecureWorks 4.0 • API d'événement Secureworks 1.0 • API d'enrichissement Secureworks 1.0	Si vous avez accès au Secureworks CTP portail, vous avez accès à l'API requise pour cette intégration. Aucune autre configuration spéciale n'est requise pour l'API.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
et activées avant d'installer l'application pour l'intégration.	activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité **2.** Ingestion d'événements et d'alertes pour Opérations de sécurité (requis pour les intégrations SIEM) : Cette application nécessite : ◦ com.glide.hub.integration.runtime => l'exécution du Centre d'intégration ServiceNow ◦ com.glide.hub.action_step.rest => Étape d'action du Centre d'intégration ServiceNow : REST **Remarque :** Les composants du concentrateur d'intégration sont installés en même temps que le module d'extension d'ingestion d'événements et d'alertes. Si ceux-ci ne sont pas installés, contactez le support client pour obtenir de l'aide. Pour plus d'informations sur l'installation des Opérations de sécurité applications principales, consultez et .

Installer et configurer l'application ServiceNow pour l'intégration d'ingestion de tickets CTP de SecureWorks

Avant d'exécuter l'intégration sur votre Now Platform instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre Réponse aux incidents de sécurité correctement aux produits et Opérations de sécurité sur votre Now Platform instance.

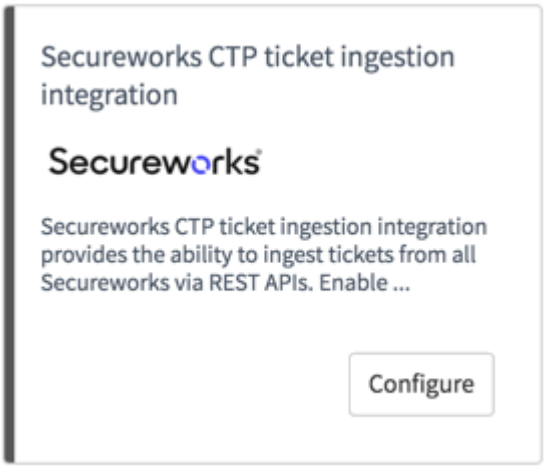
Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si vous n'avez pas installé l'application Secureworks CTP de ticket à partir de ServiceNow Store pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette Intégration de l'ingestion Secureworks CTP de tickets.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour configurer l'application, cliquez sur **Nouveau**.
4. Si un bouton **Configurer** s'affiche sur une mosaïque, cliquez dessus pour modifier une configuration existante.
5. Dans la boîte de dialogue qui s'affiche, renseignez les champs.

Champ	Description
Nom	Nom de l'instance Secureworks CTP utilisée pour l'intégration. Vous ne pouvez saisir que des valeurs alphanumériques et des traits d'union (-) dans ce champ.
Description	Entrez une description pour le compte d'utilisateur.
Nom d'utilisateur	Saisissez le nom d'utilisateur du Secureworks CTP compte API. Notez que le nom d'utilisateur est sensible à la casse. Pour trouver le nom d'utilisateur, procédez comme suit : ◦ Connectez-vous au Secureworks CTP portail. ◦ Accédez à la **Compte** > **Gestion des comptes** > **Informations d'identification d'API**. Le nom d'utilisateur est affiché sur la page Informations d'identification de l'API.
Mot de passe API	Saisissez le mot de passe de l'API Secureworks CTP . Pour trouver le mot de passe de l'API, procédez comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Connectez-vous au Secureworks CTP portail. ◦ Accédez à la **Compte** > **Gestion des comptes** > **Informations d'identification d'API**. Le mot de passe de l'API s'affiche sur la page Informations d'identification de l'API. Pour plus d'informations sur la façon d'obtenir le nom d'utilisateur et le mot de passe de l'API, suivez les étapes de la section Génération d'une clé API persistante du Guide de l'API de création de tickets SecureWorks.

6. Cliquez sur **Envoyer**.
   Une fois validée et soumise, chaque configuration est enregistrée sous forme de vignette sur la page Intégrations de sécurité.

Résultats

Si vos vignettes de configuration enregistrées ne s'affichent pas sur la page Intégrations de sécurité. Dans le coin supérieur droit de la page, à partir de la liste de choix **Afficher les configurations** , cliquez sur **Oui**.

Créer un profil pour l'intégration de l'ingestion de tickets CTP de SecureWorks

Créez un profil dans votre Now Platform instance et déterminez quels tickets doivent être ingérés et quels tickets seront utilisés pour créer des incidents de sécurité. Avant que les incidents de sécurité ne soient créés à partir de tickets ingérés, les valeurs de champ des tickets sont affichées sur la mise en page d'un Now Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera affiché.

L'intégration vous permet d'ingérer des tickets en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance. Tous les tickets sont initialement ingérés pour un type de ticket configuré dans un profil. Les tickets ingérés peuvent ensuite être filtrés pour spécifier quels tickets créent des incidents de sécurité.

Par exemple, vous pouvez préférer des filtres qui créent des incidents de sécurité uniquement pour les tickets identifiés comme présentant un risque élevé. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir des tickets ingérés, les valeurs de champ individuelles des tickets sont mappées aux champs correspondants sur une mise en page d'incident de sécurité pour un aperçu.

Identifier la source du profil

Spécifiez le nom et la source du profil.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

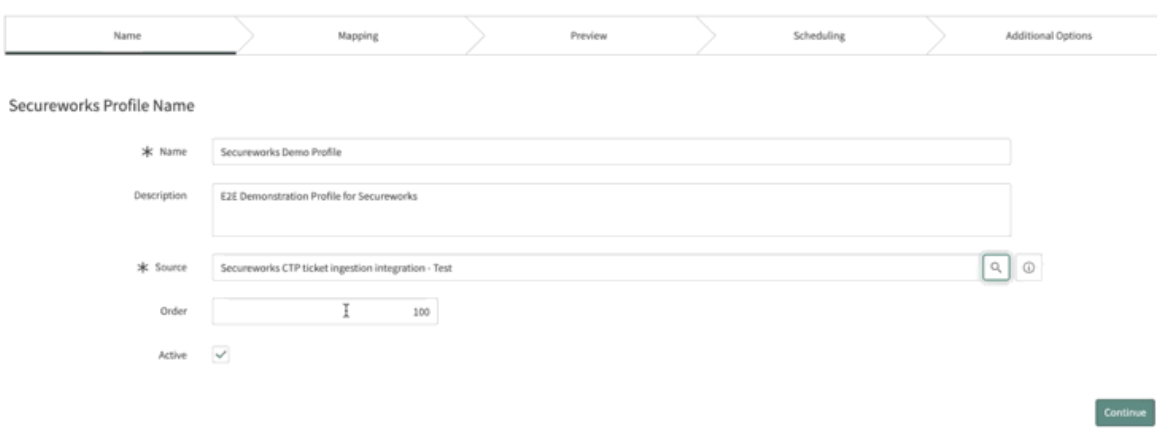
1. Pour créer un profil pour un ticket dans votre Now Platform instance, accédez à **Intégration de l'ingestion de tickets de Secureworks** > **Profils Secureworks**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le tableau ci-dessous un exemple de formulaire rempli.

Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre Now Platform instance doivent être uniques.
Source	Sélectionnez la source à partir de laquelle vous souhaitez ingérer les données.
Ordre	La valeur par défaut est 100. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Plus la valeur de l'ordre est faible, plus la priorité est élevée.
Actif	Cette option est désactivée par défaut. Si cette option est désactivée, le profil n'est pas actif. **Remarque :** Vous devez remplir toutes les sections du profil avant de l'activer.

La figure suivante est un exemple de formulaire rempli.



Que faire ensuite

Mappez les champs de ticket.

Mappage des champs de ticket pour l'intégration CTP de SecureWorks

Mappez les champs Ticket et Événement aux champs du formulaire d'incident de sécurité.

Pour l'étape de mappage, vous devez d'abord ingérer des échantillons de tickets, puis vous assurer que tous les champs de ticket pertinents sont mappés à l'emplacement approprié

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sur le Réponse aux incidents de sécurité formulaire, puis visualiser l'incident de sécurité dans la section d'aperçu.

Le mappage des champs d'échantillons de ticket implique les éléments suivants :

- Extraction et renseignement des données d'échantillon : voir Ingérer l'échantillon de tickets Secureworks
- Mappage des champs de ticket à l'incident de sécurité : voir Mappage des champs de ticket Secureworks aux champs de Security Incident Response

Ingérer l'échantillon de tickets Secureworks

Sélectionnez les échantillons de tickets à ingérer.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Vous pouvez soit extraire les cinq échantillons de tickets les plus récents, soit fournir les ID de ticket uniques pour les tickets spécifiques que vous souhaitez utiliser pour votre expérience de mappage.
   Dans la liste de choix **Préférences d'ingestion** , sélectionnez l'une des options suivantes :
   - Récupérer les tickets les plus récents : les 5 tickets les plus récents sont récupérés.
   - Sélectionner les tickets en fonction de l'ID de ticket : spécifiez l'ID du ticket à récupérer. Vous pouvez spécifier un maximum de 5 ID de tickets séparés par des virgules.
3. Cliquez sur **Extraire les données d'échantillon** pour extraire les dernières données d'échantillon de ticket du Secureworks CTP serveur.
   L'extraction des échantillons de billets peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran. Les tickets récupérés sont affichés sous forme d'onglets individuels. Cliquez sur un onglet pour afficher les données du ticket. Pour chaque ticket, vous pouvez voir les champs de ticket et leurs valeurs, ainsi que les détails de l'événement contribuant qui a déclenché le ticket.

   Remarque : Vous verrez les détails des événements de contribution uniquement s'ils se sont produits au cours des 7 derniers jours. Les événements datant de plus de 7 jours ne sont pas affichés.

Que faire ensuite
Une fois que vous avez extrait les exemples de données, l'étape suivante consiste à mapper les champs de ticket à l'incident de sécurité.

Mappage des champs de ticket Secureworks aux champs de Security Incident Response

Mappez les champs de ticket ou d'événement individuels aux champs d'un Now Platform SIR incident de sécurité.

Mappage de champs de ticket

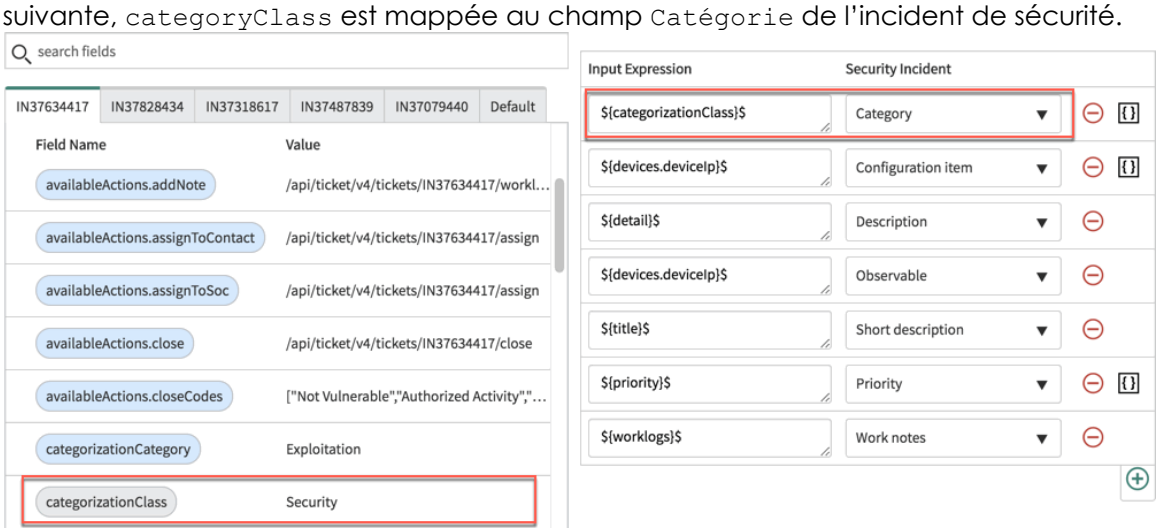
En tant qu'utilisateur disposant du rôle sn_si.admin, utilisez les champs de la section Échantillons de tickets sur la gauche et mappez-les aux champs d'incident de sécurité dans la colonne **Mappage de champ d'incident SIR** . Modifiez la configuration du mappage en faisant glisser les champs de ticket ou d'événement à gauche et en les déposant sur la section de mappage de champ d'incident SIR à droite. Le mappage sur la droite associe le champ de ticket entrant à un champ d'incident de sécurité sortant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Pour mapper une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez longuement sur un nom de champ bleu sur le côté gauche du formulaire.
2. Vous pouvez saisir manuellement le nom du champ dans la colonne Expression d'entrée ou glisser-déplacer le nom du champ. Par exemple, `description`, et déposez-la sur un champ de la colonne **Expression d'entrée** à côté d'un nom de champ dans la colonne **Incident de sécurité** .

   La valeur du champ est affichée dans la colonne Expression d'entrée. Dans l'image suivante, `categoryClass` est mappée au champ `Catégorie` de l'incident de sécurité.



> **Remarque :** Si vous saisissez manuellement le nom du champ d'événement dans la section **expression d'entrée** , vous devez ajouter un préfixe *`${Event :eventfield}$`* avant le nom du champ mappé.

Pour vous assurer qu'aucun champ de ticket ou d'événement n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par couleur. Le codage couleur des champs de ticket vous aide à suivre les valeurs de ticket que vous avez déjà mappées, car elles sont grisées tandis que tous les champs non mappés restants apparaissent en bleu. Cela vous aide à mieux visualiser quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si des informations de ticket importantes restantes restent non mappées.

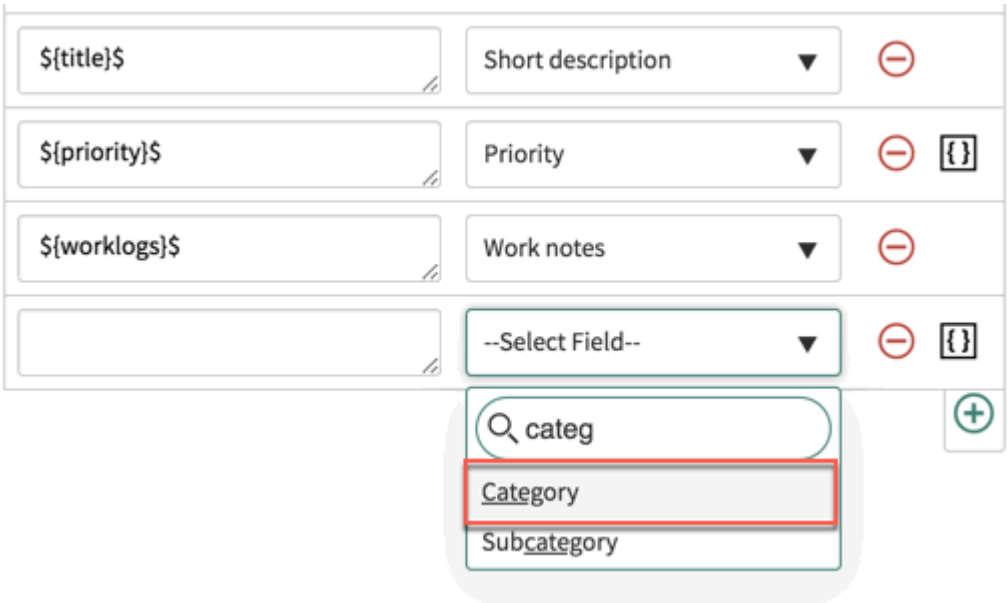
Les champs bleu clair sur la gauche indiquent qu'un champ de ticket n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un ticket entrant ou un champ d'événement à plusieurs champs sur un incident de sécurité. Un champ gris indique qu'un champ a été sélectionné et mappé à un champ sur l'incident de sécurité. Ce code couleur vous aide à suivre le mappage.

3. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit :
   a. À droite du formulaire, dans la section Mappage des champs d'incidents SIR , en bas de la grille, cliquez sur l'icône plus (+). Un nouveau champ s'affiche.
   b. Dans la colonne Incident de sécurité, développez la liste de choix qui s'affiche, puis sélectionnez un champ.

      Dans la liste de choix développée pour le nouveau champ, certains champs sont grisés. Dans la figure suivante, la catégorie a un arrière-plan gris, car elle a été mappée dans l'incident de sécurité. À l'instar du code couleur pour les champs de ticket sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident déjà mappés SIR .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Étant donné que plusieurs observables peuvent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité dispose d'une liste de choix dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affiché dans la liste de choix, le champ n'est pas renseigné sur l'incident de sécurité.

c. Vous pouvez également saisir une valeur dans le champ Rechercher pour la nouvelle ligne.

d. Sur le côté gauche du formulaire, sélectionnez le champ de ticket et glissez-le vers un champ d'incident de sécurité approprié à droite.

4. Supprimez des champs à l'aide de l'icône - en regard du nom du champ dans la section Mappage de champs d'incidents SIR.

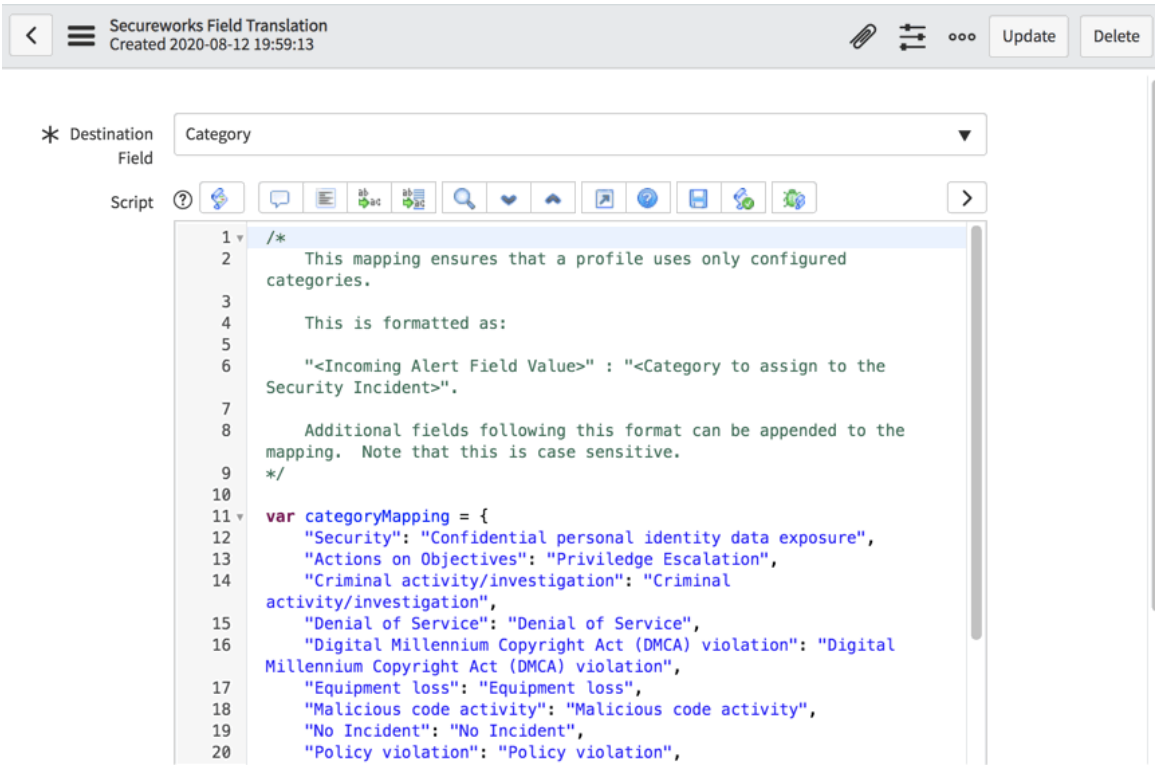
5. Poursuivez le mappage en ajoutant ou en supprimant des valeurs de champ au mappage.

Formater la traduction du champ

Dans certains cas, les champs de ticket peuvent ne pas être traduits directement dans les champs de l'incident SIR de sécurité. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez mettre en forme des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident SIR de sécurité à l'aide de la fonctionnalité Formater la traduction de champ.

Pour utiliser l'éditeur de script, cliquez sur l'icône {} en regard du champ Catégorie. L'éditeur de script s'affiche

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



.

Entrez les changements apportés au script et cliquez sur **Mettre à jour** pour enregistrer les changements et revenir à la page Mappage.

Conditions de génération d'incidents

Une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de spécifier quels tickets doivent créer des incidents de sécurité par rapport à quels tickets doivent être filtrés (par exemple, les tickets de faible priorité). Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir les critères supplémentaires qu'un ticket entrant doit satisfaire pour créer un incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

1. Faites défiler l'écran jusqu'à la section **Conditions de génération d'incidents** du formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

   Le Créateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

   Les options des listes de choix pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section **Ingestion de tickets d'échantillons** pour les tickets ingérés. Ces champs sont dynamiques et changent en fonction des tickets que vous ingérez. Les critères que vous saisissez sont sensibles à la Secureworks CTP casse et doivent correspondre exactement aux valeurs du ticket. Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférez peut-être retourner à votre Secureworks CTP console et vérifier vos tickets pour les mots-clés.

   Remarque : Les champs *de ticket worklogs*, *devices*, *attachments*, *watchers*, *availableactions* et *closeCodes* peuvent avoir plusieurs valeurs (car les valeurs sont stockées dans des tableaux). Étant donné que la condition de filtre ne peut récupérer que des chaînes, vous devez utiliser la condition de filtre *contient* pour ces champs afin de vous assurer que les données sont filtrées correctement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. À l'aide des listes de choix et des champs du générateur de conditions, définissez des filtres pour la première ligne.
3. Pour ajouter d'autres conditions, à droite des champs, cliquez sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. (Facultatif) Dans la deuxième ligne, définissez une deuxième condition de filtre.

   Ce type de filtrage des conditions de génération d'incident vous aide à affiner les tickets et à limiter le nombre d'incidents de sécurité inutiles que vous créez sans modifier la règle ou les filtres sous-jacents. Si des critères de filtrage supplémentaires sont définis, seuls les tickets qui correspondent à tous les critères sont mappés aux incidents de sécurité.

Critères d'agrégation de tickets pour traiter des tickets similaires et éviter les incidents en double

Définissez des critères d'agrégation de tickets supplémentaires qui regroupent un ticket entrant en un incident de sécurité existant SIR au lieu de créer des incidents similaires et potentiellement dupliqués. En utilisant des critères de valeur de correspondance de champ pour chaque profil, cette aptitude d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données de ticket connexes sur un seul incident de sécurité. Pour définir les critères, procédez comme suit :

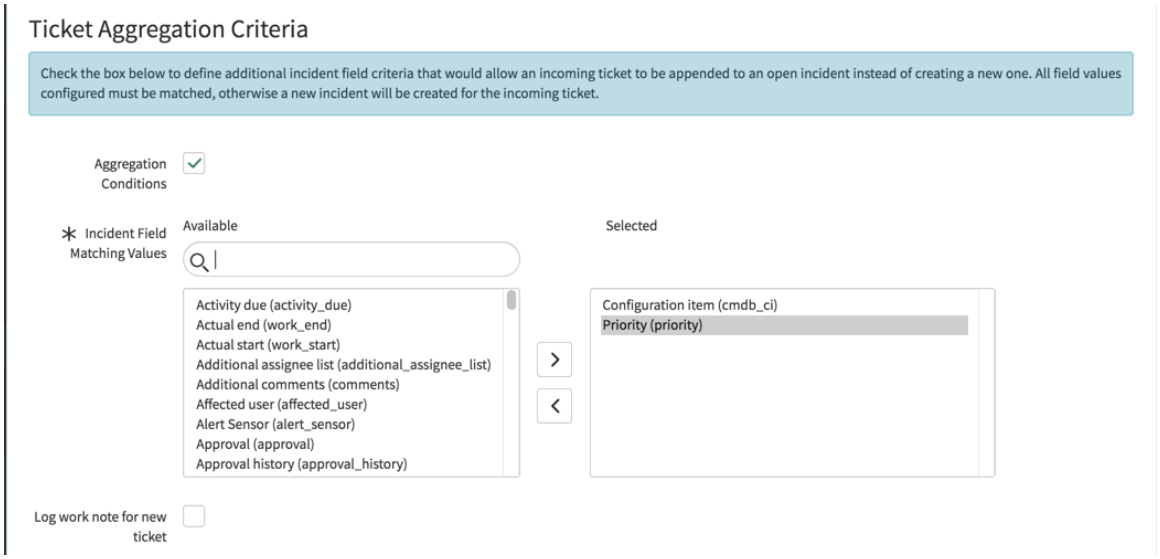
1. Faites défiler l'écran jusqu'à la section **Critères d'agrégation de tickets** du formulaire et cochez la case Conditions d'agrégation pour activer cette option.

   Les colonnes Incident Field Matching Values (Valeurs correspondantes du champ d'incident) s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés dans l'incident SIR de sécurité.

2. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre Now Platform et déplacez-les vers la liste Sélectionné.

   Toutes les valeurs de champ que vous sélectionnez doivent être mises en correspondance pour ajouter ce ticket entrant à un incident de sécurité existant. Cela inclut les champs, tels que les observables et les éléments de configuration, qui peuvent avoir plusieurs valeurs de champ de ticket mappées. Toutes les valeurs doivent correspondre. Si seul un sous-ensemble de valeurs est mis en correspondance, les conditions d'agrégation de tickets ne seront pas remplies et un nouvel incident de sécurité sera créé. Voir la capture d'écran ci-dessous pour le mappage de champs à valeurs multiples.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Si un nouveau ticket correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation de l'étape de mappage, le nouveau ticket est automatiquement ajouté à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur avec le rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher tous les tickets agrégés ajoutés sur une liste connexe sur un incident de sécurité. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi ces tickets sont regroupés aux incidents de sécurité existants. Si cet onglet n'est pas affiché dans un incident de sécurité, faites défiler l'écran vers le côté gauche de l'enregistrement sous **Liens connexes** et cliquez sur le lien **Afficher toutes les listes connexes** .

Remarque : La liste connexe des tickets agrégés SecureWorks n'est pas disponible avec le système de base. Vous devez configurer la mise en page de la liste connexe et l'inclure explicitement avec les autres listes connexes.

3. (Facultatif) Pour consigner une note de travail pour un nouveau ticket récemment ajouté à l'incident de sécurité, cochez la case pour activer cette option. La note de travail consigne qu'un nouveau ticket a été ajouté, ainsi qu'un lien vers les détails du ticket et tous les autres détails qui peuvent avoir été ajoutés au champ Note de travail dans votre section de mappage.

   Vous avez mappé avec succès les valeurs d'un Secureworks CTP ticket vers les champs d'un incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage de génération d'incidents. Vous avez également ajouté des tickets aux incidents de sécurité existants lorsque les valeurs de champ de ticket correspondent aux critères d'agrégation configurés.

4. Cliquez sur **Continuer** pour poursuivre la configuration du profil. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité

Prévisualiser les valeurs mappées dans l'incident de sécurité

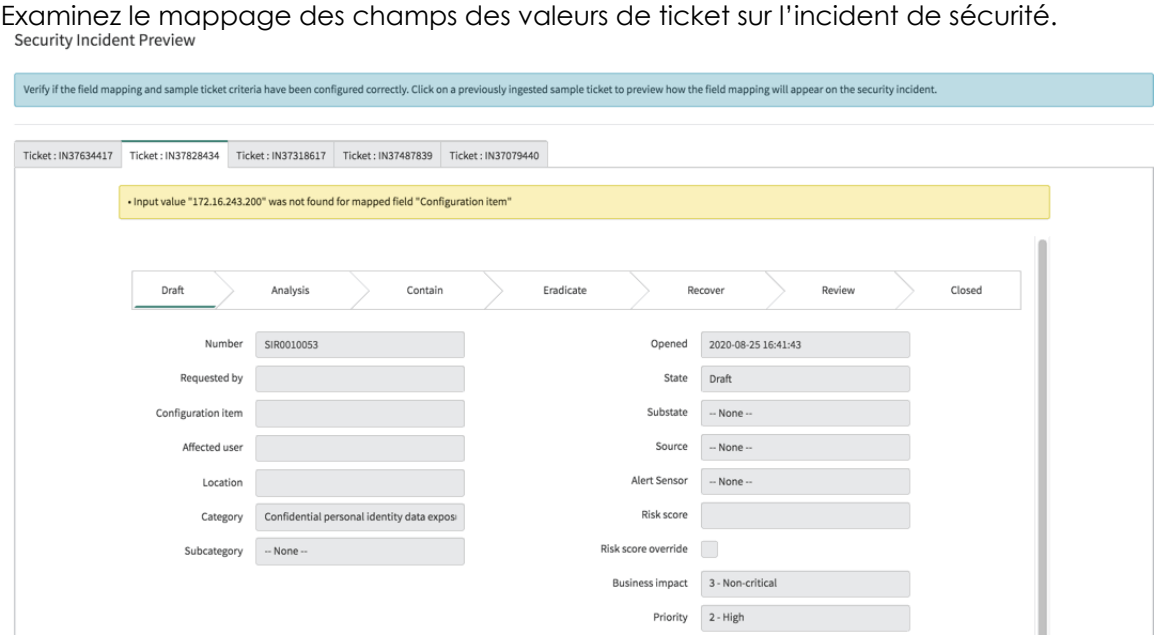
Une fois que vous avez terminé l'étape de mappage, prévisualisez les valeurs que vous avez mappées dans un SIR incident de sécurité. Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs de ticket que vous souhaitez afficher sur l'incident de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs contenant des erreurs ou pour renseigner les données manquantes. Si l'aperçu n'est pas terminé, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de SIR sécurité ne sont pas enregistrés en tant qu'incidents réels dans le produit Security Incident Response.

Procédure
1. Si l'aperçu de l'incident de sécurité n'est pas affiché, cliquez sur **Aperçu** dans la barre de progression.
   Les tickets sont affichés sous forme d'onglets.
2. Cliquez sur un onglet pour prévisualiser l'incident de sécurité.
   Il s'agit d'une vue en lecture seule et un enregistrement de cet incident de sécurité n'est pas enregistré.
3. Examinez le mappage des champs des valeurs de ticket sur l'incident de sécurité.



   L'image précédente est un exemple d'aperçu avec une erreur de mappage des échantillons qui ont été ingérés.

4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

Que faire ensuite
Si aucun message d'erreur ne s'affiche et que vous êtes satisfait du mappage de champs sur l'incident de sécurité. Définissez le calendrier.

Définir un calendrier pour l'ingestion de ticket CTP SecureWorks

Vérifiez les paramètres par défaut pour la récupération des tickets ou modifiez la planification selon vos besoins. Cette étape vous permet de filtrer votre récupération de ticket en fonction d'une plage de dates et d'un intervalle d'interrogation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Vous choisissez également la fréquence à laquelle vous interrogerez les futurs tickets qui correspondent à la configuration du profil de ticket. Configurez ces intervalles d'interrogation pour chaque profil. Lors de la planification, vous préférerez peut-être équilibrer la charge du système par rapport à l'urgence de l'incident. Une valeur par défaut d'une minute est définie pour n'importe quel profil, mais vous préférerez peut-être modifier ce paramètre en fonction de l'urgence de l'incident et de la charge prévue sur votre système.

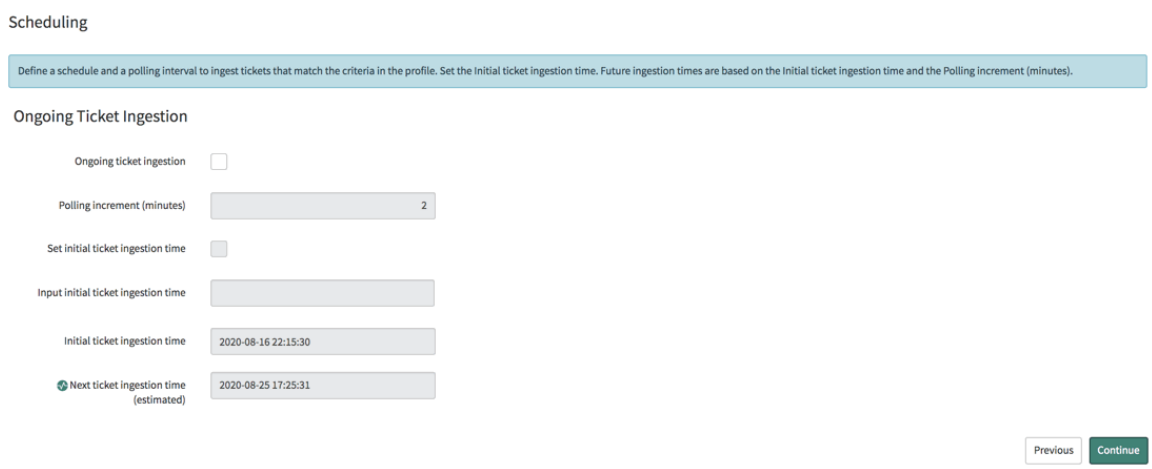
Procédure
1. Si la page Planification de la barre de progression n'est pas affichée, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les tickets sont extraits du Secureworks CTP portail.

Option	Description
Ingestion de ticket en cours sélectionnée	En fonction du paramètre par défaut, l'instance Now Platform extrait du portail pour recevoir Secureworks CTP de nouveaux tickets toutes les cinq minutes. Les incidents de sécurité sont créés si des tickets sont trouvés et si les critères de filtrage de génération d'incidents sont respectés. Pour équilibrer l'ingestion des tickets par rapport à la charge du serveur et extraire les données les plus récentes, cinq minutes sont peut-être le paramètre que vous préférez. Toutefois, cette valeur peut être modifiée si nécessaire.
◦ Ingestion de ticket en cours sélectionnée ◦ Définir le délai d'intégration du ticket initial	Délai d'ingestion initial Si vous souhaitez planifier l'ingestion initiale à une heure précise, procédez comme suit : ◦ Sélectionnez les champs Ingestion de ticket en cours et Définir la durée d'ingestion du ticket initial. ◦ Spécifiez l'heure dans le champ Délai d'intégration du ticket initial d'entrée. L'ingestion initiale aura lieu à l'heure spécifiée ici. Les ingestions suivantes seront basées sur le calendrier défini dans le champ Incrémentation de l'interrogation (minutes). À titre d'exemple de planification, si vous avez une tâche de ticket quotidien qui s'exécute une fois par jour à 4 h (heure locale), vous pouvez configurer le profil de ticket correspondant dans votre instance Now Platform pour qu'il s'exécute à 4 h 05 (heure locale) afin de capturer immédiate-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	ment le ticket et créer un incident de sécurité. Saisissez 04 05 00 dans le champ Ingestion de ticket initiale. Dans le champ Incrémentation de l'interrogation (minutes), saisissez 1 440 (24 heures) pour planifier la prochaine ingestion de ticket dans les 24 heures suivant l'ingestion initiale du ticket. Le délai d'intégration du ticket initial et le délai d'intégration du ticket suivant sont affichés dans les champs. Pour configurer les paramètres de cet exemple, procédez comme suit : ◦ Sélectionnez l'option **Ingestion de ticket en cours** . ◦ Dans le champ Incrémentation de l'interrogation (minutes), saisissez 1 440 (24 heures). ◦ Sélectionnez l'option **Définir le délai d'intégration du ticket initial** . ◦ Dans le champ Délai d'intégration du ticket initial d'entrée, saisissez 04 05 00. L'heure de la prochaine ingestion du ticket est affichée dans le champ Délai d'ingestion du ticket suivant (estimé).



3. Cliquez sur **Continuer** pour accéder à la page Options supplémentaires.

Automatiser les mises à jour et la fermeture des tickets en fonction de l'état de l'incident SIR

L'intégration Secureworks CTP de l'ingestion de tickets dispose d'une interface bidirectionnelle qui permet aux tickets de créer des incidents de sécurité, ainsi que de mettre à jour les tickets une fois l'incident de sécurité créé et/ou fermé avec les détails pertinents de l'incident tels que le numéro d'incident de sécurité, le groupe d'affectation, l'URL de l'incident de sécurité, entre autres.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.admin

Procédure
1. Si la page Options supplémentaires de la barre de progression n'est pas affichée, sélectionnez **Options supplémentaires**.
2. Terminez la configuration pour la mise à jour des tickets lors de la création de l'incident de sécurité.

Option ou champ	Description
Mettre à jour les notes de travail SIR avec les journaux de travail Secureworks	Sélectionnez cette option pour activer la fonctionnalité de synchronisation des journaux de travail et SIR des notes de travail Secureworks. Cela vous permet de suivre les mises à jour apportées au ticket après Secureworks CTP la création de l'incident de sécurité. **Remarque :** ◦ Si le champ Journaux de travail Secureworks a été mappé au champ Notes de travail SIR, les journaux de travail SecureWorks sont récupérés jusqu'à ce que l'incident de sécurité soit créé. ◦ Si la fonctionnalité de synchronisation est activée, seuls les journaux de travail créés ou mis à jour après la création d'un incident de sécurité sont récupérés.
Mettre les tickets Secureworks lors de la création d'incidents SIR	Sélectionnez cette option pour mettre à jour le Secureworks CTP ticket et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir du ticket. Cela peut se produire à la fois pour les tickets de déclenchement initiaux qui créent l'incident de sécurité et pour les tickets agrégés.
Commentaires initiaux renvoyés au ticket Secureworks	Lorsqu'un incident de sécurité est créé, le ticket est automatiquement mis à jour avec Secureworks CTP des commentaires. Vous pouvez modifier le texte par défaut et utiliser le format ${field name}$ pour ajouter ou modifier les champs disponibles dans le formulaire d'incident de sécurité.
Fermer les tickets Secureworks lors de la fermeture d'incidents SIR	Sélectionnez cette option si vous souhaitez utiliser l'option de fermeture automatisée des tickets. Cela peut se produire à la fois pour les tickets de déclenchement initiaux qui créent l'incident de sécurité et pour les tickets agrégés. Lorsqu'un incident de sé-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	curité est fermé, le ticket correspondant est automatiquement fermé Secureworks CTP avec le même code de fermeture que l'incident de sécurité et les commentaires de fermeture par défaut spécifiés dans le profil. **Remarque :** Vous ne pouvez pas utiliser cette option pour mettre à jour l'état du ticket principal.
Commentaires de fermeture renvoyés au ticket Secureworks	Les commentaires de fermeture par défaut sont affichés ici. Vous pouvez modifier le texte par défaut et utiliser le format ${field name}$ pour ajouter ou modifier des champs disponibles dans le formulaire d'incident de sécurité.

3. Cliquez sur **Terminer** pour terminer la configuration et déplacer le profil vers l'état **En attente** .
   Une boîte de dialogue de confirmation s'affiche. Vous avez correctement configuré le profil. Activez ce profil pour extraire des tickets du Secureworks CTP portail en fonction de votre planification.

Facultatif : copier un profil CTP SecureWorks

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils pour gagner du temps.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
En tant qu'utilisateur disposant du rôle sn_si.admin, si vous copiez un profil, le nom du profil est d'abord modifié pour éviter les profils en double. En outre, le profil copié est désactivé (faux) afin qu'il ne soit pas activé accidentellement avant la fin de la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure

1. Accédez à la **Tout** > **Intégration de l'ingestion de tickets de Secureworks** > **Profil Secureworks**.
2. Dans la liste des profils Secureworks qui s'affiche, sélectionnez un profil que vous souhaitez copier et, dans la liste de choix **Actions sur les lignes sélectionnées** , cliquez sur **Copier**.
   Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient (copier). Bien que le profil d'origine soit activé (`vrai`), la copie est désactivée à ce stade (`faux`). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.

   Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. Notez que l'état de la colonne **Actif** est défini sur faux, car le profil doit être activé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

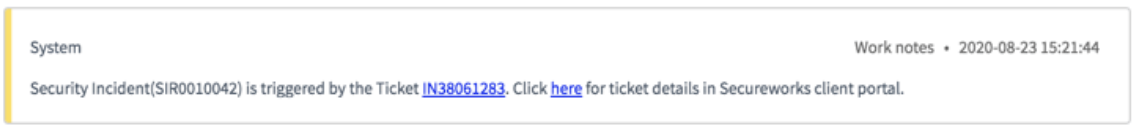
Vous êtes invité à activer le nouveau profil une fois que vous avez terminé les étapes de configuration.

Changements apportés au formulaire Security Incident Response après l'ingestion du ticket

Une fois qu'un Secureworks CTP ticket a été ingéré, un incident de sécurité est créé et les mises à jour correspondantes sont apportées à l'enregistrement d'incident de sécurité.

Notes de travail

Une note de travail est publiée avec les détails du ticket qui a déclenché l'incident de sécurité.



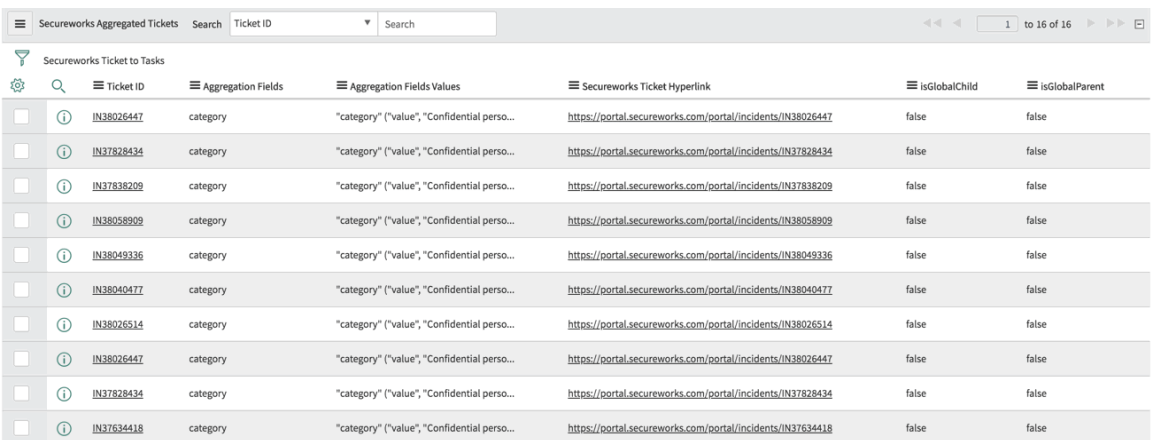
Cliquez sur le lien du ticket pour accéder à l'enregistrement interne de SecureWorks Ticket vers tâche. Le lien hypertexte **Cliquez ici** vous dirige vers le Secureworks CTP tableau de bord dans lequel vous pouvez afficher les détails du ticket.

Si vous aviez sélectionné l'option **Enregistrer la note de travail pour le nouveau ticket** dans les critères d'agrégation de tickets, comme décrit dans la page Créer un profil : mappage, une note de travail est publiée lorsque le ticket est agrégé.



Tickets agrégés

Cliquer sur **Listes connexes** > **Tickets agrégés SecureWorks** pour afficher le ticket agrégé à l'incident de sécurité. Cliquez sur le lien hypertexte du ticket pour afficher le ticket dans le Secureworks CTP tableau de bord.



Créer un incident de sécurité : sélectionnez un ticket dans la liste, cliquez sur le menu **Actions** , puis sur **Créer un incident de sécurité**. Cette option crée un nouvel incident de sécurité pour le ticket et ce ticket est désagrégé de l'incident de sécurité parent.

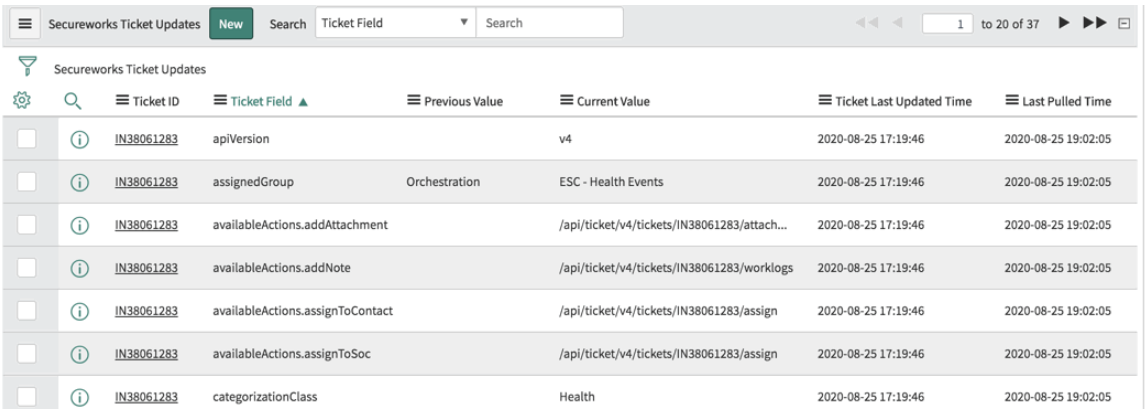
Supprimer l'enregistrement de ticket : sélectionnez un ticket dans la liste, cliquez sur le menu **Actions** , puis cliquez sur **Supprimer**. Cette option supprime l'enregistrement de ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mises à jour des tickets Secureworks

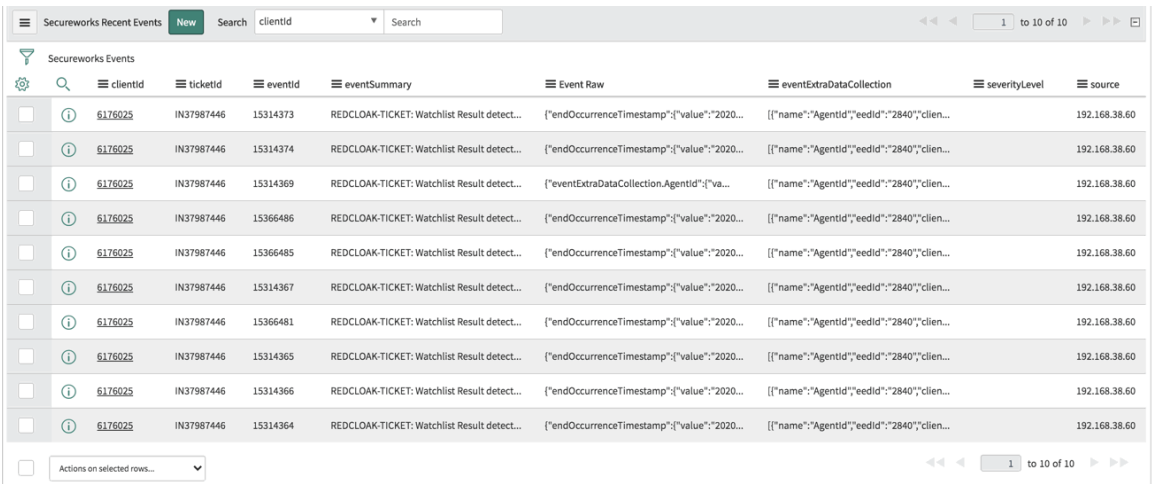
Cela affiche les champs de ticket standard et suit les changements apportés aux tickets à chaque intervalle d'interrogation. Cela est utile, car vous pouvez afficher les mises à jour de tickets directement sans avoir à accéder au Secureworks CTP tableau de bord. Tous les changements apportés aux valeurs sont affichés dans les champs Valeur précédente et Valeur actuelle.



Ticket ID	Ticket Field	Previous Value	Current Value	Ticket Last Updated Time	Last Pulled Time
IN38061283	apiVersion		v4	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	assignedGroup	Orchestration	ESC - Health Events	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.addAttachment		/api/ticket/v4/tickets/IN38061283/attach...	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.addNote		/api/ticket/v4/tickets/IN38061283/worklogs	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.assignToContact		/api/ticket/v4/tickets/IN38061283/assign	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.assignToSoc		/api/ticket/v4/tickets/IN38061283/assign	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	categorizationClass		Health	2020-08-25 17:19:46	2020-08-25 19:02:05

Événements SecureWorks récents

Cliquez sur l'option **Extraire les événements Secureworks récents** sous **Liens connexes** pour afficher les événements Secureworks les plus récents.



clientId	ticketId	eventId	eventSummary	Event Raw	eventExtraDataCollection	severityLevel	source
6176025	IN37987446	15314373	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314374	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314369	REDCLOAK-TICKET: Watchlist Result detect...	{"eventExtraDataCollection.AgentId":{"va...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15366486	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15366485	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314367	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15366481	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314365	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314366	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60
6176025	IN37987446	15314364	REDCLOAK-TICKET: Watchlist Result detect...	{"endOccurrenceTimestamp":{"value":"2020...	[{"name":"AgentId","eedId":"2840","clien...		192.168.38.60

Par défaut, un nombre maximum de 50 événements sera affiché. Vous pouvez modifier ce paramètre par défaut dans les paramètres d'intégration de Secureworks.

Afficher les tickets SecureWorks et les incidents de sécurité correspondants

Les tickets importés Secureworks CTP sont initialement stockés dans la table d'importation de tickets. Affichez tous les tickets qui ont été importés avant l'application Secureworks CTP de toute condition de filtre.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Intégration de l'ingestion de tickets de Secureworks** > **Importation sécurisée de ticket**.
2. Vous pouvez afficher tous les tickets qui ont été importés avant qu'ils Secureworks CTP ne soient agrégés ou que des conditions de filtre ne soient appliquées.
3. Cliquez sur un ID de ticket pour afficher les données brutes du ticket.
4. Accédez à la **Ingestion de tickets Secureworks** > **Ticket Secureworks vers tâche**.
   Les Secureworks CTP tickets avec leurs incidents de sécurité correspondants s'affichent.

Avis de fermeture du ticket principal CTP de SecureWorks

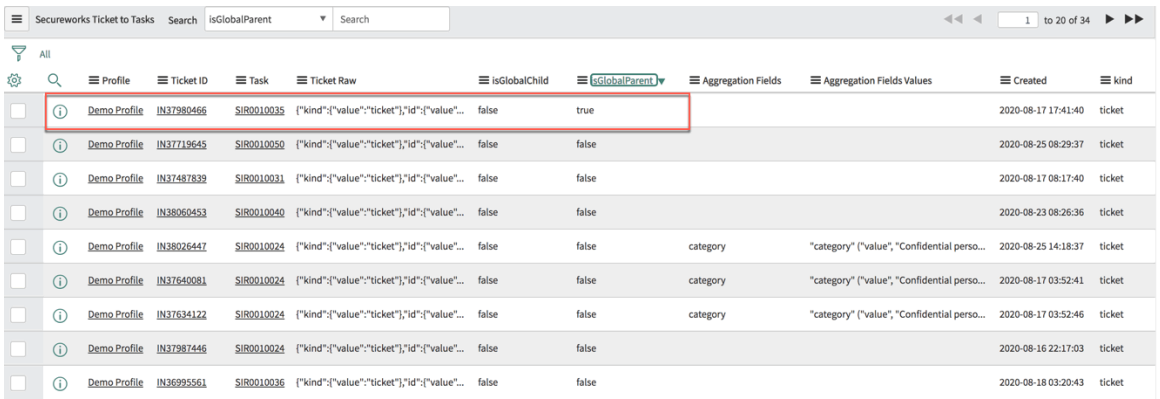
Avant de fermer un incident de sécurité créé par un Secureworks CTP ticket principal, vous devez vérifier que tous les tickets enfants associés au ticket principal sont fermés.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Ingestion de tickets Secureworks** > **Ticket Secureworks vers tâche**.
   Les Secureworks CTP tickets avec leurs incidents de sécurité correspondants s'affichent.

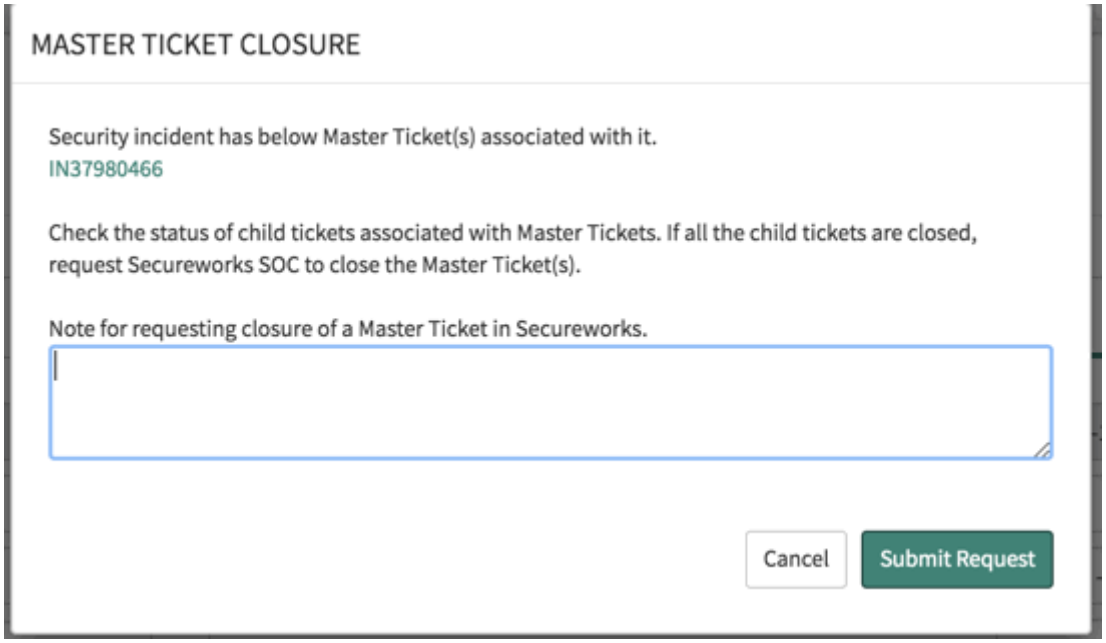


Profile	Ticket ID	Task	Ticket Raw	isGlobalChild	isGlobalParent	Aggregation Fields	Aggregation Fields Values	Created	kind
Demo Profile	IN37980466	SIR0010035	{"kind":{"value":"ticket"},"id":{"value"...	false	true			2020-08-17 17:41:40	ticket
Demo Profile	IN37719645	SIR0010050	{"kind":{"value":"ticket"},"id":{"value"...	false	false			2020-08-25 08:29:37	ticket
Demo Profile	IN37487839	SIR0010031	{"kind":{"value":"ticket"},"id":{"value"...	false	false			2020-08-17 08:17:40	ticket
Demo Profile	IN38060453	SIR0010040	{"kind":{"value":"ticket"},"id":{"value"...	false	false			2020-08-23 08:26:36	ticket
Demo Profile	IN38026447	SIR0010024	{"kind":{"value":"ticket"},"id":{"value"...	false	false	category	"category" ("value", "Confidential perso...	2020-08-25 14:18:37	ticket
Demo Profile	IN37640081	SIR0010024	{"kind":{"value":"ticket"},"id":{"value"...	false	false	category	"category" ("value", "Confidential perso...	2020-08-17 03:52:41	ticket
Demo Profile	IN37634122	SIR0010024	{"kind":{"value":"ticket"},"id":{"value"...	false	false	category	"category" ("value", "Confidential perso...	2020-08-17 03:52:46	ticket
Demo Profile	IN37987446	SIR0010024	{"kind":{"value":"ticket"},"id":{"value"...	false	false			2020-08-16 22:17:03	ticket
Demo Profile	IN36995561	SIR0010036	{"kind":{"value":"ticket"},"id":{"value"...	false	false			2020-08-18 03:20:43	ticket

2. Cliquez sur l'incident de sécurité avec le champ **isGlobalParent** défini sur **vrai.**
3. Changez l'état de l'incident de sécurité sur **Fermé**, spécifiez les codes de fermeture et cliquez sur **Enregistrer**.
   La boîte de dialogue suivante s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cet incident de sécurité est associé à un ticket principal SecureWorks. Un Master Ticket peut être associé à un ou plusieurs tickets enfants. Avant que le Master Ticket puisse être clôturé, vous devez d'abord vérifier si tous les tickets enfants associés à ce Master Ticket sont fermés.

4. Ajoutez une note demandant la fermeture du ticket principal dans Secureworks et cliquez sur **Envoyer la demande**.
   Le ticket principal est maintenant réaffecté à l'équipe SOC SecureWorks.
5. Une fois la demande envoyée, vous pouvez fermer l'incident de sécurité.
6. Accédez à la **Application** > **Module**.

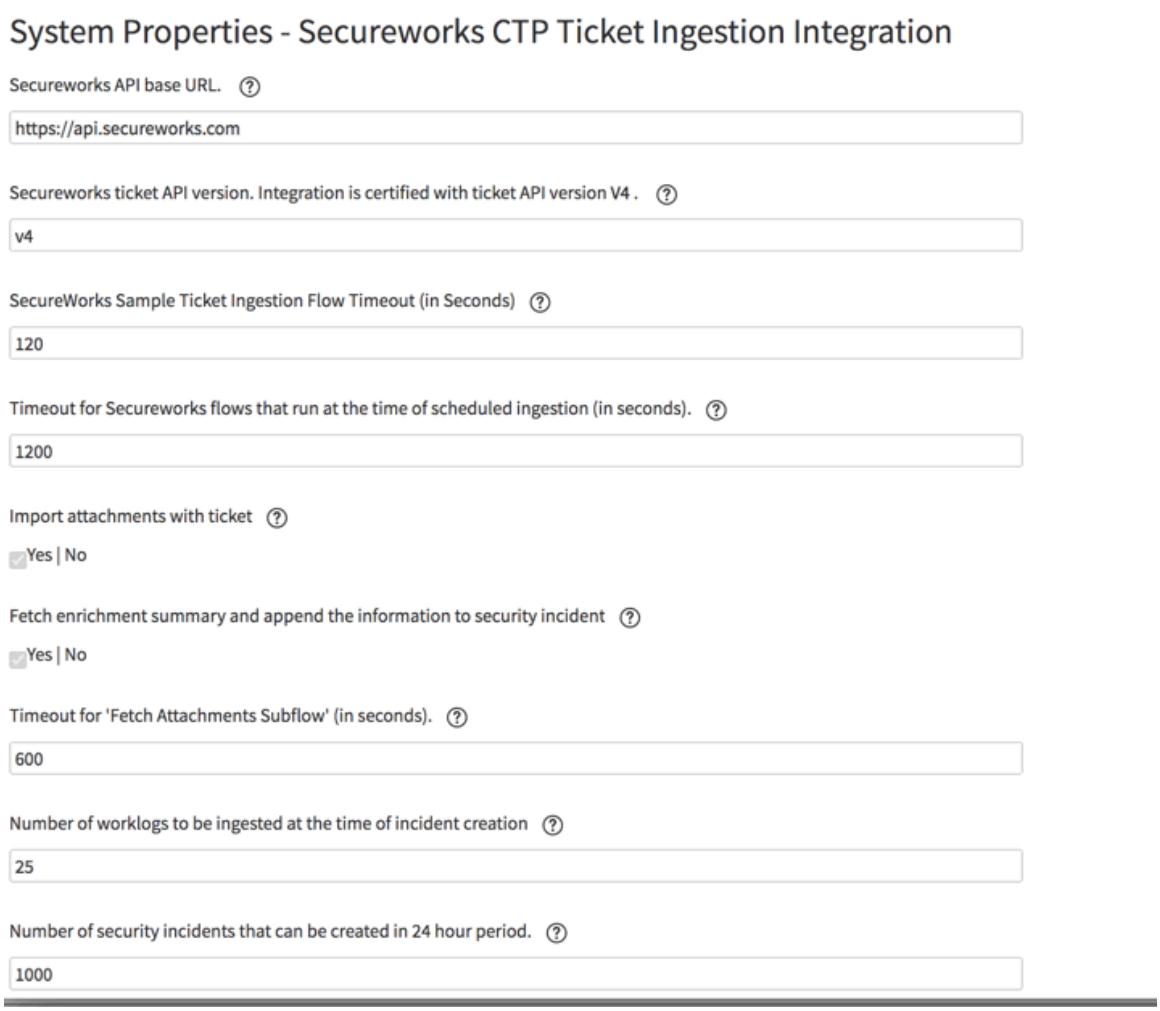
Paramètres de configuration de l'intégration CTP de SecureWorks

Utilisez cette option pour modifier les propriétés système par défaut de l'intégration de l'ingestion Secureworks CTP de tickets.

Pour modifier les propriétés système, connectez-vous en tant qu'utilisateur ayant le rôle *sn_si.admin* et accédez à **Intégration de l'ingestion de tickets de Secureworks** > **Paramètres d'intégration Secureworks**.

Les paramètres de configuration par défaut s'affichent. Vous pouvez modifier ces paramètres si nécessaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Tous les paramètres d'intégration modifiés seront appliqués lors du prochain intervalle d'interrogation, tel que défini dans le profil.

Intégration de Réponse aux incidents de sécurité à Zscaler

Vous pouvez utiliser le Intégration de Réponse aux incidents de sécurité à Zscaler produit pour connecter les journaux de votre Zscaler Internet Access serveur (ZIA) au Now Platformfichier . Cette intégration vous permet d'afficher des tableaux de bord, de créer des alertes personnalisées et d'enquêter sur les incidents de sécurité.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Vue d'ensemble

Le Zscaler produit Internet et passerelle Web est fourni à partir du cloud. Il vous fournit les points de données clés et des informations sur l'environnement de sécurité de votre entreprise. Intégration de Réponse aux incidents de sécurité à Zscaler connecte le Zscaler Internet Access produit à votre Now Platform instance. En utilisant le Zscaler produit sur , Now Platformvous obtenez plus d'informations sur l'utilisation d'Internet par votre organisation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Principales fonctionnalités de l'intégration

Cette intégration comprend les fonctionnalités clés suivantes :

- Recherche de la réputation des observables par rapport à la bibliothèque de menaces globale conservée par le Zscaler produit.

  Remarque : La Zscaler bibliothèque mondiale des menaces répertorie les menaces par tendance, pays d'origine, cible, destination, volume et différentes catégories de menaces. Cette bibliothèque de menaces globale vous permet d'examiner vos observables par rapport au paysage des menaces global.

- Conservation des observables dans une liste bloquée ou une liste d'autorisation sur le Zscaler produit.
- Possibilité d'extraire et de passer en revue les rapports de sandbox à partir Zscaler du produit pour un hachage MD5. La fonctionnalité Cloud Sandbox du produit exécute et analyse les Zscaler fichiers dans un environnement virtuel pour détecter les comportements malveillants.
- Alertes de sécurité à partir des événements Patient 0 générés dans le Zscaler produit lorsqu'un utilisateur télécharge un fichier malveillant inconnu.
- Plusieurs listes de catégories d'URL qui agissent comme des listes de blocs ou des listes d'autorisation telles que définies dans le Zscaler produit.
- Now Platform les incidents de sécurité qui peuvent être balisés pour identifier la catégorie d'URL à laquelle les observables sont ajoutés.
- Périodes d'expiration qui conservent la taille des entrées de liste de catégories d'URL en faisant automatiquement expirer ou en supprimant les entrées les plus anciennes.
- Workflow d'approbation pour l'ajout et la suppression des observables des listes de catégories d'URL.
- Entrées de catégorie d'URL qui peuvent être liées aux enregistrements d'observables et aux incidents de sécurité qui incluent des résultats de Threat Intelligence et des détails sur les raisons pour lesquelles une entrée est bloquée.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
Zscaler site web de la documentation produit	Site web de la documentation produit ZScaler
ServiceNow site web de la documentation produit	Site web de la documentation produit ServiceNow

Premiers pas avec Intégration de Réponse aux incidents de sécurité à Zscaler

Activez et configurez le Zscaler Internet Access produit pour qu'il s'interface avec votre instance et Réponse aux incidents de sécurité votre Now Platform produit.

Liste de vérification

Tâche de configuration	Description
Affectez et vérifiez les rôles requis Now Platform et Réponse aux incidents de sécurité .	Ces rôles sont requis pour la configuration et la vérification des résultats attendus :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	• Le rôle administrateur installe l'intégration à partir du ServiceNow Store rôle sn_si.admin et lui attribue le rôle. • Le rôle sn_si.admin effectue les tâches suivantes : ◦ Configure l'intégration. ◦ Crée, active et supprime les listes de catégories d'URL. ◦ Affecte le rôle sn_si.analyst. • Le rôle sn_si.analyst crée des entrées et gère les incidents de sécurité.
Vérifiez que les applications principales sont installées et activées avant de ServiceNow configurer cette intégration.	Le module d'extension Programme d'installation du ServiceNow Hub d'intégration pack Entreprise [com.glide.hub.integrations.enterprise] est requis. Le Réponse aux incidents de sécurité module d'extension (com.snc.security_incident) est requis. Ce module d'extension installe automatiquement toutes les dépendances du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres applications pour l'intégration Opérations de sécurité . Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si ces applications ne sont pas déjà installées, installez et activez chaque application une par une dans l'ordre suivant : **1.** Réponse aux incidents de sécurité Dépendance (com.snc.si_dep) **2.** Cadre de travail de Security Integration **3.** Security Support Common **4.** Orchestration de support de sécurité **5.** Renseignements sur les menaces Prise en charge commune **6.** Trusted Security Circles

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	7. Opérations de sécurité Assistant de configuration **8.** Réponse aux incidents de sécurité
Vérifiez les Zscaler versions.	• Cette intégration est prise en charge à partir de la Zscaler Internet Access version 1.0 ou ultérieure. • Cette intégration est testée avec les versions suivantes Zscaler : ◦ Connecteur client Zscaler pour Windows : 3.0 ◦ Connecteur client Zscaler pour macOS : 3.0 ◦ Connecteur client Zscaler pour Linux : bêta ◦ Connecteur cloud Zscaler - 6.1
Vérifiez que vous disposez des autorisations requises Zscaler et que vous avez configuré l'accès à l' Zscaler Internet Access API.	• Vous devez disposer des informations d'identification d'administrateur pour Zscaler Internet Access. • Vous devez avoir un abonnement valide à l'API de service dans le cloud. Zscaler L'assistance doit vous fournir votre clé. • Vous devez disposer Zscaler Internet Access des informations d'identification d'administrateur (nom d'utilisateur et mot de passe). L'authentification API repose sur la combinaison de la clé API et Zscaler Internet Access des informations d'identification administrateur. **Remarque :** Pour plus d'informations sur la Zscaler Internet Access gestion des clés API, consultez la documentation Zscaler .

Configurer l'accès aux Zscaler Internet Access API

Configurez l'accès Zscaler Internet Access au serveur pour authentifier la connexion sécurisée entre l'instance et le Now PlatformZscaler serveur.

Avant de commencer
Rôle requis : Zscaler Internet Access admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Une fois Zscaler votre abonnement API activé pour le service cloud de votre organisation, il est disponible dans la Zscaler Internet Access page de gestion des clés API avec l'URL de base. Votre organisation ne peut avoir qu'une seule clé API ou jeton. Supprimez la clé ou le jeton existant avant d'en ajouter un nouveau.

L'URL de base de l'API est `${Cloud_Name}/api/v1`. Vérifiez le nom du Zscaler cloud qui a été mis en service pour votre organisation et utilisez-le pour remplacer `{Cloud_Name}` dans l'URI de base. Voici quelques exemples d'URL de base :

- example.zscalerbeta.net
- example.zscalerone.net
- example.zscalertwo.net
- example.zscaler.net
- example.zscloud.net

Remarque : Pour plus d'informations sur le portail d'administration Zscaler Internet Access , consultez la documentation de gestion des clés API Zscaler et la documentation du portail Zscaler .

Procédure

1. Connectez-vous en tant qu'administrateur au portail d'administration Zscaler Internet Access .
2. Accédez à la **Administration** > **Gestion des clés API**.
3. Cliquez sur **Ajouter une clé API**.
   Si l'option Ajouter une **clé API** n'est pas disponible, supprimez la clé existante.
   La nouvelle clé API est immédiatement valide et s'affiche dans l'onglet.

Résultats

Vous avez récupéré l'URL de base et la clé API pour configurer l'accès à Zscaler partir de l'instance Now Platform .

Installer et configurer Intégration de Réponse aux incidents de sécurité à Zscaler

Installez et configurez le Intégration de Réponse aux incidents de sécurité à Zscaler produit Accès Internet à partir du ServiceNow Store pour commencer à utiliser l'intégration sur votre Now Platform instance.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Téléchargez le Intégration de Réponse aux incidents de sécurité à Zscaler produit à partir de et ServiceNow Store installez-le.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la Intégration de Réponse aux incidents de sécurité à Zscaler tuile et cliquez sur **Configurer** > **Créer une configuration**.
4. Renseignez les champs du formulaire.

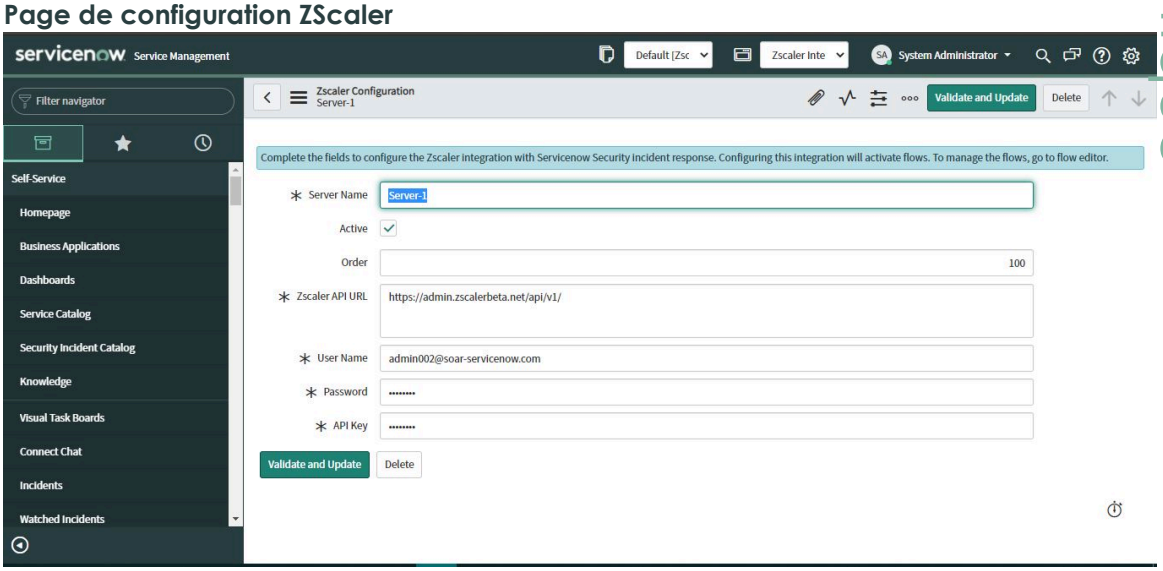
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Zscaler Formulaire de configuration

Champ	Description
Nom du serveur	Zscaler Nom du serveur. Par exemple, ZSserver.
Actif	Indicateur indiquant que le profil est actif.
Ordre	Priorité du flux. La valeur de ce champ indique l'ordre des workflows lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux doté du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400. La valeur par défaut est 100.
Zscaler URL D'API	URL de base qui héberge l'API Zscaler . Par exemple https://example.zscalerbeta.net
Noms d'utilisateur	Nom d'utilisateur du Zscaler Internet Access compte administrateur.
Mot de passe	Mot de passe du Zscaler Internet Access compte administrateur.
Clé API	Clé API que vous avez obtenue à partir du portail d'administration Zscaler Internet Access .

L'exemple suivant montre la page de configuration Zscaler.

Page de configuration ZScaler



5. Cliquez sur **Valider et mettre à jour**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Une fois que vous avez validé et enregistré cette configuration, revenez à la Zscaler page Configurations.

Ajouter des Zscaler Internet Access listes de catégories d'URL

Ajoutez les catégories d'URL disponibles dans le Zscaler produit Accès Internet à l'instance Now Platform afin de spécifier une action pour chaque URL afin de disposer d'un accès facile pour le filtrage granulaire et la création de politiques.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Le Intégration de Réponse aux incidents de sécurité à Zscaler fournit une liste d'autorisation et une liste de refus par défaut : listes de catégories d'URL pour aider à filtrer le contenu.

Les catégories d'URL que vous ajoutez dans l'instance Now Platform doivent déjà se trouver dans votre Zscaler Internet Access environnement. Vous ne pouvez pas utiliser Intégration de Réponse aux incidents de sécurité à Zscaler pour créer des catégories d'URL sur Zscaler.

Remarque : Pour plus d'informations sur les listes de catégories d'URL dans le produit, consultez la documentation Zscaler sur les catégories d'URL Zscaler.

Procédure
1. Accédez à la **Tout** > **Intégration ZScaler** > **Listes de catégories d'URL ZScaler**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Zscaler Formulaire Listes de catégories d'URL

Champ	Description
Source	Nom du serveur. Vous ne pouvez afficher que les serveurs précédemment configurés Zscaler Internet Access à partir de la liste des catégories d'URL.
Actif	Indicateur indiquant que la liste des catégories d'URL est active.
Catégorie d'URL	Champ qui est activé une fois que vous avez sélectionné la source. Vous pouvez afficher la liste des catégories d'URL créées dans Zscaler.
Période d'expiration (jours)	Période d'expiration de la liste des catégories d'URL. 0 (par défaut) indique que l'entrée de la liste des catégories d'URL n'expire jamais. En modifiant cette valeur, tout observable qui a été ajouté à cette catégorie d'URL est actif pendant le nombre de jours que vous entrez. Vous pouvez saisir une valeur minimale de 1.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par exemple, si vous définissez la période d'expiration sur 30 jours, les entrées sont supprimées de la liste des catégories après 30 jours.
Balise d'affichage	Balise de sécurité qui apparaît sur l'incident SIR de sécurité. Lorsque vous activez l'option **Balise d'affichage** , le Zscaler champ Balise pour les observables est disponible sur le formulaire.
Créer une demande de changement	Demande de changement et tâches de changement dans votre Now Platform instance pour les enregistrements qui sont joints à la liste de catégories d'URL. Lorsque vous activez l'option **Créer une demande de changement** , le champ **Demande de changement** est disponible sur le formulaire.
Exiger l'approbation	Liste des groupes d'approbateurs. Une fois que vous avez soumis une demande, une approbation du groupe est requise pour terminer la demande. Lorsque vous activez l'option **Exiger l'approbation** , les champs **Approbateurs pour l'ajout d'observables** et **Approbateurs pour la suppression des observables** sont disponibles sur le formulaire. ◦ **Approbateurs pour l'ajout d'observables** : sélectionnez les approbateurs à l'aide de la fonction de recherche pour ajouter les observables à partir de la page Liste des catégories **d'URL Zscaler** . Cette option vous permettra d'ajouter le(s) groupe(s) d'utilisateurs pour les approbations. ◦ **Approbateurs de la suppression des observables** : sélectionnez les approbateurs de la suppression des observables à l'aide de la recherche dans la page Liste des catégories **d'URL Zscaler** . Cette option vous permet de supprimer le(s) groupe(s) d'utilisateurs de la liste d'approbation.
Description	Description de la liste des catégories d'URL Zscaler . Utilisez ce champ pour ajouter plus de détails sur l'enregistrement de catégorie d'URL.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Envoyer**.
   Une soumission réussie déclenche une notification par e-mail au groupe d'approbation.

Soumettre les observables d'un enregistrement d'incident de sécurité à une liste de catégories d'URL

Soumettez les observables joints à un enregistrement d'incident de sécurité à une liste de catégories d'URL configurée à l'aide de la demande d'autorisation ou de blocage. L'ajout d'observables à la liste d'autorisation ou de blocage pour les analyses de sécurité permet aux utilisateurs d'examiner le contenu de ces URL et d'accéder au contenu de confiance.

Avant de commencer

Rôle requis : sn_si.analyst

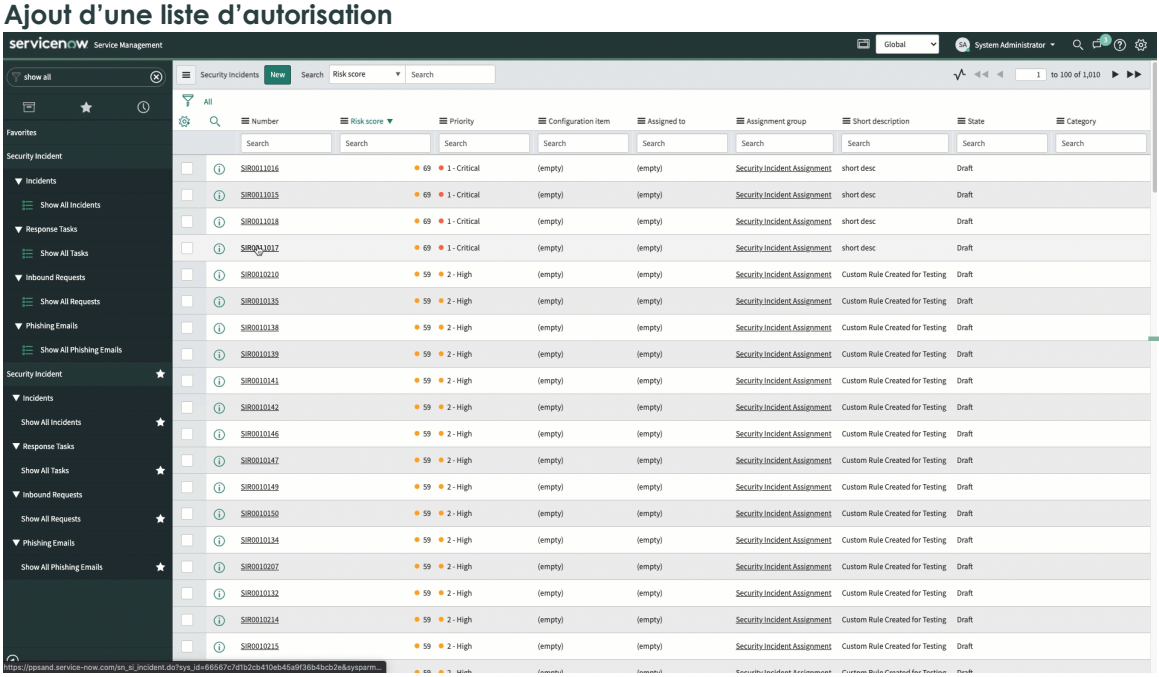
Pourquoi et quand exécuter cette tâche

Vous soumettez des entrées d'observables à l'aide de l'action Autoriser ou bloquer la demande de la liste connexe Observables associés. Les observables sont des artefacts présents sur un réseau ou un système d'exploitation susceptibles d'indiquer une intrusion. Utilisez la liste des catégories d'URL configurées précédemment pour sélectionner l'observable que vous souhaitez soumettre. Une fois la demande envoyée, une demande d'approbation est envoyée à votre groupe d'approbation.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
   Dans cet exemple, vous voyez comment sélectionner un incident de sécurité et un observable, et comment ajouter une liste d'autorisation.

Ajout d'une liste d'autorisation



2. Sélectionnez l'incident de sécurité que vous souhaitez associer à la demande d'autorisation ou de Zscaler bloc.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
   Si vous ne trouvez aucun observable, cliquez sur **Nouveau**.
4. Sélectionnez un observable, puis dans le menu Actions, cliquez sur **Autoriser/Bloquer la demande**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans la boîte de dialogue Autoriser/Bloquer la demande, indiquez s'il faut effectuer la demande d'autorisation ou de blocage sur l'observable.
6. Cliquez sur **Envoyer**.
7. Affichez les notes de travail pour voir l'état de votre soumission et les balises de sécurité. Cliquez sur les liens dans les notes de travail pour obtenir plus d'informations sur l'état ou pour analyser les détails sur le Concepteur de flux. Les balises de sécurité désignent des métadonnées sur l'enregistrement répondant et définissent qui doit avoir accès à des types spécifiques de contenu de sécurité.
8. Pour afficher l'état de l'observable que vous avez sélectionné, accédez à **Intégration Zscaler** > **URL Zscaler Entrées de liste de catégories**.
9. Sur la page Entrées de la liste des catégories d'URL Zscaler, cliquez sur l'observable pour afficher l'enregistrement.

Approuver les observables dans les listes de catégories d'URL

Approuvez les observables qui sont ajoutés à une liste de catégories d'URL afin que les entrées d'observables figurent dans les listes d'autorisation ou de refus appropriées.

Avant de commencer
Rôle requis : sn_si.analyst

Procédure
1. Accédez à la **Tout** > **Intégration Zscaler** > **Approbations Zscaler**.
2. Sélectionnez l'enregistrement à approuver.
3. Cliquez sur **Approuver**.
   Le groupe d'approbateurs reçoit une notification par e-mail pour la demande d'approbation. Une fois que les approbateurs ont cliqué sur le lien **Approuver/Rejeter** dans l'e-mail, l'état devient Approuvé.

Soumettre l'incident de sécurité à la liste des catégories d'URL Zscaler

Soumettez directement les entrées pour les observables qui ne sont pas associés à un enregistrement d'incident de sécurité spécifique Now Platform afin que les entrées observables figurent dans les listes d'autorisation ou de refus appropriées.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez également ajouter des observables à la liste des catégories d'URL directement à partir de l'enregistrement Observable.

Procédure
1. Accédez à la **Tout** > **Intégration Zscaler** > **URL Zscaler Entrées de liste de catégories**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Zscaler Formulaire d'entrées de listes de catégories d'URL

Champ	Description
Valeur d'entrée	Nom de l'observable.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si un observable correspondant est trouvé, le reste du formulaire est automatiquement rempli. Si aucun observable correspondant n'est trouvé, vous devez remplir le reste des informations manuellement.
Observable	Valeur (par exemple, adresse IP ou hachage) associée à l'observable.
Type d'observable	Classification des observables, telle qu'une adresse IP ou un hachage de fichier.
Liste des catégories d'URL	Catégorie d'URL. Par exemple, si une organisation utilise example.com pour les services Office 365, elle Zscaler example.com classe en tant que services professionnels et Office 365.
Source	Nom du serveur. Vous ne pouvez afficher que les serveurs précédemment configurés Zscaler à partir de la liste des catégories d'URL.
Nombre d'incidents	Nombre d'incidents dans lesquels cet observable apparaît. Cette valeur est automatiquement mise à jour lorsque l'observable est ajouté à un autre incident manuellement ou via un workflow.
Actif	Indicateur indiquant que la liste des catégories d'URL est active.
Statut	État si l'observable est approuvé ou rejeté.
Période d'expiration (jours)	Période d'expiration de la liste des catégories d'URL. 0 (par défaut) indique que l'entrée de la liste des catégories d'URL n'expire jamais. Si vous modifiez cette valeur, tous les observables que vous ajoutez à cette catégorie d'URL sont actifs pendant le nombre de jours que vous entrez. Vous pouvez saisir une valeur minimale de 1. Par exemple, si vous définissez la période d'expiration sur 30 jours, les entrées sont supprimées de la liste des catégories après 30 jours.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si vous modifiez la période d'expiration par défaut de l'entrée de la liste des catégories d'URL, un avertissement s'affiche indiquant que la période diffère de la période configurée dans la liste des catégories d'URL sélectionnée.
Informations supplémentaires	Champ dans lequel vous pouvez ajouter plus de détails sur l'observable.

4. Cliquez sur **Envoyer**.

Exécuter une recherche de menace à l'aide de la Zscaler bibliothèque de menaces globale

Exécutez une recherche de menace sur un observable à l'aide de la bibliothèque de menaces globale du produit. Zscaler prend en charge les Zscaler Internet Access recherches par rapport aux types d'éléments observables IP, URL et domaines.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez effectuer des recherches de renseignements sur les menaces sur un ou plusieurs observables pour déterminer s'ils sont associés à des menaces de sécurité connues. Lorsqu'un observable est associé à un incident de sécurité pour la première fois, toutes les implémentations de recherche de menaces actives dans le Now Platform effectuent une recherche automatique des menaces. Vous pouvez les comparer à la liste connexe Résultats de la recherche de menace.

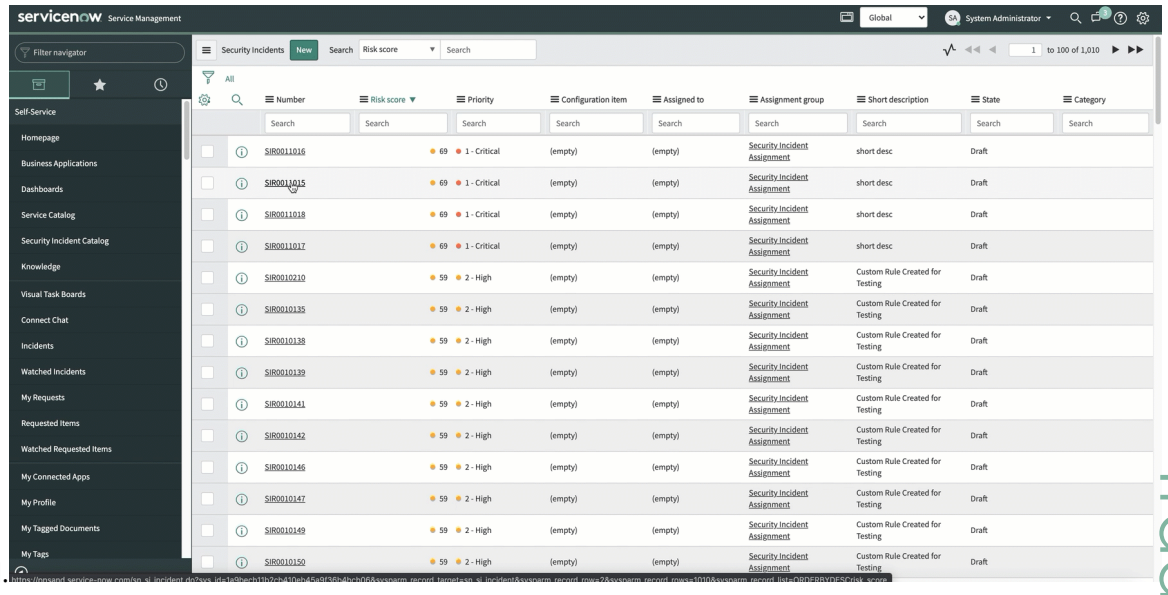
Par défaut, la configuration avec l'ordre le plus faible est sélectionnée pour effectuer la recherche de menaces par rapport Zscaler Internet Access à la bibliothèque de menaces globale du produit. Vous pouvez également effectuer la recherche de menaces manuellement.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité sur lequel vous souhaitez exécuter la recherche de menace.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Sélectionnez l'observable, puis dans le menu Actions, cliquez sur **Exécuter la recherche de menace**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans cet exemple, vous voyez comment sélectionner un incident de sécurité et un observable, comment exécuter une recherche de menace et comment afficher les résultats dans les notes de travail.



Résultats

Une fois que vous avez initié la recherche de menaces, vous pouvez consulter les notes de travail pour voir l'état de votre soumission.

Soumettre à l'analyse du bac à Zscaler sable

Utilisez le Zscaler Internet Access service de bac à sable des produits pour analyser les fichiers dans un environnement virtuel afin de détecter les comportements malveillants.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Lorsque vous créez une Zscaler configuration, une Zscaler soumission de bac à sable est créée par défaut dans le module Configuration de bac à sable Zscaler.

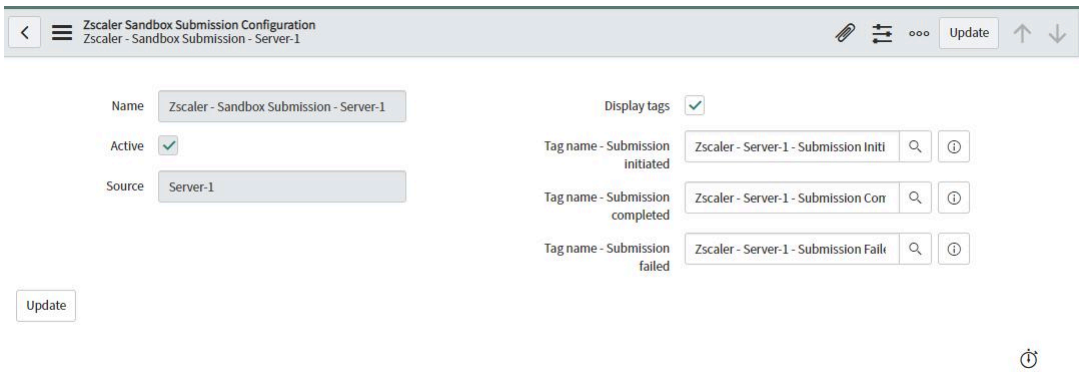
Les champs Nom et Source sont renseignés automatiquement et la configuration est activée par défaut. Vous ne pouvez modifier que la balise d'affichage et les options actives. Zscaler Internet Access vous permet d'extraire uniquement le rapport de bac à sable pour les observables de type hachage MD5.

L'analyse du fichier associé au hachage MD5 doit être terminée et le rapport correspondant doit se trouver dans le bac à Zscaler sable. Si le hachage MD5 que vous envoyez n'a pas de rapport dans Zscaler, vous obtenez un message d'erreur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Soumission à Zscaler Sandbox



Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité sur lequel vous souhaitez exécuter l'analyse du bac à sable.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Sélectionnez un observable de type hachage MD5, puis dans le menu Actions, sélectionnez **Soumettre au bac à sable**.
   Créez un observable de type hachage MD5 si vous ne trouvez pas d'observable de type hachage MD5 existant.
5. Dans la boîte de dialogue Soumission de fichier, sélectionnez l'option **Zscaler - Soumission en bac à sable - Serveur** dans la configuration Soumission et cliquez sur **Soumettre au bac à sable**.
   Une fois que vous avez initié la soumission du bac à sable, vous pouvez afficher les notes de travail pour voir l'état de votre soumission. Une balise est également ajoutée à l'incident de sécurité.
6. Dans les notes de travail, cliquez sur le lien dans la publication Résultat de soumission de Sandbox.

Résultats

Vous pouvez également afficher les résultats à partir de l'onglet Afficher toutes les listes connexes et Résultats de soumission du bac à sable.

Configurer des alertes par e-mail pour les événements Patient 0

Configurez Zscaler Internet Access le produit pour identifier et analyser les fichiers inconnus et potentiellement malveillants, tels que les événements Patient 0, afin de protéger votre réseau contre les fichiers malveillants.

Avant de commencer

Rôle requis : sn_si.admin, Zscaler Internet Access admin

Pourquoi et quand exécuter cette tâche

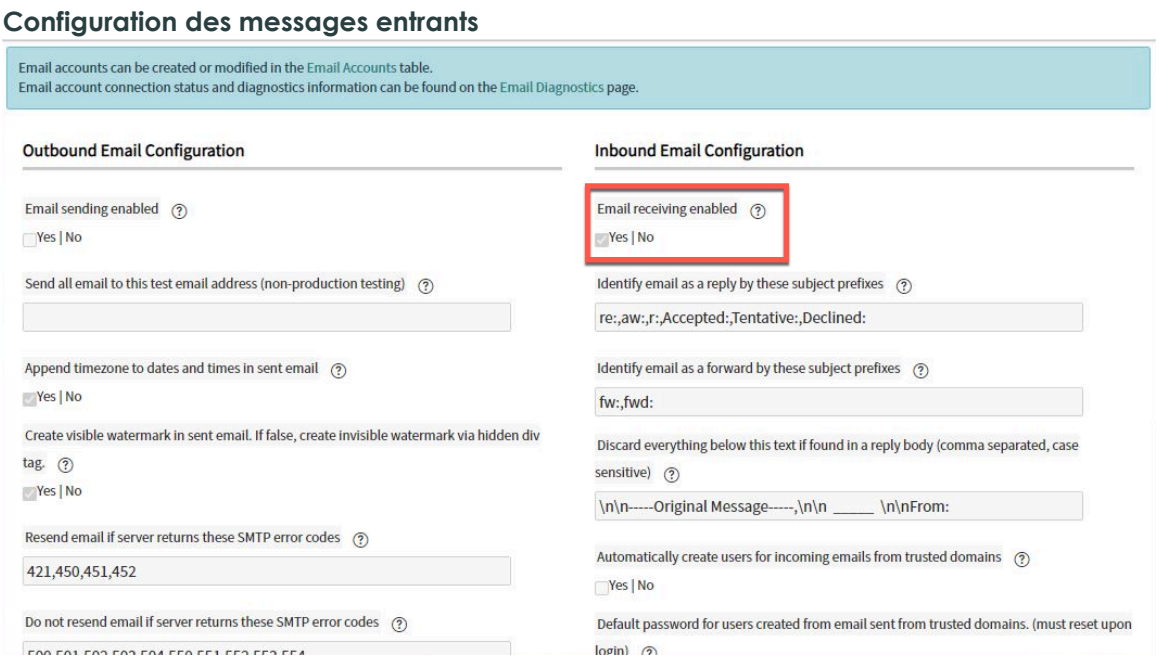
Le patient O est une classe d'alertes qui inclut un fichier inconnu dont le téléchargement a été autorisé, mais qui s'avère malveillant. L'événement patient 0 est classé comme critique. Vous pouvez configurer le Now Platform pour recevoir des alertes par e-mail à intervalles réguliers pour les événements Patient 0.

Traduction automatique

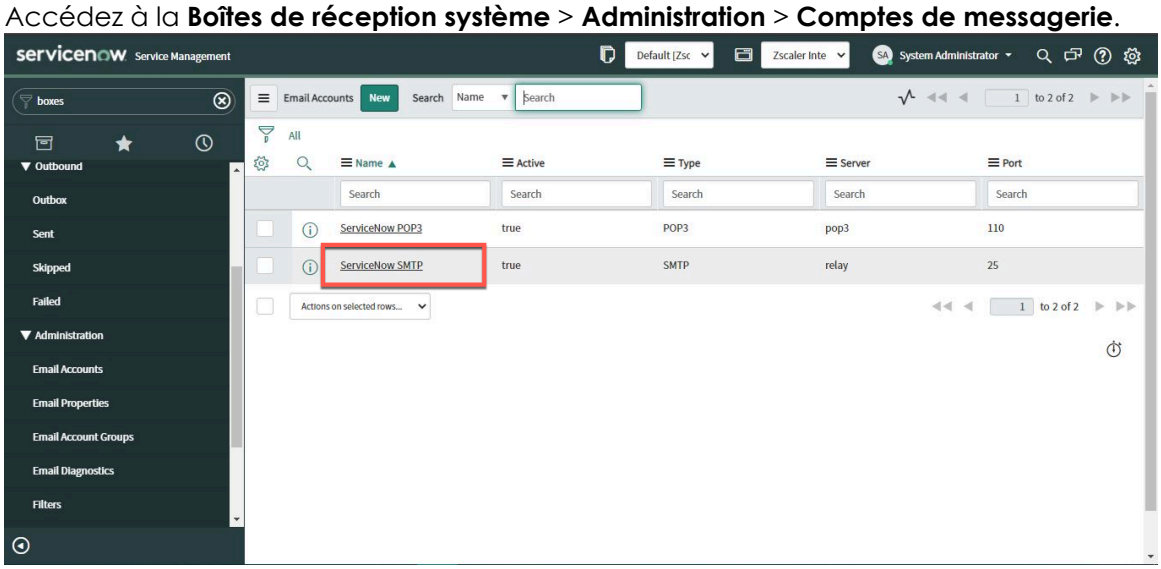
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Boîtes de réception système** > **Administration** > **Propriétés d'e-mail**.
2. Dans la section Configuration des e-mails entrants, sélectionnez l'option **Réception des e-mails activée** .



3. Cliquez sur **Enregistrer**.
4. Accédez à la **Boîtes de réception système** > **Administration** > **Comptes de messagerie**.

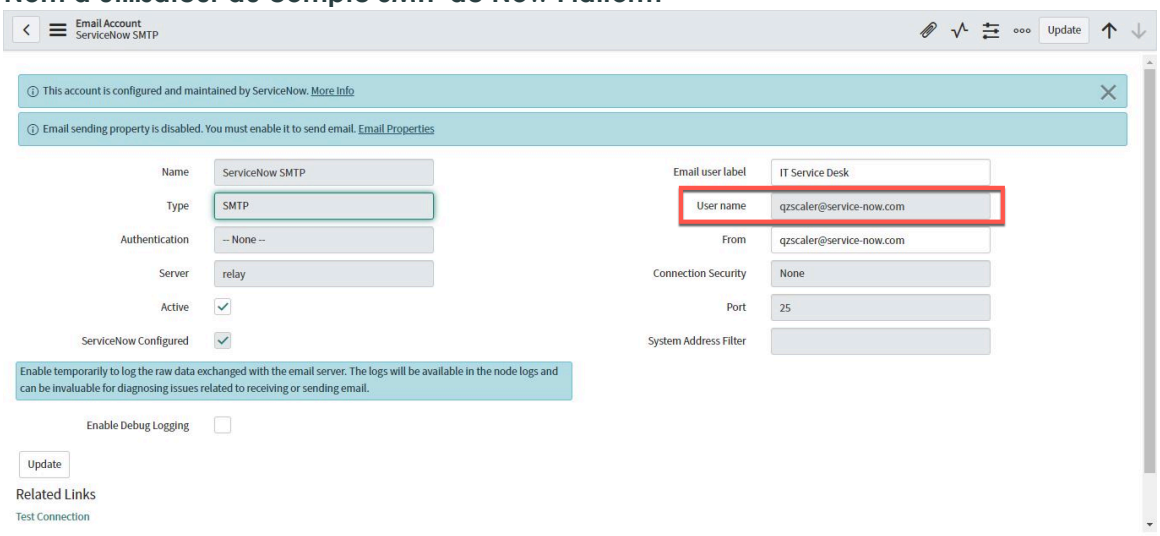


5. Sélectionnez le compte de messagerie **SMTP ServiceNow** .
   Notez le nom d'utilisateur. Le nom d'utilisateur identifié ici est l'adresse Now Platform e-mail que vous utilisez pour configurer les Zscaler alertes du patient 0.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom d'utilisateur du compte SMTP de Now Platform



6. Connectez-vous au portail d'administration Zscaler Internet Access .

> **Remarque :** Pour plus d'informations sur le portail d'administration Zscaler Internet Access , consultez la documentation Zscaler .

7. Accédez à la **Administration** > **Alertes** > **Publier des alertes**.
8. Cliquez sur **Ajouter un abonnement aux alertes**.
9. Renseignez les champs du formulaire.

Ajouter une alerte Formulaire d'abonnement

Champ	Description
E-mail	Now Platform Adresse e-mail du compte SMTP.
Description	Champ permettant d'ajouter plus de détails sur les alertes Patient 0.

10. Cliquez sur **Enregistrer**.

ServiceNow Opérations de sécurité Vue d'ensemble du module complémentaire pour Splunk

Le ServiceNow Opérations de sécurité module complémentaire permet Splunk à un Splunk administrateur logiciel de collecter des données et de créer des incidents et des événements dans le Now Platform.

Le module complémentaire est installé à partir de Splunkbase.

> **Important :** Splunk est également pris en charge pour l'environnement Managed Service Provider (MSP).

Configuration de l'intégration Splunk

Les procédures de configuration du ServiceNow Opérations de sécurité module complémentaire pour Splunk comprennent le téléchargement du fichier complémentaire

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

dans Splunk, l'installation du module complémentaire et la configuration de l'instance ServiceNow où les incidents et événements de sécurité sont créés.

Rôle requis

Avant d'exécuter les procédures de configuration de l'intégration Splunk, assurez-vous de définir un utilisateur d'intégration avec les rôles sn_si.integration_user et sn_si.analyst sur votre instance ServiceNow. En outre, pour effectuer des importations, vous devez disposer du rôle import_transformer pour obtenir une autorisation de lecture et d'écriture sur les tables de sécurité. Le rôle sn_si.integration_user doit être défini avec la partie import_transformer du rôle.

Télécharger l'application ServiceNow Security Operations

La première étape de configuration de l'intégration ServiceNow à Splunk consiste à télécharger l'application à partir de Splunkbase ServiceNow Opérations de sécurité .

Avant de commencer
Rôle requis : administrateur

Procédure

1. Ouvrez Splunkbase.
2. Recherchez l'intégration de ServiceNow Security Operations .
3. Téléchargez l'application.

Installer le module complémentaire ServiceNow Security Operations pour Splunk

Installez le **module complémentaire ServiceNow Security Operations pour Splunk** afin de lier Splunk à ServiceNow.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Ouvrez Splunk.
2. Cliquez sur l'icône **d'engrenage Applications** ou sur l'élément de menu contextuel **Gérer les applications** .
3. Cliquez sur **Installer l'application à partir d'un fichier**.
4. Cliquez sur **Choisir un fichier**, sélectionnez sn_sec_ops.spl, puis cliquez sur **Télécharger**.
5. Si vous y êtes invité, redémarrez Splunk.
   Le ServiceNow Opérations de sécurité module complémentaire pour Splunk est installé et prêt à être configuré.

Configurer ou modifier l'instance où les incidents ou les événements sont créés

Pour configurer ou modifier l'instance ServiceNow dans laquelle les nouveaux incidents de sécurité et événements de sécurité sont créés, utilisez l'action Configuration de la liste d'applications.

Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. **Ouvrez Splunk**.
2. Cliquez sur l'icône **d'engrenage Applications** ou sur l'élément de menu contextuel **Gérer les applications** .
3. Dans la liste des applications, recherchez les applications **ServiceNow** à l'aide du filtre.
4. Recherchez **l'intégration de ServiceNow Security Operations et** cliquez sur l'action **Configurer** correspondante.
5. Renseignez les champs du formulaire.

Champ	Description
Spécifier ServiceNow Server	
URL	URL de votre console ou Splunk Cloud de votre Splunk Enterprise Security instance. L'URL doit inclure le port API, par exemple : `https://mysplunkserver.com:8089`
Type d'authentification	Option permettant de sélectionner le type d'authentification. Vous pouvez sélectionner **Authentification de base** ou **Authentification OAuth 2.0**. ◦ Si vous utilisez le nom d'utilisateur du compte API et le mot de passe API pour la configuration, cochez la case **Authentification de base**. La valeur par défaut est désactivée. ◦ Si vous utilisez l'authentification OAuth 2.0 pour la configuration, cochez la case **Authentification OAuth 2.0** . La valeur par défaut est désactivée.
Authentification de base	
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour votre compte utilisateur API dans la Splunk Enterprise Security console.
Mot de passe	Mot de passe que vous avez créé pour votre compte utilisateur API dans la Splunk Enterprise Security console.
Confirmer le mot de passe	Saisissez le mot de passe pour le confirmer.
Authentification OAuth 2.0	
ID client	ID client de l'application créée sur le serveur ServiceNow.
Secret client	Secret client de l'application créée sur ServiceNow Server.
URL de redirection	L'URL vers laquelle vous souhaitez être redirigé. Vous pouvez copier et coller cette URL

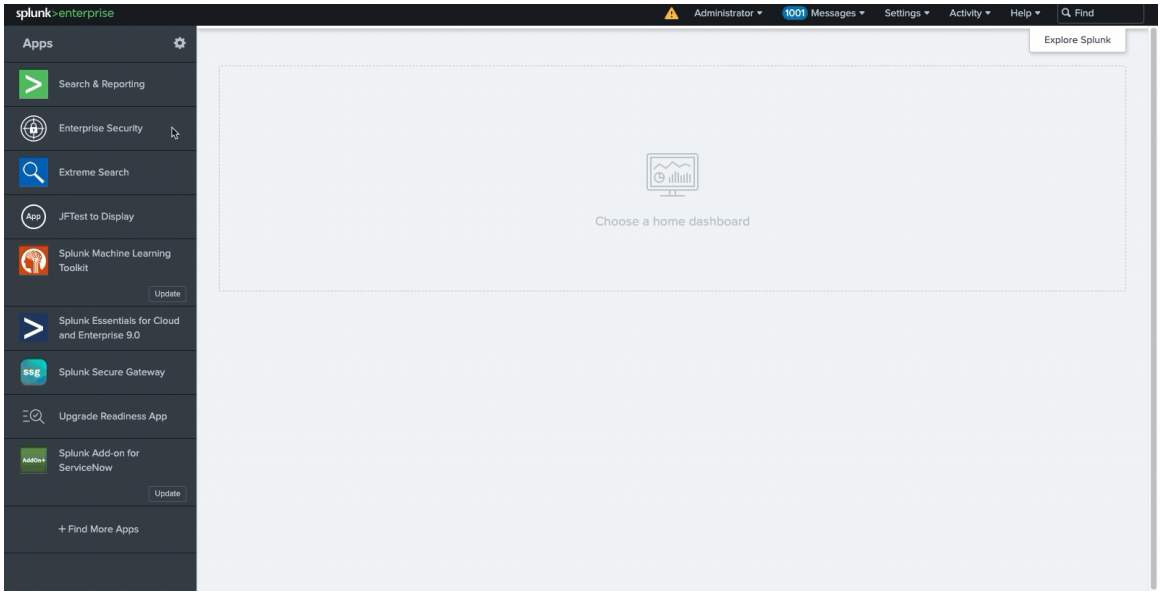
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	dans votre URL de redirection du registre ServiceNow.
Proxy facultatif	
Proxy URL	URL proxy de votre Splunk Enterprise Security console ou Splunk Cloud instance.
Port	Adresse du port.
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console.
Mot de passe	Mot de passe que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console.
Confirmer le mot de passe	Saisissez le mot de passe pour le confirmer.
Configuration du niveau de connexion	
Niveau de connexion	Niveau de journaux de reporting générés par l'intégration, c'est-à-dire le nom du type d'informations. Vous pouvez également mettre à jour la valeur pour les options suivantes : ◦ **info** ◦ **erreur** ◦ **avertir** ◦ **debug** Par défaut, la valeur est **info**.
Sélection d'API	
Sélection d'API	Sélectionnez l'une des API suivantes : ◦ API de table ◦ API de jeu d'importation

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Enregistrer**.
7. Vous pouvez également rechercher **l'intégration d'ingestion d'événements ServiceNow** et cliquer sur l'action **Configurer** correspondante.

   L'intégration de l'ingestion d'événements ServiceNow est configurée en trois onglets différents.

   - **Splunk primaire** : configuration Splunk principale ou par défaut.
   - **Splunk secondaire** : (facultatif) la configuration de sauvegarde ou de deuxième Splunk.
   - **Niveau de connexion** : niveau des journaux de rapports générés par l'intégration, c'est-à-dire le nom du type d'informations.
8. Sélectionnez l'onglet **Splunk Primaire** .
9. Renseignez les champs du formulaire.

Champ	Description
Étiquette de l'action de workflow	Nom de la Splunk Enterprise Security console primaire ou de l'instance Splunk Cloud primaire utilisée pour l'intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge. Par exemple, saisissez `SplunkES2`.
URL	URL de votre Splunk Enterprise Security console primaire ou de votre Splunk Cloud instance primaire. L'URL doit inclure le port API, par exemple : `https://mysplunkserver.com:8089`
Point de terminaison	Point de terminaison de votre Splunk Enterprise Security console primaire ou de votre Splunk Cloud instance primaire.

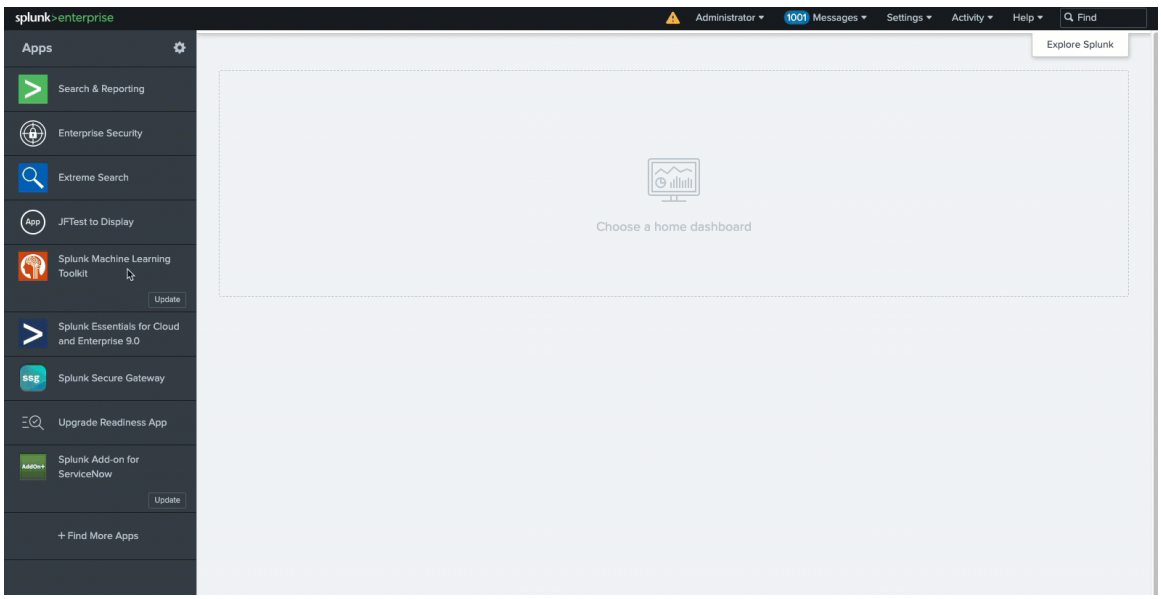
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type d'authentification	Option permettant de sélectionner le type d'authentification. Vous pouvez sélectionner **Authentification de base** ou **Authentification OAuth 2.0**. ◦ Si vous utilisez le nom d'utilisateur du compte API et le mot de passe API pour la configuration, cochez la case **Authentification de base**. La valeur par défaut est désactivée. ◦ Si vous utilisez l'authentification OAuth 2.0 pour la configuration, cochez la case **Authentification OAuth 2.0** . La valeur par défaut est désactivée.
Authentification de base	
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour votre compte utilisateur API dans la Splunk Enterprise Security console.
Mot de passe	Mot de passe que vous avez créé pour votre compte utilisateur API dans la Splunk Enterprise Security console.
Confirmer le mot de passe	Saisissez le mot de passe pour le confirmer.
Authentification OAuth 2.0	
ID client	ID client de l'application créée sur le serveur ServiceNow. Pour en savoir plus sur l'obtention de l'ID client, reportez-vous à la section Configurer le registre d'application sur l'instance ServiceNow
Secret client	Secret client de l'application créée sur le serveur. Pour plus d'informations sur la façon d'obtenir le secret client, consultez Configurer le registre d'application sur l'instance ServiceNow
URL de redirection	L'URL vers laquelle vous souhaitez être redirigé. Vous pouvez copier et coller cette URL dans votre URL de redirection du registre ServiceNow. Pour plus d'informations, voir Configurer le registre d'application sur l'instance ServiceNow
Configuration de proxy facultative	
Proxy URL	URL proxy de votre console secondaire ou Splunk Cloud de votre Splunk Enterprise Security instance secondaire.
Port	Adresse du port.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console secondaire.
Mot de passe	Mot de passe que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console secondaire.
Confirmer le mot de passe	Saisissez le mot de passe pour le confirmer.



10. Facultatif : Sélectionnez l'onglet **Splunk Second** .
11. Facultatif : Renseignez les champs du formulaire.

Champ	Description
Étiquette de l'action de workflow	(Optional) Nom de la Splunk Enterprise Security console secondaire ou de l'instance Splunk Cloud secondaire utilisée pour l'intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge. Par exemple, saisissez `SplunkES2`.
URL	URL de votre Splunk Enterprise Security console secondaire ou de l'instance Splunk Cloud secondaire. L'URL doit inclure le port API, par exemple : `https://mysplunkserver.com:8089`
Point de terminaison	Point de terminaison de votre console secondaire ou de l'instance Splunk Enterprise SecuritySplunk Cloud secondaire.
Type d'authentification	Option permettant de sélectionner le type d'authentification. Vous pouvez sélection-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	ner **Authentification de base** ou **Authentification OAuth 2.0**. ◦ Si vous utilisez le nom d'utilisateur du compte API et le mot de passe API pour la configuration, cochez la case **Authentification de base**. La valeur par défaut est désactivée. ◦ Si vous utilisez l'authentification OAuth 2.0 pour la configuration, cochez la case **Authentification OAuth 2.0** . La valeur par défaut est désactivée.
Authentification de base	
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour votre compte utilisateur API dans la Splunk Enterprise Security console.
Mot de passe	Mot de passe que vous avez créé pour votre compte utilisateur API dans la Splunk Enterprise Security console.
Confirmer le mot de passe	Saisissez le mot de passe pour le confirmer.
Authentification OAuth 2.0	
ID client	ID client de l'application créée sur le serveur ServiceNow.
Secret client	Secret client de l'application créée sur ServiceNow Server.
URL de redirection	L'URL vers laquelle vous souhaitez être redirigé. Vous pouvez copier et coller cette URL dans votre URL de redirection du registre ServiceNow.
Configuration de proxy facultative	
Proxy URL	URL proxy de votre console secondaire ou Splunk Cloud de votre Splunk Enterprise Security instance secondaire.
Port	Adresse du port.
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console secondaire.
Mot de passe	Mot de passe que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console secondaire.
Confirmer le mot de passe	Saisissez le mot de passe pour le confirmer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

12. Sélectionnez l'onglet **Niveau de connexion** .
13. Renseignez les champs du formulaire.

Champ	Description
Niveau de journal	Niveau de journaux de reporting générés par l'intégration, c'est-à-dire le nom du type d'informations. Vous pouvez également mettre à jour la valeur pour les options suivantes : ◦ **info** ◦ **erreur** ◦ **avertir** ◦ **debug** Par défaut, la valeur est **info**.

14. Cliquez sur **Enregistrer**.
    Une fois la validation terminée, la page Intégrations de sécurité s'affiche avec chacune de vos configurations. Sur chaque vignette de configuration valide, les boutons **Mettre à jour** et **Supprimer** sont affichés, comme illustré dans la figure suivante.

    Remarque : Vous devez utiliser soit l'authentification de base, soit l'authentification OAuth 2.0 uniquement. Activez l'une des authentifications et saisissez les détails d'authentification correspondants. L'activation des deux affichera une erreur.

    Une fois validée et soumise, chaque configuration du serveur d'ingestions d'événements Splunk est enregistrée sous forme de vignette dans la page Intégrations de sécurité. Si vos vignettes de configuration enregistrées ne s'affichent pas sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste Afficher les configurations, cliquez sur **Oui**.

Configurer le registre d'application sur l'instance ServiceNow

Enregistrez l'application auprès de l'instance pour utiliser l'autorisation OAuth.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Registre d'application**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Créer un point de terminaison d'API OAuth pour les clients externes**.
4. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès OAuth.
ID client	(Lecture seule) ID unique de l'application généré automatiquement. L'instance uti-

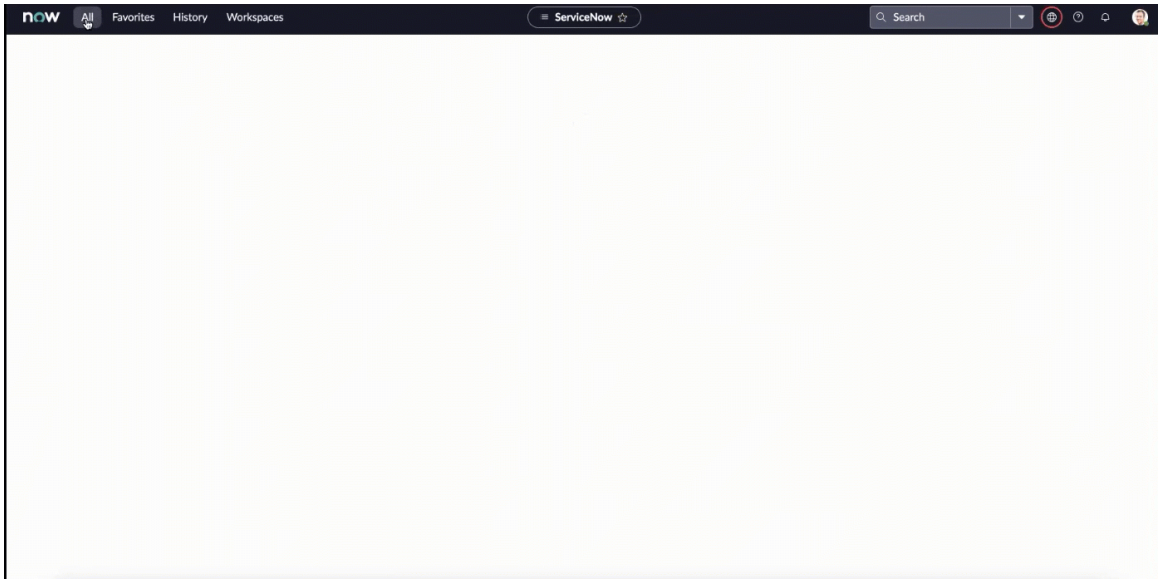
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	lise l'ID client lors de la demande d'un jeton d'accès.
Secret client	Chaîne secrète partagée que l'instance et l'application cliente ou le site web utilisent pour autoriser les communications entre eux. L'instance utilise le secret client lors de la demande d'un jeton d'accès. Laissez ce champ vide pour que l'instance génère automatiquement un secret client. Pour afficher les secrets client existants, cliquez sur l'icône de verrouillage.
URL de redirection	URL de rappel vers laquelle le serveur d'autorisation redirige. Saisissez autant d'URL que nécessaire pour tous les consommateurs de jetons possibles. L'instance associe l'URL de la demande entrante à l'une des URL de redirection. Si aucune correspondance n'est établie, l'instance utilise la première URL de redirection.
URL du logo	URL qui contient une image à utiliser comme logo de l'application. Le logo apparaît sur la page d'approbation lorsque l'utilisateur reçoit une demande d'octroi à une application cliente l'accès à une ressource restreinte sur l'instance.
Application	Le nom de l'application.
Accessible depuis	Définissez le périmètre de l'application. Sélectionnez l'une des options suivantes : ◦ **Tous les champs d'application de l'application** ◦ **Ce périmètre de l'application uniquement**
Actif	Cochez la case pour activer le registre d'application.
Durée de vie du jeton d'actualisation	Nombre de secondes pendant lesquelles un jeton d'actualisation est valide. L'instance utilise la valeur de durée de vie lorsqu'elle demande un jeton d'actualisation. Par défaut, les jetons d'actualisation expirent au bout de 100 jours (8640 000 secondes).
Durée de vie du jeton d'accès	Nombre de secondes pendant lesquelles un jeton d'accès est valide. L'instance utilise la valeur de durée de vie lors de la demande d'un jeton d'accès. Par défaut, les jetons d'accès expirent au bout de 30 minutes (1 800 secondes).
Commentaires	Informations supplémentaires à associer à l'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
6. Cliquez sur **Envoyer**.

Commandes de recherche manuelle

Les commandes de recherche manuelle sont saisies à partir de n'importe quelle fenêtre de recherche. Vous pouvez créer un incident ou un événement de sécurité. Après la commande, des paires de noms de champs et de valeurs sont utilisées pour créer l'enregistrement souhaité.

Événement de sécurité

La commande d'événement de sécurité, **snsecevent**, crée un événement dans ServiceNow avec la classification de sécurité.

Ces événements peuvent être examinés indépendamment, ou des règles d'alerte intégrées ServiceNow ou des actions manuelles peuvent transformer un événement ou une collection d'événements en incident de sécurité.

Si l'événement devient un incident de sécurité et que chaque paramètre est envoyé dans l'événement, ces données sont utilisées pour renseigner l'incident de sécurité comme suit :

Événement de sécurité

Nom de paramètre	Obligatoire	Utiliser	Utiliser dans un incident de sécurité
nœud	Oui	Le nœud représente le serveur ou l'élément de configuration pour l'événement. Idéalement, ce nœud est mappé à un CI existant dans ServiceNow.	Utiliser dans un incident de sécurité
type	Oui	La catégorie de l'événement.	Description brève

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Événement de sécurité (suite)

Nom de paramètre	Obligatoire	Utiliser	Utiliser dans un incident de sécurité
resource	Oui	L'élément de configuration.	Description brève
source	Non	L'origine de ces données. Par défaut, c'est le serveur Splunk qui génère les données.	Journal d'activité
external_url	Non	URL d'exploration vers le bas à utiliser pour ServiceNow revenir aux données Splunk concernant cet événement. Par défaut, cette URL contient le lien de résultat de toute alerte ou un lien vers la page de recherche Splunk par défaut.	URL externe accessible via le bouton **Exploration vers le bas** du formulaire d'incident de sécurité
time_of_event	Non	Heure à laquelle l'événement a été enregistré dans Splunk.	N/A
Toutes les autres valeurs (catégorie, sous-catégorie dans l'exemple)	Non	Tout champ qui ne fait pas partie du champ d'information dans l'événement. Si un incident de sécurité est créé, il est utilisé.	Si le champ existe et qu'il n'est pas renseigné, c'est que l'incident de sécurité utilise cette valeur. Par exemple, la catégorie transmise par l'événement devient la catégorie du nouvel incident de sécurité. Si aucun champ portant ce nom n'existe, la valeur est placée dans le journal d'activité.

Incident de sécurité

La commande d'incident de sécurité, **snsecincident**, crée un incident de sécurité dans votre ServiceNow instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incident de sécurité

Paramètre	Obligatoire	Utiliser
short_description	Oui	Description brève d'une ligne de l'incident.
catégorie	Non	Catégorie de l'incident de sécurité. Si cette catégorie n'existe pas, elle est créée.
sous-catégorie	Non	La sous-catégorie. Si cette sous-catégorie n'existe pas, elle est créée.
cmdb_ci	Non	Élément de configuration pour l'incident de sécurité. Idéalement, cet élément est mappé à un CI existant dans ServiceNow.
description	Non	La description la plus longue et la plus détaillée de l'incident.

Il existe de nombreuses colonnes utiles possibles : tout ce qui se trouve dans la carte de transformation des incidents de sécurité peut être utilisé. Si de nouvelles colonnes sont ajoutées à l'incident de sécurité, elles sont également utilisées, à condition qu'elles se trouvent dans la carte de transformation. Quelques colonnes utiles : emplacement, priorité, assignment_group, assigned_to, affected_user, attack_vector et watch_list.

Actions d'événement Splunk

Lors de l'examen des journaux Splunk, vous pouvez rapidement créer des événements de sécurité et des incidents de sécurité à partir de n'importe quel élément du journal à l'aide des actions d'événement.

Cliquez sur l'une de ces actions pour créer une commande de recherche manuelle remplie avec les données de l'entrée de journal et exécutez-la pour générer le nouvel enregistrement.

Ces actions sont facilement configurées pour ajouter des champs dans vos données normalisées. Dans Splunk, à l'aide de **Paramètres** > **Champs** > **Actions du workflow**, vous pouvez sélectionner et modifier l'une ou l'autre de ces actions à l'aide des champs de recherche manuelle.

Vous pouvez choisir l'emplacement où l'action est affichée, pour quels champs, et modifier la chaîne de recherche qui contient une commande de recherche pour créer votre enregistrement.

Alertes Splunk à enregistrement unique

Dans n'importe quelle alerte, vous pouvez spécifier des événements de sécurité ou des incidents de sécurité à créer lorsque l'alerte est déclenchée.

Ouvrez ou créez votre alerte. Lors de la modification des actions, sélectionnez le type d'enregistrement souhaité et renseignez la boîte de dialogue d'alerte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Alertes Splunk à champs personnalisés à plusieurs enregistrements

Les alertes multi-enregistrements (définies à l'aide des actions de déclenchement **Créer plusieurs incidents de sécurité ServiceNow** et **Créer plusieurs événements de sécurité ServiceNow**) peuvent créer automatiquement des enregistrements avec n'importe quel ensemble de champs pris en charge.

Celles-ci agissent différemment des autres actions d'alerte dans la mesure où des valeurs par défaut sont fournies. Toutefois, la plupart des données proviennent des résultats de recherche de cette alerte.

Remarque : Dans les versions précédentes du module complémentaire et dans cette documentation, les alertes scriptées étaient prises en charge. Cette fonctionnalité a été dépréciée et remplacée par ces instructions.

Créer une alerte Splunk à champs personnalisés à plusieurs enregistrements

Pour créer une alerte Splunk à plusieurs enregistrements avec des champs personnalisés, vous devez générer une recherche conçue pour correspondre aux colonnes ServiceNow que vous souhaitez renseigner.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à **Rechercher**.
2. Dans la zone **Rechercher** , créez une recherche qui génère les données de votre enregistrement.
   Consultez les exemples de critères de recherche recommandés.
3. Cliquez sur **Enregistrer sous** et sélectionnez **Alerte**.
4. Définissez le nom, les autorisations et le calendrier selon vos besoins.
5. Cliquez sur **Ajouter des actions**.
6. Effectuez l'une des sélections suivantes.
   - Pour créer un événement par résultat à partir de votre recherche, sélectionnez **Créer plusieurs événements de sécurité ServiceNow**.
   - Pour créer un incident par résultat à partir de votre recherche, sélectionnez **Créer plusieurs incidents de sécurité ServiceNow**.
7. Définissez les valeurs par défaut selon vos besoins.
   Si le champ dans les résultats de la recherche est vide ou absent, les valeurs par défaut sont utilisées. S'il y a une valeur dans le résultat, les valeurs par défaut sont remplacées.

Champs personnalisés à plusieurs enregistrements Exemples d'alertes Splunk

Lorsque vous créez plusieurs alertes Splunk d'enregistrement avec des champs personnalisés, vous devez définir des critères de recherche pour générer des données d'alerte. Des exemples de critères de recherche pour les incidents de sécurité et les événements de sécurité sont présentés.

Recherche d'incident de sécurité

Pour un incident de sécurité, ce critère génère une recherche pour remplir les colonnes de la table Incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Recherche d'événement de sécurité

Pour un événement de sécurité, il s'agit de la même recherche, mais elle remplit les champs d'événement à la place. Si cet événement est transformé en incident de sécurité et que tous les champs qui n'existent pas dans l'événement sont renseignés, ils sont transférés vers l'incident de sécurité. Dans le cas contraire, ils restent dans le champ d'informations supplémentaires de l'événement et de l'alerte.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Remarque : Les critères de recherche que vous utilisez ajouteront autant d'enregistrements que la recherche en trouvera. Il peut ajouter 5 ou 10 000 000 000 d'enregistrements. Il ne s'agit donc PAS d'une méthode recommandée pour le transfert en masse de données. L'intention de cette méthode est d'ajouter un enregistrement par appel REST dans l'instance ServiceNow.

Rapports d'erreur Splunk

Chaque fois qu'un problème de connectivité se produit avec votre instance ServiceNow, une erreur est consignée dans Splunk avec des informations décrivant le problème.

Les messages d'erreur sont stockés dans un nouvel index nommé **servicenow** avec sourcetype **servicenow**.

Pour rechercher des journaux d'erreurs, assurez-vous de spécifier l'index **ServiceNow** dans votre recherche. Vous pouvez également consulter la documentation Splunk actuelle pour savoir comment ajouter le nouvel index **ServiceNow** aux index de recherche par défaut.

Splunk Enterprise Event Ingestion intégration pour Opérations de sécurité par ServiceNow

L'intégration Splunk Enterprise des données d'événements Réponse aux incidents de sécurité et d'alertes au produit (SIR) permet aux analystes d'incidents de sécurité de collecter et de traiter les journaux de sécurité et les données d'événements connexes.

Vue d'ensemble

Les données sont collectées en temps réel et sont utilisées par les analystes pour identifier et signaler les cybermenaces potentielles. Les événements de sécurité collectés peuvent être transformés en alertes déclenchées qui sont ingérées automatiquement avec cette intégration. En outre, les événements de sécurité individuels peuvent être transférés manuellement à la demande depuis l'interface Splunk Enterprise de recherche et de génération de rapports vers le Réponse aux incidents de sécurité produit de pour Now Platform créer des incidents de sécurité. Vous pouvez récupérer des événements notables à partir d'une recherche avec la configuration de la grappe de têtes de Splunk Enterprise

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

recherche. Pour ce faire, vous pouvez utiliser l'URL et le port API de n'importe quel moteur de recherche appartenant au cluster.

Cette intégration fournit à un analyste du centre des opérations de sécurité (SOC) une visibilité sur les événements et les données d'alerte connexes. Ces données peuvent être intégrées dans Now Platform Réponse aux incidents de sécurité (SIR) des incidents de sécurité pour une enquête et une correction plus approfondies. Les profils des Splunk alertes ingérées en cours et des événements transférés sont créés dans votre Now Platform instance. Ces profils personnalisent l'affichage des différents Splunk champs d'alerte et d'événement sur SIR les incidents de sécurité. Un mappage par défaut des champs d'alerte est fourni, qui peut être modifié et complété pour répondre aux besoins spécifiques du client.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

- Créez plusieurs profils d'ingestion d'alertes pour créer des incidents de sécurité SIR pour des types de menaces spécifiques tels que l'hameçonnage et les programmes malveillants.
- Créez plusieurs profils d'événements pour le transfert d'événements à la demande à partir de votre Splunk console afin de créer des incidents de sécurité SIR.
- Glisser-déposer le mappage des valeurs de champ d'alerte et d'événement Splunk vers les champs d'incident de sécurité SIR associés.
- Un aperçu de la mise en page de l'incident SIR de sécurité basée sur des échantillons d'alertes ou d'événements pour valider la configuration du profil.
- Ingérer les alertes historiques, ainsi que les alertes futures en cours à intervalles configurables.
- Regroupez les événements ou les alertes concernant les incidents de sécurité existants SIR en fonction des valeurs de champ correspondantes pour éviter les incidents de sécurité en double.

Versions prises en charge Now Platform

Le module d'extension com.snc.si_dep est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications.

Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour garantir une installation fluide :

1. Cadre de travail de Security Integration
2. Security Support Common
3. Orchestration de support de sécurité
4. Réponse aux incidents de sécurité

Pour plus d'informations sur l'installation des Opérations de sécurité applications principales, consultez et .

ServiceNow Modules complémentaires

Le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise n'est requis que si vous préférez transférer manuellement des événements de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

votre Splunk Enterprise console vers votre Now Platform instance. Cet ServiceNow addon est disponible dans splunkbase .

Ce ServiceNow module complémentaire d'ingestion d'événement de sécurité pour Splunk Enterprise l'application dans Splunkbase n'est pas requis pour l'ingestion d'alerte automatisée prise en charge par l'intégration.

Versions prises en charge par Splunk

Cette intégration prend en charge la version 6.0 ou ultérieure de Splunk Enterprise. L'intégration prend également en charge le Splunk service Enterprise Cloud.

Serveur MID

Cette intégration nécessite l'installation et la configuration d'un serveur MID Server dans votre Now Platform® instance pour se Splunk connecter au service si le Splunk serveur est déployé au sein de votre réseau d'entreprise. Si vous utilisez le Splunk Cloud service, un serveur MID n'est pas nécessaire. Pour plus d'informations sur les MID Servers, reportez-vous à la section Serveur MID .

Architecture d'intégration et connexion des systèmes

Pour plus d'informations sur l'architecture de l'intégration, y compris les termes clés et les détails de connexion des systèmes externes, reportez-vous à Architecture d'intégration et connexion de systèmes externes pour l'intégration Splunk Enterprise Event Ingestion.

Liste de vérification

Pour obtenir une liste de contrôle imprimable de ces sujets, reportez-vous à la section Liste de vérification pour l'intégration de l'ingestion d'événements Splunk Enterprise Security notables. Vous pouvez utiliser cette liste pour surveiller votre progression au fur et à mesure que vous accomplissez les tâches de l'intégration.

Les images utilisées dans les rubriques suivantes ont été générées pour la version Kingston du Now Platformfichier . Pour plus d'informations sur l'interface utilisateur de San Diego, consultez Gérer les menaces de sécurité à l'aide de Security Analyst Workspace.

Les sujets suivants sont numérotés. Suivez les rubriques énumérées ci-dessous dans l'ordre dans lequel elles sont présentées pour une installation et une configuration fluides de l'application.

Configurer votre Now Platform® instance pour l'intégration Splunk Enterprise Event Ingestion

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform® instance avant d'installer l'application à partir du ServiceNow Store.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application pour garantir une installation et une configuration fluides.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Vérifiez que vous avez affecté les rôles requis Now Platform® et Réponse aux incidents de sécurité (SIR).

   Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre Now Platform® instance.

   - Un utilisateur disposant du rôle administrateur Now Platform® (admin) installe l'application à partir de et ServiceNow Store affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin).
   - Si vous souhaitez transférer manuellement des événements à partir de Splunk Enterprise pour cette intégration, un utilisateur ayant le rôle administrateur affecte un utilisateur ayant le Now Platform® rôle (sn_sec_splunk_v2.api_account_access) dans le Now Platform®. Ce rôle permet à un utilisateur ayant le rôle d'administrateur Splunk Enterprise d'accéder à l'API dans le qui est requis pour le Now Platform® transfert manuel d'événements pour cette intégration.

     Le rôle (sn_sec_splunk_v2.api_account_access) n'est pas requis pour l'intégration si vous ingérez automatiquement des alertes à partir de Splunk Enterprise votre Now Platform® instance.

   - Un utilisateur disposant du rôle sn_si.admin supervise les tâches suivantes dans :Now Platform®
     - Nomme, crée et modifie les profils d'alerte et d'événement.
     - Sélectionne et mappe les valeurs des alertes, des événements et des incidents de Now Platform® sécurité.
     - Prévisualise l'exactitude des détails de l'incident de sécurité avant de finaliser la configuration.
     - Planifie l'ingestion d'alerte en cours.
     - Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst).
     - Les utilisateurs avec l'sn_si.analyst travaillent avec des incidents de sécurité.

   Pour en savoir plus sur les rôles et l'affectation de rôles aux utilisateurs, reportez-vous à la section Gestion des rôles .

2. Vérifiez que vous utilisez la version 6.0 ou ultérieure de l'API Splunk .

   Si vous avez accès à la Splunk Enterprise console, vous avez accès à l'API requise pour cette intégration. Aucune autre configuration spéciale n'est requise pour l'API.

3. Vérifiez que vous avez installé et configuré un serveur MID.

   Un serveur MID dans votre Now Platform® instance est requis pour se connecter au Splunk service si le Splunk serveur est déployé au sein de votre réseau d'entreprise. Pour plus d'informations sur les MID Servers, reportez-vous à la section Serveur MID

   Si vous utilisez le Splunk Cloud service, un serveur MID n'est pas nécessaire.

4. Vérifiez que les ServiceNow applications de base requises pour prendre en charge l'intégration sont installées et activées.

   Le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration.

Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide.

a. Réponse aux incidents de sécurité

b. Cadre de travail de Security Integration

c. Security Support Common

d. Orchestration de support de sécurité

Pour plus d'informations sur l'installation des Opérations de sécurité applications principales, consultez et .

Que faire ensuite

Vous avez correctement configuré votre Now Platform® instance pour l'intégration. L'étape suivante consiste à installer l'application Splunk Enterprise Event Ingestion à partir de ServiceNow Store pour l'intégration. Pour plus d'informations, consultez Installer et configurer l'application ServiceNow pour l'intégration Splunk Enterprise Event Ingestion.

Si vous n'avez pas enregistré les recherches dans votre Splunk Enterprise console pour l'ingestion, ou si vous effectuez simultanément la configuration initiale pour cette intégration dans votre Splunk Enterprise console et dans le produit de votre Now Platform® instance, reportez-vous à la Opérations de sécurité section Enregistrer les recherches de l'intégration dans votre Splunk EnterpriseSplunk Enterprise Event Ingestion console pour plus d'informations.

Si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise console pour l'intégration, reportez-vous à la section Configurez votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise pour plus d'informations.

Installer et configurer l'application ServiceNow pour l'intégration Splunk Enterprise Event Ingestion

Avant d'exécuter l'intégration sur votre Now Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre Réponse aux incidents de sécurité correctement aux produits et Opérations de sécurité sur votre Now Platform® instance.

Avant de commencer

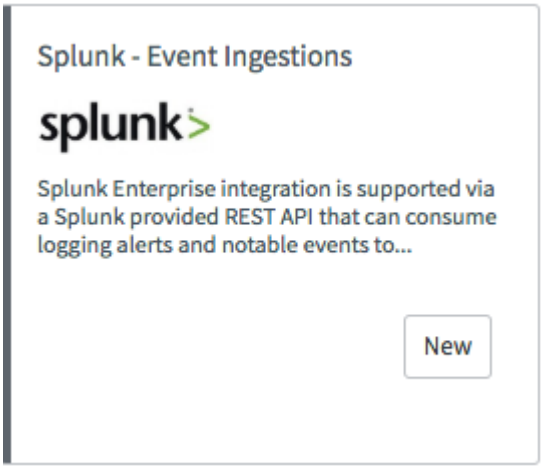
Rôle requis : administrateur

Procédure

1. Si vous n'avez pas installé l'application Splunk Enterprise Event Ingestion à partir de ServiceNow Store pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette Ingestions d'événements Splunk .
3. Pour configurer l'application, cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Si un bouton **Configurer** s'affiche sur une mosaïque, cliquez dessus pour modifier une configuration existante.
5. Dans la boîte de dialogue Configuration des ingestions d'événements qui s'affiche, renseignez les champs.

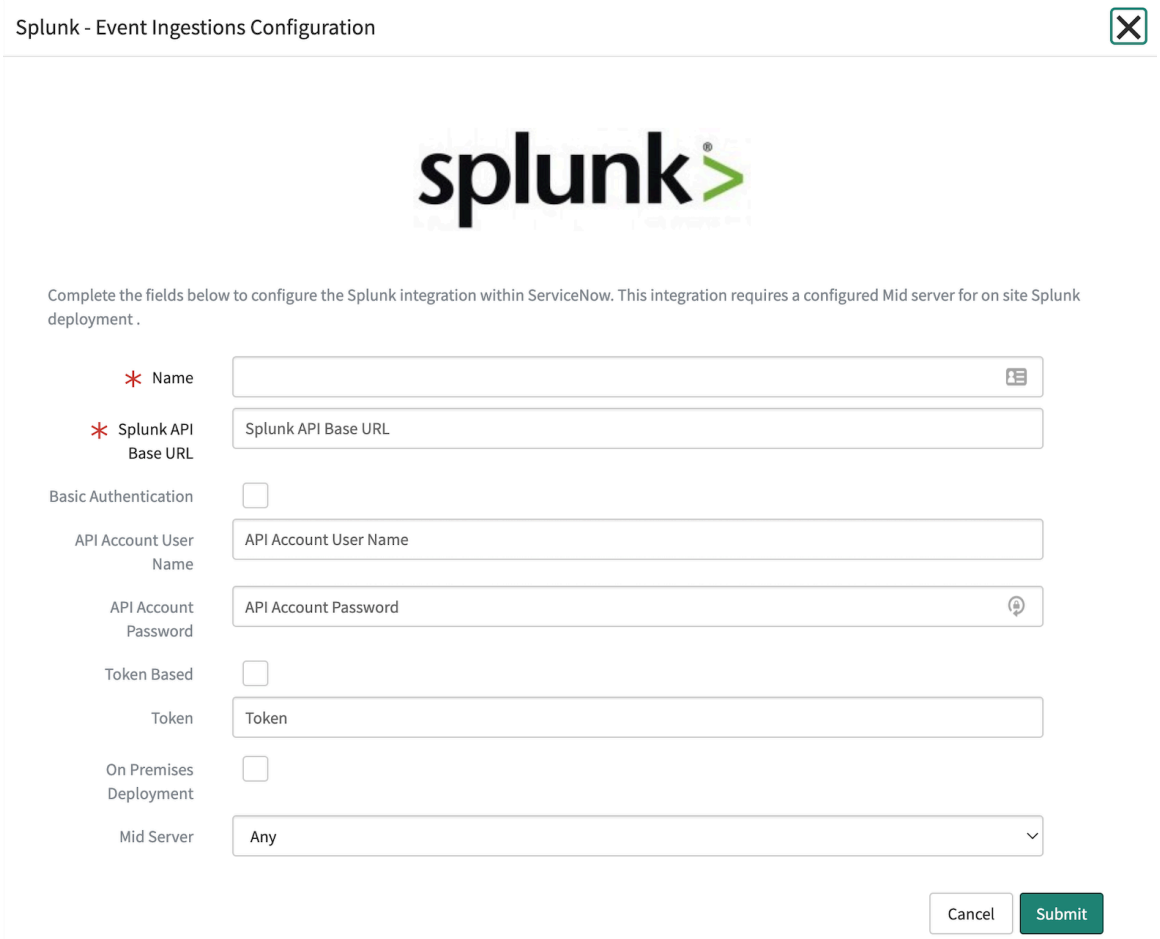
Champ	Description
Nom	Nom de la console ou Splunk Cloud de l'instance Splunk Enterprise utilisée pour l'intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge. Par exemple, entrez `HQ-USA` ou `HQ USA`.
URL de Base de l'API Splunk	URL de votre console ou Splunk Cloud de votre Splunk Enterprise instance.
Authentification de base	La valeur par défaut est désactivée. Si vous utilisez le nom d'utilisateur du compte API et le mot de passe API pour la configuration, cochez la case.
Nom d'utilisateur du compte API	Nom d'utilisateur que vous avez créé pour votre compte d'utilisateur individuel dans la Splunk Enterprise console.
Mot de passe API	Mot de passe que vous avez créé pour votre compte d'utilisateur individuel dans la Splunk Enterprise console.
Basé sur un jeton (disponible à partir de la version 12.0.0)	Authentification basée sur le jeton que vous avez créée pour votre compte d'utilisateur API sur la Splunk Enterprise console.
Jeton	Jeton que vous avez créé pour votre compte d'utilisateur d'API dans la Splunk Enterprise console.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Serveur MID	Serveur MID spécifique configuré dans votre environnement. Seuls les MID Servers actifs et validés sont disponibles dans cette liste de choix.
Déploiement sur site	La valeur par défaut est désactivée. Si vous utilisez la version cloud de Splunk Enterprise, vérifiez que la case n'est pas cochée. Si cette option est activée, la liste de choix du Serveur MID s'affiche. Si vous utilisez une version locale de Splunk Enterprise, procédez comme suit pour sélectionner un serveur MID. **a.** Cochez la case. Une liste de choix s'affiche. La valeur par défaut est **N'importe lequel**. **b.** Sélectionnez **N'importe lequel** uniquement si ce MID Server est configuré pour l'intégration Splunk Enterprise Event Ingestion . **c.** Dans la liste de choix, sélectionnez le Now Platform® MID Server que vous avez configuré dans votre instance pour cette intégration spécifique.

La figure suivante est un exemple de formulaire rempli pour la configuration d'une version locale avec Splunk Enterprise un MID Server.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Chaque Splunk Enterprise alerte que vous ingérez à partir de votre Splunk Enterprise console nécessite un profil d'événement unique dans votre Now Platform® instance. Toutefois, la source que vous configurez sur le formulaire de configuration des ingestions d'événements peut être réutilisée pour plusieurs Now Platform® profils, à condition que chaque profil ingère des alertes déclenchées uniques Splunk .

6. Cliquez sur **Envoyer**.
   Une fois la validation terminée, la page Intégrations de sécurité s'affiche avec chacune de vos configurations. Sur chaque vignette de configuration valide, les boutons **Configurer** et **Supprimer** s'affichent comme illustré dans la figure suivante.

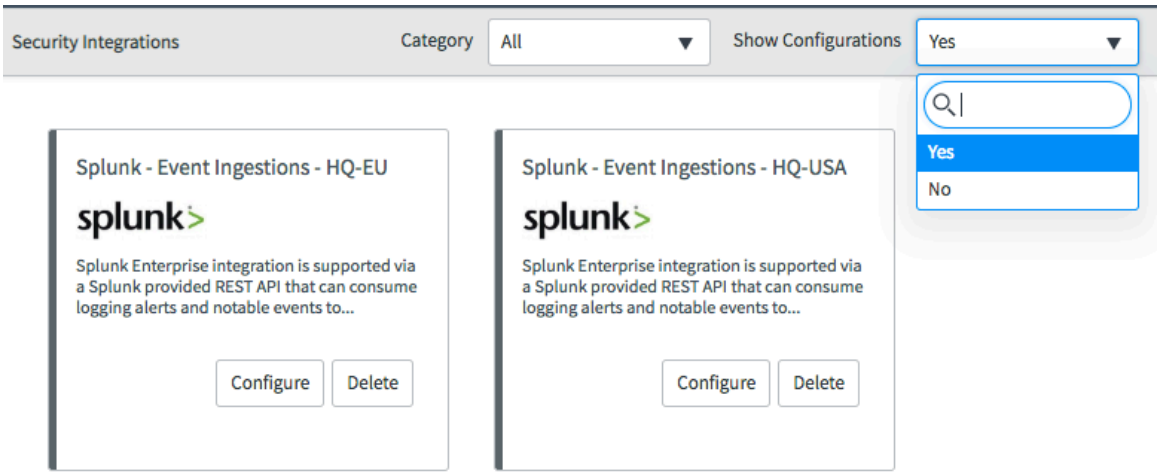
   Remarque : Vous devez utiliser uniquement l'authentification de base ou l'authentification basée sur les jetons. Activez l'une des authentifications et saisissez les détails d'authentification correspondants. L'activation des deux affichera une erreur.

   Une fois validée et soumise, chaque configuration du serveur d'ingestions d'événements Splunk est enregistrée sous forme de vignette dans la page Intégrations de sécurité. Si vos vignettes de configuration enregistrées ne s'affichent pas sur la page Intégrations

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de sécurité, dans le coin supérieur droit de la page, dans la liste de choix Afficher les configurations, cliquez sur **Oui**.



Trouble?

Si un message d'erreur s'affiche après avoir cliqué sur **Soumettre**, entrez à nouveau vos renseignements et cliquez sur **Soumettre**.

Que faire ensuite

Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer un profil d'événement.

Configurer les paramètres d'ingestion d'événements Splunk Enterprise

Utilisez les paramètres d'ingestion d'événements Splunk Enterprise pour modifier les configurations prédéfinies et leurs valeurs en fonction de vos besoins.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Splunk Integration** > **Paramètres d'intégration Splunk**.
2. Renseignez les champs du formulaire.

Paramètres d'intégration Splunk

Champ	Description
Nombre maximal d'alertes à afficher dans la création de profil	Option permettant de définir le nombre maximal d'alertes que vous souhaitez afficher lors de la création d'un profil d'événement. Par défaut, cette valeur est définie sur 500.
Nombre maximal d'incidents de sécurité à créer en une journée	Option permettant de définir le nombre maximal d'incidents de sécurité qui peuvent être créés en une journée.

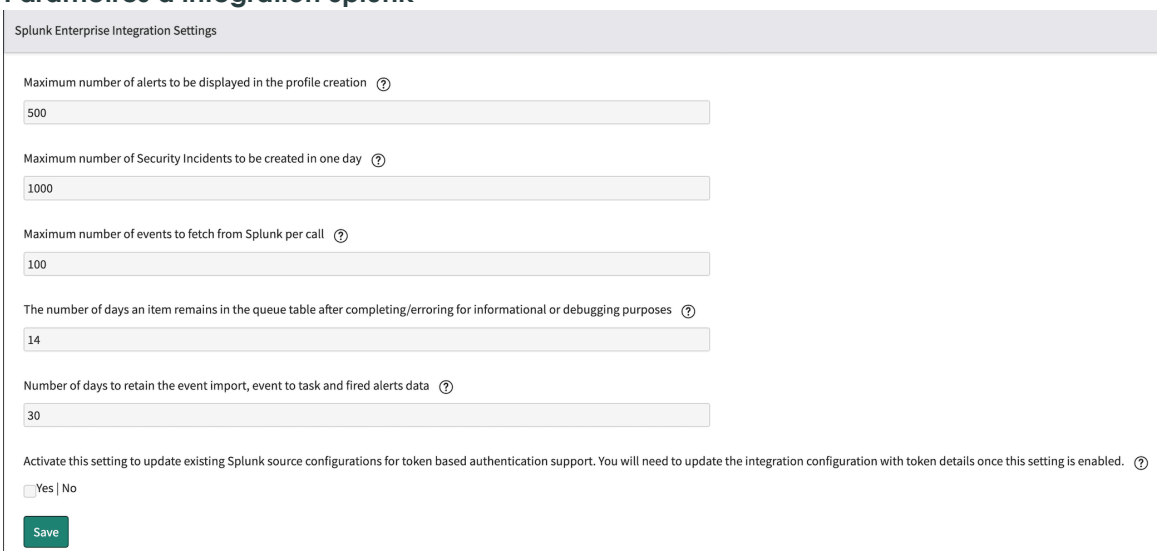
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par défaut, cette valeur est définie sur 1 000.
Nombre maximal d'événements à extraire de Splunk par appel	Option permettant de définir le nombre maximal d'événements à extraire de Splunk pour chaque appel. Par défaut, cette valeur est définie sur 100.
Nombre de jours durant lesquels un élément reste dans la table de file d'attente après l'achèvement ou la création d'erreurs à des fins d'informations ou de débogage	Option permettant de définir le nombre de jours pendant lesquels un élément doit rester dans la table de file d'attente après l'achèvement ou la survenue d'une erreur à des fins d'informations ou de débogage. Par défaut, cette valeur est définie sur 14.
Nombre de jours de conservation des données d'importation d'événement, d'événement vers tâche et d'alertes déclenchées	Option permettant de déterminer le nombre de jours pendant lesquels vous souhaitez conserver les données d'importation d'événement, d'événement en tâche et d'alertes déclenchées. Par défaut, cette valeur est définie sur 30.
Activez ce paramètre pour mettre à jour les configurations de source Splunk existantes pour la prise en charge de l'authentification basée sur le jeton. Une fois ce paramètre activé, vous devez mettre à jour la configuration d'intégration avec les détails du jeton.	Option permettant de mettre à jour la configuration source Splunk existante vers la prise en charge de l'authentification basée sur les jetons à partir d'une version existante. **Remarque :** Après la mise à niveau vers la nouvelle version, le champ Jeton devient indisponible. Vous devez activer ce paramètre pour obtenir l'authentification basée sur le jeton, après quoi vous devez mettre à jour la configuration d'intégration avec les détails du jeton. Par défaut, cette valeur est définie sur Non.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres d'intégration Splunk



3. Cliquez sur **Enregistrer**.

Créer et nommer un profil d'événement pour l'intégration Splunk Enterprise Event Ingestion

Créez un profil d'événement dans votre Now Platform instance et déterminez quelles Splunk alertes créent des incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Avant Now Platform Réponse aux incidents de sécurité que les incidents de sécurité (SIR) ne soient créés à partir d'alertes ingérées, les valeurs de champ des alertes sont affichées dans la mise en page d'un Now Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera affiché.

Du point de vue de l'intégration, à l'aide des API disponibles, Splunk les événements sont transmis individuellement et manuellement en tant qu'événements discrets, ou ils sont combinés en alertes déclenchées qui sont automatiquement ingérées dans l'environnement Opérations de sécurité de votre Now Platform instance. Les workflows d'intégration ingèrent différents types d'alertes, comme les tentatives d'accès non autorisé et les logiciels malveillants, par exemple.

Ces alertes sont ingérées en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance. Toutes les alertes sont initialement ingérées pour un type d'alerte configuré dans un profil. Les alertes ingérées peuvent ensuite être filtrées pour spécifier quelles alertes créent des incidents de sécurité. Par exemple, vous pouvez préférer les filtres qui créent des incidents de sécurité uniquement pour les alertes identifiées comme présentant un risque élevé. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir d'alertes ingérées, les valeurs de champ individuelles des alertes filtrées sont mappées aux champs correspondants sur une mise en page de l'incident de sécurité pour un aperçu.

Les noms d'alerte pour les profils d'événement dans votre Now Platform instance doivent être uniques et ne peuvent être mappés qu'à un profil d'événement actif à la fois. Il s'agit des noms d'alertes déclenchées que vous avez configurés dans votre Splunk service dans le cadre de la configuration de l'intégration. Pour plus d'informations sur la configuration des alertes dans votre Splunk Enterprise environnement, reportez-vous à la section Enregistrer

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les recherches de l'intégration dans votre Splunk EnterpriseSplunk Enterprise Event Ingestion console.

Il Now Platform ingère des alertes spécifiques à l'aide des workflows de l'intégration. Toutes les alertes qui répondent aux critères de sélection de votre Splunk console d'entreprise sont initialement ingérées dans votre Now Platform instance.

Un profil dans votre Now Platform est une encapsulation d'une Splunk alerte dans votre Splunk console d'entreprise. Il existe une relation biunivoque entre les alertes ingérées avec un profil et les connexions à votre Splunk console d'entreprise : une alerte pour une connexion. Il n'y a qu'une seule connexion https à une tête de recherche dans votre Splunk Enterprise console. Plusieurs alertes peuvent provenir d'une seule tête de recherche. Si vous vous connectez à plusieurs têtes de recherche dans votre Splunk Enterprise console, vous devez créer plusieurs profils dans votre Now Platform instance pour ingérer ces alertes.

Étapes de création des profils pour l'ingestion d'alerte planifiée

Procédure

1. Pour créer un profil d'événement pour une alerte, dans votre Now Platform instance, accédez à **Splunk Integration** > **Profil d'événement Splunk**.
2. Si le formulaire Profil d'événement n'est Splunk pas affiché, cliquez sur **Nom** dans la barre de progression.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs.

   Le tableau ci-dessous un exemple de formulaire rempli.

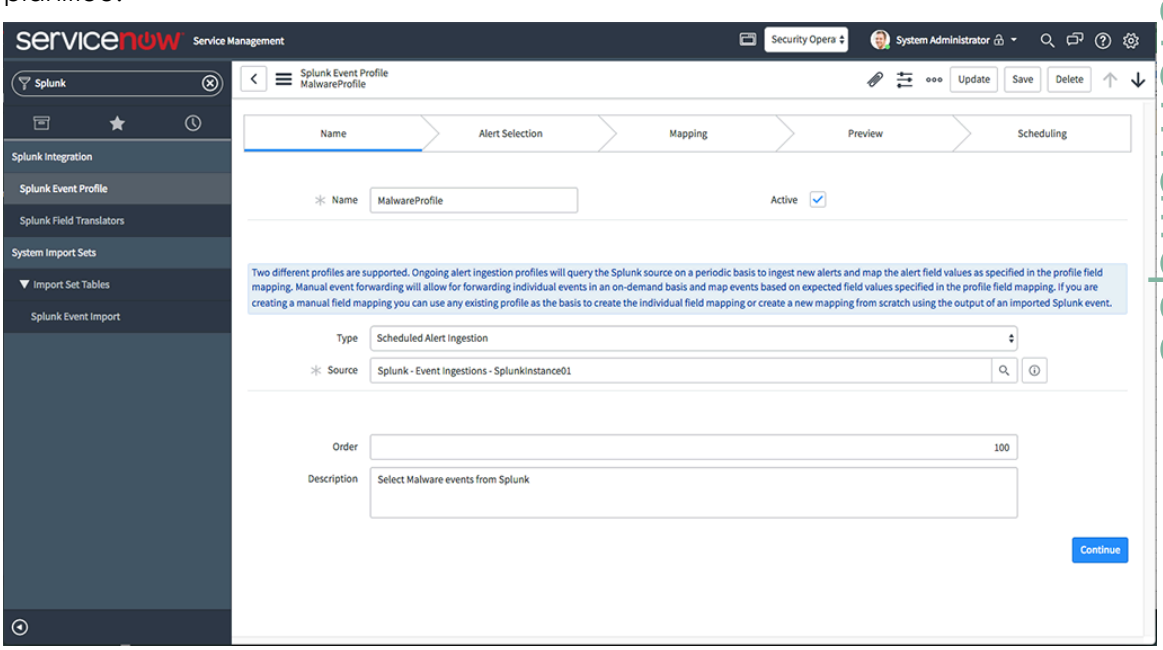
Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre Now Platform instance doivent être uniques.
Actif	La case n'est pas cochée par défaut. L'option Actif est désactivée et n'est pas disponible pour la sélection tant que vous n'avez pas terminé toutes les étapes de configuration du profil et cliqué sur **Terminer**.
Type	Sélectionnez le type de profil dans la liste de choix. ◦ Ingestion d'alerte planifiée : ce type de profil prend en charge les alertes déclenchées qui sont ingérées selon un calendrier que vous configurez. Renseignez les champs et cliquez sur **Continuer** pour passer à l'étape Sélection d'alerte du profil. ◦ Transfert manuel d'événements : ce type de profil prend en charge les événe-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	ments individuels qui sont transférés manuellement à partir de votre Splunk Enterprise console sur demande. Reportez-vous aux étapes suivantes pour remplir le formulaire pour ces types de profils.
Type de source	Splunk Fin de serveur ou de recherche que vous avez configurée pour ingérer des alertes. Si vous avez configuré plusieurs Splunk serveurs, sélectionnez le serveur approprié pour les types d'alertes que vous prévoyez d'ingérer pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Laissez ce paramètre sur la valeur par défaut. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Le workflow du profil dont le numéro est le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

La figure suivante est un exemple de formulaire rempli pour une alerte planifiée.



5. Dans le cas d'un profil avec une alerte planifiée, choisissez une option pour poursuivre la configuration du profil.

Option	Description
Continuer	Enregistrez le profil et passez à l'étape Sélection d'alerte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Mettre à jour	Enregistrez les mises à jour de ce profil et revenez à la liste des profils d'événements Splunk .
Enregistrer	Enregistrer ce profil et rester sur la page.
Supprimer	Supprimez cet enregistrement de profil et revenez à la liste des profils d'événements Splunk .

Étapes de création de profils pour le transfert manuel d'événements

6. Pour créer un profil qui prend en charge le transfert manuel d'événements, procédez comme suit.

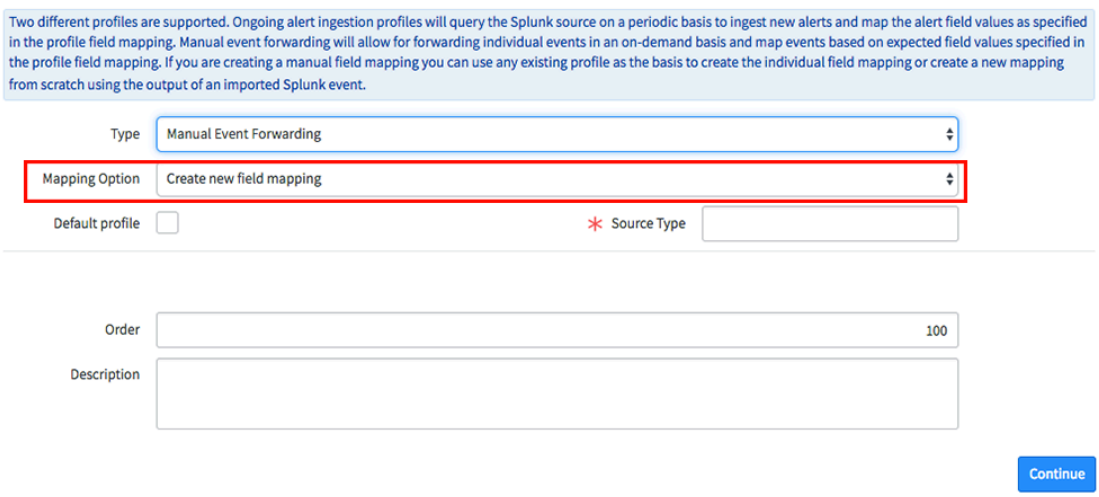
   Pour les événements que vous transférez à la demande à partir de votre Splunk console d'entreprise, vous pouvez baser le mappage de champs individuel sur n'importe quel profil existant. Vous pouvez également créer une nouvelle grille de mappage pour les données de pièce jointe exportées. Les événements que vous transférez manuellement ne sont pas planifiés dans le profil d'événement.

   a. Si ce n'est pas déjà fait, dans la liste de choix du champ Type, sélectionnez **Transfert manuel d'événements**.

   b. Dans le champ Option de mappage qui s'affiche, dans la liste de choix, choisissez une option de mappage pour continuer.

      Reportez-vous aux figures et tableaux suivants pour plus d'informations sur les options de mappage disponibles dans la liste de choix Options de mappage.

Créer une nouvelle option de mappage de champs



Créer une nouvelle option de mappage de champs

Option ou champ	Description
Créer une nouvelle option de mappage de champs	Nouveau mappage de champs pour votre événement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	Si vous n'avez pas de mappage de champs existant similaire au profil que vous créez, sélectionnez cette option pour créer une nouvelle carte.
Profil par défaut	Profil de transfert d'événement par défaut pour tous les Splunk événements. Désactivé par défaut. Lorsque cette option est activée, ce profil devient le profil par défaut pour le transfert manuel d'événements. Ce profil est le seul profil actif et utilisé pour chaque Splunk mappage de champ d'événement à un SIR incident de sécurité. Un seul profil s'adapte à tous les événements transférés. Le champ Source n'est pas disponible si l'option de profil par défaut est activée.
Type de source	Splunk serveur. Ce champ n'est pas disponible si l'option de profil par défaut est activée. Si disponible, l'option Type de source permet le mappage de champs d'événements uniques aux champs d'incidents de sécurité en fonction du type de Splunk source. Si vous souhaitez gérer les événements de journal de pare-feu différemment des événements de détection de point de terminaison et qu'ils ont différents Splunk types de sources, vous pouvez créer différents profils d'événements basés sur les types de sources pour répondre à cette exigence.
Ordre	La valeur par défaut est 100. Laissez ce paramètre sur la valeur par défaut. Si vous avez créé un grand nombre de profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow du profil dont le numéro est le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour un profil avec un nouveau mappage de champ, vérifiez que vous avez saisi une valeur dans le champ Type de source et cliquez sur **Continuer** pour passer à l'étape de mappage de la configuration.

Pour un profil avec un mappage de champ existant, reportez-vous à la figure et au tableau suivants pour plus d'informations.

Sélectionner un profil existant pour l'option de mappage de champ



Sélectionner un profil existant pour l'option de mappage de champ

Option ou champ	Description
Sélectionner un profil existant pour le mappage de champs	Un mappage de champs existant pour votre événement. Le champ Copier à partir du profil s'affiche. Procédez comme suit pour copier un mappage de champ existant pour ce profil. **i.** À gauche du champ Copier à partir du profil qui s'affiche, cliquez sur l'icône de recherche. **ii.** Dans la liste Event Profiles (Profils d'événements Splunk qui s'affiche), cliquez sur le nom du profil contenant la carte que vous souhaitez copier. Le nom du profil s'affiche dans le champ Copier à partir du profil.
Profil par défaut	Profil de transfert d'événement par défaut pour tous les Splunk événements. Désactivé par défaut. Lorsque cette option est activée, ce profil devient le profil par défaut pour le transfert manuel d'événements. Ce profil est le seul profil actif. Il est utilisé pour chaque Splunk mappage de champ d'événement à un SIR incident de sécurité. Un seul profil s'adapte à tous les événements transférés. Le champ Source n'est pas disponible si l'option de profil par défaut est activée.
Type de source	Splunk serveur. Ce champ n'est pas disponible si l'option de profil par défaut est sélectionnée. Si disponible, l'option Type de source permet le mappage de champs

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	d'événements uniques aux champs d'incidents de sécurité en fonction du type de Splunk source. Si vous souhaitez gérer les événements de journal de pare-feu différemment des événements de détection de point de terminaison et qu'ils ont différents Splunk types de sources, vous pouvez créer différents profils d'événements basés sur les types de sources pour répondre à cette exigence.
Ordre	La valeur par défaut est 100. Laissez ce paramètre sur la valeur par défaut. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow du profil dont le numéro est le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

Au bas du formulaire de sélection d'un mappage existant pour votre profil, cliquez sur **Terminer** pour finaliser la configuration du profil.

Que faire ensuite

Vous avez terminé avec succès les étapes de création de profils pour les alertes planifiées et le transfert manuel d'événements. Pour les profils pour le transfert manuel d'événements, vous avez terminé la configuration du profil. L'étape suivante consiste à charger les données de pièce jointe dans l'étape de mappage.
Pour les profils d'alertes planifiées, l'étape suivante consiste à sélectionner les alertes pour l'ingestion automatique.

Sélectionner les alertes planifiées pour l'intégration Splunk Enterprise Event Ingestion

Après avoir créé un profil pour une alerte planifiée, sélectionnez une Splunk alerte pour ce profil que vous souhaitez associer à un Now Platform Réponse aux incidents de sécurité incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Affichez les alertes disponibles dans votre Now Platform instance afin de savoir quelles valeurs de champ sont disponibles pour le mappage. Sélectionnez une alerte pour vous assurer que vous recevez les résultats attendus sur la mise en page de formulaire de base avant de mapper les valeurs aux champs des SIR incidents de sécurité. Vous ne pouvez sélectionner qu'une seule alerte dans la liste de ce formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

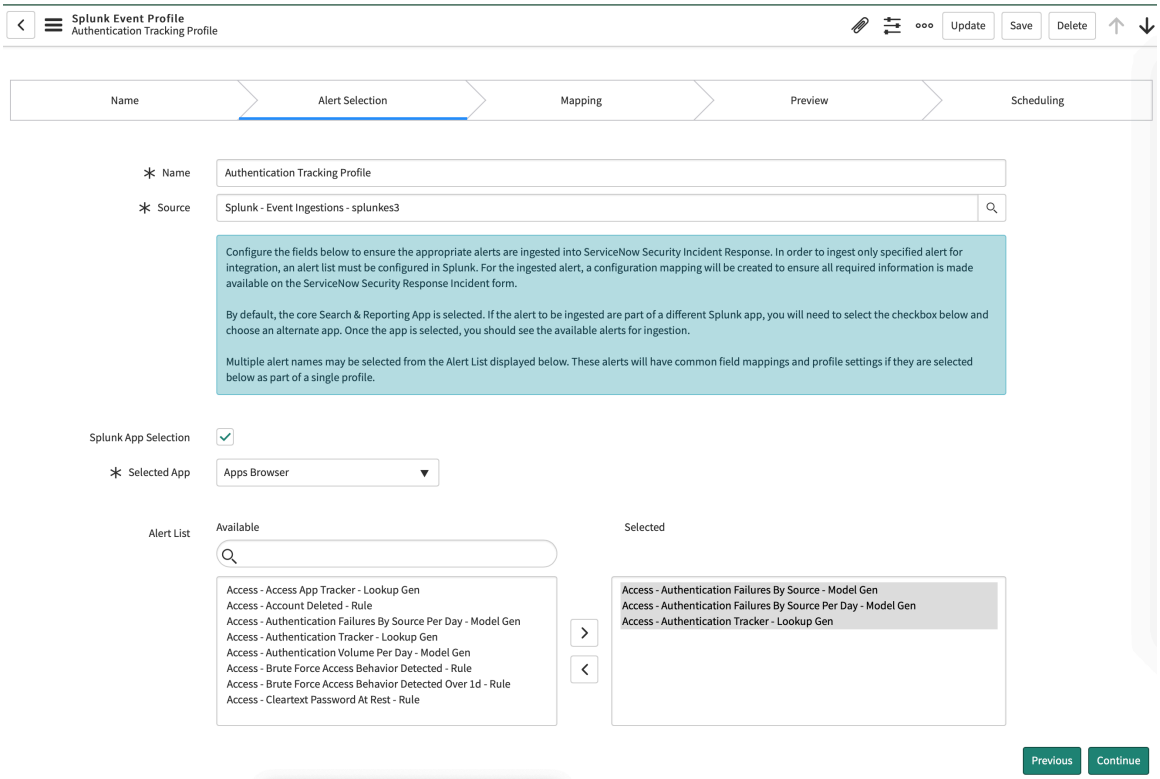
1. Si la page de sélection d'alerte n'est pas affichée, sélectionnez-la dans la barre de progression pour l'afficher.
   Par défaut, l'application Search & Reporting principale est sélectionnée.
2. Si l'alerte à ingérer fait partie d'une autre Splunk application, sélectionnez **Sélection d'application Splunk** et choisissez votre Splunk application dans la liste **Application sélectionnée** .
3. Dans la **liste d'alertes**, choisissez une alerte et déplacez-la de la colonne **Disponible** vers la colonne **Sélectionnée** .
   Vous pouvez également choisir plusieurs alertes. Si les alertes sont sélectionnées dans le cadre d'un profil unique, les alertes auront des mappages de champs et des paramètres de profil communs.

   La liste des alertes de ce formulaire correspond à la liste des alertes de votre Splunk console. Jusqu'à 500 alertes sont affichées sur ce formulaire. Si plus de 500 alertes sont répertoriées dans votre console Splunk sur la page Alertes, seules les 500 premières alertes sont affichées sur ce formulaire dans votre Now Platform instance.

Option	Description
Dans le champ de recherche Liste d'alertes, saisissez du texte.	La colonne sous le champ de recherche est filtrée avec les options disponibles en fonction du texte que vous saisissez. Sélectionnez une alerte, puis avec les touches fléchées, déplacez l'alarme sélectionnée de **Disponible** à **Sélectionné**.
Dans la liste d'alertes, double-cliquez sur une alerte.	La colonne **Sélectionné** est renseignée avec votre sélection.
Dans la liste d'alertes, cliquez une fois sur une règle d'alarme.	L'alarme est sélectionnée. À l'aide des touches fléchées, déplacez l'alerte sélectionnée de **Disponible** à **Sélectionné**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Choisissez une option pour continuer.

Option	Description
Poursuivez ou cliquez sur Mappage dans la barre de progression	Le formulaire de mappage s'affiche. **Le mappage** est sélectionné dans la barre de progression. L'étape suivante consiste à mapper les champs d'alerte à un SIR incident de sécurité.
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements Splunk s'affiche.
Précédent	L'étape **Nom** s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements Splunk s'affiche.

Que faire ensuite

Vous avez sélectionné avec succès une alerte pour un profil d'alerte planifiée. L'étape suivante consiste à mapper les valeurs d'alerte aux champs d'un incident de sécurité.

Mapper les alertes et les événements pour l'intégration Splunk Enterprise Event Ingestion

Une fois que vous avez identifié les sources pour l'ingestion d'alerte planifiée ou le transfert manuel d'événements, l'étape suivante consiste à mapper les champs d'événements individuels aux champs d'un Now Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

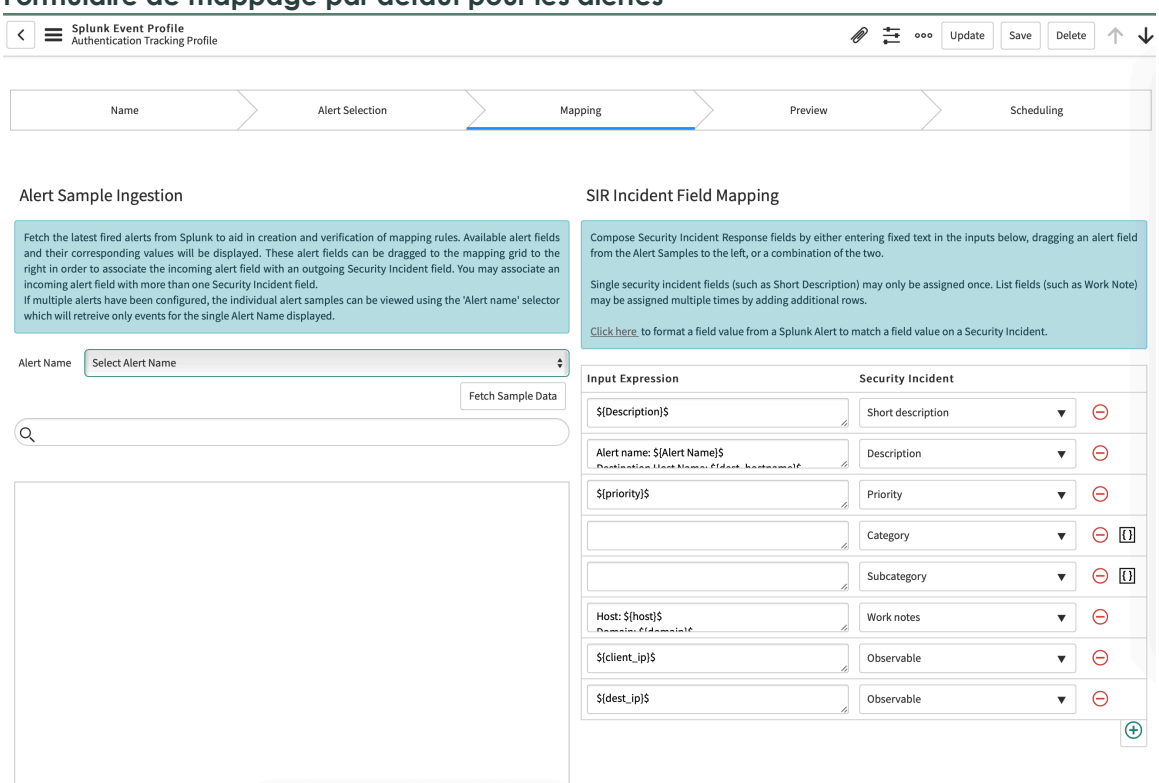
Vue d'ensemble

Pour l'étape de mappage, en tant qu'utilisateur disposant du rôle sn_si.admin, vous ingérez des échantillons d'alertes à partir de votre Splunk Enterprise console ou vous exportez les données d'événement d'un Splunk Enterprise événement.

Les figures suivantes sont des exemples de grilles de mappage par défaut fournies pour chaque type de profil d'événement. Ce mappage par défaut peut être modifié. Cette modification vous permet de personnaliser les champs qui renseignent l'incident de sécurité. Avec l'étape de mappage, vous pouvez visualiser l'impact de l'ajout ou de la suppression de champs d'événements sur les valeurs de champ d'incident SIR de sécurité.

Sélectionnez le **nom de l'alerte** et, après avoir cliqué pour **extraire les données d'échantillon**, les valeurs du champ d'alerte Splunk sont renseignées sur le côté gauche du formulaire lorsque des échantillons d'alertes sont ingérés par le profil. Il s'agit des champs d'alerte Splunk que vous mappez aux champs d'incident SIR de sécurité.

Formulaire de mappage par défaut pour les alertes

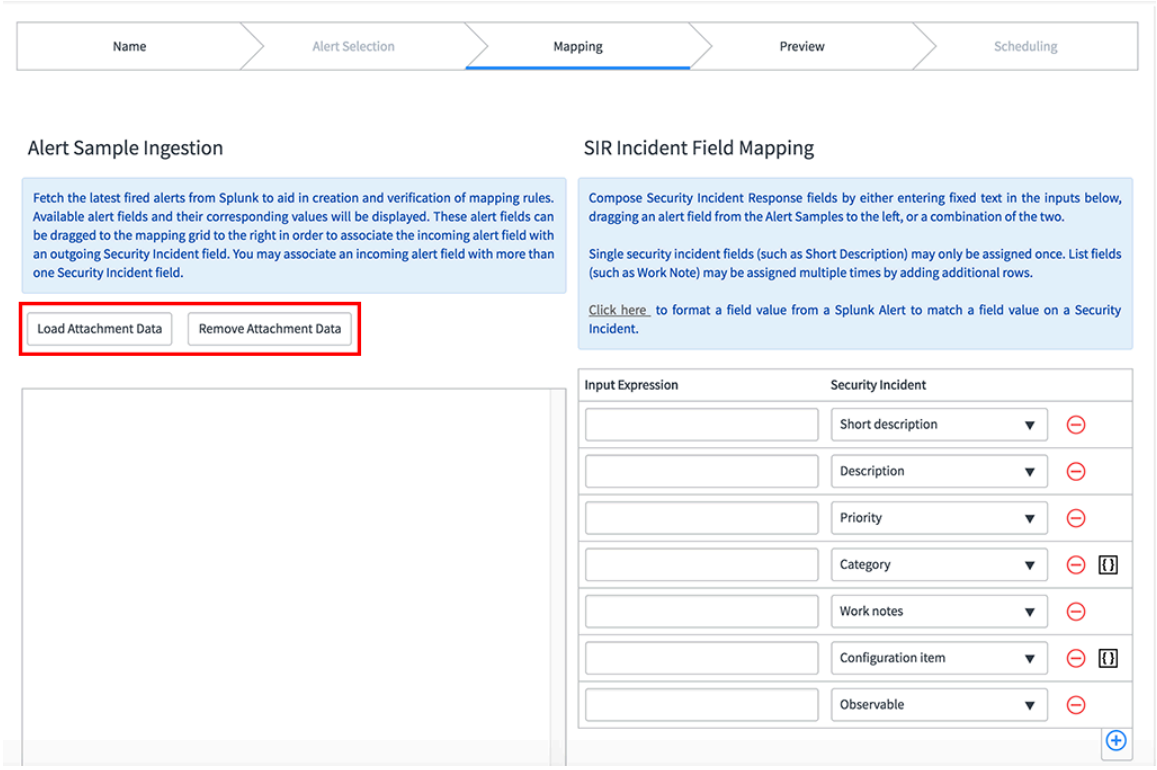


Une fois que vous avez cliqué pour charger les données de pièce jointe pour les événements transférés, les champs d'événement Splunk sont renseignés sur le côté gauche du formulaire. Il s'agit des Splunk champs de données qui sont mappés aux champs d'incident SIR de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de mappage par défaut pour les événements transférés



Vous préférez peut-être examiner quelques exemples d'alertes sur votre Splunk console à ingérer pour l'étape de configuration du mappage de champ. Cette étape s'intitule **Mappage** sur la barre de progression. Si cette page n'est pas affichée, cliquez sur **Mappage** dans la barre de progression.

Le mappage des alertes et l'exportation d'événements à la demande à partir de votre Splunk console d'entreprise incluent les concepts et les tâches suivants :

- Extraire des exemples de données pour les profils d'alerte ingérés automatiquement. Une fois que les données sont extraites (extraites) à partir d'une alerte déclenchée sur la console, les Splunk Enterprise champs d'alerte disponibles et leurs valeurs correspondantes sont affichés dans une mise en page de mappage par défaut sur le côté gauche du formulaire de mappage. Des onglets s'affichent pour vous permettre d'afficher les valeurs d'un ID d'alerte que vous avez extrait. Vérifiez que tous les champs critiques de la section Ingestion d'échantillons d'alerte à gauche du formulaire sont mappés à la grille à droite du formulaire.
- Si nécessaire, chargez des données d'échantillon d'événement pour tous les profils d'événements transférés manuellement. Les données d'exemple pour ces événements sont exportées dans un fichier `.xml` à partir de la Splunk Enterprise console et chargées dans votre Now Platform® instance. Les données importées sont affichées dans la section Ingestion d'échantillons d'alerte à gauche du formulaire.
- Modifiez la configuration de mappage en faisant glisser les alertes sur le côté gauche et en les déposant sur la grille de mappage à droite. La grille de mappage sur la droite associe le champ d'alerte entrante à un champ d'incident de sécurité sortant.
- Personnalisez la grille de mappage en ajoutant ou en supprimant des champs. Suivez les champs négligés ou dupliqués grâce au code couleur fourni.
- Définissez des conditions de filtre afin de pouvoir spécifier les alertes ingérées dans l'application SIR et celles qui sont filtrées.
- Définissez des critères de champ d'incident supplémentaires qui regroupent une alerte entrante en un incident de sécurité existant SIR afin d'éviter les incidents en double.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

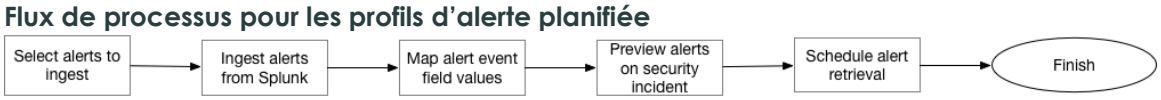
Ce filtrage supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données relatives aux événements de sécurité connexes sur un seul incident de sécurité.

- Dans certains cas, les valeurs de champ d'événement de la Splunk console Enterprise peuvent ne pas se traduire directement dans les champs de l'incident SIR de sécurité. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez mettre en forme des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, les valeurs des champs Alerte de programme malveillant et Infection par un virus de la Splunk console se traduisent toutes deux par activité de code malveillant dans le champ Catégorie de l'incident SIR de sécurité.

Profils d'alerte planifiée

Après la création d'un profil d'alerte planifiée, le flux de processus pour la configuration est illustré dans la figure suivante.

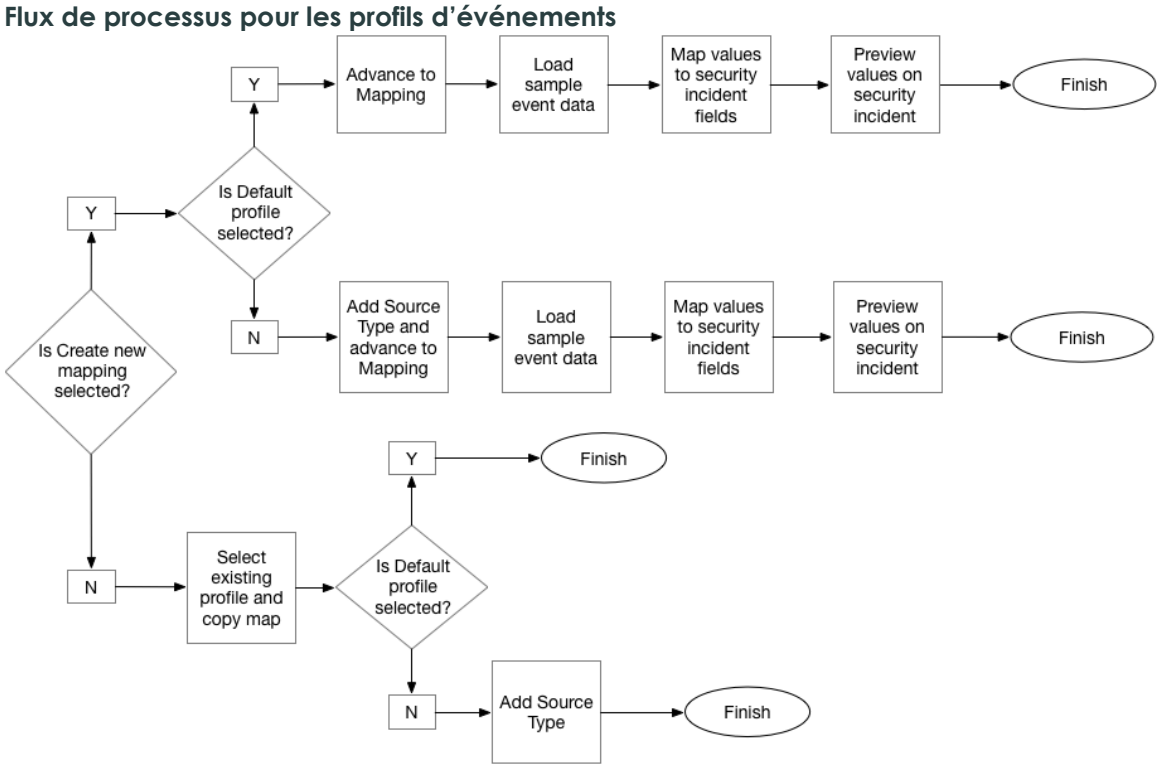
Flux de processus pour les profils d'alerte planifiée



Profils de transfert d'événements manuels

Après la création d'un profil pour un événement, le flux de processus pour la configuration est illustré dans la figure suivante.

Flux de processus pour les profils d'événements



L'étape suivante consiste à ingérer des alertes déclenchées ou à exporter des données et à mapper des valeurs aux champs d'incident SIR de sécurité.

Alertes de carte pour l'intégration Splunk Enterprise Event Ingestion

Au cours de l'étape de mappage des champs d'événements, vous mappez les champs d'événements individuels à partir d'alertes déclenchées ou de données d'événements

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

importées aux champs d'un Now Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
La grille de mappage préconfigurée des champs d'incident de sécurité par défaut peut être modifiée. Le codage couleur des champs d'événement vous aide à surveiller les valeurs de champ que vous avez déjà mappées. Cette étape vous permet de visualiser l'impact de vos modifications sur les champs de l'incident de sécurité.

Mappez jusqu'à cinq alertes de la colonne Ingestion d'échantillons d'alerte à gauche du formulaire aux champs d'incident de sécurité dans la colonne Mappage de champs d'incident SIR à droite.

Créez des cartes personnalisées en ajoutant ou en supprimant les champs de la grille de mappage sur le côté droit du formulaire. La personnalisation des champs vous permet de mapper Splunk des champs qui ne sont pas affichés sur la grille de mappage par défaut sur l'incident SIR de sécurité.

Procédure
1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Pour un profil avec une alerte planifiée, sous Ingestion d'échantillon d'alarme, sélectionnez l'alerte dans le **nom de l'alerte** et cliquez sur **Extraire des données d'échantillon** pour extraire la dernière instance d'une alerte déclenchée à partir de la Splunk Enterprise console.

   Les alertes sont affichées sous forme d'onglets. Vous pouvez ingérer jusqu'à cinq alertes les plus récentes.

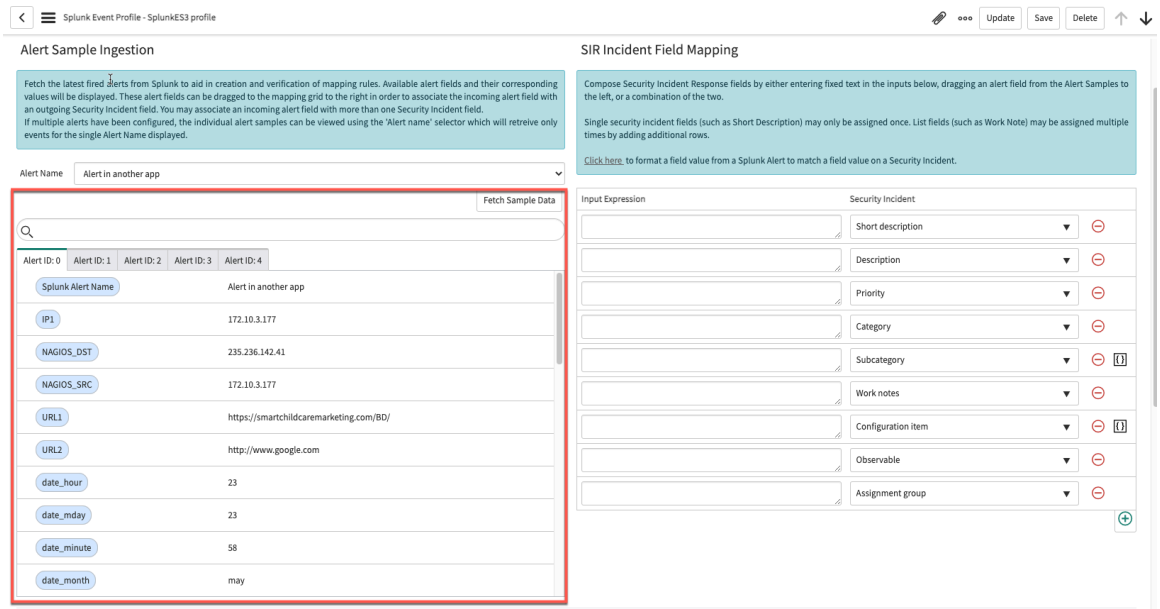
   L'extraction d'exemples d'événements peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran.

   Remarque : Un champ de mappage supplémentaire, **Nom d'alerte Splunk**, est ajouté par l'intégration pour permettre de remonter d'un événement à la règle d'alerte source dans Splunk. Cela peut être utile dans les scénarios où plusieurs Splunk alertes sont combinées en un seul profil.

   Lorsqu'un champ unique contient plusieurs valeurs, celles-ci sont analysées et mises en correspondance avec des entrées de champ individuelles dans la section de mappage de champs d'incidents SIR. Par exemple, les adresses IP sources, les noms d'actifs ou les URL peuvent avoir plusieurs entrées de champ observables ou plusieurs CI, qui sont analysés et mis en correspondance avec des entrées de champ individuelles dans la section de mappage de champ d'incident SIR.

   Dans la figure suivante, les paires champ-valeur de l'alerte ingérée ou de l'échantillon d'événement importé s'affichent sur le côté gauche de ce formulaire une fois l'extraction terminée. Ces valeurs sont les valeurs que vous mappez aux champs d'incident de sécurité du côté Mappage de champs d'incident SIR du formulaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour les profils d'alerte planifiée, passez à l'étape cinq pour mapper les valeurs.

4. De même, pour un profil d'un type d'événement que vous souhaitez exporter à partir de votre Splunk Enterprise console, procédez comme suit pour charger les données de pièce jointe dans votre Now Platform® instance.

a. Si vous n'êtes pas déjà connecté, connectez-vous à votre Splunk Enterprise console.

b. Accédez à l'onglet Rechercher et entrez un nom pour une recherche contenant les données d'événement que vous souhaitez exporter.

Par exemple, programme malveillant est un terme de recherche utilisé pour tous les événements de programme malveillant que vous pouvez transférer avec le workflow de cette intégration.

c. Développez l'événement et, dans la colonne Champ, sélectionnez les champs que vous souhaitez importer.

Ces champs correspondent aux paires champ-valeur qui sont exportées et affichées sur la page de mappage de votre Now Platform® instance.

d. Dans votre Splunk Enterprise console, en haut à droite de la page de recherche, cliquez sur l'icône **Exporter** .

e. Dans la liste du champ Format de la boîte de dialogue qui s'affiche, cliquez sur **Format XML**.

f. Facultatif : Entrez un nouveau nom de fichier.

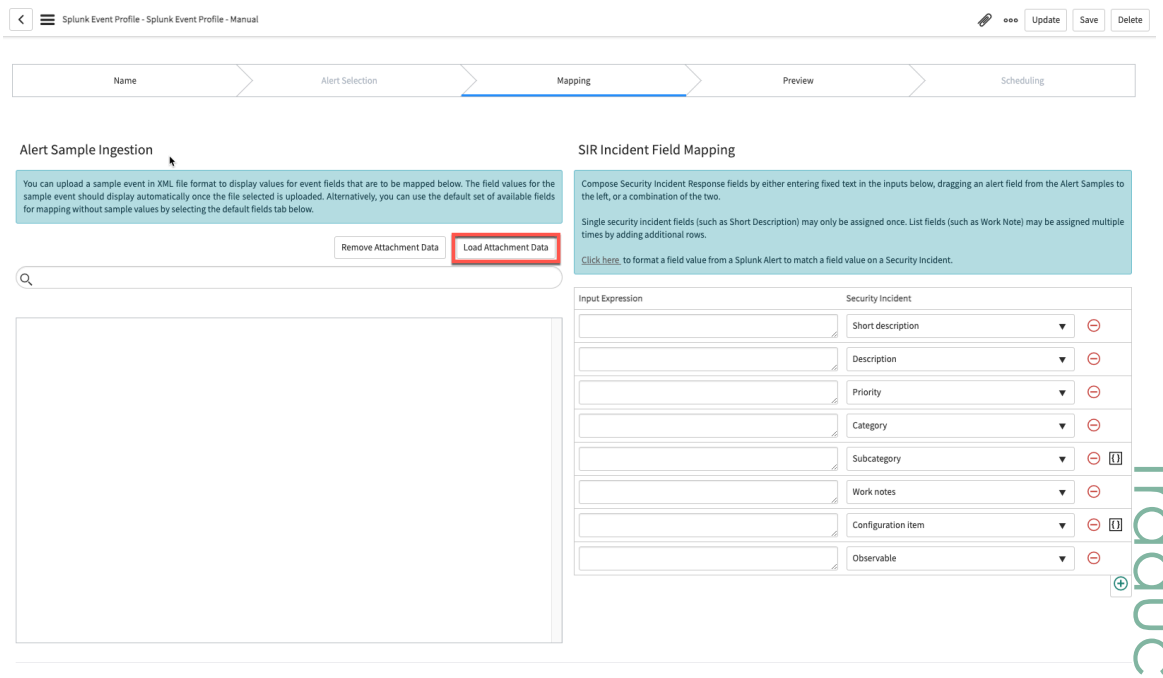
g. Cliquez sur **Exporter**.
Le fichier est téléchargé sur votre Now Platform® instance.

h. Si la page de mappage n'est pas déjà affichée dans votre Now Platform® instance, cliquez sur **Mappage** dans la barre de progression.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Dans la colonne Ingestion d'échantillon d'alerte, cliquez sur **Charger les données de la pièce jointe**.



j. Dans la boîte de dialogue qui s'affiche, cliquez sur **Choisir des fichiers** et accédez au `fichier .xml` que vous avez exporté, puis cliquez sur **Ouvrir**.
Les paires de valeurs des champs que vous avez exportés pour l'événement s'affichent sur le côté gauche du formulaire de mappage.

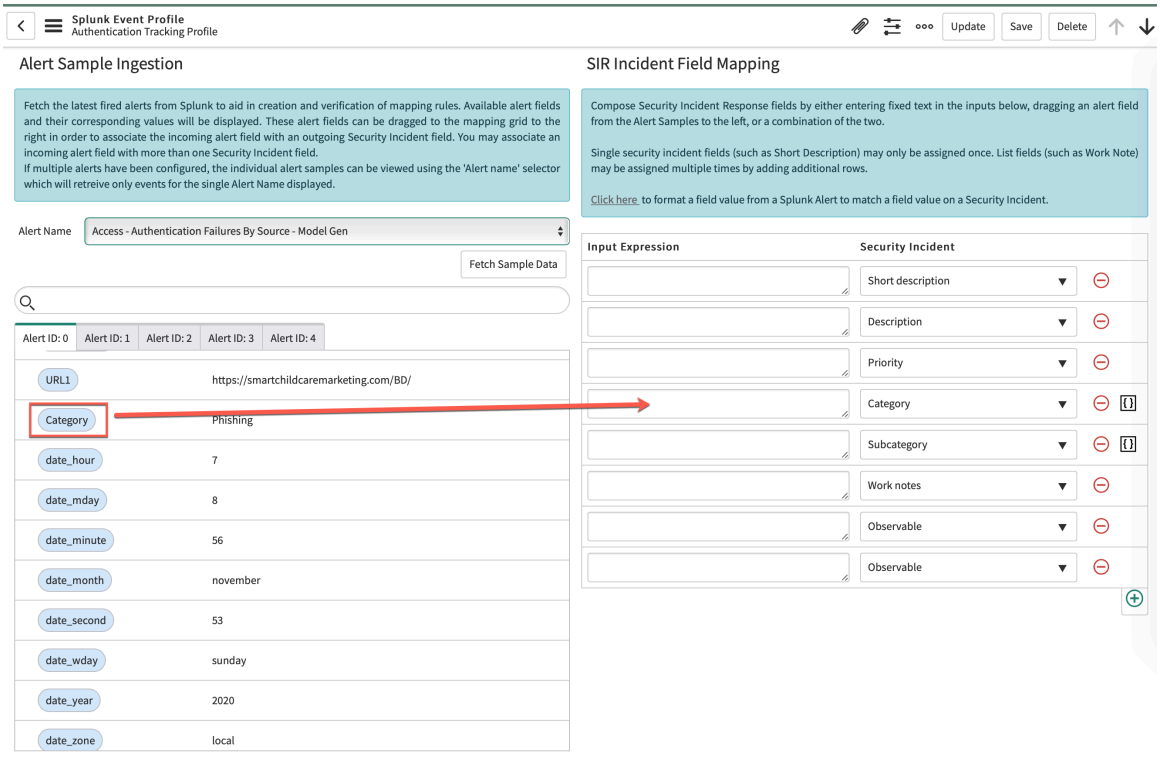
Dans la figure suivante, les paires de données d'une alerte planifiée ingérée s'affichent sur le côté gauche de ce formulaire. Les paires de valeurs pour les événements importés sont également affichées de ce côté du formulaire. Ces valeurs correspondent aux valeurs de champ que vous mappez aux champs d'incident de sécurité du côté du formulaire Mappage de champs d'incident SIR.

5. Pour mapper une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez longuement sur un nom de champ bleu sur le côté gauche du formulaire.

6. Faites glisser le nom du champ, par `exemple catégorie`, et déposez-le sur un champ de la colonne Expression d'entrée en regard d'un nom de champ dans la colonne Incident de sécurité.

Traduction automatique

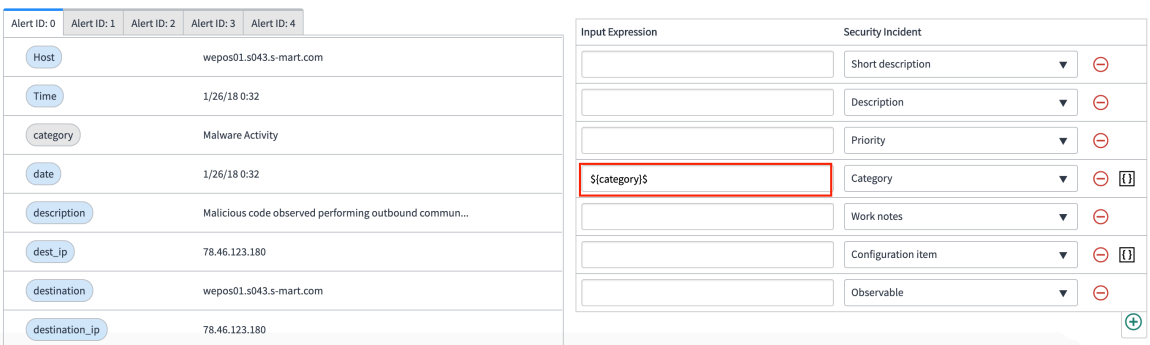
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La valeur du champ est affichée dans la colonne Expression d'entrée. Dans l'image suivante, la `catégorie` est mappée au champ de `catégorie` de l'incident de sécurité. Toutefois, vous pouvez faire correspondre n'importe quelle valeur du côté gauche à un champ de droite. Vérifiez que la valeur est correctement mappée sur l'incident de sécurité pendant l'étape de prévisualisation.

Pour vous assurer qu'aucun événement n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par couleur. Les champs bleu clair sur la gauche indiquent qu'un champ n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ d'alerte entrante à plusieurs champs sur un incident de sécurité.

Un champ gris indique qu'un champ a été sélectionné et mappé à un champ sur l'incident de sécurité. Ce code couleur vous aide à suivre le mappage, car dans certains cas, les champs d'événement d'alerte peuvent n'être affectés qu'une seule fois. Par exemple, vous ne pouvez affecter des valeurs à des champs tels que Description brève qu'une seule fois. Toutefois, vous pouvez affecter plusieurs fois des champs de liste tels que Note de travail en ajoutant des lignes supplémentaires à la grille de mappage.

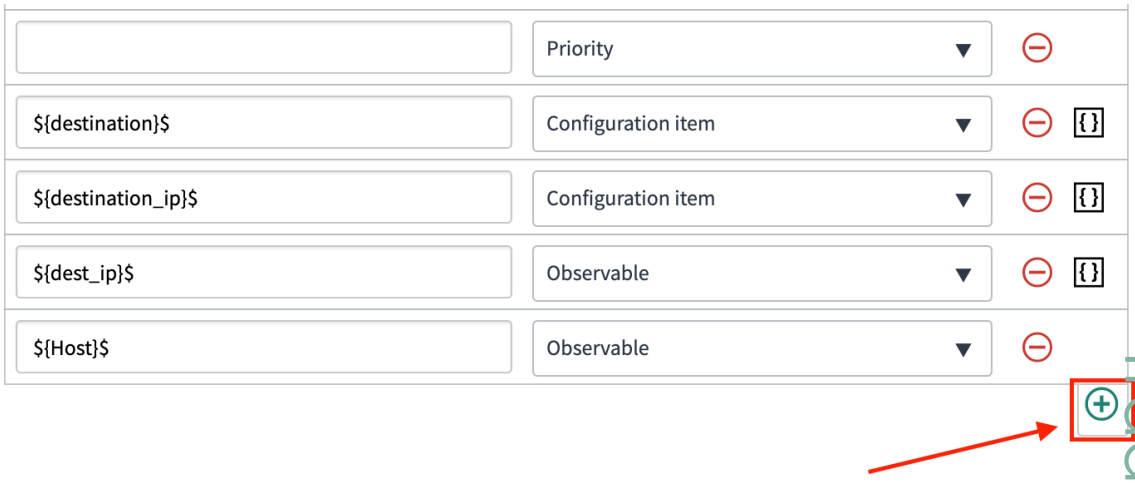


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Pour ajouter des champs au mappage par défaut de l'incident de sécurité sur le côté droit du formulaire, procédez comme suit.

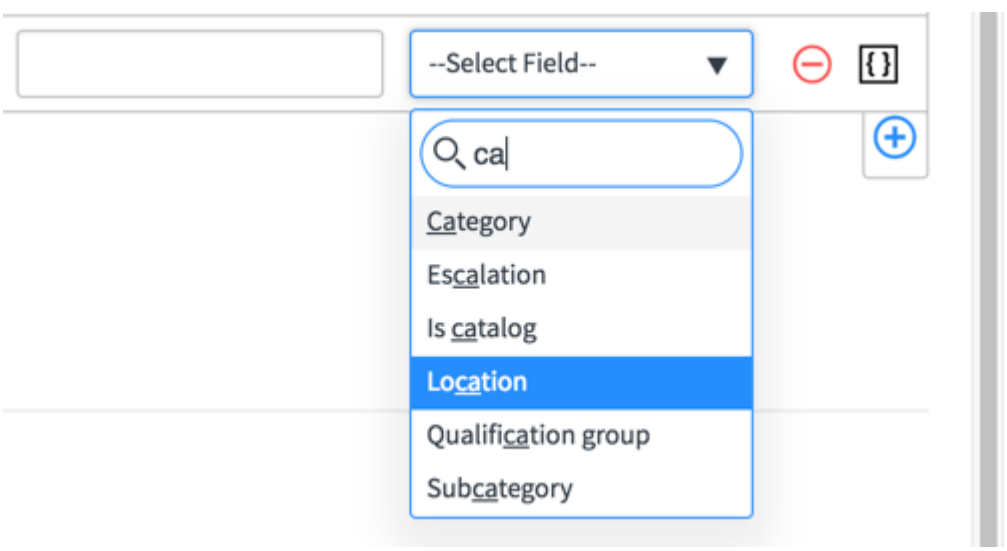
   a. À droite du formulaire, dans la section Mappage des champs d'incidents SIR, en bas de la grille, cliquez sur l'icône plus.



   Un nouveau champ s'affiche.

   b. Dans la colonne Incident de sécurité, développez la liste qui s'affiche, puis sélectionnez un champ.

   Dans la liste développée pour le nouveau champ, certains champs sont ombrés. Dans la figure suivante, la `catégorie` a un arrière-plan gris, car elle a été mappée dans l'incident de sécurité. À l'instar du code couleur des champs d'alerte sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre le mappage.



Traduction automatique

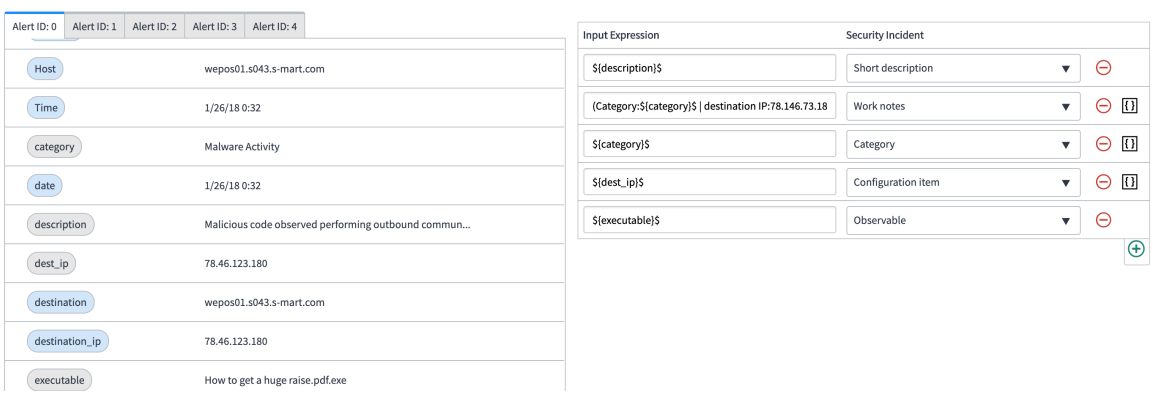
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Afin que plusieurs observables puissent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité dispose d'une liste dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affiché dans la liste, le champ n'est pas renseigné sur l'incident de sécurité.

c. Vous pouvez également saisir une valeur dans le champ Rechercher pour la nouvelle ligne.

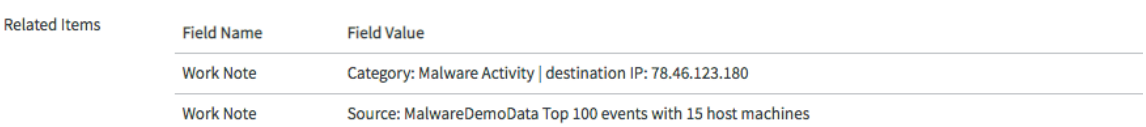
d. Sur le côté gauche du formulaire, cliquez avec le bouton gauche de la souris pour sélectionner **l'ID d'alerte** souhaité dans le champ expression d'entrée.
Grâce à la fonction de glisser-glisser, mappez-la à côté de votre nouveau champ.

8. Poursuivez le mappage en ajoutant ou en supprimant des champs et en ajoutant des valeurs à la carte.
La figure suivante est un exemple de grille de mappage modifiée. Dans le champ inférieur à droite, le champ Notes de travail est ajouté et il a plusieurs valeurs. Les valeurs sont séparées par des espaces et des signes de ponctuation (`Category :${category} | destination IP :78.146.73.180`).



Dans l'aperçu, ces valeurs sont affichées dans les notes de travail sur l'incident de sécurité. Étant donné que la valeur correspond à un champ que vous avez ajouté à la grille et que plusieurs valeurs sont mappées au champ Notes de travail, les valeurs s'affichent telles qu'elles sont saisies. Dans cet exemple, les espaces et les signes de ponctuation que vous avez saisis dans le champ sont affichés dans la section Éléments connexes sous forme de note de travail dans l'aperçu de l'incident de sécurité.

L'image suivante est un exemple de la façon dont les valeurs de l'image précédente sont affichées sur l'incident de sécurité.



Conditions de filtrage de génération d'incidents

Traduction automatique

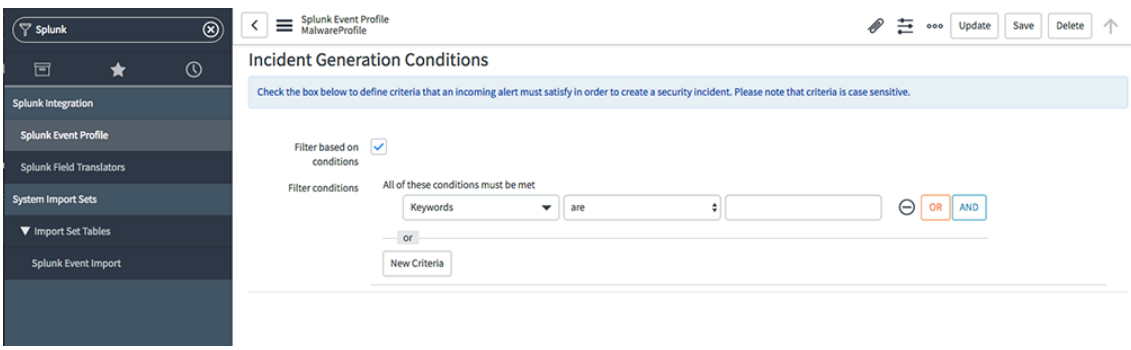
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Facultatif : Une fois que vous avez terminé les étapes de mappage au niveau des champs précédentes, vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de filtre pour définir les critères supplémentaires qu'une alerte entrante doit satisfaire pour créer un SIR incident de sécurité.
Pour définir les conditions de filtrage, procédez comme suit.

a. Faites défiler l'écran jusqu'à la section Conditions de génération d'incidents du formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

(Optional) Le Créateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

Les options des listes pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Ingestion d'échantillons d'alerte pour l'alerte que vous avez ingérée. Ces champs sont dynamiques et changent en fonction de l'alerte Splunk que vous ingérez ou de l'événement que vous transférez manuellement. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'alerte ou de l'événement Splunk Enterprise . Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférez peut-être revenir à votre Splunk Enterprise console et consulter vos alertes et événements à la recherche de mots clés.



b. À l'aide des listes et des champs du générateur de conditions, définissez des filtres pour la première ligne.

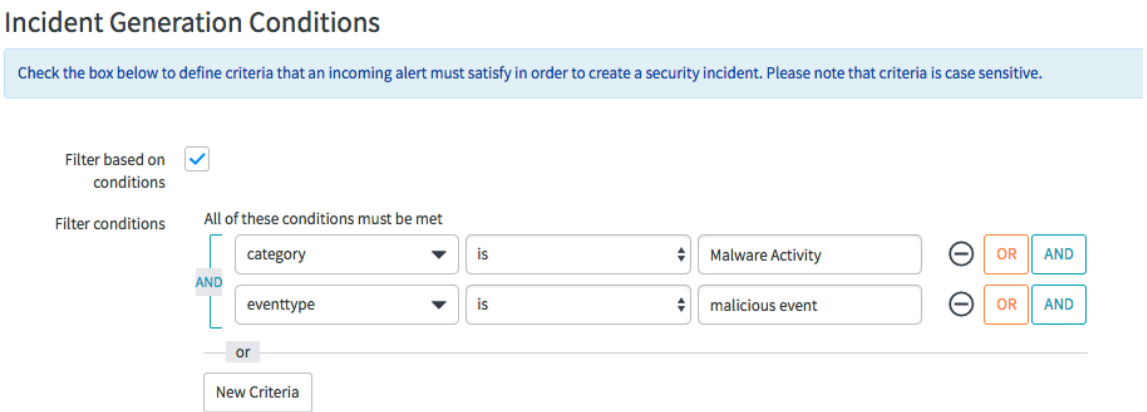
c. Pour ajouter d'autres conditions, à droite des champs, cliquez sur **ET** ou **OU**.
Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

d. Facultatif : Dans la deuxième ligne, définissez une deuxième condition de filtre.

(Optional) L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création des incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



(Optional) Vous avez défini les conditions de déclenchement de sorte que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

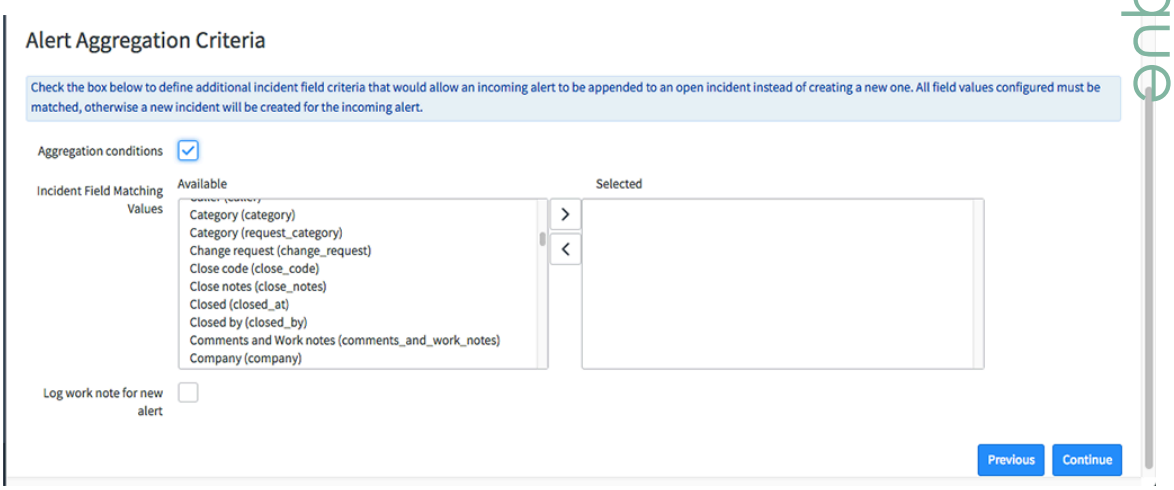
Ce type de filtrage vous aide à isoler les événements de sécurité et limite le nombre d'incidents de sécurité que vous créez. Si des critères de filtrage supplémentaires sont définis, seules les alertes requises sont ingérées sans avoir à modifier la Splunk requête ou la configuration des alertes déclenchées.

Alertes d'agrégation pour éviter les incidents en double

10. Facultatif : Pour éviter de créer des incidents de sécurité en double, définissez des critères de champ d'incident supplémentaires afin que les alertes entrantes soient regroupées en un incident de sécurité ouvert.
Pour définir ce critère, procédez comme suit.

a. Faites défiler l'écran jusqu'à la section Critères d'agrégation d'alertes du formulaire et cochez la case Conditions d'agrégat pour activer cette option.

(Optional) Les colonnes Incident Field Matching Values (Valeurs correspondantes du champ d'incident) s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés dans l'incident SIR de sécurité.



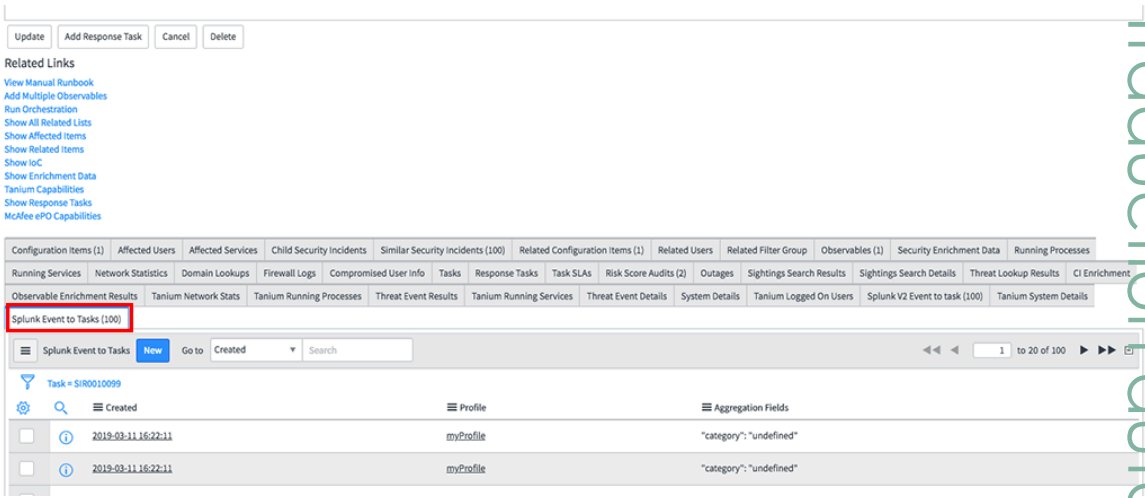
b. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre Now Platform et déplacez-les vers la liste Sélectionné.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(Optional) Toutes les valeurs de champ que vous sélectionnez doivent correspondre pour ajouter cette alerte entrante à un incident de sécurité existant. Si vous préférez examiner les valeurs de champ des incidents de sécurité à utiliser pour ce critère, accédez à **Incidents** > **Afficher tous les incidents**.

Si une nouvelle alerte correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation de l'étape de mappage, l'alerte est automatiquement ajoutée à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher toutes les alertes agrégées ajoutées dans une liste connexe d'un incident de sécurité. Toutes les alertes regroupées sur un incident de sécurité sont affichées dans la Splunk liste connexe Événements à tâches. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi des alertes sont ajoutées aux incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de l'enregistrement sous Liens connexes et cliquez sur le lien **Afficher toutes les listes connexes** .



c. Facultatif : Pour consigner une note de travail pour une nouvelle alerte récemment ajoutée à l'incident de sécurité, cochez la case pour activer cette option.
La note de travail consigne qu'une nouvelle alerte a été ajoutée, ainsi qu'un lien vers les détails de l'alerte.

Vous avez mappé avec succès les valeurs d'une alerte ou d'un Splunk événement aux champs d'un SIR incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage. Vous avez également ajouté des alertes ou des événements aux incidents de sécurité existants SIR .

11. Facultatif : Ouvrez l'éditeur de script et poursuivez la modification.

(Optional) Pour plus d'informations sur l'éditeur de script, reportez-vous à la section Utiliser l'éditeur de script pour formater les valeurs d'alerte pour l'intégration Splunk Enterprise Event Ingestion.

12. Choisissez-en un pour poursuivre la configuration du profil.

Option	Description
Continuer	Le formulaire de mappage s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	L'aperçu est sélectionné dans la barre de progression. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité.
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements s'affiche Splunk .
Précédent	Le formulaire Alert Selection (Sélection d'alerte) s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements s'affiche Splunk .

Que faire ensuite

L'étape suivante consiste à prévisualiser les valeurs que vous avez mappées sur l'incident de sécurité.

Prévisualiser l'incident de sécurité pour l'intégration Splunk Enterprise Event Ingestion

Une fois que vous avez terminé l'étape de mappage, prévisualisez les valeurs que vous avez mappées dans un Now Platform® Réponse aux incidents de sécurité incident de sécurité (SIR). Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs d'alerte que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer

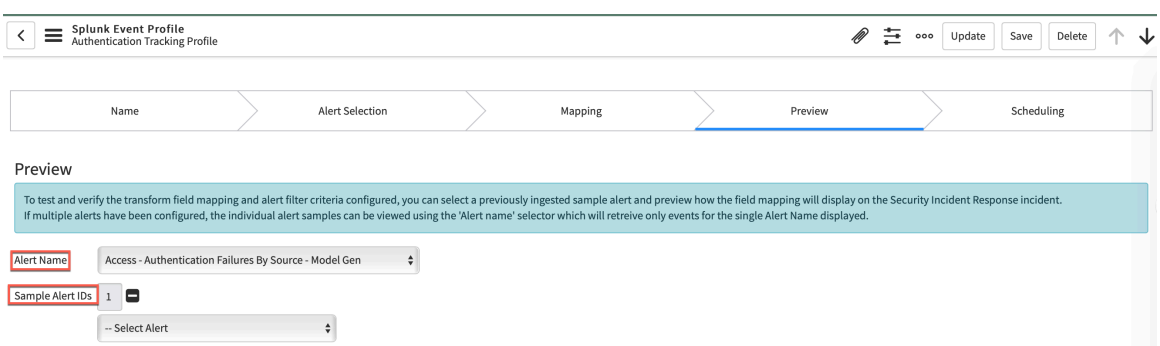
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs contenant des erreurs ou pour renseigner les données manquantes. Si l'aperçu n'est pas terminé, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de SIR sécurité ne sont pas enregistrés en tant qu'incidents réels dans le SIR produit.

Procédure

1. Si l'aperçu de l'incident de sécurité n'est pas affiché, cliquez sur **Aperçu** dans la barre de progression.
2. Sélectionnez le **nom de l'alerte** , puis sélectionnez un élément dans la liste **des ID d'échantillons d'alerte** .

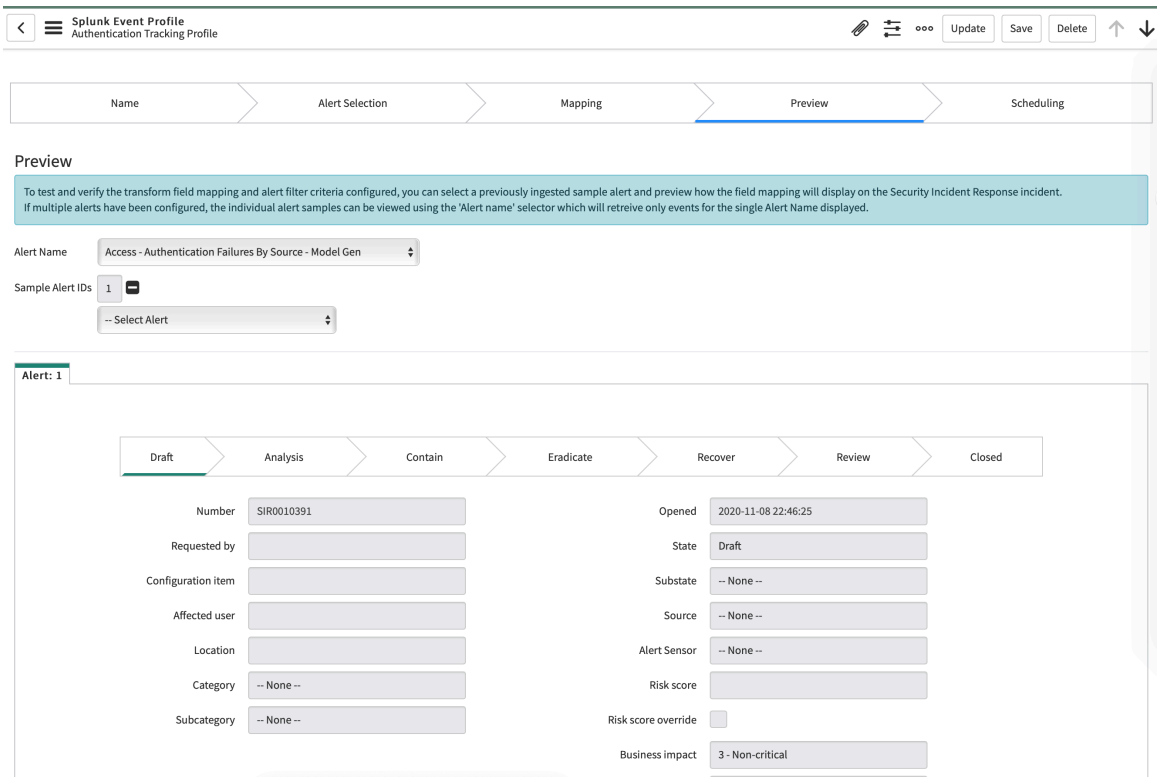


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'incident de sécurité s'affiche. Ne modifiez aucune information dans les champs. Il s'agit d'une vue en lecture seule et un enregistrement de cet incident de sécurité n'est pas enregistré.

3. Examinez le mappage des champs des valeurs d'alerte sur l'incident de sécurité.



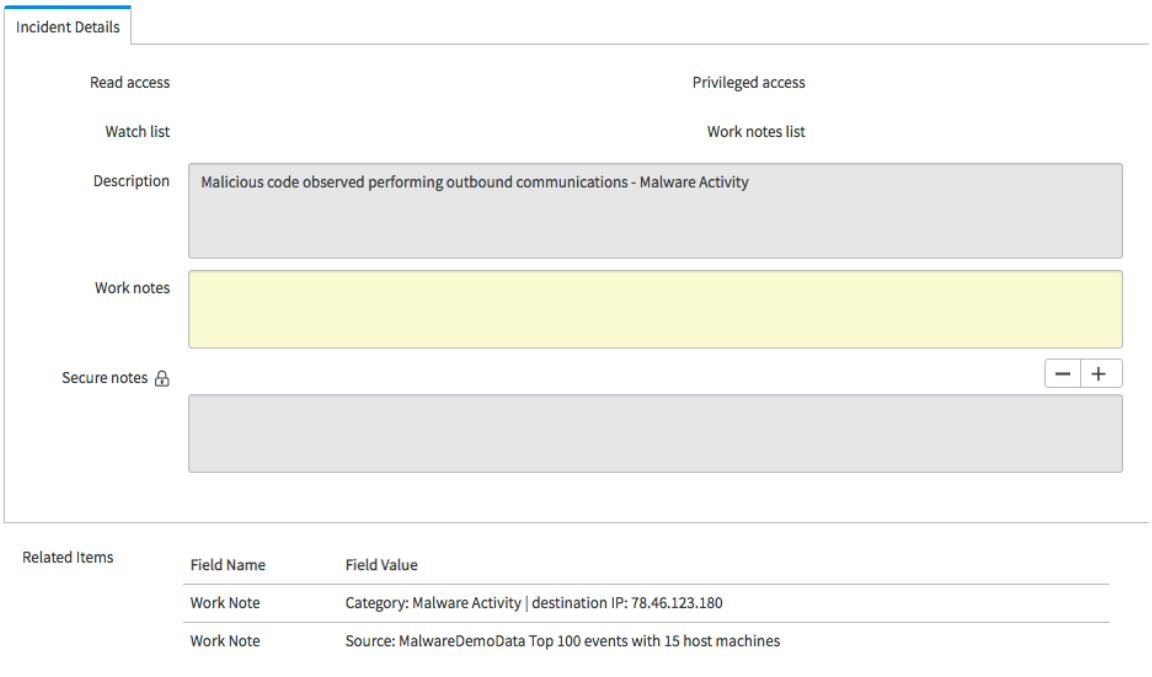
L'image précédente est un exemple d'aperçu avec une erreur de mappage. Dans cet exemple, un champ sur l'incident de sécurité n'existe pas pour une valeur, ou le champ ne prend pas en charge la valeur que vous avez mappée. Un message d'erreur s'affiche qui indique qu'une valeur d'entrée est introuvable pour le champ `Élément de configuration`.

4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

   La figure suivante est un exemple de l'onglet Détails de l'incident dans la moitié inférieure d'un SIR incident de sécurité, une fois que tous les messages d'erreur ont été résolus. Pour cet exemple, les champs Description et Notes de travail ont été mappés, et ces champs sont renseignés avec les valeurs des paires de valeurs extraites de la Splunk Enterprise console. Le premier champ Notes de travail n'a aucune valeur. Ce champ a été laissé vide dans la grille de mappage lors de l'étape de mappage. Les champs Note de travail supplémentaires qui ont des valeurs ont été ajoutés à la grille de mappage au cours de l'étape de mappage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Après avoir corrigé les erreurs et vérifié que les champs sont comme vous le souhaitez, choisissez une option pour continuer.

Option	Description
Continuer	Le formulaire Planification s'affiche pour les profils avec des alertes planifiées. **La planification** est sélectionnée dans la barre de progression.
Terminer	Pour les profils configurés pour le transfert manuel d'événements, cliquez sur **Terminer**. Il n'y a pas d'étape de planification pour les profils comportant des données d'événement qui sont exportés à la demande directement à partir de la Splunk Enterprise console.
Mettre à jour	Vos données sont enregistrées et vous êtes renvoyé à la liste des profils d'événements Splunk .
Précédent	L'étape Mappage de la barre de progression s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements s'affiche Splunk .

Que faire ensuite

Si aucun message d'erreur ne s'affiche et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à Planifier et récupérer les alertes pour l'intégration Splunk Enterprise Event Ingestion.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Planifier et récupérer les alertes pour l'intégration Splunk Enterprise Event Ingestion

Pour les profils d'ingestion d'alertes automatisées, cette étape est la dernière étape de la configuration du profil d'événement. Au cours de cette étape, vous pouvez vérifier les paramètres par défaut pour la récupération d'alerte ou modifier la planification selon vos besoins. Cette étape vous permet de filtrer votre récupération d'alerte en fonction d'une plage de dates.

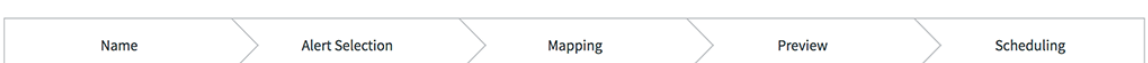
Avant de commencer

Rôle requis : rôle sn_si.admin

Pourquoi et quand exécuter cette tâche

Une fois que vous avez terminé toutes les étapes de la barre de progression de la configuration des profils, comme illustré dans la figure suivante, vous avez terminé la configuration des profils pour le transfert manuel des événements. Aucune planification n'est disponible pour les événements transférés manuellement à partir de votre Splunk Enterprise console. Pour les profils destinés à l'ingestion automatisée d'alertes, vous choisissez d'ingérer des alertes historiques au cours de l'étape de planification. Vous choisissez également la fréquence à laquelle vous procéderez à une interrogation pour les alertes futures qui correspondent à la configuration du profil d'alerte.

Barre de progression



Pour les profils d'ingestion d'alertes automatisées, avant d'activer le profil, vous vérifiez et modifiez la planification et la récupération des alertes. Cette étape est la dernière étape du processus de configuration du profil d'événement pour les profils d'alerte planifiée.

Configurez ces intervalles d'interrogation pour chaque profil. Les performances de l'intégration de l'ingestion Splunk d'événements sont impactées par les différents intervalles d'interrogation. Lors de la planification, vous préférerez peut-être équilibrer la charge du système par rapport à l'urgence de l'incident. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférerez peut-être modifier ce paramètre en fonction de l'urgence de l'incident et de la charge prévue sur votre système.

Dans la Splunk Enterprise console, vous définissez une alerte à déclencher en fonction d'incréments ou d'une heure spécifique. Utilisez ce paramètre pour vous aider à configurer la planification dans votre Now Platform instance afin que les incréments de temps de votre Splunk Enterprise console se synchronisent avec la planification que vous avez configurée dans votre Now Platform instance.

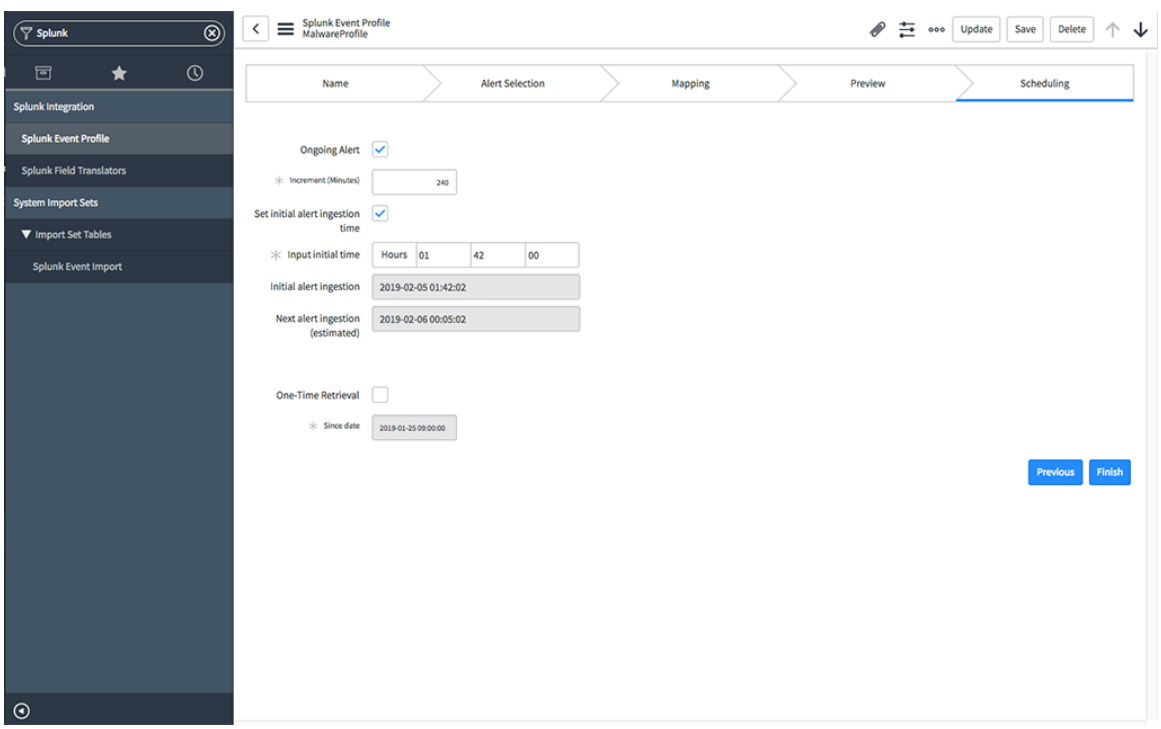
Procédure

1. Si la page Planification de la barre de progression n'est pas affichée, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les alertes sont extraites de la Splunk Enterprise console.

Option	Description
◦ Champ d'alerte en cours sélectionné ◦ Champ de récupération ponctuelle effacé	Alerte en cours En fonction du paramètre par défaut, l'instance Now Platform extrait du serveur pour de Splunk Enterprise nouvelles alertes toutes les cinq minutes. Les incidents de sécurité sont créés si des alertes déclenchées

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	sont détectées et si les critères de filtrage sont respectés. Pour équilibrer l'ingestion d'alertes par rapport à la charge du serveur et pour extraire les données les plus récentes, cinq minutes est le paramètre que vous préférez. Toutefois, cette valeur peut être modifiée si nécessaire.
◦ Champ d'alerte en cours effacé ◦ Champ de récupération ponctuelle sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhaitez une extraction unique pour ingérer des alertes basées sur des événements historiques. Lorsqu'il est configuré, un profil est utilisé une fois pour récupérer les alertes déclenchées, y compris les alertes d'événements historiques basés sur une plage de dates. À droite du champ **Depuis date** , cliquez sur l'icône Calendrier. Dans le calendrier qui s'affiche, sélectionnez la date à laquelle vous souhaitez commencer à extraire les alertes. À partir de la valeur **Date de début** , les alertes déclenchées sont récupérées jusqu'à la date actuelle. Une fois les alertes extraites, ce paramètre ne récupérera pas les alertes déclenchées pour ce profil à partir de la date actuelle. Ce paramètre remplit l'incident de sécurité avec toutes les alertes trouvées pour la plage que vous saisissez.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, pour la planification, si vous avez une alerte quotidienne Splunk qui s'exécute une fois par jour à 4 h (heure locale), vous pouvez configurer le profil d'alerte correspondant dans votre Now Platform instance pour qu'il s'exécute à 4 h 05 (heure locale) afin de capturer immédiatement l'alerte et créer un incident de sécurité. Entrez `04 05 00` dans le champ **Ingestion d'alerte initiale** . Dans le champ **Incrémentation (minutes)**, saisissez `1 440` (24 heures) pour planifier la prochaine ingestion d'alerte pendant 24 heures à compter de l'ingestion d'alerte initiale. L'heure d'ingestion d'alerte initiale et l'heure d'ingestion d'alerte suivante sont affichées dans les champs.

3. Pour configurer les paramètres de cet exemple, procédez comme suit.

   a. Une fois la page Planification affichée, cochez la case **Alerte en cours** pour activer cette option.

   b. Dans le champ **Incrémentation (minutes)**, saisissez `1 440` (24 heures).

   c. Cochez la case **Sélectionner l'ingestion d'alerte initiale** pour activer la modification des champs d'ingestion d'alerte initiale et d'ingestion d'alerte suivante.

   d. Dans le champ Ingestion d'alerte initiale, saisissez `04 05 00`.
   Le champ **Ingestion d'alerte suivante (estimée)**, l'heure de l'ingestion d'alerte suivante s'affiche.

4. Cliquez sur **Terminer** pour terminer la configuration.
   Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Ce profil est activé et extrait des alertes de la Splunk Enterprise console en fonction de votre planification. Il existe une limite de 1 000 incidents de sécurité qui peuvent être créés dans un délai de 24 heures. Jusqu'à 100 événements sont par alerte déclenchée. Les événements suivants seront ignorés une fois les limites atteintes.

Architecture d'intégration et connexion de systèmes externes pour l'intégration Splunk Enterprise Event Ingestion

La rubrique suivante décrit l'architecture d'intégration développée pour prendre en charge l'ingestion d'alertes déclenchées à partir de la Splunk Enterprise console. Ces informations clarifient, à un niveau élevé, le fonctionnement conceptuel de l'intégration. Il explique également pourquoi des étapes de configuration sont requises avant l'installation de l'application à partir du ServiceNow Store.

Termes clés utilisés pour cette intégration

Les termes clés suivants sont utilisés lors de l'installation et de la configuration. Pour plus d'informations sur ces conditions, consultez le site Web de la documentation produit ServiceNow et le site Web et les ressources Splunk sur la page Ressources Splunk .

Now Platform

Un produit d'entreprise ServiceNow Il Now Platform s'agit de la base sur laquelle reposent les composants individuels tels que Réponse aux incidents de sécurité (),SIR IT Service Management (ITSM) et d'autres produits.

ServiceNow Complément Splunkbase

Une ServiceNow application installée sur votre Splunk Enterprise console qui prend en charge l'option de transfert manuel d'événements de l'intégration. Le transfert manuel d'événements est une fonctionnalité facultative de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'intégration. Ce ServiceNow module complémentaire Splunkbase n'est pas requis pour l'ingestion d'alerte automatisée fournie par l'intégration.

Réponse aux incidents de sécurité (SIR)

Application Now Platform qui suit la progression des incidents de sécurité, depuis la détection et l'analyse initiale, en passant par le confinement, l'éradication et la récupération, jusqu'à l'examen final et la fermeture post-incident.

Splunk Enterprise

Produit ou service cloud automatisé de gestion des événements d'incident de sécurité (SIEM) qui collecte les données utilisées pour l'analyse et la gestion des incidents. Ce service se trouve sur un hôte qui est parfois également appelé Splunk console dans ce guide.

alerte Splunk

Une recherche que vous configurez et enregistrez pour Splunk rechercher des données spécifiques en fonction des paramètres que vous définissez dans le Splunk Enterprise service. Lorsque vous extrayez des alertes à partir de Splunk, vous extrayez également tous les événements associés à cette alerte.

Splunk Alerte déclenchée

Une recherche configurée dans la Splunk Enterprise console qui renvoie des résultats et marque ces résultats comme alertes déclenchées. Les alertes déclenchées sont ingérées de la Splunk console vers votre Now Platform instance pour cette intégration. Les alertes déclenchées ont un ou plusieurs Splunk événements.

Splunk événement

Un ou plusieurs éléments de données qui entraînent le déclenchement d'alertes du Splunk service. À partir de votre Now Platform instance, vous pouvez rechercher les événements qui Splunk ont déclenché Now Platform des incidents de sécurité.

Serveur MID

Cette application facilite la communication et le mouvement de données entre les applications, sources de Now Platform données et services externes. Cette application est généralement requise pour l'intégration avec des technologies locales et, pour cette Splunk Enterprise Event Ingestion intégration, le serveur MID facilite la communication entre l'instance locale et l'instance Now Platform locale de Splunk Enterprise. Un serveur MID n'est pas nécessaire si vous intégrez votre Now Platform instance à une Splunk Cloud instance.

Administrateur d'incident de sécurité (sn_si.admin)

L'utilisateur disposant de ce rôle supervise la configuration de l'intégration au SIR produit dans votre Now Platform instance.

Analyste des incidents de sécurité (sn_si.analyst)

L'utilisateur disposant de ce rôle interagit avec les incidents de sécurité du ServiceNow Réponse aux incidents de sécurité produit et les analyse.

Connexion à des systèmes externes

Un profil d'événement est un conteneur que vous créez, nommez et configurez pour une connexion et un appel uniques au service afin d'extraire les alertes déclenchées les plus récentes qui correspondent à Splunk des critères spécifiques. Une fois que les alertes déclenchées correspondant à votre profil ont été extraites de Splunk, vous sélectionnez celle que vous souhaitez afficher en tant qu'incident Now Platform Réponse aux incidents de sécurité SIR de sécurité. Une vue par défaut des champs d'alerte Splunk Enterprise est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

disponible, et vous modifiez ce mappage des champs d'alerte aux champs d'un SIR incident de sécurité pour répondre à vos besoins. Vous prévisualisez votre mappage pour vérifier que toutes les valeurs de champ d'alerte requises sont renseignées sur l'incident SIR de sécurité. Pour terminer la configuration du profil d'alerte, vous devez planifier la récupération des alertes, puis activer le profil. Après avoir activé le profil dans le Now Platform, vous êtes prêt à ingérer automatiquement des alertes historiques et en cours Splunk .

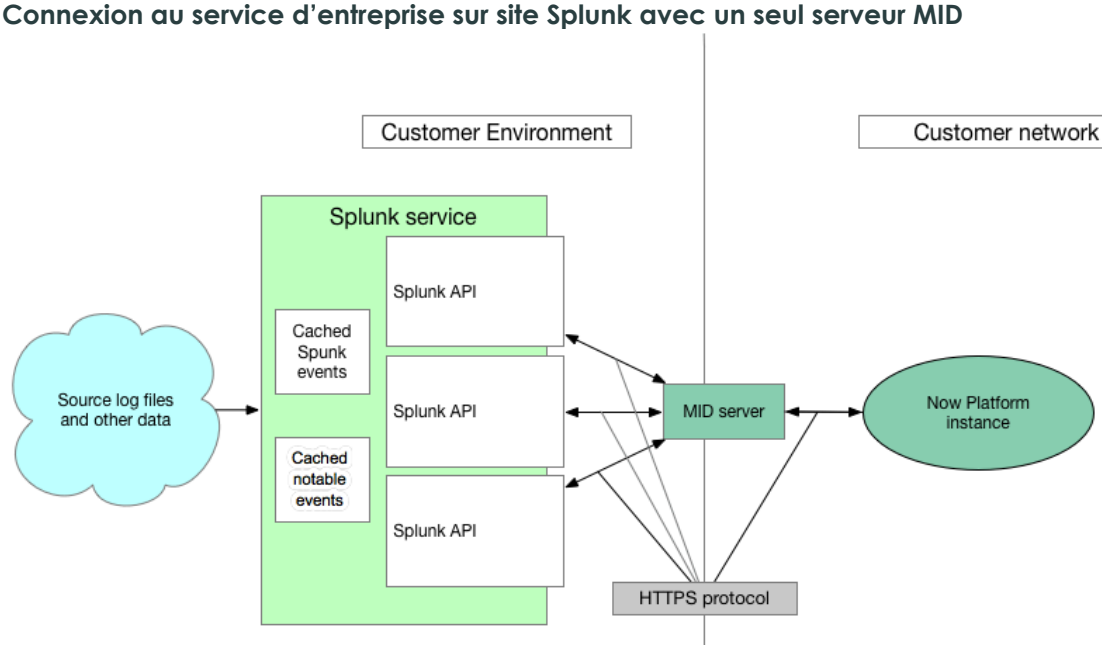
En tant qu'utilisateur disposant du rôle sn_si.admin, si vous déterminez qu'une nouvelle alerte déclenchée est similaire aux alertes précédemment ingérées, vous pouvez regrouper les nouvelles alertes déclenchées en incidents de sécurité existants SIR . Vous définissez des critères pour spécifier les valeurs de champ cible correspondantes dans le profil d'alerte Splunk Enterprise qui définissent quand un incident de sécurité existant est mis à jour et quand un nouvel incident de sécurité est créé. Si la fonctionnalité d'agrégation est activée dans votre profil d'événement, lorsque le jeu d'importation est transformé, votre Now Platform instance recherche un enregistrement existant dans la table cible qui a la même valeur dans les champs cible et source. Si un enregistrement existant avec une valeur correspondante dans la table cible est trouvé, cet enregistrement est mis à jour. Si aucun enregistrement correspondant n'est trouvé, un nouvel enregistrement est créé dans la table cible. Si elle est activée, l'option d'agrégation met à jour les incidents de sécurité existants avec de nouvelles alertes déclenchées, ce qui vous permet d'éviter de créer plusieurs incidents de sécurité. Pour plus d'informations sur la mise à jour des enregistrements à l'aide des options d'agrégation, voir Mise à jour des enregistrements à l'aide de la fusion .

Cette application utilise le Splunk service API pour récupérer des informations à partir Splunk du service. Une connexion HTTPS sortante du MID Server vers cet environnement est nécessaire pour le bon fonctionnement de l'intégration.

Une fois connectée au Splunk service, l'intégration prend en charge l'extraction et l'ingestion des alertes et des événements déclenchés qui déclenchent des incidents de sécurité.

Le flux de données de base est illustré dans les figures suivantes. Dans chaque figure, votre Now Platform extrait (ingère) des données. Splunk n'envoie pas de données pour les alertes planifiées.

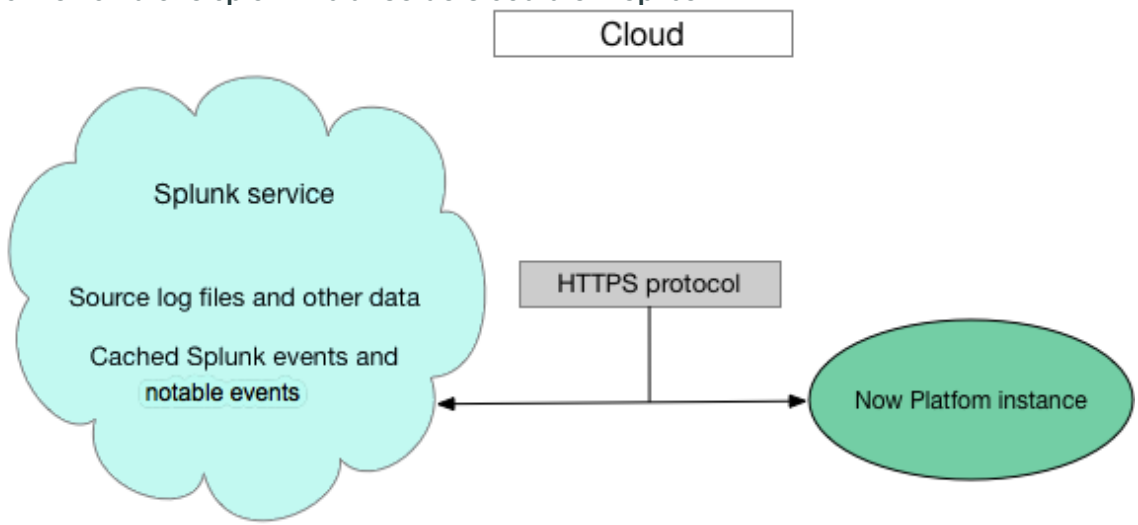
Connexion au service d'entreprise sur site Splunk avec un seul serveur MID



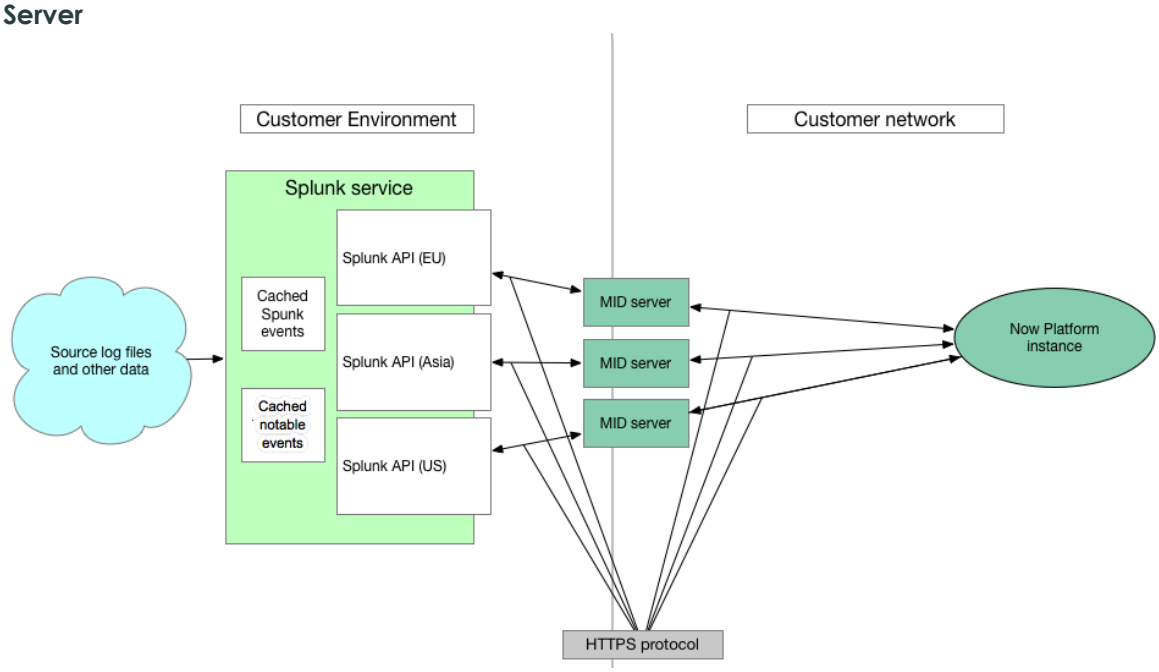
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connexion à une Splunk instance de cloud d'entreprise



Connexions multiples au service d'entreprise à l'aide Splunk de plusieurs MID Server



Traduction automatique

Copier Splunk Enterprise Event Ingestion les profils d'une instance à l'autre à l'aide de la fonctionnalité d'exportation/importation

Vous pouvez exporter et importer Splunk Enterprise Event Ingestion les paramètres des profils d'une Now Platform instance à une autre Now Platform .

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

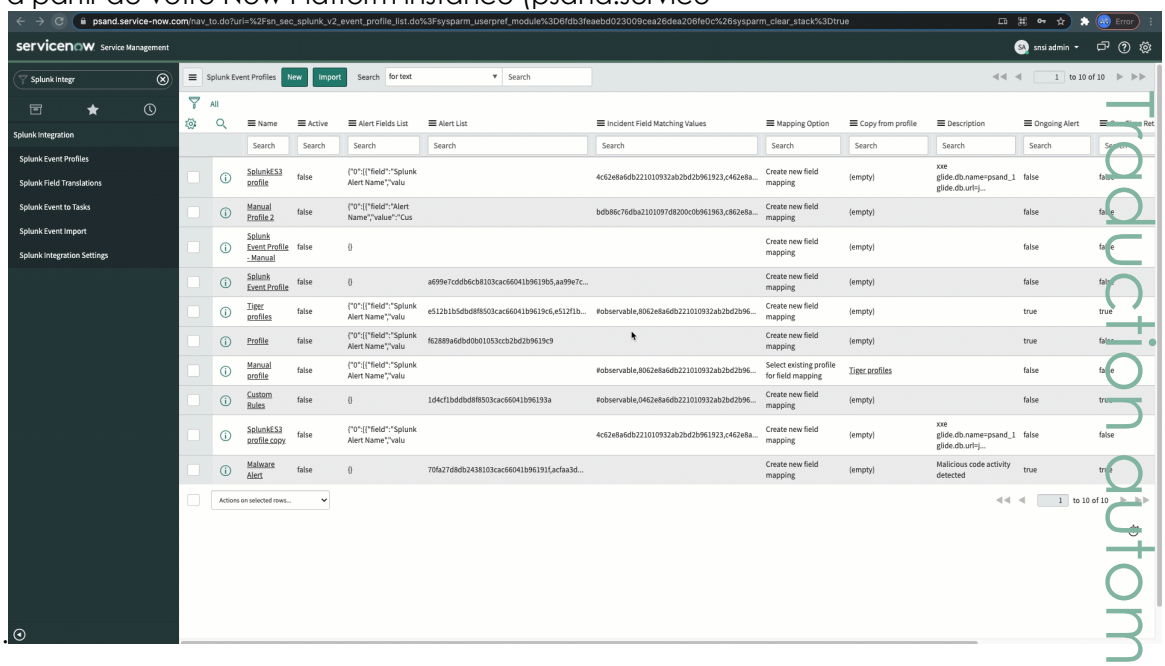
Cette fonctionnalité permet à l'administrateur de sécurité de copier des profils qui ont été testés et vérifiés sur une instance, par exemple en non-production, vers une Now Platform autre Now Platform instance, par exemple en production, sans avoir à refaire tous les paramètres de configuration. Les paramètres exportés et importés comprennent le nom du profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les données d'échantillon extraites, la planification et les informations sur la source des vignettes de configuration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous exportez un type de profil de transfert d'événements manuel, les données de pièce jointe utilisées pour l'exemple de mappage de champ sont copiées, mais le fichier de pièce jointe lui-même n'est pas exporté.

Procédure

1. Accédez à la **Tout** > **Splunk Integration** > **Profils d'événements Splunk**.
2. Sélectionnez un profil que vous souhaitez exporter vers une autre Now Platform instance. Vous pouvez sélectionner plusieurs profils pour l'exportation.
3. Dans le menu Actions, cliquez sur **Exporter**.
4. Une fois que le message « Exportation terminée » s'affiche, cliquez sur **Télécharger**. L'illustration suivante montre l'exportation d'un Splunk profil (profil manuel 2) à partir de votre Now Platform instance (psand.service-now.com).



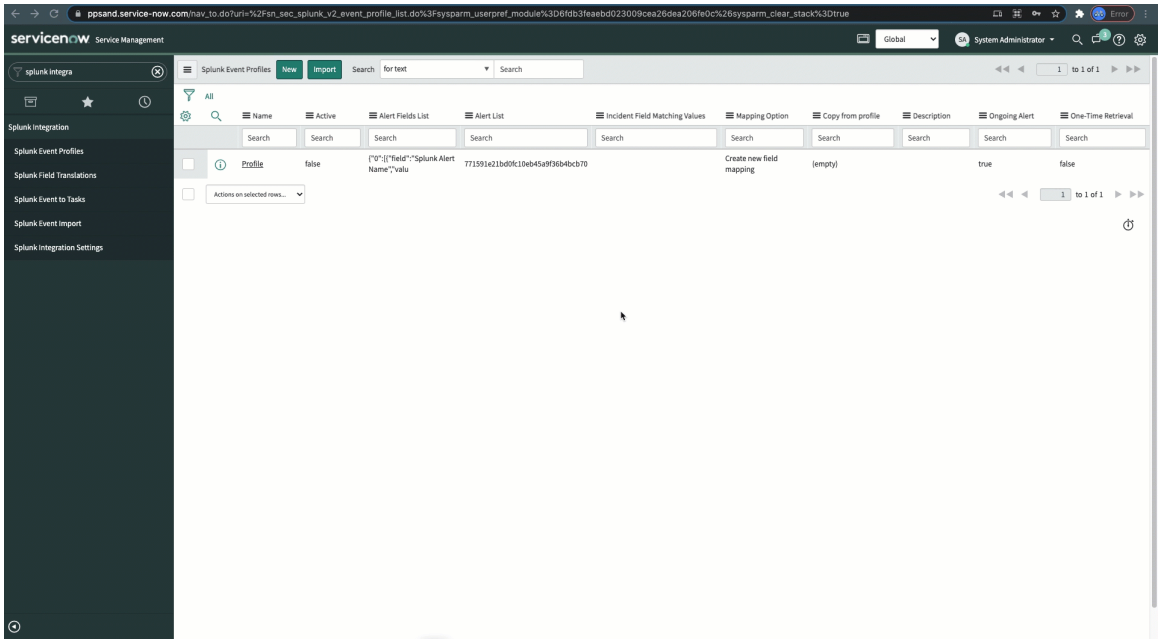
Le fichier payload.xml exporté est téléchargé sur votre ordinateur. Le fichier contient le nom du profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les exemples de données récupérées, la planification et les informations sur la source des vignettes de configuration. Lorsque vous sélectionnez et téléchargez plusieurs profils, ils apparaissent dans le même fichier payload.xml.

Vous pouvez maintenant procéder à l'importation du profil dans une autre Now Platform instance.

5. Accédez à la **Splunk Integration** > **Profils d'événements Splunk**.
6. Cliquez sur **Importer**.
7. Cliquez sur **Choisir un fichier** et sélectionnez le fichier xml sur votre ordinateur.
8. Cliquez sur **Charger**.
9. Cliquez sur **Fermer et recharger les profils**. L'illustration suivante montre l'importation d'un Splunk profil (profil manuel 2) de l'instance Now Platform (psand.service-now.com) vers une autre Now Platform instance (ppsand.service-now.com).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous avez importé le profil avec succès à partir d'une autre Now Platform instance.

Vérifiez que les paramètres de configuration de la source exportée (Splunk compte API et Splunk URL du serveur) et du serveur MID sont valides et disponibles dans l'instance importée Now Platform . Mettez à jour votre Splunk Enterprise Event Ingestion configuration si nécessaire.

10. Facultatif : Vérifiez les paramètres du Serveur MID après l'importation d'un profil.
11. Facultatif : Accédez à la **Security Operations** > **Configurations d'intégration**.
12. Facultatif : Sélectionnez la vignette de Splunk Enterprise Event Ingestion configuration, puis cliquez sur **Mettre à jour**.
13. Facultatif : Examinez et mettez à jour les détails de la source et du serveur MID selon les besoins.

Copier un profil d'événement pour l'intégration Splunk Enterprise Event Ingestion

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils d'alarme pour gagner du temps.

Avant de commencer
Rôle requis : sn_si.admin

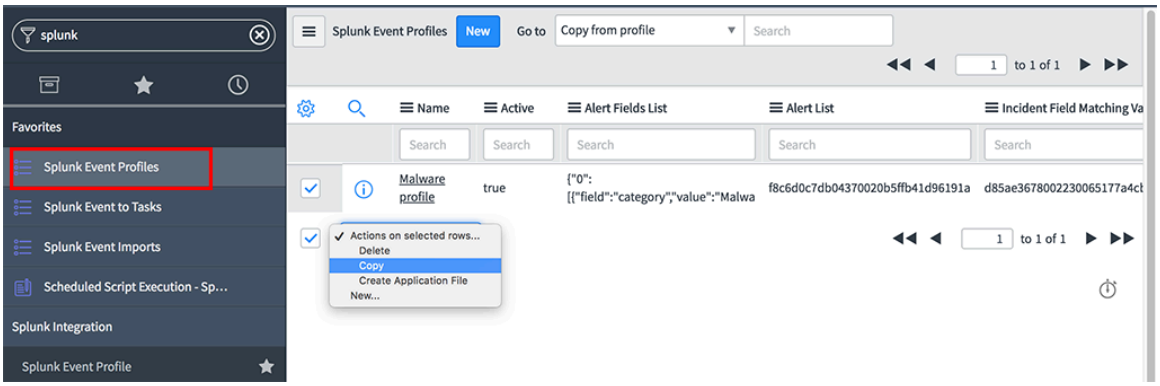
Pourquoi et quand exécuter cette tâche
La copie d'un profil existant et de ses paramètres associés est facultative.

Si vous copiez un profil, le nom du profil est d'abord modifié pour éviter les doublons. En outre, le profil copié est désactivé (faux) afin qu'il ne soit pas activé accidentellement avant la fin de la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

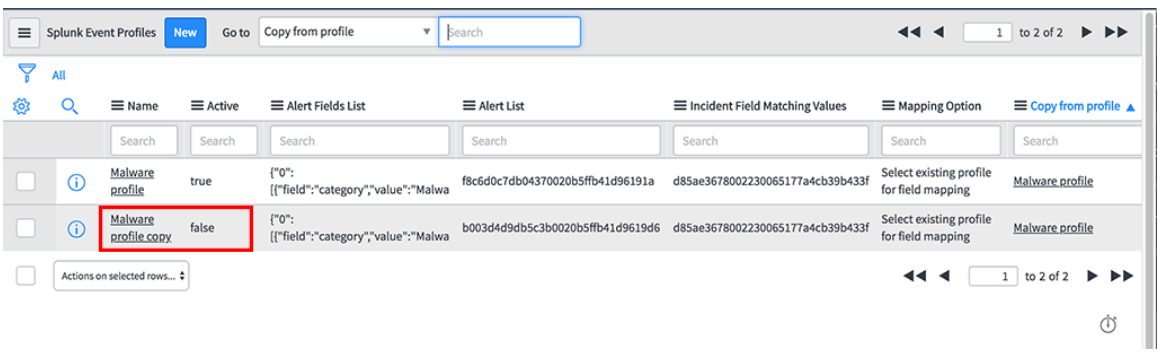
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Splunk Integration** > **Profil d'événement Splunk**.
2. Dans la liste Profils d'événements Splunk qui s'affiche, sélectionnez un profil que vous souhaitez copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier**.



Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (`vrai`), la copie est désactivée à ce stade (`faux`). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil.

Que faire ensuite

Vous êtes invité à activer le nouveau profil une fois que vous avez terminé les étapes de configuration.

Configurez votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise

Si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise console pour cette intégration, installez et configurez le ServiceNow module complémentaire Security Operations Event Ingestion pour l'application dans Splunk Enterprise votre console d'entreprise ou votre Splunk instance Splunk Cloud.

Avant de commencer

Vérifiez que vous avez installé l'application pour cette intégration ServiceNow Store avant d'installer le module d'extension Splunkbase requis pour l'ingestion manuelle d'événements. Si vous n'avez pas installé l'application pour l'intégration à partir de , consultez ServiceNow StoreInstaller et configurer l'application ServiceNow pour l'intégration Splunk Enterprise Event Ingestion et suivez les instructions pour l'installer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : Now Platform administrateur (admin)

Pourquoi et quand exécuter cette tâche
L'installation et la configuration du ServiceNow module complémentaire Security Operations Event Ingestion sont facultatives.

Si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise console pour l'intégration, téléchargez, installez et configurez le ServiceNow module complémentaire Security Operations Event Ingestion pour Splunkbase dans Splunk Enterprise votre Splunk Enterprise console.

Ce ServiceNow module complémentaire d'extension est requis pour que les incidents de sécurité puissent être créés à partir d'événements exportés manuellement dans votre Now Platform instance. Ce ServiceNow module complémentaire d'ingestion d'événements de Security Operations pour Splunk Enterprise l'application est disponible sur splunkbase .

Pour le transfert manuel d'événements, vous pouvez identifier jusqu'à deux points de terminaison (instances) différents Now Platform dans votre Splunk Enterprise console. Vous transférez manuellement les événements au ou aux points de terminaison pour créer des incidents de sécurité. Par exemple, vous pouvez spécifier à la fois une instance de stockage intermédiaire (développement) et une instance de production. En spécifiant des instances distinctes et en nommant des workflows primaires et secondaires pour chaque instance, vous pouvez choisir où vous souhaitez transférer les différents événements.

Procédure

1. Si vous n'avez pas encore installé le ServiceNow module complémentaire Security Operations Event Ingestion pour Splunk Enterprise, procédez comme suit pour l'installer et le configurer.

   a. Accédez à splunkbase .

   b. Recherchez le module complémentaire ServiceNow Opérations de sécurité Security Operations Event Ingestion for Splunk Enterprise.

      Remarque : Vérifiez que vous avez sélectionné ServiceNow Opérations de sécurité le module complémentaire d'ingestion d'événements pour Splunk Enterprise. Il existe d'autres ServiceNow addons qui sont affichés dans cette liste. Ces modules complémentaires sont destinés à différentes ServiceNow Splunk intégrations et ne sont pas requis pour cette intégration.

   c. Téléchargez l'application.

   d. Ouvrez votre Splunk Enterprise compte.

   e. Sur la page Applications, cliquez sur l'icône d'engrenage ou sur le raccourci **Gérer les applications** dans la liste déroulante du menu.

   f. Dans le coin supérieur gauche de la page Applications qui s'affiche, cliquez sur **Installer l'application à partir d'un fichier**.

   g. Cliquez sur **Choisir un fichier**, sélectionnez ServiceNow Security Operations Event Ingestion Addon pour Splunk Enterprise, puis cliquez sur **Télécharger**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

h. Si vous y êtes invité, redémarrez Splunk Enterprise.
Le module complémentaire Splunk Enterprise d'ingestion ServiceNow d'événements pour Security Operations est installé dans votre Splunk Enterprise console d'entreprise. L'étape suivante pour configurer l'Addon.

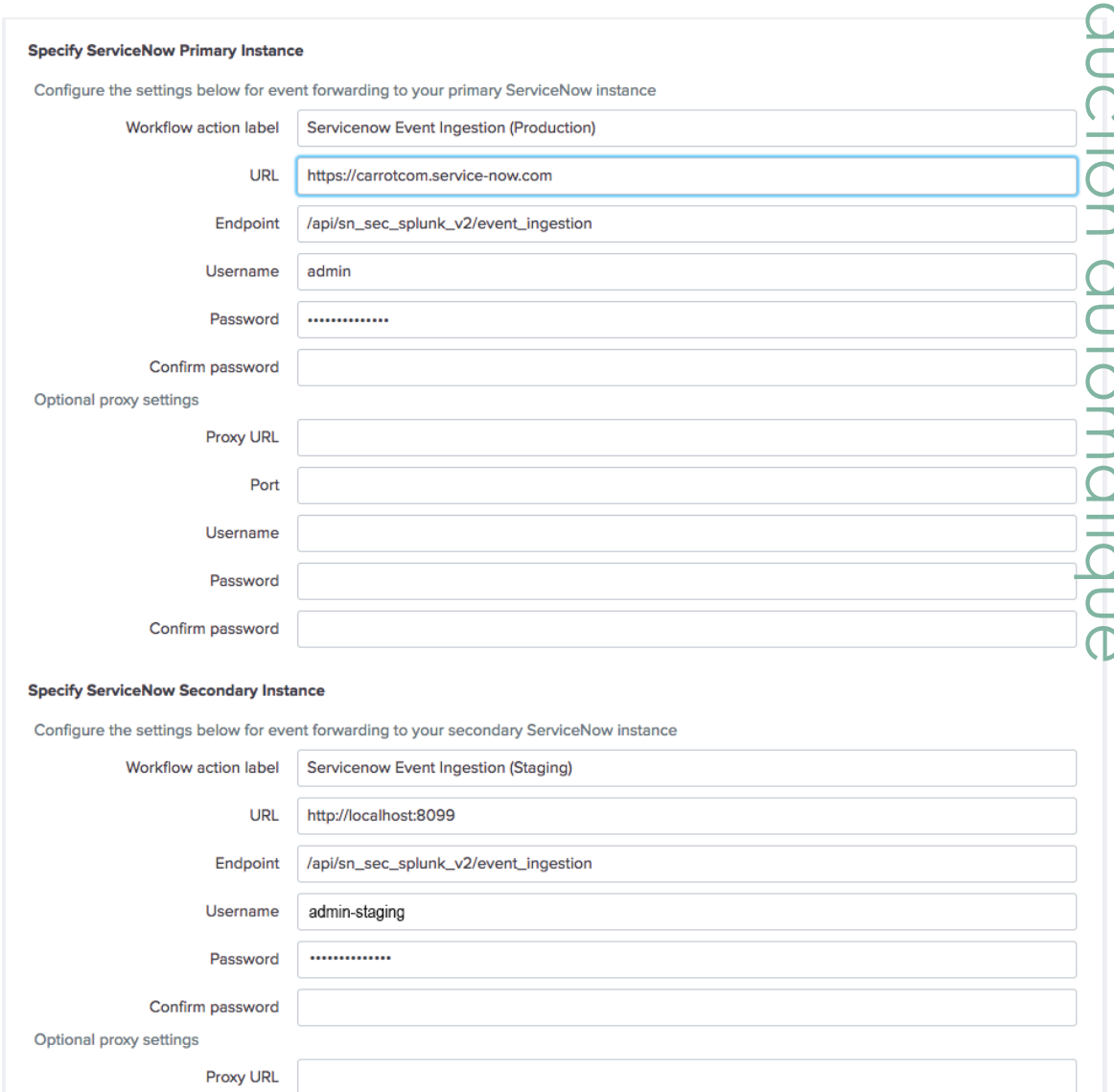
2. Pour configurer le complément, procédez comme suit.

a. Dans Splunk Enterprise, cliquez sur l'icône **d'engrenage Applications** ou sur **Gérer les applications** dans la liste déroulante du menu.

b. Dans la liste des applications qui s'affiche, dans la colonne **Actions** , cliquez sur **Configurer** pour ServiceNow Opérations de sécurité le complément d'ingestion d'événements pour Splunk Enterprise.

c. Remplissez le formulaire.

La figure suivante est un exemple de formulaire rempli dans votre Splunk Enterprise console.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ dans la section Spécifier l'instance primaire ServiceNow	Description
Étiquette de l'action de workflow	Nom du workflow pour votre Now Platform instance de production (principale). Ce nom est le nom d'une Now Platform instance que les utilisateurs qui surveillent les Splunk événements identifient comme instance principale, par exemple, Servicenow Event Ingestion (Production). La valeur par défaut pour ce champ est Ingestion d'événements ServiceNow (production). Dans votre Splunk Enterprise console, ce nom de workflow s'affiche pour l'instance de production (principale) dans la liste déroulante `Actions d'événement` développée d'une recherche. Ce nom est le nom de votre instance de production. Vous pouvez modifier le nom.
URL	URL de l'instance Now Platform que vous avez saisie dans le champ Étiquette de l'action de workflow précédent. Copiez l'URL dans votre navigateur et collez-la dans ce champ du formulaire.
Point de terminaison	Chemin de l'API de base. Pour plus d'informations, reportez-vous à la figure qui suit le tableau. Si vous n'avez pas de valeur pour le point de terminaison de votre Now Platform instance de production, procédez comme suit. **a.** Connectez-vous à votre Now Platform instance de production en tant qu'utilisateur disposant du rôle d'administrateur système (admin). **b.** `Entrez les API REST basées sur un script` dans le panneau de navigation. **c.** Une fois le panneau de navigation actualisé, sélectionnez le module **API REST scripté** qui s'affiche. **d.** Si l'ingestion d'événement n'est pas répertoriée dans la colonne Nom de la liste API `REST scriptées` qui s'affiche, dans le champ de recherche en haut, saisissez `l'ingestion d'événement`. **e.** Dans la colonne Chemin d'accès de l'API de base sur la page actualisée, copiez

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

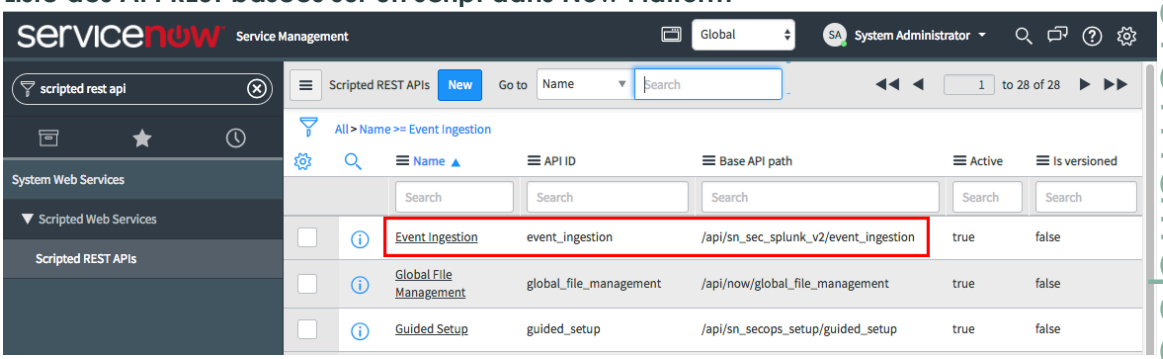
Champ dans la section Spécifier l'instance primaire ServiceNow	Description
	cette valeur et collez-la dans le champ Point de terminaison du formulaire. Un exemple de chemin d'accès de l'API de base est `/api/sn_sec_splunk_v2/event_ingestion`.
Nom d'utilisateur	Nom d'utilisateur de votre Now Platform instance. Ce nom est le nom d'utilisateur de l'instance Now Platform dans laquelle vous avez affecté un utilisateur avec le rôle (sn_sec_splunk_v2.api_account_access) pour le transfert manuel d'événements. Pour en savoir plus sur l'affectation de ce rôle, reportez-vous à Configurer votre Now Platform instance pour l'intégration Splunk Enterprise Event Ingestion.
Mot de passe	Mot de passe de votre Now Platform instance. Ce mot de passe est le mot de passe de l'instance Now Platform dans laquelle vous avez affecté un utilisateur avec le rôle (sn_sec_splunk_v2.api_account_access) pour le transfert manuel d'événements.
(Facultatif) Champs dans la section Spécifier l'instance secondaire ServiceNow	Description Ces champs sont facultatifs. Vous n'êtes pas obligé de spécifier une instance secondaire.
Étiquette de l'action de workflow	Nom du workflow pour votre Now Platform instance secondaire (intermédiaire). Ce nom correspond au nom d'une Now Platform instance que les utilisateurs qui surveillent les Splunk événements identifient comme instance secondaire, par exemple, ServiceNow Ingestion d'événements (intermédiaire). Dans votre Splunk Enterprise console, ce nom de workflow s'affiche pour l'instance intermédiaire (secondaire) dans la liste déroulante Actions d'événement développée d'une recherche. Cette Now Platform instance est votre instance intermédiaire. Vous pouvez modifier le nom.
URL	URL de l'instance Now Platform que vous avez saisie dans le champ Étiquette de l'action de workflow précédent pour l'instance secondaire Now Platform .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ dans la section Spécifier l'instance primaire ServiceNow	Description
	Copiez l'URL dans votre navigateur et collez-la dans ce champ du formulaire.
Point de terminaison	Chemin de l'API de base. Cette valeur du chemin d'accès de l'API de base pour votre instance secondaire est la même que celle du chemin de l'API de base pour votre instance primaire. Consultez la figure précédente du formulaire pour plus d'informations.
Nom d'utilisateur	Nom d'utilisateur de votre Now Platform instance de stockage intermédiaire. L'utilisateur doit disposer du rôle (sn_sec_splunk_-v2.api_account_access).
Mot de passe	Mot de passe de votre Now Platform instance de stockage intermédiaire. L'utilisateur doit disposer du rôle (sn_sec_splunk_-v2.api_account_access).

La figure suivante est un exemple de la liste des API REST scriptées dans votre Now Platform. La liste affiche l'emplacement de la valeur de point de terminaison d'une Now Platform instance que vous entrez dans le formulaire dans le cadre de la configuration ServiceNow du module complémentaire Security Operations Event Ingestion pour extension dans Splunk Enterprise votre Splunk Enterprise console.

Liste des API REST basées sur un script dans Now Platform



3. Dans le formulaire de configuration de votre Splunk Enterprise console, cliquez sur **Enregistrer** pour enregistrer vos modifications.

   Après quelques instants, en haut à gauche du formulaire de votre Splunk Enterprise console, un message s'affiche indiquant que l'enregistrement a été mis à jour.

   Une fois le formulaire enregistré, les noms (étiquettes d'action de workflow) de votre Now Platform ou vos instances que vous avez créées dans le formulaire sont disponibles dans la liste de choix Actions d'événement sur un événement sélectionné d'une recherche dans votre Splunk Enterprise console.

Que faire ensuite

Si vous n'avez pas encore enregistré les recherches dans votre Splunk Enterprise console, l'étape suivante consiste à enregistrer les recherches en tant qu'alertes dans votre Splunk Enterprise console.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrer les recherches de l'intégration dans votre Splunk EnterpriseSplunk Enterprise Event Ingestion console

Les étapes suivantes d'enregistrement des recherches dans votre Splunk Enterprise console sont fournies pour un utilisateur disposant du rôle administrateur Splunk Enterprise .

Avant de commencer

Si vous avez déjà des recherches enregistrées et des alertes déclenchées dans votre Splunk Enterprise console, vous n'êtes pas obligé de modifier ces recherches pour cette intégration.

L'intégration du produit au service de notification d'événement Splunk extrait les informations sur les Now Platform® Opérations de sécurité événements et les alertes de Splunk.

Avant d'ingérer des alertes dans votre Opérations de sécurité environnement, configurez les recherches dans votre Splunk Enterprise console afin d'extraire automatiquement les événements de sécurité pertinents que Splunk Enterprise vous souhaitez enregistrer en tant qu'alertes.

Si vous n'avez pas enregistré vos recherches et déclenché des alertes établies pour vous avertir lorsque des événements de sécurité importants se produisent dans votre Splunk Enterprise console, procédez comme suit pour enregistrer les recherches.

Rôle requis : Splunk Enterprise administrateur

Procédure

1. Connectez-vous à votre compte Splunk Enterprise.
2. Cliquez sur l'onglet **Rechercher** .
3. Dans le champ Nouvelle recherche qui s'affiche, saisissez une valeur pour l'alerte, par exemple Programme malveillant.
4. Pour afficher les événements associés à votre recherche, à droite du champ Nouvelle recherche, cliquez sur l'icône de recherche ou appuyez sur Entrée.
   Les résultats de la recherche avec les événements s'affichent.
5. Pour enregistrer la recherche en tant qu'alerte, dans le coin supérieur droit de la page, développez la liste de choix Enregistrer sous et sélectionnez **Alerte**.
6. Dans le formulaire qui s'affiche, renseignez les champs.

Champ	Description
Titre	Nom descriptif de l'alerte, par exemple, Événements de programme malveillant. Une fois que vous avez enregistré cette recherche en tant qu'alerte, les événements d'une alerte déclenchée dans le service sont automatiquement traités en alertes déclenchées à l'aide Splunk de ces données de recherche. Ce titre d'alerte déclenchée est utilisé dans le profil d'événement que vous créez dans votre Now Platform instance pour identifier les événements qui sont ingérés dans votre instance pour Now Platform® Réponse aux incidents de sécurité SIR la création d'un incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
(Facultatif) Description	Texte pour vous aider à distinguer cette alerte des autres alertes.
Type d'alerte	Dans les champs qui s'affichent, sélectionnez **Planifié** pour rechercher cette alerte dans une planification ou **Temps réel** pour rechercher cette alerte en continu.
Résultats du déclencheur	Vous préférez peut-être définir l'une des conditions de filtre suivantes : ◦ Le nombre de résultats est supérieur ou inférieur à ◦ Unique (une fois) pour chaque résultat
Actions de déclencheurs	Ajoutez des actions pour déclencher cette alerte. Développez la liste Ajouter un choix et cliquez sur **Ajouter aux alertes déclenchées** pour qu'elle s'affiche sur le formulaire. Vous préférerez peut-être ce paramètre pour les alertes que vous ingérez dans votre Now Platform instance.

7. Cliquez sur **Enregistrer**.
   Votre alerte est enregistrée et s'affiche sous l'onglet Alertes de la page de recherche. Le Splunk service extrait les événements en faisant correspondre les critères que vous avez configurés dans l'alerte. Il met en cache les événements, puis vous demandez ces événements à partir des profils que vous avez configurés dans votre Now Platform instance. Étant donné que l'ingestion-pull d'événements se produit à partir d'un cache dans le service, cette ingestion à partir de votre Now Platform n'a pas d'impact sur les Splunk performances de votre Splunk plateforme.

Que faire ensuite

Vous avez terminé avec succès la configuration requise pour l'intégration dans votre Splunk Enterprise console. Si vous n'avez pas encore installé l'application pour l'intégration à partir de , ServiceNow Storel'étape suivante consiste à installer l'application pour l'intégration et à la configurer.

Utiliser l'éditeur de script pour formater les valeurs d'alerte pour l'intégration Splunk Enterprise Event Ingestion

Utilisez l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage.

Avant de commencer

Outre les champs directement mappés à partir des valeurs d'alerte extraites et les valeurs d'alerte que vous saisissez manuellement, vous pouvez éventuellement utiliser l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. L'éditeur de script modifie les valeurs d'une Splunk alerte afin que les valeurs prises en charge par l'incident Now Platform® Réponse aux incidents de sécurité de sécurité soient mappées aux champs Catégorie, Élément de configuration (CI) et Observable.

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Dans certains cas, Splunk Enterprise les valeurs d'alerte sont mappées aux champs Catégorie, Élément de configuration (CI) et Observable de l'incident SIR et ne sont pas prises

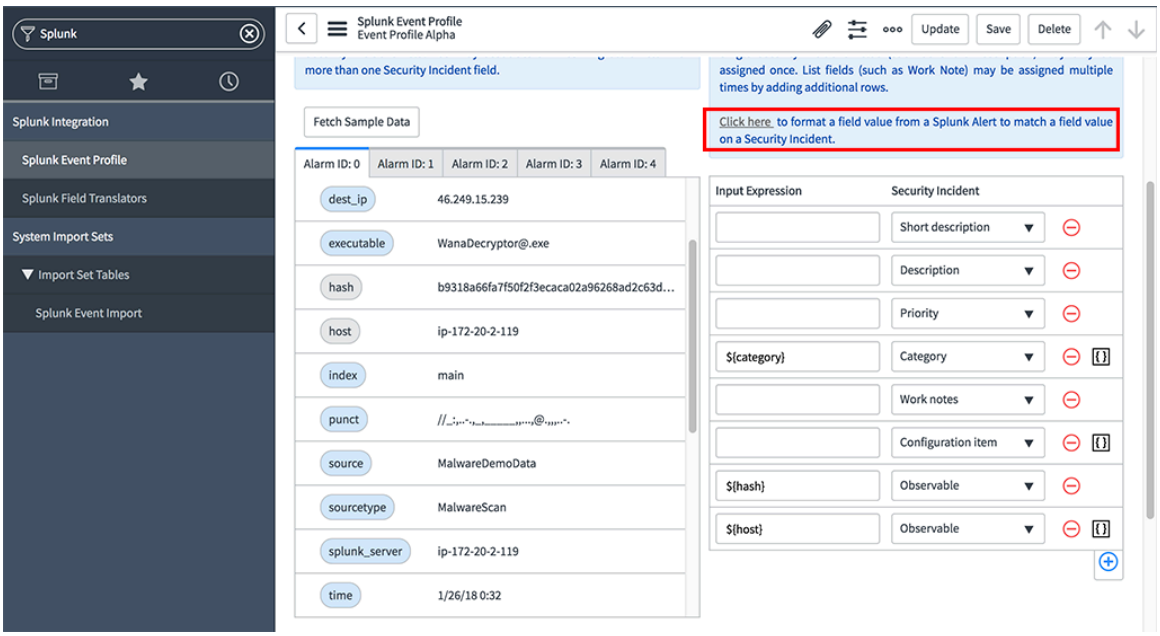
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

en charge. Vous préférez peut-être modifier les valeurs mappées. Si vous souhaitez convertir la valeur d'une Splunk Enterprise alerte en une valeur prise en charge par ces champs sur l'incident SIR de sécurité, utilisez l'éditeur de script.

Procédure

1. Une fois le formulaire de mappage affiché, cliquez sur le lien pour ouvrir l'éditeur de script.



2. Dans la liste de choix, sélectionnez un champ de destination pour la valeur que vous souhaitez modifier.
3. Dans la section Mappage de champs d'incidents SIR, vous pouvez également cliquer sur l'icône de crochet `[{}]` en regard d'un champ pour ouvrir l'éditeur de script relatif à ce champ.

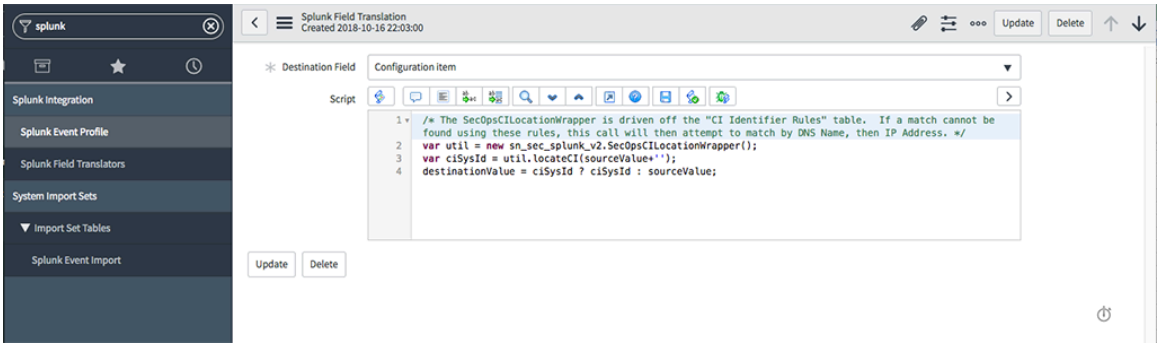
   Dans certains cas, un include de script peut être approprié pour le champ Élément de configuration. Pour une alerte, par exemple, une valeur pour l'élément de configuration peut ne pas correspondre.

   Comme le montre la figure suivante, si une correspondance pour un nom d'hôte est introuvable dans le Now Platform® CMBD pour le champ Élément de configuration, vous pouvez modifier la règle de sorte que, si une adresse IP est trouvée, elle remplisse le champ Élément de configuration. S'il n'y a pas de valeur pour l'alarme, le champ de l'incident de sécurité est défini sur null.

   L'éditeur s'ouvre avec le champ affiché dans Champ de destination. L'image suivante montre l'éditeur avec le champ `Élément de configuration` comme champ de destination.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Entrez toutes les modifications dans le script, puis cliquez sur **Mettre à jour** pour enregistrer vos modifications.
   La Splunk table Traductions de champ s'affiche.
5. Fermez la table pour revenir au formulaire de mappage.

Liste de vérification pour l'intégration Splunk Enterprise Event Ingestion

Utilisez cette liste de vérification pour vous guider dans toutes les tâches de l'intégration. La liste de vérification suivante comprend les tâches de configuration et d'installation, ainsi que des exemples de cas d'utilisation incluant les résultats attendus pour l'intégration.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Suivez la progression de l'installation, de l'installation et de la configuration de l'intégration à l'aide de la table suivante. Terminez toutes les tâches d'une étape avant de passer à l'étape suivante. Chaque ligne du tableau répertorie les tâches et identifie les rôles requis pour effectuer les tâches. Les rubriques numérotées du guide d'installation et de configuration sont également référencées.

Rôles requis : les rôles sont répertoriés pour chaque étape ci-dessous.

Procédure

1. En tant qu'utilisateur disposant du Now Platform rôle administrateur, configurez votre Now Platform instance.
   - Affectez des utilisateurs ayant les rôles sn_si.admin et sn_si.analyst, selon les besoins.
   - Installez et configurez un serveur MID si le Splunk serveur est déployé au sein de votre réseau d'entreprise.
   - Vérifiez que les modules d'extension ServiceNow Réponse aux incidents de sécurité sont activés pour votre version du Now Platformfichier .
   - Si vous souhaitez transférer manuellement des événements de votre Splunk Enterprise console vers votre Now Platform instance, vérifiez que vous avez affecté le rôle (sn_sec_splunk_v2.api_account_access) à un utilisateur ayant l'autorisation d'administrateur d'entreprise Splunk Enterprise .

   Pour plus d'informations, consultez Configurer votre Now Platform instance pour l'intégration Splunk Enterprise Event Ingestion.

   Vous avez terminé avec succès les étapes de configuration et vérifié les résultats attendus pour l'intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. En tant qu'utilisateur disposant du Now Platform rôle administrateur, installez et configurez l'application Splunk Enterprise Event Ingestion à partir du ServiceNow Store.
   a. Téléchargez et installez l'application sur votre Now Platform instance.
   b. Configurez l'application et connectez-vous à votre Splunk Enterprise console.

   Pour plus d'informations, consultez Installer et configurer l'application ServiceNow pour l'intégration Splunk Enterprise Event Ingestion.

3. Facultatif : Si vous avez l'intention d'exporter manuellement des événements de votre Splunk Enterprise console vers votre Now Platform instance, effectuez les tâches suivantes :
   a. En tant qu'administrateur Splunk Enterprise , installez, configurez et activez le ServiceNow module complémentaire Security Operations Event Ingestion pour Splunk Enterprise à partir de splunkbase dans votre Splunk Enterprise console.
   b. En tant qu'administrateur Splunk Enterprise , si ce n'est pas déjà fait, enregistrez les recherches en tant qu'alertes dans votre Splunk Enterprise console.

      (Optional) Pour plus d'informations, consultez Configurez votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise et Enregistrer les recherches de l'intégration dans votre Splunk EnterpriseSplunk Enterprise Event Ingestion console.

4. En tant qu'utilisateur disposant du Now Platform rôle sn_si.admin, créez et nommez un profil d'événement.

   Sélectionnez le type de profil dans la liste de choix. Les options sont un profil d'alerte planifiée que vous utilisez pour ingérer des exemples de données ou un profil d'événement que vous utilisez pour exporter manuellement des données de pièce jointe à partir de votre Splunk Enterprise console.

   - Pour une alerte planifiée, sélectionnez une alerte disponible.
   - Pour le profil des données exportées manuellement, créez une nouvelle carte ou copiez une carte existante.

   Pour plus d'informations, consultez Créer et nommer un profil d'événement pour l'intégration Splunk Enterprise Event Ingestion.

5. En tant qu'utilisateur disposant du Now Platform rôle sn_si.admin, mappez les valeurs ingérées ou les données de pièce jointe exportées Splunk Enterprise vers Now Platform les incidents de sécurité.
   a. Extrayez des exemples de données pour une alerte planifiée.
   b. Exporter manuellement des données de pièce jointe à partir d'un Splunk Enterprise événement.
   c. Modifiez la configuration de mappage par défaut.
   d. Vous pouvez également ajouter des critères de filtrage, ajouter une alerte à un incident de sécurité existant et utiliser l'éditeur de script.

   Pour plus d'informations, reportez-vous aux sectionsMapper les alertes et les événements pour l'intégration Splunk Enterprise Event Ingestion et Alertes de carte pour l'intégration Splunk Enterprise Event Ingestion.

6. En tant qu'utilisateur disposant du Now Platform rôle sn_si.admin, prévisualisez les données qui Splunk Enterprise s'affichent sur un Now Platform incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Corrigez les erreurs ou ajoutez des données manquantes afin qu'aucun message d'erreur ne s'affiche.

Pour plus d'informations, consultez Prévisualiser l'incident de sécurité pour l'intégration Splunk Enterprise Event Ingestion.

7. En tant qu'utilisateur disposant du Now Platform rôle sn_si.admin, planifiez la récupération d'alerte pour un profil avec une alerte planifiée.

   Pour plus d'informations, consultez Planifier et récupérer les alertes pour l'intégration Splunk Enterprise Event Ingestion.

Splunk Enterprise Security Intégration de l'ingestion d'événements pour Opérations de sécurité par ServiceNow

L'intégration Splunk Enterprise Security de l'ingestion d'événements notables avec le Réponse aux incidents de sécurité produit (SIR) permet aux analystes d'incidents de sécurité de collecter et de traiter des données d'événements notables (appelées notables).

Vue d'ensemble

Les données sont ingérées en continu en fonction d'un calendrier d'interrogation configuré et sont utilisées par les analystes pour identifier les cybermenaces potentielles et y répondre. Les événements de sécurité qui sont collectés peuvent être corrélés à des événements notables dans Splunk Enterprise Security cette intégration, puis ingérés automatiquement avec cette intégration. En outre, les événements notables individuels peuvent être transférés manuellement à la demande à partir de la console d'examen Splunk Enterprise Security des incidents et de l'interface de génération de rapports vers le Réponse aux incidents de sécurité produit de pour Now Platform créer des incidents de sécurité.

Cette intégration fournit à un analyste du centre des opérations de sécurité (SOC) une visibilité sur les événements notables et les données connexes sur les événements contributifs. Ces données peuvent être intégrées dans Now Platform Réponse aux incidents de sécurité (SIR) des incidents de sécurité pour une enquête et une correction plus approfondies. Les profils sont créés dans votre Now Platform instance pour gérer différents types d'événements notables créés via des recherches de corrélation dans Splunk Enterprise Security. Ces profils personnalisent l'affichage des différents Splunk champs d'événement dans SIR les incidents de sécurité.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

- Créez plusieurs profils d'ingestion d'événements notables pour créer des incidents de sécurité SIR pour des types de menaces spécifiques tels que l'hameçonnage, les programmes malveillants et les tentatives d'accès non autorisé.
- Créez plusieurs profils d'événements pour le transfert d'événements à la demande à partir de votre Splunk ES console d'examen des incidents afin de créer des incidents de sécurité SIR.
- Glisser-déplacer le mappage des valeurs de champ d'événement Splunk notables vers les champs d'incident de sécurité SIR associés.
- Aperçu de la mise en page de l'incident de sécurité basée sur des SIR exemples d'événements notables pour valider les détails du mappage d'événements.
- Ingérer les événements notables historiques, ainsi que les événements notables en cours, nouveaux et mis à jour à intervalles configurables.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Filtrez les événements notables qui ne répondent pas aux critères de génération d'incidents SIR, par exemple, les événements de faible priorité, les événements qui n'ont pas encore atteint un état spécifique, etc.
- Regroupez les événements ou les alertes concernant les incidents de sécurité existants SIR en fonction des valeurs de champ correspondantes pour éviter les incidents de sécurité en double.
- Mettre à jour les événements notables en fonction des conditions de création et/ou de fermeture d'incident SIR via une interface bidirectionnelle pour synchroniser Splunk ES les mises à jour des événements notables avec l'état de l'incident ServiceNow SIR.

Versions prises en charge Now Platform

Le module d'extension com.snc.si_dep est requis pour cette intégration. Ce module d'extension installe automatiquement toutes les dépendances nécessaires à la prise en charge du Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications.

Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour garantir une installation fluide :

1. Cadre de travail de Security Integration
2. Security Support Common
3. Réponse aux incidents de sécurité

Pour plus d'informations sur l'installation des Opérations de sécurité applications principales, consultez et .

ServiceNow Modules complémentaires

Le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk ES n'est requis que si vous préférez transférer manuellement les événements depuis votre Splunk Enterprise Security console d'examen des incidents vers votre Now Platform instance. Cet ServiceNow addon est disponible dans splunkbase .

Ce ServiceNow module complémentaire d'ingestion d'événement de sécurité pour Splunk Enterprise l'application dans Splunkbase n'est pas requis pour l'ingestion d'alerte automatisée prise en charge par l'intégration.

Versions prises en charge par Splunk

Cette intégration a été testée avec Splunk Enterprise la version 8.0.1 et avec Splunk Enterprise Security la version d'application 6.2.1.

Serveur MID

Cette intégration nécessite l'installation et la configuration d'un serveur MID Server dans votre Now Platform® instance pour se connecter au Splunk service lorsque le Splunk serveur est déployé au sein de votre réseau d'entreprise. Si vous utilisez le Splunk Cloud service, un serveur MID n'est pas nécessaire. Voir Serveur MID pour plus d'informations sur les serveurs MID.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Références

Référence	Identificateur de document	Titre de document
1	Splunk Site web du produit	Site Web du produit Splunk Enterprise Security .

Liste de vérification

Pour obtenir une liste de contrôle imprimable de ces sujets, reportez-vous à la section Liste de vérification pour l'intégration de l'ingestion d'événements Splunk Enterprise Security notables. Vous pouvez utiliser cette liste pour surveiller votre progression au fur et à mesure que vous accomplissez les tâches de l'intégration.

Termes clés utilisés dans cette intégration

Cette section décrit certains des termes clés utilisés dans cette intégration.

Les termes clés suivants sont utilisés lors de l'installation et de la configuration. Pour plus d'informations sur ces conditions, consultez le site Web de la documentation produit ServiceNow et le site Web et les ressources Splunk sur la page Ressources Splunk .

Now Platform

Un produit d'entreprise ServiceNow Il Now Platform s'agit de la base sur laquelle reposent les composants individuels tels que Réponse aux incidents de sécurité (),SIR IT Service Management (ITSM) et d'autres produits.

ServiceNow Complément Splunkbase

Une ServiceNow application installée sur votre Splunk Enterprise Security console qui prend en charge l'option de transfert manuel d'événements de l'intégration. Le transfert manuel d'événements est une fonctionnalité facultative de l'intégration. Ce ServiceNow module complémentaire Splunkbase n'est pas requis pour l'ingestion automatisée d'événements notables fournie par l'intégration qui extrait les événements à partir de Splunk.

Réponse aux incidents de sécurité (SIR)

Application Now Platform qui suit la progression des incidents de sécurité, depuis la détection et l'analyse initiale, en passant par le confinement, l'éradication et la récupération, jusqu'à l'examen final et la fermeture post-incident.

Splunk Enterprise Security

Splunk Enterprise Security aide les équipes à bénéficier d'une visibilité et d'une intelligence de sécurité à l'échelle de l'organisation pour la surveillance continue, la réponse aux incidents, les opérations SOC et fournit aux dirigeants une fenêtre sur les risques commerciaux. Splunk Enterprise Security est une solution de sécurité premium nécessitant une licence payante. Ce service se trouve sur un hôte ou une offre cloud Splunk qui est appelée Splunk console dans ce guide.

Splunk Enterprise Security Événement notable

Lorsqu'une recherche de corrélation identifie un événement ou un modèle d'événements, elle crée un événement notable. Les recherches de corrélation filtrent les données de sécurité et établissent une corrélation entre les événements pour identifier un type particulier d'incident (ou un modèle d'événements), puis créer des événements notables.

Splunk événement

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un ou plusieurs éléments de données qui entraînent les événements notables du Splunk service. À partir de votre Now Platform instance, vous pouvez rechercher les événements qui Splunk ont déclenché Now Platform des incidents de sécurité.

Serveur MID

Cette application facilite la communication et le mouvement de données entre les applications, sources de Now Platform données et services externes. Cette application est généralement requise pour l'intégration avec les technologies locales et, pour cette Splunk Enterprise Security intégration d'ingestion d'événementsSplunk Enterprise Security, le serveur MID facilite la communication entre l'instance Now Platform locale et . Un serveur MID n'est pas nécessaire si vous intégrez votre Now Platform instance à une Splunk Cloud instance.

Administrateur d'incident de sécurité (sn_si.admin)

L'utilisateur disposant de ce rôle supervise la configuration de l'intégration au SIR produit dans votre Now Platform instance.

Analyste des incidents de sécurité (sn_si.analyst)

L'utilisateur disposant de ce rôle interagit avec les incidents de sécurité du ServiceNow Réponse aux incidents de sécurité produit et les analyse.

Installez et configurez l'application ServiceNow pour l'intégration d'ingestion d'événements Splunk Enterprise Security notables

Avant d'exécuter l'intégration sur votre Now Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre Réponse aux incidents de sécurité correctement aux produits et Opérations de sécurité sur votre Now Platform® instance.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Si vous n'avez pas installé l'application d'ingestion d'événements Splunk Enterprise SecurityServiceNow Store à partir de pour l'intégration, consultez et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette Ingestions d'événements Splunk .
3. Pour configurer l'application, cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Si un bouton **Configurer** s'affiche sur une mosaïque, cliquez dessus pour modifier une configuration existante.
5. Dans la boîte de dialogue Configuration des ingestions d'événements qui s'affiche, renseignez les champs.

Champ	Description
Nom	Nom de la console ou Splunk Cloud de l'instance Splunk Enterprise Security utilisée pour l'intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge. Par exemple, saisissez `SplunkES2`.
URL de Base de l'API Splunk	URL de votre console ou Splunk Cloud de votre Splunk Enterprise Security instance. L'URL doit inclure le port API, par exemple : `https://mysplunkserver.com:8089`
Authentification de base	La valeur par défaut est désactivée. Si vous utilisez le nom d'utilisateur du compte API et le mot de passe API pour la configuration, cochez la case.
Nom d'utilisateur du compte API	Nom d'utilisateur que vous avez créé pour votre compte utilisateur API dans la Splunk Enterprise Security console.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mot de passe API	Mot de passe que vous avez créé pour votre compte utilisateur API dans la Splunk Enterprise Security console.
Basé sur un jeton (disponible à partir de la version 12.0.0)	Jeton que vous avez créé pour votre compte d'utilisateur API sur la console Splunk Enterprise Security.
Jeton	Jeton que vous avez créé pour votre compte d'utilisateur API sur la Splunk console Enterprise Security.
Déploiement sur site	La valeur par défaut est désactivée. Si vous utilisez une version sur site de Splunk Enterprise Security, vérifiez que cette case est cochée.
Serveur MID	Option permettant de choisir un serveur MID particulier à configurer dans votre environnement, qui sera utilisé par cette intégration pour extraire les événements notables vers ServiceNow. Vous pouvez sélectionner un serveur MID spécifique dans la liste ou sélectionner **n'importe lequel** pour activer la sélection automatique d'un serveur MID valide dans la liste pour cette intégration. **Remarque :** ◦ Le serveur MID sélectionné pendant cette période de configuration s'applique à l'ensemble de cette intégration. ◦ Seuls les MID Servers actifs et validés sont affichés dans cette liste. Par défaut, cette valeur est définie sur **N'importe lequel**. Par exemple, il existe trois MID Servers A, B et C. Si vous sélectionnez **N'importe lequel**, l'un de ces MID Servers est automatiquement sélectionné et s'applique à l'ensemble de cette intégration. Si vous sélectionnez un serveur MID spécifique, disons C, le C du serveur MID sélectionné s'applique à l'ensemble de cette intégration. Si vous souhaitez modifier le MID Server, vous devez le reconfigurer à partir de la vignette Configuration de l'application.

La figure suivante est un exemple de formulaire rempli pour la configuration d'une version locale avec Splunk Enterprise Security un MID Server.

Traduction automatique

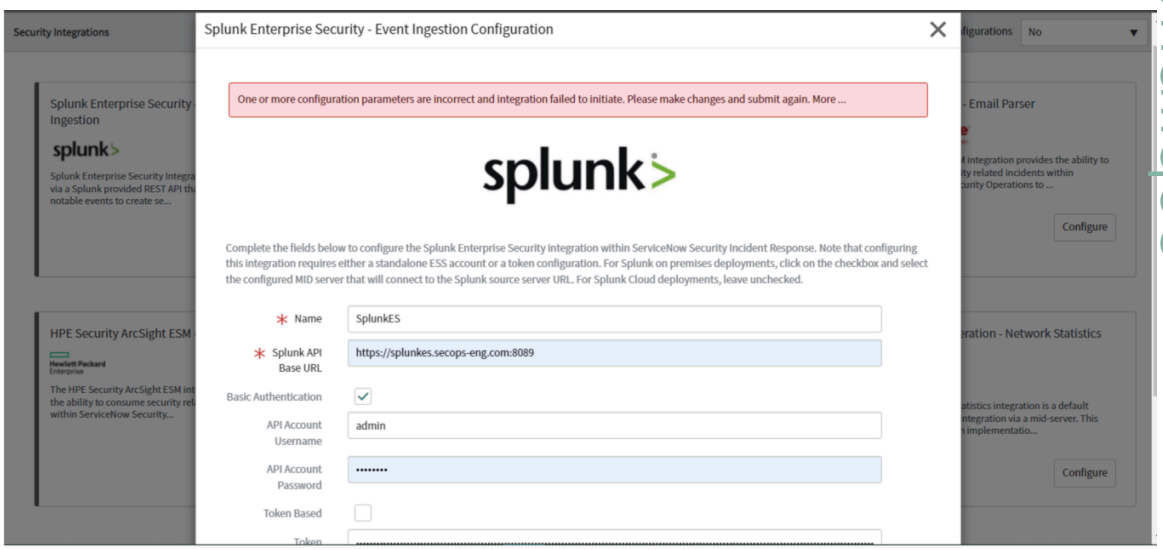
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Chaque Splunk Enterprise Security type d'événement notable que vous ingérez à partir de votre Splunk Enterprise Security console d'examen d'incident nécessite un profil d'événement unique dans votre Now Platform® instance. Toutefois, la source que vous configurez sur le formulaire de configuration des ingestions d'événements peut être réutilisée pour plusieurs Now Platform® profils, à condition que chaque profil ingère des types d'événements notables uniques.

6. Cliquez sur **Envoyer**.
   Une fois la validation terminée, la page Intégrations de sécurité s'affiche avec chacune de vos configurations. Sur chaque vignette de configuration valide, les boutons **Mettre à jour** et **Supprimer** sont affichés, comme illustré dans la figure suivante.

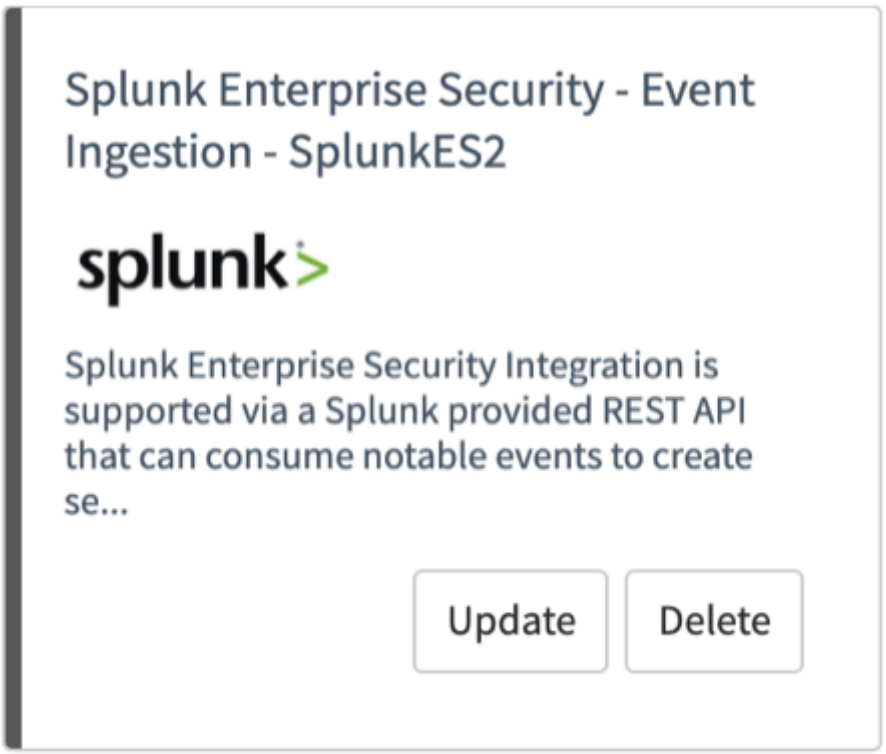
Remarque : Les utilisateurs doivent utiliser soit l'authentification de base, soit l'authentification basée sur les jetons. Si vous activez les deux, l'erreur suivante s'affiche.



Remarque : Si les utilisateurs préfèrent mettre à jour les vignettes de configuration existantes en fonction des jetons, ils doivent activer Activer ce paramètre pour mettre à jour les configurations sources existantes Splunk pour le paramètre de prise en charge de l'authentification basée sur les jetons dans le Splunk module Paramètres d'entreprise.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois validée et soumise, chaque configuration du serveur d'ingestions d'événements Splunk est enregistrée sous forme de vignette dans la page Intégrations de sécurité. Si vos vignettes de configuration enregistrées ne s'affichent pas sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste Afficher les configurations, sélectionnez **Oui**.

Que faire ensuite

Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer un profil d'événement.

Configurer les Splunk paramètres de sécurité d'entreprise

Utilisez les paramètres de sécurité d'entreprise Splunk (ES) pour modifier les configurations prédéfinies et leurs valeurs en fonction de vos besoins.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Intégration de Splunk ES** > **Paramètres Splunk ES**.
2. Renseignez les champs du formulaire.

Paramètres Splunk ES

Champ	Description
Appliquez une limite au nombre d'événements notables qui peuvent être regroupés en un seul incident.	Option permettant d'appliquer une limite au nombre de vos événements notables que vous souhaitez regrouper en un seul incident.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par défaut, cette valeur est définie sur 100.
Appliquer une limite au nombre d'incidents de sécurité qui peuvent être créés dans un délai de 24 heures.	Option permettant d'appliquer une limite au nombre d'incidents de sécurité qui peuvent être créés dans une période de 24 heures. Par défaut, cette valeur est définie sur 1 000.
Appliquer une limite au nombre de valeurs à analyser dans chaque champ reçu de Splunk.	Option permettant d'appliquer une limite au nombre de valeurs que vous souhaitez analyser pour chaque champ reçu de Splunk. Par défaut, cette valeur est définie sur 1 000.
Nombre de règles de corrélation à extraire Splunk.	Option permettant de définir le nombre de règles de corrélation à extraire de .Splunk Par défaut, cette valeur est définie sur 500.
Paramètre de durée de vie de la Splunk tâche de recherche, en secondes.	Option permettant de définir le paramètre Time-to-Live pour la Splunk recherche sous la forme de secondes. Par défaut, cette valeur est définie sur 600.
Nombre de types notables à regrouper en une seule recherche.	Option permettant de définir le nombre total de types notables que vous souhaitez regrouper en une seule recherche. Par défaut, cette valeur est définie sur 20.
Nombre de jours de conservation des métadonnées de la Splunk tâche de recherche dans ServiceNow	Option permettant de définir le nombre de jours pendant lesquels vous souhaitez conserver les métadonnées de la tâche de recherche Splunk dans ServiceNow. Par défaut, cette valeur est définie sur 30.
Caractère de délimitation pour diviser les valeurs dans les mappages de champs.	Option permettant de définir le caractère de délimitation pour fractionner les valeurs dans les mappages de champs. Par défaut, la valeur est définie sur (,).
Nombre de minutes de chevauchement à ajouter lors de l'extraction des événements Splunk (pour surmonter le délai d'indexation de Splunk)	Option permettant de définir le nombre de minutes de chevauchement à ajouter lors de la récupération des événements Splunk pour surmonter le délai d'indexation à partir de Splunk. Par défaut, cette valeur est définie sur 30.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Transmettre par pull les événements notables mis à jour	Option permettant de récupérer les événements notables mis à jour. Par défaut, cette valeur est définie sur Non.
Activez ce paramètre pour mettre à jour les configurations sources existantes Splunk pour la prise en charge de l'authentification basée sur le jeton. Vous devez mettre à jour la configuration d'intégration avec les détails du jeton après l'activation de ce paramètre.	Option permettant de mettre à jour la configuration source existante Splunk vers la prise en charge de l'authentification basée sur le jeton à partir d'une version existante. **Remarque :** Après la mise à niveau vers la nouvelle version, le champ Jeton devient indisponible. Vous devez activer ce paramètre pour obtenir l'authentification basée sur le jeton, après quoi vous devez mettre à jour la configuration d'intégration avec les détails du jeton. Par défaut, cette valeur est définie sur Non.

3. Cliquez sur **Enregistrer**.

Erreurs d'authentification

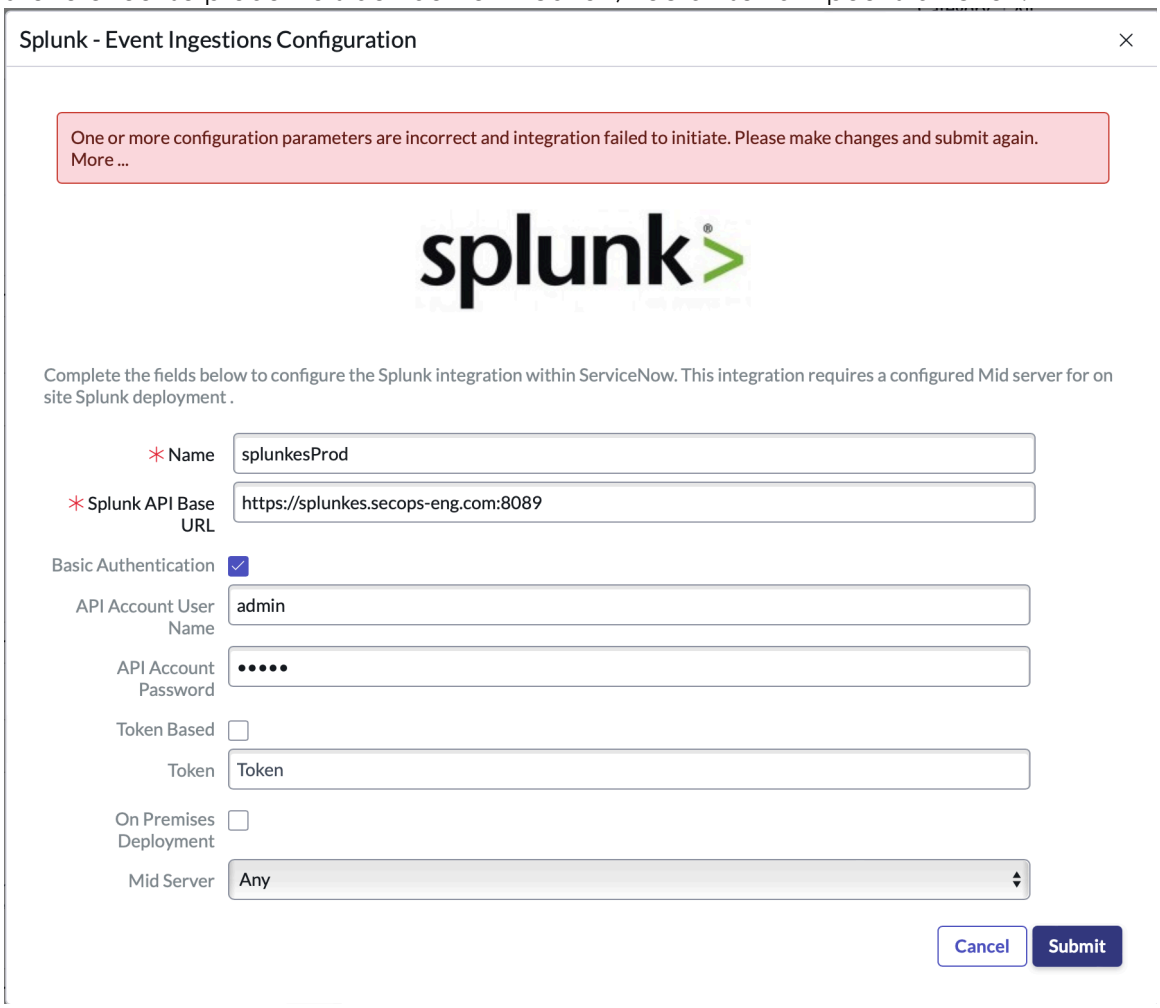
Cette section décrit certaines erreurs d'authentification courantes et comment elles peuvent être résolues.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

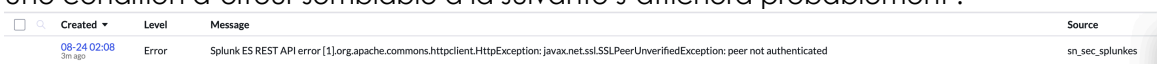
Problème de validation du certificat

Si une erreur se produit lors de l'authentification, l'écran suivant peut s'afficher :



Si vous avez vérifié que les informations d'identification de votre compte API et les informations de l'URL de base Splunk sont correctes, cette erreur peut être due à un problème avec le certificat Splunk pour la communication du port 8089. ServiceNow® L'instance nécessite un certificat valide avec un nom commun qui correspond au nom d'hôte du serveur pour établir des connexions sécurisées. Pour plus d'informations, consultez Certificats . Si cette erreur s'affiche, vous pouvez vérifier que le problème est dû à un problème de certificat en consultant les journaux système.

Une condition d'erreur semblable à la suivante s'affichera probablement :



Pour procéder à l'authentification, vous devez remplacer le certificat Splunk par défaut fourni pour l'accès à l'API sur le port 8089. Pour obtenir des instructions détaillées sur le remplacement du certificat SSL, consultez KB0778285 .

Créer et nommer un profil d'événement pour l'intégration d'ingestion d'événements Splunk Enterprise Security

Vous créez un profil d'événement dans votre Now Platform instance et déterminez quels Splunk événements notables créent des incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Avant Now Platform Réponse aux incidents de sécurité que les incidents de sécurité (SIR) ne soient créés à partir d'événements notables ingérés, les valeurs de champ des alertes sont affichées sur la mise en page d'un Now Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera créé.

Du point de vue de l'intégration, à l'aide des API disponibles, Splunk ES les événements notables sont transférés individuellement et manuellement en tant qu'événements notables discrets, ou ils sont automatiquement ingérés dans l'environnement Opérations de sécurité de votre Now Platform instance en fonction du type de profil défini.

Les workflows d'intégration ingèrent différents types d'événements notables, tels que des tentatives d'accès non autorisé et des logiciels malveillants, par exemple. Ces événements notables sont ingérés en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance.

Tous les notables sont initialement ingérés pour un type de recherche de corrélation configuré dans un profil. Les notables ingérés peuvent ensuite être filtrés pour spécifier quels notables créent des incidents de sécurité. Par exemple, vous pouvez préférer les filtres qui créent des incidents de sécurité uniquement pour les événements notables identifiés comme à haut risque. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir d'événements notables ingérés, les valeurs de champ individuelles des événements notables sont mappées aux champs correspondants sur une mise en page de l'incident de sécurité pour un aperçu.

Procédure

1. Les noms des profils d'événements dans votre Now Platform instance doivent être uniques et ne peuvent être mappés qu'à un profil d'événement actif à la fois.
2. Il Now Platform ingère des notables spécifiques à l'aide des workflows de l'intégration. Tous les événements notables qui répondent aux critères de sélection de votre Splunk ES console sont initialement ingérés dans votre Now Platform instance.
3. Un profil dans votre Now Platform est une encapsulation d'un événement notable dans votre Splunk ES console.
   Il existe une relation un-à-un entre les événements notables qui sont ingérés avec un profil et les connexions à votre Splunk ES console : un type d'événement notable pour une connexion.
4. Pour créer des profils pour les événements notables planifiés, reportez-vous à la section Configurer un profil pour l'ingestion d'événements notables planifiés.
5. Pour créer des profils pour le transfert manuel d'événements, reportez-vous à la section Configurer un profil pour le transfert manuel d'événements.

Configurer un profil pour l'ingestion d'événements notables planifiés

Selon le profil défini, Splunk ES les événements notables sont automatiquement ingérés dans l'environnement Opérations de sécurité de votre Now Platform instance.

Le tableau suivant présente la liste des tâches que vous devez suivre pour configurer un profil pour l'ingestion planifiée d'événements notables :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étapes de configuration d'un profil pour l'ingestion d'événements notables planifiés

Tâche	Section
Créer un profil d'événement	Reportez-vous à la rubrique Créer des profils pour l'ingestion d'événements notables planifiés.
Sélectionner les événements notables en fonction du nom de recherche de corrélation	Reportez-vous à la rubrique Sélectionner les événements notables en fonction du nom de la règle de corrélation pour le profil pour Splunk ES l'intégration de l'ingestion d'événements.
Mapper les champs d'événements notables	Reportez-vous à la rubrique Mapper les champs d'événements notables pour l'intégration Splunk Enterprise Security.
Créer des mappages personnalisés	Reportez-vous à la rubrique Créer des mappages pour Splunk ES la revue des incidents d'événements notables et la contribution aux détails de l'événement (ingestion planifiée).
Prévisualiser l'incident de sécurité	Reportez-vous à la rubrique Prévisualiser l'incident de sécurité pour l'intégration de l'ingestion d'événements Splunk Enterprise Security.
Planifier et récupérer des événements notables nouveaux ou mis à jour	Reportez-vous à la rubrique Planifiez et récupérez les événements notables nouveaux ou mis à jour pour l'intégration de l'ingestion d'événements Splunk Enterprise Security.
Automatisez les mises à jour et la fermeture des événements notables en fonction de l'état de l'incident SIR	Reportez-vous à la rubrique Automatisez les mises à jour et la fermeture des événements notables en fonction de l'état de l'incident SIR.

Créer des profils pour l'ingestion d'événements notables planifiés

Vous pouvez configurer un profil afin que les événements notables soient automatiquement ingérés.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Pour créer un profil d'événement pour un événement notable ou un type de règle de corrélation dans votre Now Platform instance, accédez à **Splunk Integration** > **Profil d'événement Splunk**.
2. Si le formulaire Profil d'événement n'est Splunk pas affiché, cliquez sur **Nom** dans la barre de progression.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs.

   Le tableau ci-dessous un exemple de formulaire rempli.

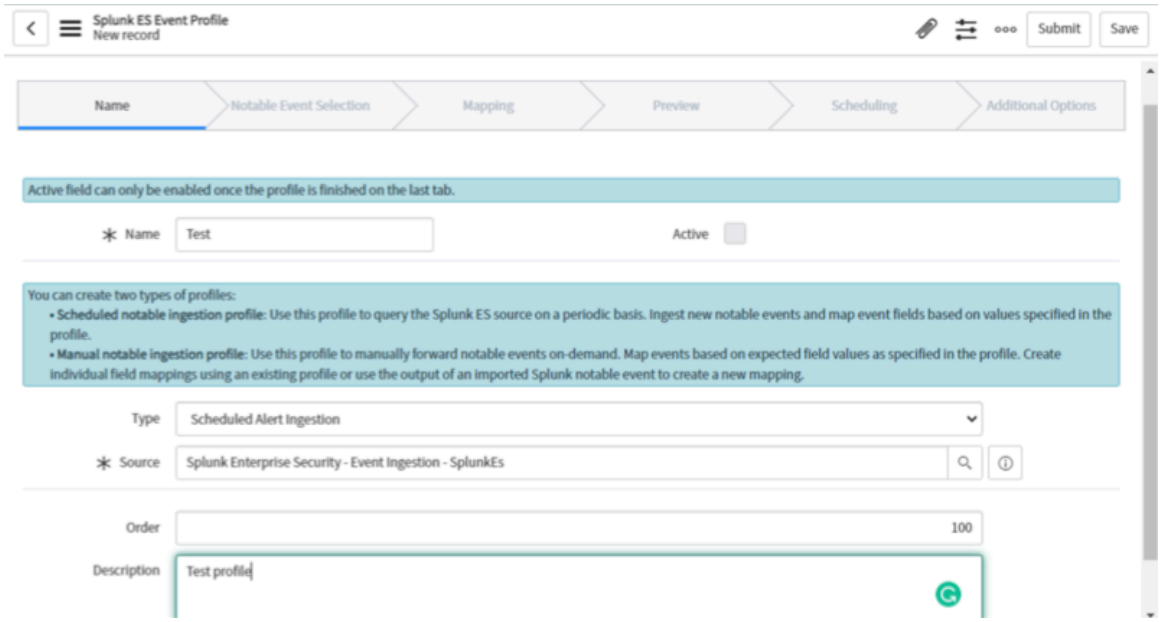
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre Now Platform instance doivent être uniques.
Actif	La case à cocher est décochée et désactivée par défaut. Vous devez remplir toutes les sections du profil avant de l'activer.
Type	Sélectionnez le type de profil dans la liste de choix. ◦ Ingestion d'événements planifiés : ce type de profil prend en charge les événements notables qui sont ingérés selon un calendrier configuré. Renseignez les champs. ◦ Transfert manuel d'événements : ce type de profil prend en charge les événements notables qui sont transférés manuellement à partir de votre Splunk Enterprise Security console d'examen d'incident sur demande. Reportez-vous aux étapes suivantes pour remplir le formulaire pour ces types de profils.
Source	Splunk Fin de serveur ou de recherche que vous avez configurée pour ingérer des événements notables. Si vous avez configuré plusieurs Splunk serveurs, sélectionnez le serveur approprié pour les types d'événements notables qui seront ingérés pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Le workflow du profil dont le numéro est le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

La figure suivante est un exemple de formulaire rempli pour un type d'événement notable planifié.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Dans le cas d'un profil avec un événement notable planifié, choisissez une option pour poursuivre la configuration du profil.

Option	Description
Continuer	Enregistrez le profil et passez à l'étape de sélection de l'événement.
Mettre à jour	Enregistrez les mises à jour de ce profil et revenez à la liste des profils d'événements Splunk .
Enregistrer	Enregistrer ce profil et rester sur la page.
Supprimer	Supprimez cet enregistrement de profil et revenez à la liste des profils d'événements Splunk .

Que faire ensuite
L'étape suivante consiste à sélectionner les événements notables pour une ingestion automatique.

Sélectionner les événements notables en fonction du nom de la règle de corrélation pour le profil pour Splunk ES l'intégration de l'ingestion d'événements

Une fois que vous avez créé un profil pour une ingestion planifiée de type événement notable, sélectionnez un nom de règle de Splunk Enterprise Security corrélation pour ce profil pour lequel vous souhaitez mapper les événements notables correspondants à un Now Platform Réponse aux incidents de sécurité incident de sécurité.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Affichez les règles de corrélation disponibles dans votre Now Platform instance afin de connaître les types d'événements notables pour lesquels vous souhaitez ingérer et créer des incidents de sécurité. Sélectionnez une règle de corrélation. Vous pouvez sélectionner un ou plusieurs événements notables dans la liste de ce formulaire.

Traduction automatique

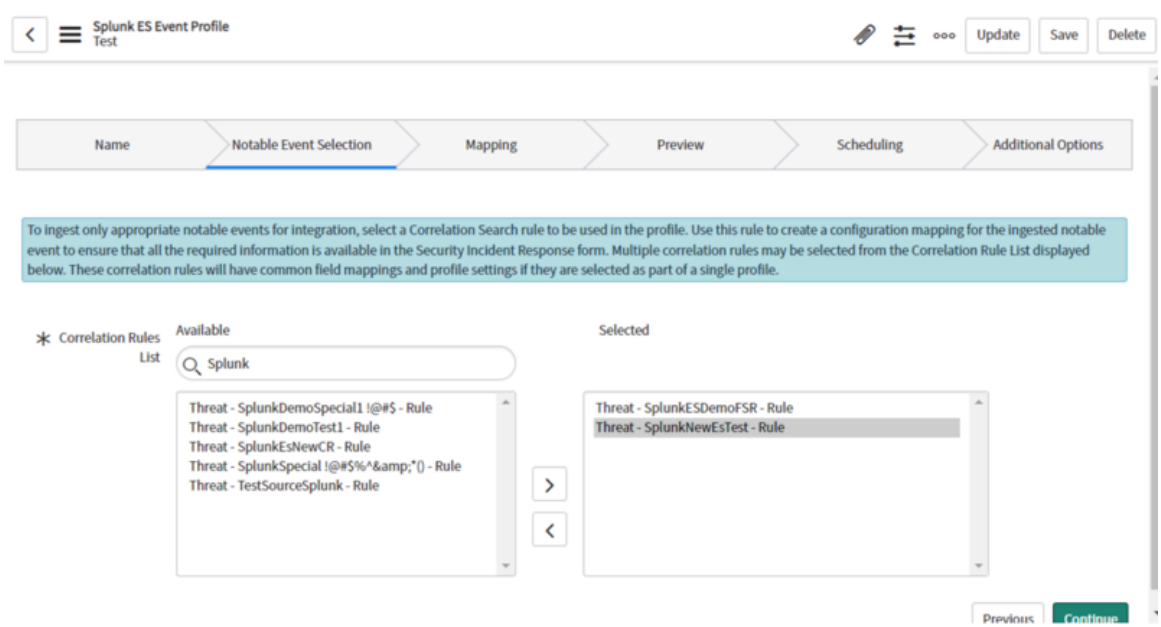
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si la page Sélection des événements notables n'est pas affichée, sélectionnez-la dans la barre de progression pour l'afficher.
2. Dans la liste Règle de corrélation, choisissez l'une des options suivantes pour sélectionner une ou plusieurs règles de corrélation, puis déplacez-les de la colonne Disponible vers la colonne Sélectionné.

   La liste des règles de corrélation de ce formulaire correspond à la liste des règles de corrélation de votre Splunk ES console d'examen des incidents. Jusqu'à 500 règles de corrélation sont affichées sur ce formulaire. Si plus de 500 règles de corrélation sont répertoriées dans votre Splunk ES, seuls les 500 premiers événements notables sont affichés sur ce formulaire dans votre Now Platform instance.

Option	Description
Dans le champ de recherche Liste de règles de corrélation, saisissez du texte.	La colonne sous le champ de recherche est filtrée avec les options disponibles en fonction du texte que vous saisissez. Sélectionnez une règle de corrélation et, à l'aide des touches fléchées, déplacez l'alarme sélectionnée de **Disponible** à **Sélectionné**.
Dans la liste Règle de corrélation, double-cliquez sur une règle de corrélation.	La colonne **Sélectionné** est renseignée avec votre sélection.
Dans la liste Règle de corrélation, cliquez une fois sur une règle de corrélation.	La règle de corrélation est sélectionnée. À l'aide des flèches, déplacez la règle de corrélation sélectionnée de **Disponible** à **Sélectionné**.



3. Choisissez une option pour continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Poursuivez ou cliquez sur Mappage dans la barre de progression	Le formulaire de mappage s'affiche. **Le mappage** est sélectionné dans la barre de progression. L'étape suivante consiste à mapper les champs d'événements notables à un SIR incident de sécurité.
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements notables Splunk s'affiche.
Précédent	L'étape **Nom** s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements notables Splunk s'affiche.

Que faire ensuite

Vous avez sélectionné avec succès une règle de corrélation pour un profil planifié Splunk Enterprise Security . L'étape suivante consiste à mapper les valeurs d'événements notables aux champs d'un incident de sécurité.

Mapper les champs d'événements notables pour l'intégration Splunk Enterprise Security

Une fois que vous avez identifié la règle de corrélation et le type d'événement notable spécifiques pour le profil, l'étape suivante consiste à mapper les champs d'événements notables individuels aux champs d'un Now Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Vue d'ensemble

Pour l'étape de mappage, vous pouvez ingérer un échantillon d'événements notables pour la règle de corrélation sélectionnée ou exporter des données d'événements notables pour les événements notables transférés manuellement. Le processus de mappage d'événements est identique quel que soit le type de profil que vous créez.

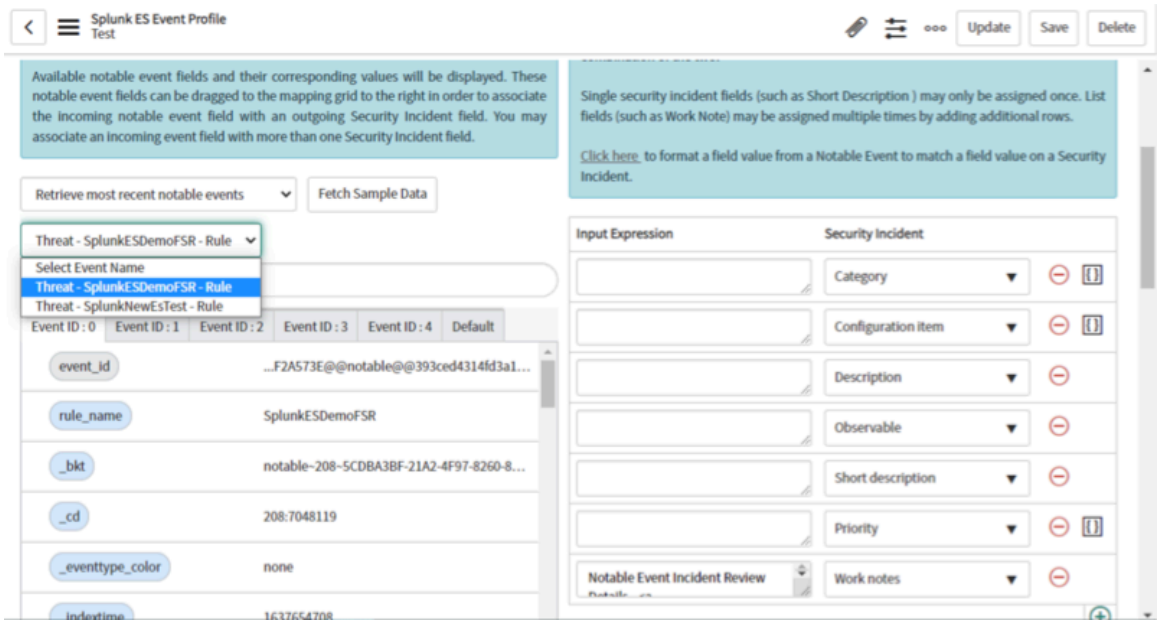
Les figures suivantes sont des exemples de configurations de mappage par défaut fournies pour chaque type de profil d'événement. Vous pouvez personnaliser les champs qui renseignent l'incident de sécurité. Au cours de cette phase de mappage, vous pouvez vous assurer que toutes les données pertinentes de champ d'événement notable sont mappées à l'emplacement approprié sur le formulaire d'incident SIR, puis visualiser l'incident SIR dans la section d'aperçu.

Si plusieurs corrélations sont utilisées, les événements notables peuvent être extraits en sélectionnant l'événement requis. Utilisez **Nom d'alerte** pour choisir votre alerte si vous avez configuré plusieurs alertes pour l'ingestion.

Une fois que vous avez cliqué pour extraire les données, les noms de champs d'événements Splunk notables et les valeurs correspondantes sont renseignés sur le côté gauche du formulaire. Il s'agit des champs d'événements Splunk notables qui peuvent être mappés aux champs d'incident SIR de sécurité. Certains champs peuvent être mappés plusieurs fois aux champs d'incident de sécurité SIR.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous préférez peut-être examiner quelques exemples d'événements notables sur votre Splunk console afin de les ingérer pour l'étape de configuration du mappage de champs. Cette étape s'intitule Mappage dans la barre de progression. Si cette page n'est pas affichée, cliquez sur **Mappage** dans la barre de progression. Vous pouvez ingérer jusqu'à cinq échantillons d'événements notables pour faciliter le processus de mappage des champs d'événements Splunk Enterprise Security notables. Il existe des options permettant soit d'ingérer les cinq événements notables les plus récents pour la règle de corrélation sélectionnée, soit d'ingérer jusqu'à cinq événements notables spécifiques en fonction des ID d'événements notables.

Vous trouverez ci-dessous un résumé des étapes nécessaires pour cartographier les événements notables :

- Ingestion d'échantillons de données d'événements notables planifiés : pour les exemples de données utilisés pour ingérer automatiquement les profils d'événements notables, les champs d'événements notables disponibles et leurs valeurs correspondantes sont affichés dans une disposition de mappage par défaut sur le côté gauche du formulaire de mappage une fois les données d'échantillon récupérées. Des onglets s'affichent pour vous permettre d'afficher les valeurs d'un ID d'événement notable spécifique que vous avez extrait. Vérifiez que tous les champs critiques de la section d'ingestion d'échantillons d'événements notables à gauche du formulaire sont mappés aux champs d'incident ServiceNow de sécurité à droite du formulaire.
- Mappage de champs : modifiez la configuration du mappage en faisant glisser les champs d'événements notables depuis le côté gauche et en les déposant sur la section de mappage des ServiceNow incidents SIR à droite. Le mappage sur la droite associe le champ d'événement notable entrant à un champ d'incident de sécurité sortant.
- Expérience de mappage : personnalisez la grille de mappage en ajoutant ou en supprimant des champs à l'aide de l'icône + en bas de la section de mappage de champs d'incidents SIR. Suivez les champs négligés ou dupliqués avec le code couleur fourni (les champs mappés sont grisés, les champs bleus ne sont pas mappés).
- Conditions de génération d'incidents : une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de pouvoir spécifier quels événements notables doivent créer des incidents de sécurité par rapport à quels événements notables doivent être filtrés (par exemple, les événements notables de faible priorité). Pour ce faire, consultez la section Conditions de génération d'incidents située sous la section Mappage des événements notables.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Critères d'agrégation d'événements : définissez des critères d'agrégation d'événements supplémentaires qui regroupent un événement notable entrant en un incident de sécurité existant SIR au lieu de créer des incidents similaires et potentiellement dupliqués. En utilisant des critères de valeur de correspondance de champ pour chaque profil, cette option d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données relatives aux événements notables de sécurité connexes sur un seul incident de sécurité.
- Formater la traduction des champs : dans certains cas, les valeurs des champs d'événement dans les événements notables de l'entreprise Splunk peuvent ne pas se traduire directement dans les champs de l'incident SIR de sécurité. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez mettre en forme des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident SIR de sécurité à l'aide de la fonctionnalité Formater la traduction de champ.

L'étape suivante consiste à ingérer les événements notables et à mapper les valeurs aux champs d'incident SIR de sécurité.

Créer des mappages pour Splunk ES la revue des incidents d'événements notables et la contribution aux détails de l'événement (ingestion planifiée)

Au cours de l'étape de mappage des champs d'événements notables, vous mappez les champs d'événements individuels des événements notables aux champs d'un Now Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

La grille de mappage peut être personnalisée en fonction du type d'événement notable sélectionné dans la sélection de la règle de corrélation. Le codage couleur des champs d'événement vous aide à suivre les valeurs d'événement que vous avez déjà mappées à mesure qu'elles sont grisées tandis que tous les champs non mappés restants apparaissent en bleu. Cela vous aide à mieux visualiser quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si des informations d'événements importantes restantes restent non mappées.

Mappez jusqu'à cinq événements notables de la colonne Ingestion d'échantillons d'événements notables à gauche du formulaire aux champs d'incident de sécurité dans la colonne Mappage de champs d'incidents SIR à droite.

Créez des mappages personnalisés en ajoutant ou en supprimant les champs de la grille de mappage sur le côté droit du formulaire. Les champs par défaut qui sont généralement des champs importants à renseigner sur le formulaire de réponse aux incidents de sécurité s'affichent. Toutefois, ces champs peuvent être supprimés et tous les champs supplémentaires peuvent être affichés à l'aide des boutons + et -. Créez des cartes personnalisées en ajoutant ou en supprimant les champs de la grille de mappage sur le côté droit du formulaire. La personnalisation des champs vous permet de mapper Splunk des champs qui ne sont pas affichés sur la grille de mappage par défaut sur l'incident SIR de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

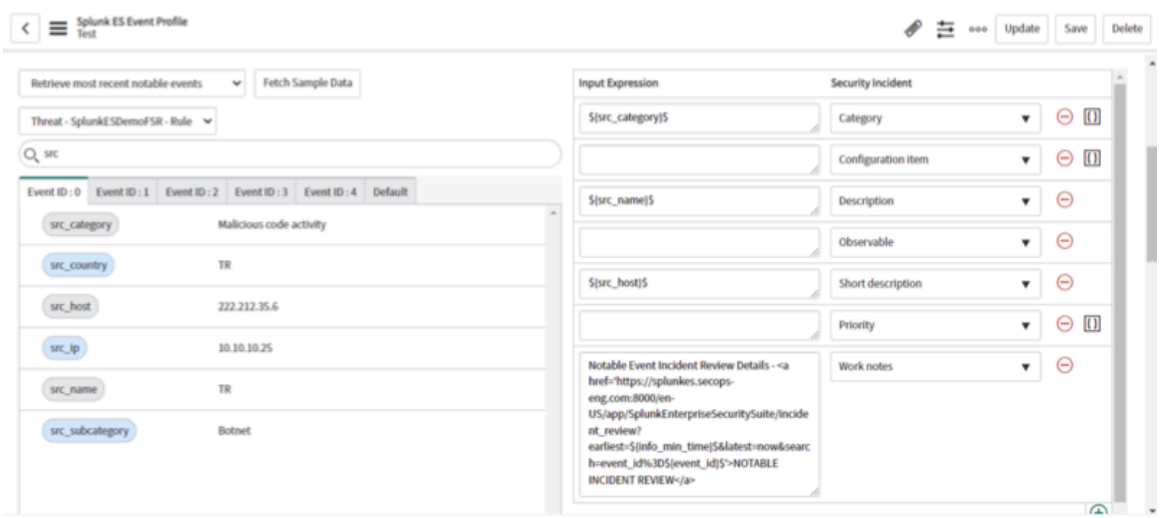
1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Pour un profil avec une ingestion planifiée, cliquez sur **Extraire les données d'échantillon** pour extraire le dernier échantillon d'événements notables de la Splunk Enterprise console pour la règle de corrélation sélectionnée.

   Remarque : Vous pouvez soit extraire l'échantillon d'événements notables le plus récent, soit fournir les ID d'événements notables uniques pour les événements notables spécifiques que vous souhaitez utiliser pour votre expérience de mappage d'événements notables.

   Les champs et valeurs des événements notables sont affichés sous forme d'onglets individuels. Vous pouvez ingérer jusqu'à cinq événements notables.

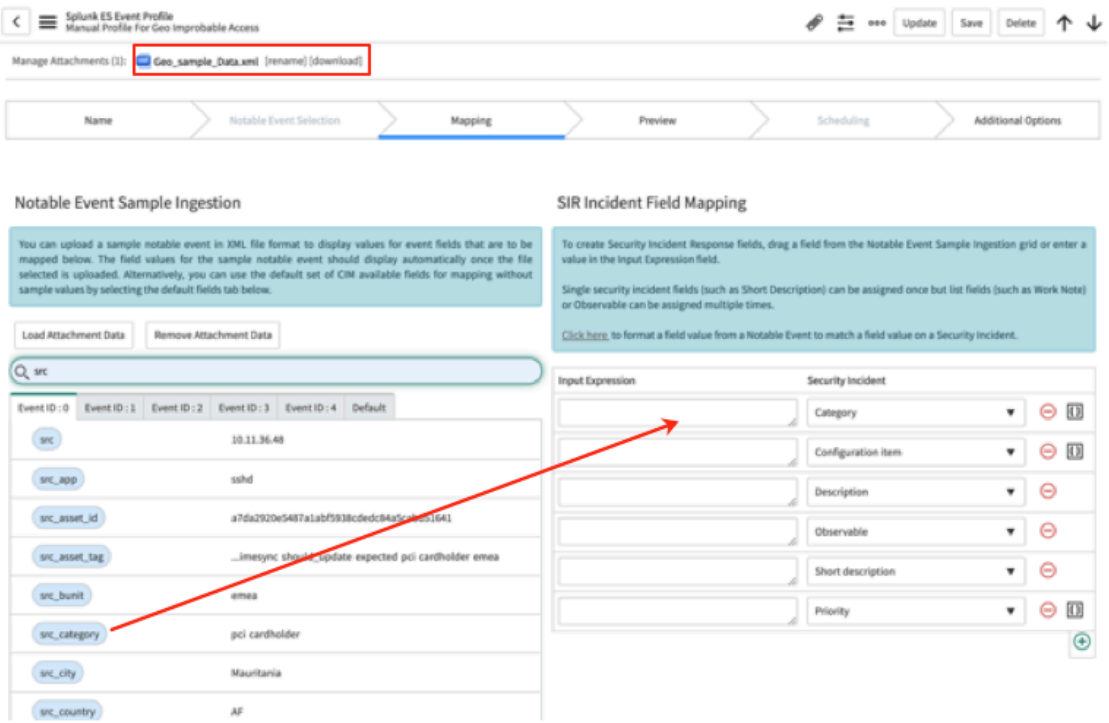
   L'extraction d'échantillons d'événements notables peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran.

   Dans la figure suivante, les paires de valeurs de nom de champ pour l'événement notable ingéré, ou les échantillons d'événements importés, s'affichent sur le côté gauche de ce formulaire une fois l'extraction d'ingestion terminée. Ces valeurs sont les valeurs que vous mappez aux champs d'incident de sécurité du côté Mappage de champs d'incident SIR du formulaire.



3. Pour mapper une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez longuement sur un nom de champ bleu sur le côté gauche du formulaire.
4. Faites glisser le nom du champ, par exemple `src_category`, et déposez-le sur un champ de la colonne Expression d'entrée en regard d'un nom de champ dans la colonne Incident de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

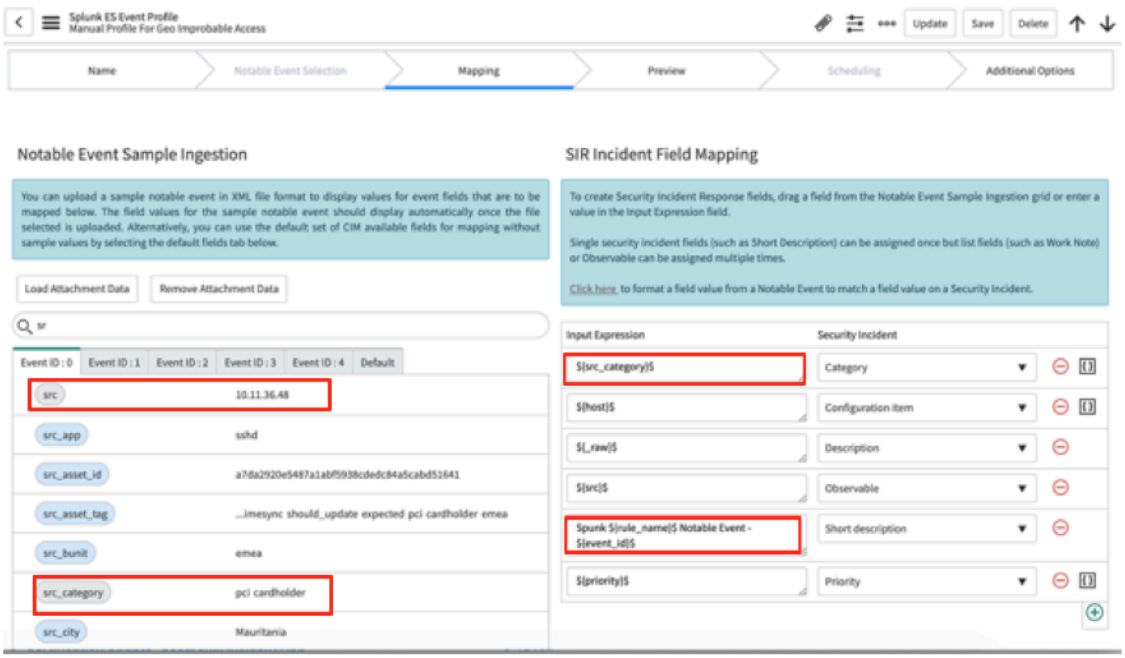


La valeur du champ est affichée dans la colonne Expression d'entrée. Dans l'image suivante, `src_category` est mappé au champ `de catégorie` de l'incident de sécurité. Toutefois, vous pouvez faire correspondre n'importe quelle valeur du côté gauche à un champ de droite. Vérifiez que la valeur est correctement mappée sur l'incident de sécurité pendant l'étape de prévisualisation.

Pour vous assurer qu'aucun champ d'événement n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par couleur. Les champs bleu clair sur la gauche indiquent qu'un champ d'événement notable n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ notable entrant à plusieurs champs sur un incident de sécurité.

Un champ gris indique qu'un champ a été sélectionné et mappé à un champ sur l'incident de sécurité. Ce code couleur vous aide à suivre le mappage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit.

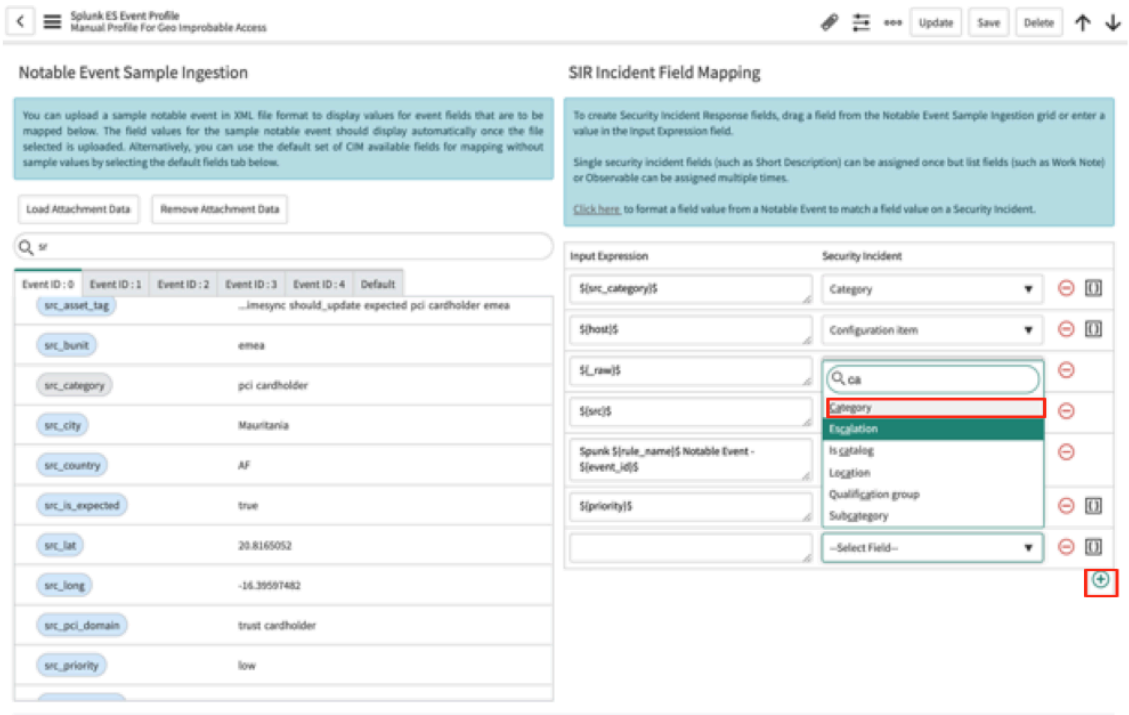
a. À droite du formulaire, dans la section Mappage des champs d'incidents SIR, en bas de la grille, cliquez sur l'icône plus.
Un nouveau champ s'affiche.

b. Dans la colonne Incident de sécurité, développez la liste qui s'affiche, puis sélectionnez un champ.

Dans la liste développée pour le nouveau champ, certains champs sont ombrés. Dans la figure suivante, la `catégorie` a un arrière-plan gris, car elle a été mappée dans l'incident de sécurité. À l'instar du code couleur pour les champs d'événements notables sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident SIR déjà mappés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



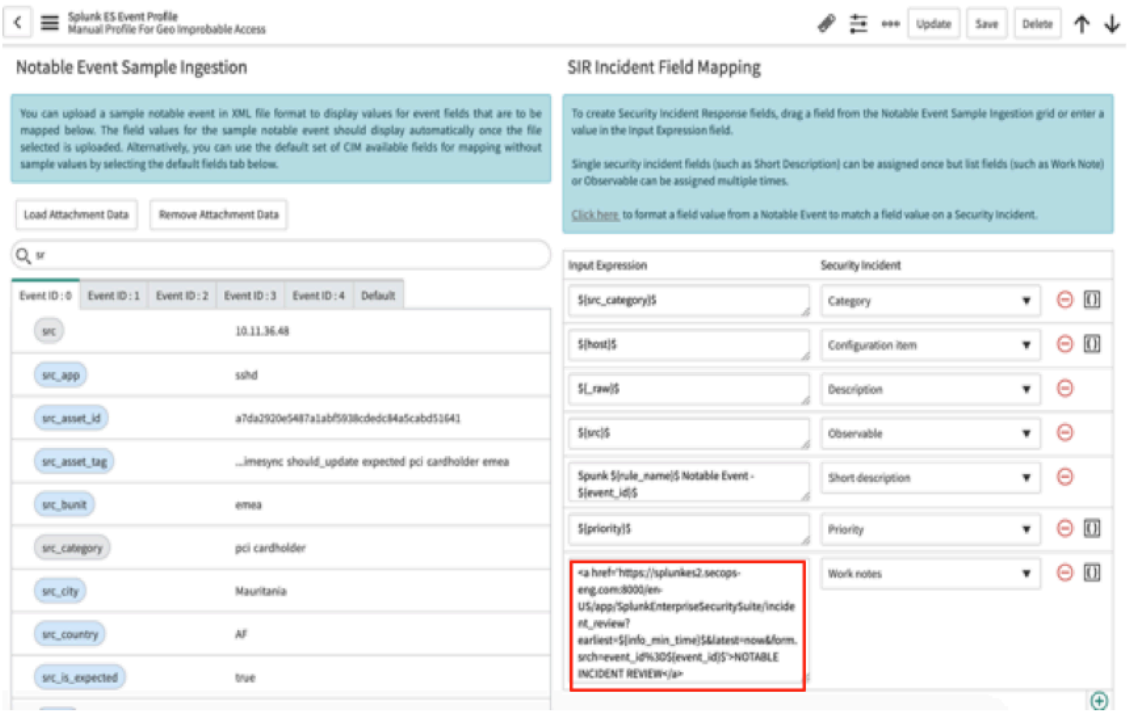
Remarque : Afin que plusieurs observables puissent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité dispose d'une liste dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affiché dans la liste, le champ n'est pas renseigné sur l'incident de sécurité.

c. Vous pouvez également saisir une valeur dans le champ Rechercher pour la nouvelle ligne.

d. Sur le côté gauche du formulaire, cliquez avec le bouton gauche de la souris pour sélectionner **l'ID d'événement** souhaité dans le champ expression d'entrée.

6. Poursuivez le mappage en ajoutant ou en supprimant des valeurs de champ au mappage.
La figure suivante est un exemple de mappage modifié. Dans le champ inférieur à droite, le champ Notes de travail est ajouté et il a plusieurs valeurs. Notez que pour un champ de chaîne de texte long, vous pouvez développer le champ de mappage pour voir la chaîne complète et le redimensionner selon vos besoins en tirant le coin inférieur droit du champ, comme indiqué dans la capture d'écran ci-dessous avec le champ Notes de travail ajouté :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Avertissement : Veuillez noter que dans la section **Mappage de champ d'incident SIR** , l'URL et le numéro de port mentionnés dans le champ **expression d'entrée** ne sont qu'un exemple et non l'URL ou le numéro de port fournis prêts à l'emploi.

Dans l'aperçu, ces valeurs sont affichées dans les notes de travail sur l'incident de sécurité. Étant donné que la valeur correspond à un champ que vous avez ajouté à la section de mappage et que plusieurs valeurs sont mappées au champ Notes de travail, les valeurs s'affichent telles qu'elles sont saisies. Dans cet exemple, les espaces et les signes de ponctuation que vous avez saisis dans le champ sont affichés dans la section Éléments connexes sous forme de note de travail dans l'aperçu de l'incident de sécurité.

L'image suivante est un exemple de la façon dont les valeurs de l'image précédente sont affichées sur l'incident de sécurité.



7. Facultatif : Ouvrez l'éditeur de script et poursuivez la modification.

(Optional) Pour plus d'informations sur l'éditeur de script, reportez-vous à la section Utiliser l'éditeur de script pour formater les valeurs d'alerte pour l'intégration Splunk Enterprise Event Ingestion.

Inclure des liens hypertexte pour l'événement notable, l'examen des incidents et les événements contribuant

En plus de mapper les champs, le *sn_si.admin* peut mapper une valeur de chaîne qui permet à l'analyste de sécurité travaillant sur un incident d'établir un lien hypertexte vers l'examen de l'incident d'événement notable dans la Splunk Enterprise Security console,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ainsi que vers les événements contributeurs sous-jacents qui font partie de la recherche approfondie.

Les valeurs de chaîne suivantes contiennent le nom du serveur et les Splunk Enterprise Security variables appropriées qui peuvent être utilisées pour créer des liens hypertexte entre ces détails :

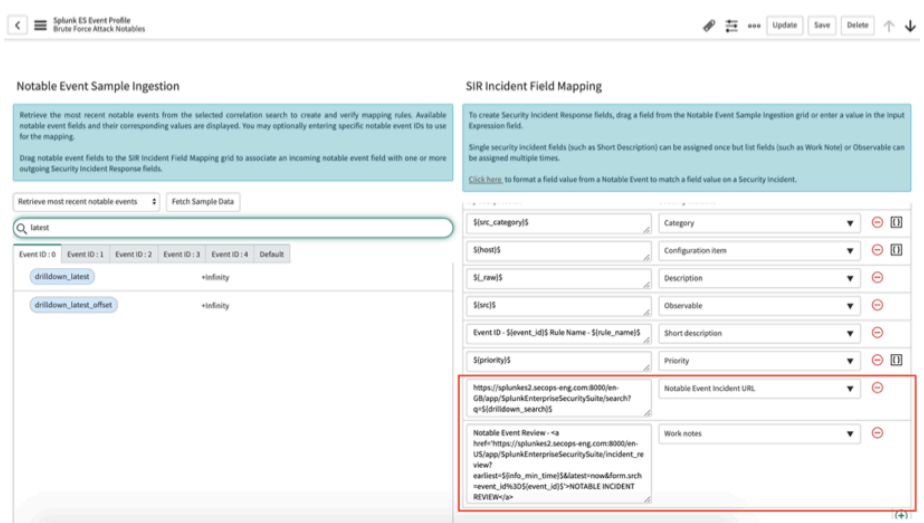
- **Lien hypertexte de l'examen des incidents d'événements notables** : `https://splunkes2.secops-eng.com:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=${info_min_time}$&latest=now&form.srch=event_id%3D${event_id}$`

  où `splunkes2.secops-eng.com:8000` est la source du serveur Splunk et `info_min_time` et `event_id` sont des valeurs de champ d'événement extraites des événements notables.

- **Événements de contribution à un événement notable (recherche détaillée) Lien hypertexte** : `https://splunkes2.secops-eng.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/search?q=${drilldown_search}$`

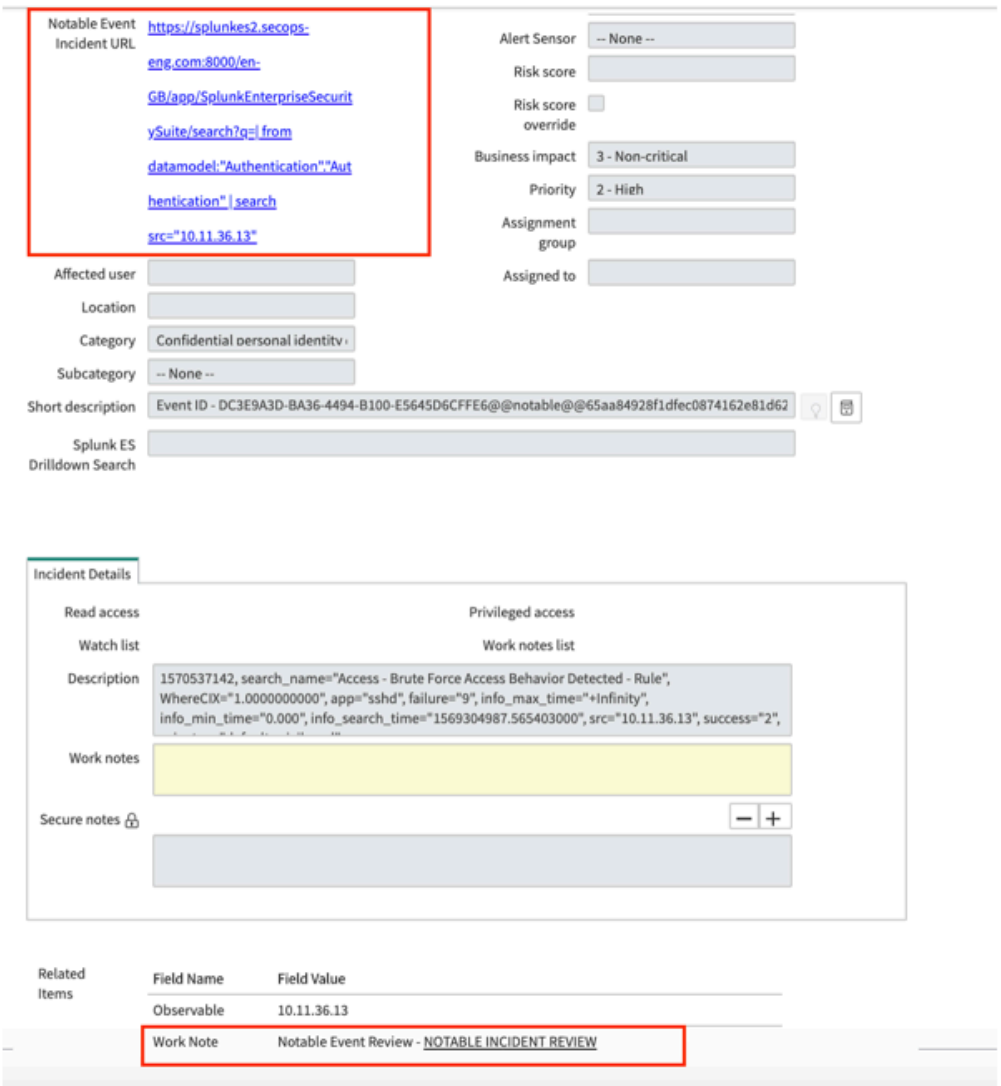
  où `splunkes2.secops-eng.com:8000` est la source du serveur Splunk et `drilldown_search` est une valeur de champ d'événement extraite des événements notables.

L'image suivante montre l'URL d'examen des incidents d'événements notables mappée au champ Note de travail et l'hyperlien Événements contribuant à l'événement notable (recherche approfondie) mappé vers un champ personnalisé appelé URL d'incident d'événement notable :



L'image suivante est l'aperçu de l'incident SIR avec l'hyperlien Revue des incidents d'événements notables et l'URL des événements contribuant :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Conditions de filtrage de génération d'incidents

8. Facultatif : Une fois que vous avez terminé les étapes de mappage de champs précédentes, vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir les critères supplémentaires qu'un événement notable entrant doit satisfaire pour créer un SIR incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

a. Faites défiler l'écran jusqu'à la section Conditions de génération d'incidents du formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

(Optional) Le Créateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les options des listes pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Ingestion d'échantillons d'événements notables pour les événements que vous avez ingérés. Ces champs sont dynamiques et changent en fonction des Splunk événements notables que vous ingérez ou de l'événement que vous sélectionnez pour les échantillons d'événements notables transférés manuellement. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'événement Splunk Enterprise Security notable. Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférez peut-être revenir à votre Splunk Enterprise Security console et passer en revue vos événements notables pour les mots-clés.



b. À l'aide des listes et des champs du générateur de conditions, définissez des filtres pour la première ligne.

c. Pour ajouter d'autres conditions, à droite des champs, cliquez sur **ET** ou **OU**. Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

d. Facultatif : Dans la deuxième ligne, définissez une deuxième condition de filtre.

(Optional) L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création des incidents de sécurité.



(Optional) Vous avez défini les conditions de génération d'incident de sorte que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

Ce type de filtrage des conditions de génération d'incident vous permet d'affiner les événements de sécurité et de limiter le nombre d'incidents de sécurité inutiles que vous créez sans modifier la recherche de corrélation sous-jacente ou les filtres dans Splunk. Si

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

des critères de filtrage supplémentaires sont définis, seuls les événements notables qui correspondent à tous les critères sont mappés aux incidents.

> **Remarque :** Si l'un des noms de champs d'événements contient des caractères spéciaux tels que des guillemets ("), des traits d'union (-), des traits de soulignement (_), at (@) ou des esperluettes (&), ces caractères peuvent devoir être remplacés à des fins de traduction de mappage et éventuellement créer un nom d'événement en double. Le mappage peut être effectué correctement, mais un suffixe numérique est ajouté pour différencier les champs avec des noms d'événements en double. Par exemple, si le premier champ d'événement est `alerts.alert` et que le deuxième champ d'événement est `alerts@alerts`, ces champs ne peuvent pas être identifiés de manière unique car les caractères de texte standard restants sont les mêmes. Dans ce cas, un suffixe est ajouté au deuxième champ d'événement et le champ est renommé `en alerts@alert(1).`

(Optional) Critères d'agrégation d'événements pour gérer des notables similaires et éviter les incidents en double

9. Facultatif : Pour éviter de créer des incidents de sécurité en double, définissez des critères d'agrégation d'événements supplémentaires afin que les événements notables entrants soient agrégés en un incident de sécurité ouvert.
   Pour définir les critères, procédez comme suit ci-dessous.

   a. Faites défiler la page jusqu'à la section Critères d'agrégation d'événements du formulaire et cochez la case Conditions **d'agrégat** pour activer cette option.

      (Optional) Les champs Incident avec les valeurs correspondantes s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés dans l'incident SIR de sécurité.

   b. Dans le champ d'entrée à sélection multiple, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre Now Platform.

   c. Utilisez **l'option Ajouter de nouveaux critères** pour sélectionner plusieurs conditions de correspondance de champ.
      Toutes les valeurs de champ que vous sélectionnez dans le champ d'entrée de sélection multiple sont mises en correspondance pour les critères d'agrégation à l'aide de la condition ET. Cliquez sur **Ajouter de nouveaux critères** pour sélectionner plusieurs conditions de correspondance de champ où l'agrégation se produit si l'une des conditions de champ multi-sélectionnées qui sont définies est remplie à l'aide de la condition OU.

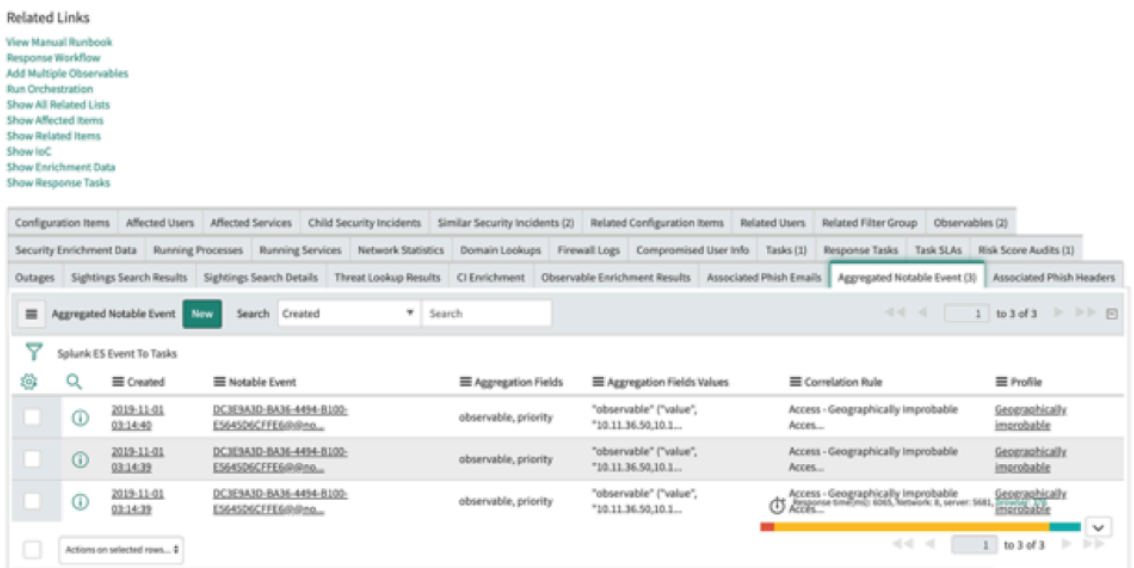


Si un nouvel événement notable correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation de l'étape de mappage, le nouvel événement notable est automatiquement ajouté à l'incident de sécurité le plus récemment ouvert

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher tous les événements notables d'agrégat ajoutés dans une liste connexe sur un incident de sécurité. Tous les événements notables regroupés sur un incident de sécurité sont affichés dans la Splunk liste connexe Événements à tâches. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi ces événements notables sont regroupés aux incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de l'enregistrement sous Liens connexes et cliquez sur le lien **Afficher toutes les listes connexes** .



d. Facultatif : Pour consigner une note de travail pour un nouvel événement notable récemment ajouté à l'incident de sécurité, cochez la case pour activer cette option. La note de travail consigne qu'un nouveau notable a été ajouté, ainsi qu'un lien vers les détails de l'alerte et tous les autres détails qui ont pu être ajoutés au champ Note de travail dans votre section de mappage.

Vous avez mappé avec succès les valeurs d'un Splunk événement notable aux champs d'un SIR incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage de génération d'incidents. Vous avez également ajouté des événements notables à des incidents de sécurité existants SIR lorsque les valeurs de champ d'événement correspondent aux critères d'agrégation configurés.

10. Choisissez-en un pour poursuivre la configuration du profil.

Option	Description
Continuer	Le formulaire de mappage s'affiche. **L'aperçu** est sélectionné dans la barre de progression. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité.
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements Splunk s'affiche.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Précédent	Le formulaire Sélection de l'événement notable s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements Splunk s'affiche.

Que faire ensuite
L'étape suivante consiste à prévisualiser les valeurs que vous avez mappées sur l'incident de sécurité.

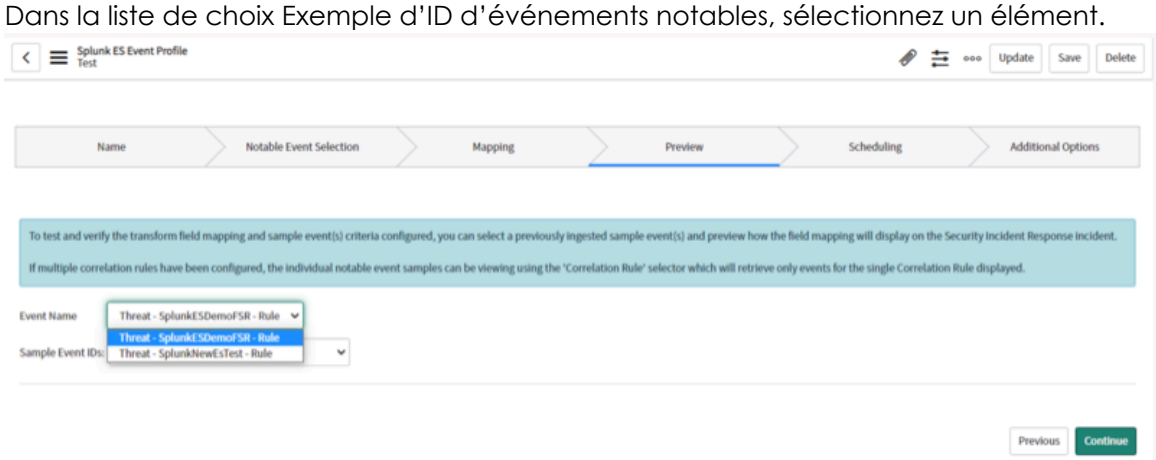
Prévisualiser l'incident de sécurité pour l'intégration de l'ingestion d'événements Splunk Enterprise Security

Une fois que vous avez terminé l'étape de mappage, prévisualisez les valeurs que vous avez mappées dans un Now Platform® Réponse aux incidents de sécurité incident de sécurité (SIR). Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs notables que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs contenant des erreurs ou pour renseigner les données manquantes. Si l'aperçu n'est pas terminé, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de SIR sécurité ne sont pas enregistrés en tant qu'incidents réels dans le SIR produit.

Procédure
1. Si l'aperçu de l'incident de sécurité n'est pas affiché, cliquez sur **Aperçu** dans la barre de progression.
2. Dans la liste de choix Nom d'événement, sélectionnez un élément si plusieurs événements ont été utilisés.
3. Sélectionnez des ID d'événements dans la liste de choix Exemples d'ID d'événements notables.
4. Dans la liste de choix Exemple d'ID d'événements notables, sélectionnez un élément.

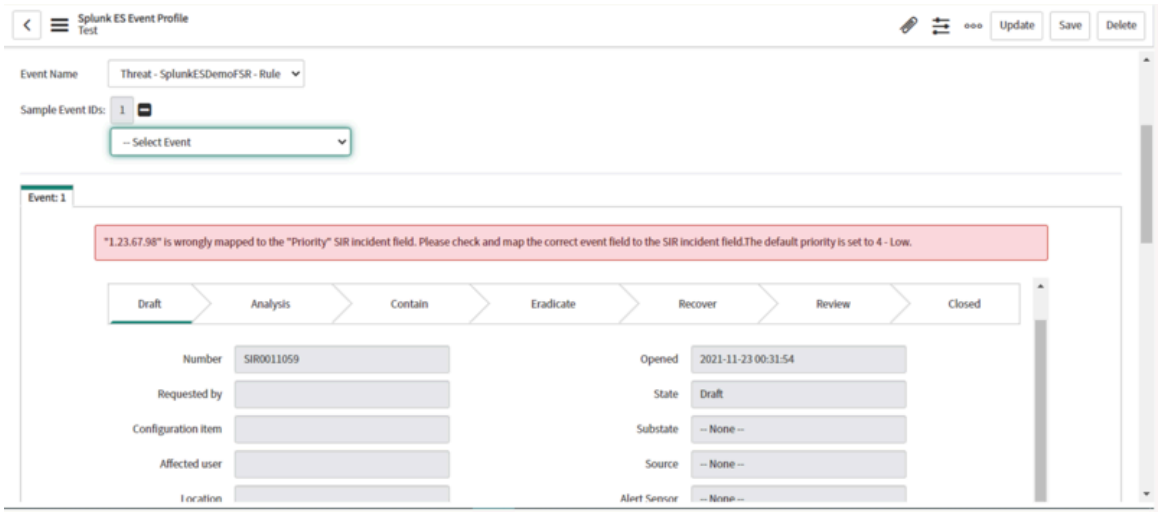


L'incident de sécurité s'affiche. Ne modifiez aucune information dans les champs. Il s'agit d'une vue en lecture seule et un enregistrement de cet incident de sécurité n'est pas enregistré.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Examinez le mappage de champs des valeurs d'événements notables sur l'incident de sécurité.

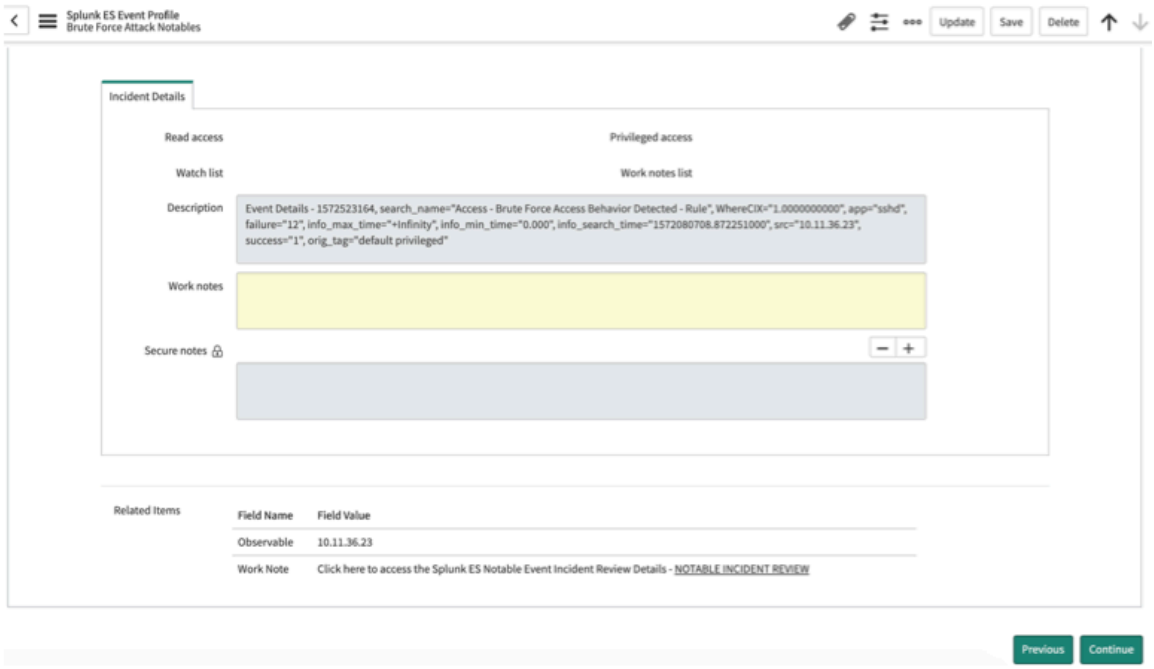


L'image précédente est un exemple d'aperçu avec une erreur de mappage. Dans cet exemple, une valeur de champ de l'événement notable n'a pas de valeur acceptable pour le champ de référence sur le formulaire d'incident SIR. Un message d'erreur s'affiche pour indiquer qu'une valeur d'entrée est introuvable pour le champ `Élément de configuration` dans la ServiceNow® base de données de gestion des clients (CMDB). Par conséquent, cette valeur de champ mappée n'apparaît pas sur le formulaire d'incident de sécurité SIR sans autre modification.

6. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
7. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
8. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

   La figure suivante est un exemple de l'onglet Détails de l'incident dans la moitié inférieure d'un SIR incident de sécurité, une fois que tous les messages d'erreur ont été résolus. Pour cet exemple, les champs Description et Notes de travail ont été mappés, et ces champs sont renseignés avec les valeurs des paires de valeurs extraites des échantillons d'événements Splunk Enterprise Security notables. Le premier champ Notes de travail n'a aucune valeur. Ce champ a été laissé vide sur la grille de mappage lors de l'étape de mappage. Les champs Note de travail supplémentaires qui ont des valeurs ont été ajoutés à la section de mappage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Après avoir corrigé les erreurs et vérifié que les champs sont comme vous le souhaitez, choisissez une option pour continuer.

Option	Description
Continuer	Le formulaire Planification s'affiche pour les profils avec des événements notables planifiés. **La planification** est sélectionnée dans la barre de progression.
Terminer	Pour les profils configurés pour le transfert manuel d'événements, cliquez sur **Terminer**. Il n'y a pas d'étape de planification pour les profils comportant des données d'événement qui sont exportés à la demande directement à partir de la Splunk Enterprise Security console.
Mettre à jour	Vos données sont enregistrées et vous êtes renvoyé à la liste des profils d'événements Splunk .
Précédent	L'étape Mappage de la barre de progression s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements s'affiche Splunk .

Que faire ensuite

Si aucun message d'erreur ne s'affiche et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à Planifier et récupérer les alertes pour l'intégration Splunk Enterprise Event Ingestion.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Planifiez et récupérez les événements notables nouveaux ou mis à jour pour l'intégration de l'ingestion d'événements Splunk Enterprise Security

Pour les profils automatisés d'ingestion d'événements notables, cette étape est requise dans la configuration du profil d'événement. Au cours de cette étape, vous pouvez vérifier les paramètres par défaut pour la récupération des événements notables ou modifier la planification selon vos besoins. Cette étape vous permet également de récupérer des événements notables historiques à l'aide d'une plage de dates.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Pour les profils pour l'ingestion automatisée d'événements notables, vous choisissez si vous souhaitez ingérer des événements notables historiques au cours de l'étape de planification. Vous choisissez également la fréquence à laquelle vous procéderez à une interrogation pour les futurs nouveaux événements notables et les événements notables mis à jour qui correspondent à la configuration du profil d'alerte.

Pour les profils d'ingestion d'événements notables automatisés, avant que le profil ne soit activé, vous vérifiez et modifiez la planification et la récupération des alertes. Il s'agit d'une étape requise pour tout le processus de configuration de profil d'événement pour les profils d'alerte planifiée.

Vous configurez ces intervalles d'interrogation pour chaque profil. Les performances de l'intégration d'ingestion Splunk d'événements peuvent être impactées par les différents intervalles d'interrogation. Lors de la planification, vous préférerez peut-être trouver un équilibre entre la réduction de la surcharge d'interrogation sur le serveur et le Splunk Enterprise Security désir d'être averti dès que possible lorsqu'un événement notable est créé ou mis à jour. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférerez peut-être modifier ce paramètre à une minute si nécessaire.

Extraction d'événements notables nouveaux ou mis à jour

Lorsque le calendrier d'interrogation est défini, la tâche planifiée extrait les événements notables nouveaux et mis à jour qui ont été extraits précédemment mais ne répondaient pas aux critères de filtrage des incidents. Vous pouvez ainsi créer des incidents en fonction de critères qui peuvent ne pas être présents lors de la création d'un événement notable, mais qui deviennent disponibles après une mise à jour, par exemple pendant la phase d'enquête. Une fois qu'un incident est créé pour un événement notable spécifique, ses mises à jour ultérieures sont ignorées, car il est prévu que le notable soit maintenant traité comme un incident de sécurité actif ServiceNow® . Toutefois, tous les autres notables qui ont déjà été ingérés, mais qui ne répondent pas aux critères de génération d'incidents, continueront d'être extraits et vérifiés par rapport aux critères de génération d'incidents jusqu'à ce qu'ils fassent partie d'un incident actif.

Procédure

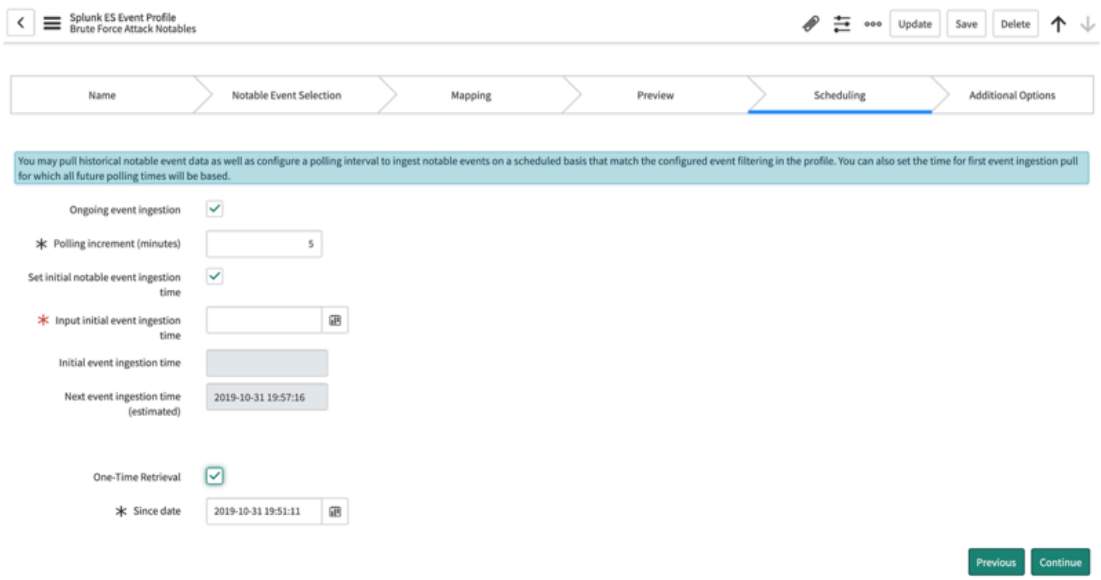
1. Si la page Planification de la barre de progression n'est pas affichée, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les événements notables sont extraits de la Splunk Enterprise Security console.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
◦ Champ d'ingestion d'événement en cours sélectionné ◦ Champ de récupération ponctuelle effacé	Événement en cours En fonction du paramètre par défaut, l'instance Now Platform effectue une extraction du serveur pour les Splunk Enterprise Security événements notables nouveaux ou mis à jour toutes les cinq minutes. Les incidents de sécurité sont créés si des événements notables sont détectés et si les critères de filtrage de génération d'incident sont respectés. Pour équilibrer les frais généraux d'interrogation d'ingestion afin d'obtenir les données les plus récentes, le paramètre par défaut est de cinq minutes. Toutefois, cette valeur peut être modifiée jusqu'à une minute si nécessaire.
◦ Événement notable en cours effacé ◦ Champ de récupération ponctuelle sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhaitez une transmission par pull unique pour ingérer des événements notables historiques. Lorsque ce paramètre est configuré, un profil est utilisé une fois pour récupérer les événements notables à partir des événements historiques basés sur une plage de dates. À droite du champ Depuis date, cliquez sur l'icône Calendrier. Dans le calendrier qui s'affiche, sélectionnez la date à laquelle vous souhaitez commencer à extraire les alertes. À partir de la valeur Date de début, les événements notables sont récupérés jusqu'à la date actuelle. Notez que vous pouvez remonter jusqu'à sept jours en arrière à partir de la date actuelle. Cette fonctionnalité n'est pas destinée à récupérer des quantités importantes d'événements historiques à des Splunk Enterprise Security fins d'archivage, mais plutôt une quantité minimale d'événements en cours qui sont activement traités au moment de l'activation du profil. Une fois les événements notables extraits, ce paramètre ne récupérera pas les événements notables de ce profil à partir de la date actuelle. Ce paramètre remplit l'incident de sécurité avec tous les événements notables qui sont trouvés pour la plage que vous entrez.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Par exemple, pour planifier un délai d'intégration d'un événement notable initial, si vous avez un contrôle de sécurité quotidien Splunk qui s'exécute une fois par jour à 4 h (heure locale), vous pouvez configurer le profil d'événement notable correspondant dans votre Now Platform instance pour qu'il s'exécute à 4 h 05 (heure locale) afin de capturer immédiatement l'événement de défaillance de sécurité et créer un incident de sécurité. Entrez `04 05 00` dans le champ Ingestion de l'événement initial. Dans le champ Incrémentation (minutes), saisissez `1 440` (24 heures) pour planifier la prochaine ingestion d'événement pendant 24 heures à compter de l'ingestion d'événement initiale. L'heure d'ingestion de l'événement initial et l'heure d'ingestion de l'événement suivant sont affichées dans les champs.

3. Pour configurer les paramètres de cet exemple, procédez comme suit.

a. Une fois la page Planification affichée, cochez la case **Ingestion d'événements en cours** pour activer cette option.

b. Dans le champ Incrémentation (minutes), saisissez `1 440` (24 heures).

c. Cochez la case **Sélectionner l'ingestion d'événement initial** pour activer la modification des champs Ingestion d'événement initiale et Ingestion d'événement suivant.

d. Dans le champ Ingestion de l'événement initial, saisissez `04 05 00`.
Dans le champ Prochaine ingestion d'événement (estimée), l'heure de la prochaine ingestion d'événement s'affiche.

4. Cliquez sur l'un des onglets suivants pour poursuivre la configuration du profil.

Option	Description
Continuer	Le formulaire Options supplémentaires s'affiche. **Options supplémentaires** est sélectionnée dans la barre de progression. L'étape suivante consiste à mettre à jour les événements notables lorsque l'incident SIR est créé et/ou fermé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Mettre à jour	Vos données sont enregistrées et la liste des profils de sécurité d'événement s'affiche Splunk .
Précédent	Le formulaire de planification s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements s'affiche Splunk Enterprise Security .

Automatisez les mises à jour et la fermeture des événements notables en fonction de l'état de l'incident SIR

Les incidents de sécurité peuvent être créés et mis à jour une fois qu'ils ont été créés avec une interface bidirectionnelle avec l'intégration Splunk Enterprise Security .

Avant de commencer

L'intégration Splunk Enterprise Security dispose d'une interface bidirectionnelle qui permet aux événements notables de créer des incidents de sécurité et de mettre à jour les événements notables après la création et/ou la fermeture de l'incident de sécurité.

Les détails pertinents de l'incident comprennent le numéro d'incident, le groupe d'affectation et SIRSIR l'URL de l'incident. Cette section est la dernière partie de la configuration du profil qui fournit des options facultatives pour mettre à jour les Splunk Enterprise Security événements notables.

Rôle requis : sn_si.admin

Procédure

1. Si la page Options supplémentaires de la barre de progression n'est pas affichée, sélectionnez **Options supplémentaires**.
2. Suivez les instructions ci-dessous pour terminer la configuration de mise à jour des événements notables en fonction des mises à jour d'incident de sécurité.

Option ou champ	Description
Mettre à jour les événements notables lors de la création de l'incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour le statut de l'événement notable et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir de l'événement notable. Cela peut se produire à la fois pour le déclenchement initial des événements notables qui créent l'incident de sécurité et pour les événements agrégés.
Mise à jour de l'état de l'événement notable initial	Vous devez sélectionner une option d'état dans le menu qui affiche toutes les valeurs d'état disponibles récupérées à partir du Splunk Enterprise Security serveur. Il peut s'agir d'un statut créé personnalisé, tel que ServiceNow : Affecté comme indiqué dans la capture d'écran ci-dessous. Sélectionnez la valeur d'état à définir pour tous les événements notables lorsqu'un incident de sécurité est créé pour un événement notable

Traduction automatique

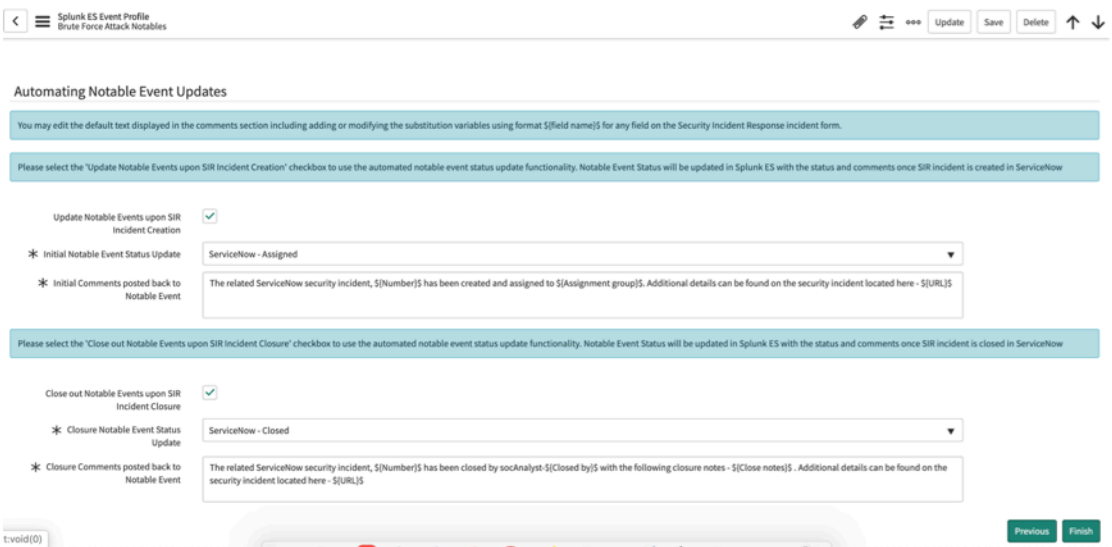
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	ingéré. Cela inclut les notables qui créent de nouveaux incidents et les notables qui sont ingérés et agrégés à un incident ouvert existant.
Commentaires initiaux renvoyés à l'événement notable	En plus de mettre à jour la valeur de l'état notable, vous pouvez également publier des commentaires sur l'historique d'examen des incidents d'événements notables. Comme indiqué dans les instructions, vous pouvez modifier le texte par défaut affiché dans la section des commentaires, y compris ajouter ou modifier les variables de substitution en utilisant le format ${nom du champ}$ pour n'importe quel champ du formulaire d'incident Réponse aux incidents de sécurité .
Fermer les événements notables lors de la fermeture de l'incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour le statut de l'événement notable et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est fermé à partir de l'événement notable. Cela se produira à la fois pour les événements notables déclencheurs initiaux qui créent l'incident de sécurité ainsi que pour les événements agrégés.
Mise à jour de l'état de l'événement notable de fermeture	Vous devez sélectionner une option d'état dans le menu Liste qui affiche toutes les valeurs d'état disponibles récupérées à partir du Splunk Enterprise Security serveur. Il peut s'agir d'un statut créé personnalisé, tel que ServiceNow : Affecté comme indiqué dans la capture d'écran ci-dessous. Sélectionnez la valeur d'état à définir pour tous les événements notables lorsqu'un incident de sécurité est créé pour un événement notable ingéré. Cela inclut les notables qui créent de nouveaux incidents ainsi que les notables qui sont ingérés et agrégés à un incident ouvert existant.
Commentaires de fermeture renvoyés à l'événement notable	En plus de mettre à jour la valeur de l'état notable, vous pouvez également publier des commentaires de fermeture dans l'historique d'examen des incidents d'événements notables. Comme indiqué dans les instructions, vous pouvez modifier le texte par défaut affiché dans la section des commentaires, y compris ajouter ou modifier les variables de substitution en utilisant le format ${nom du champ}$ pour n'importe quel champ du formulaire d'incident Réponse aux incidents de sécurité .

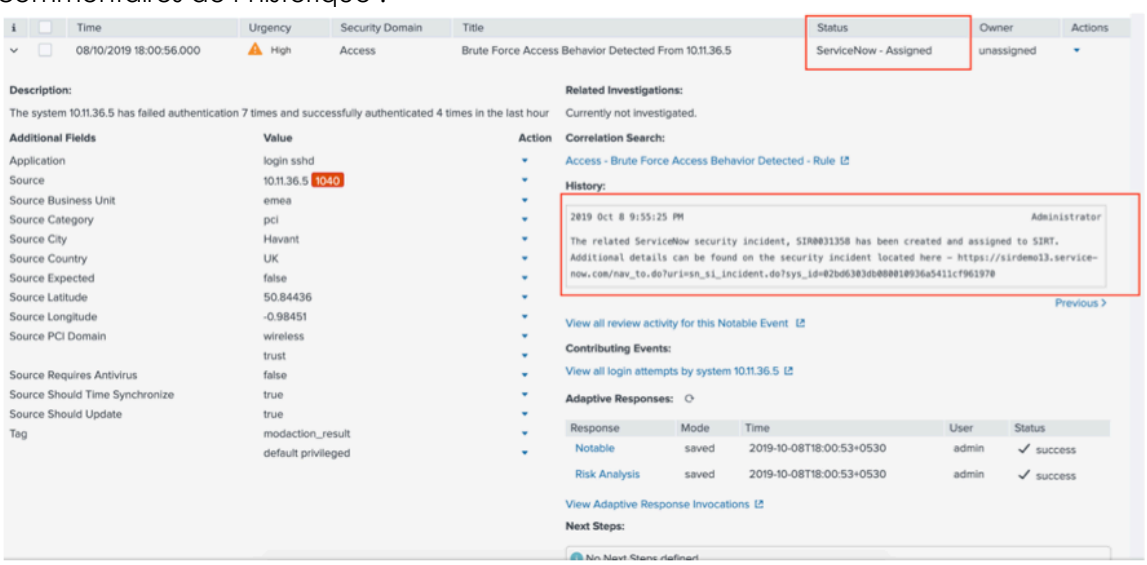
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Terminer** pour terminer la configuration.
   Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Activez ce profil pour extraire les événements notables de la Splunk Enterprise Security console en fonction de votre planification. Il existe une limite de 1 000 incidents de sécurité qui peuvent être créés dans un délai de 24 heures. Jusqu'à 100 événements notables sont par alerte déclenchée. Les événements notables suivants seront ignorés une fois les limites atteintes.

   L'image suivante montre l'onglet Options supplémentaires avec les valeurs par défaut renseignées :



   Lorsque la configuration des options supplémentaires est activée, l'examen de l'incident d'événement notable affiche le changement de statut et une mise à jour des commentaires de l'historique :



Configurer un profil pour le transfert manuel d'événements

Selon le profil défini, Splunk ES les événements notables sont transférés manuellement en tant qu'événements notables discrets dans l'environnement Opérations de sécurité de votre Now Platform instance.

Pour configurer un profil pour le transfert manuel d'événements notables :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Section
Créer un profil d'événement	Reportez-vous à la rubrique Créer des profils pour les événements transférés manuellement.
Mapper les champs d'événements notables	Reportez-vous à la rubrique Mapper les champs d'événements notables pour l'intégration Splunk Enterprise Security.
Créer des mappages personnalisés	Reportez-vous à la rubrique Créer des mappages pour Splunk ES l'événement notable, l'examen des incidents et la contribution aux détails de l'événement (transfert manuel).
Prévisualiser l'incident de sécurité	Reportez-vous à la rubrique Prévisualiser l'incident de sécurité pour l'intégration de l'ingestion d'événements Splunk Enterprise Security.
Configurer votre environnement pour l'ingestion Splunk manuelle	Reportez-vous à la rubrique Configurez votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise Security notables.
Automatisez les mises à jour et la fermeture des événements notables en fonction de l'état de l'incident SIR	Reportez-vous à la rubrique Automatisez les mises à jour et la fermeture des événements notables en fonction de l'état de l'incident SIR.

Créer des profils pour les événements transférés manuellement

Vous pouvez configurer un profil pour les événements transférés manuellement.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

Pour créer un profil qui prend en charge le transfert manuel d'événements, procédez comme suit.

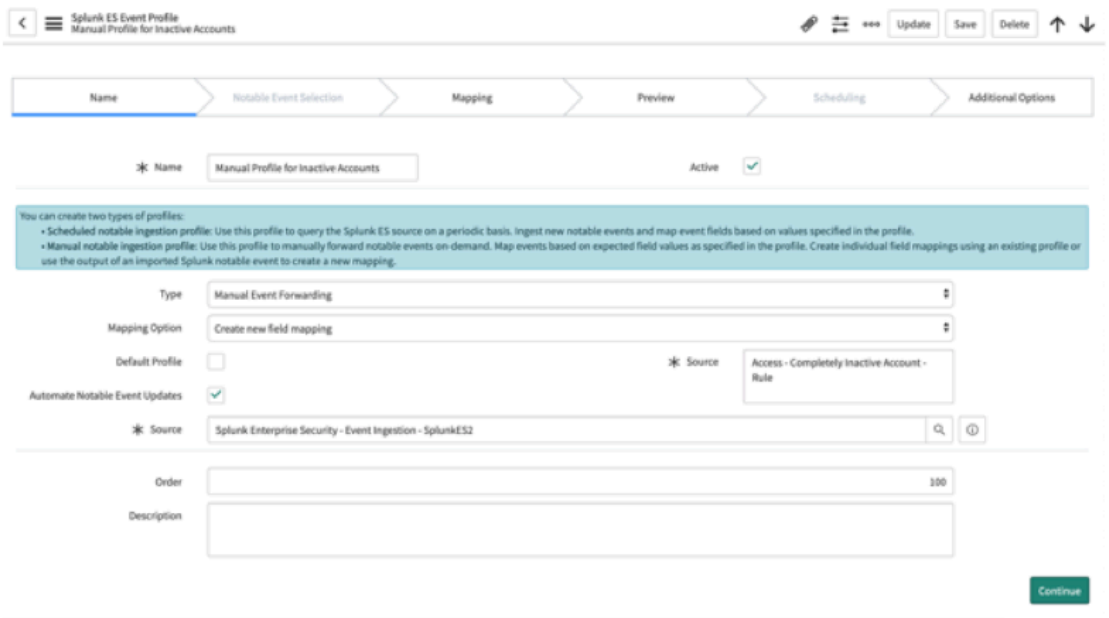
Pour les événements que vous transférez à la demande à partir de votre Splunk Enterprise Security console, vous pouvez baser le mappage de champs individuel sur n'importe quel profil existant. Vous pouvez également créer une nouvelle grille de mappage pour les données de pièce jointe exportées. Les événements que vous transférez manuellement ne sont pas planifiés dans le profil d'événement.

a. Si ce n'est pas déjà fait, dans la liste de choix du champ Type, sélectionnez **Transfert manuel d'événements**.

b. Dans le champ Option de mappage qui s'affiche, dans la liste de choix, choisissez une option de mappage pour continuer.

Reportez-vous aux figures et tableaux suivants pour plus d'informations sur les options de mappage disponibles dans la liste de choix Options de mappage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Créer une nouvelle option de mappage de champs

Option ou champ	Description
Créer une nouvelle option de mappage de champs	Nouveau mappage de champs pour votre événement. Si vous n'avez pas de mappage de champs existant similaire au profil que vous créez, sélectionnez cette option pour créer une nouvelle carte.
Profil par défaut	Profil de transfert d'événement par défaut pour tous les Splunk événements. La valeur par défaut est effacée (désactivée). Lorsque cette option est activée, ce profil devient le profil par défaut pour le transfert manuel d'événements. Ce profil est utilisé lorsqu'il n'y a aucune correspondance sur la source de l'événement transféré manuellement. Il devient le profil par défaut pour tous les événements dont les sources sont inconnues. Le champ Source n'est pas disponible si l'option de profil par défaut est activée.
Source (champ d'événement notable)	Il s'agit d'un champ qui définit généralement la règle de corrélation qui a déclenché les attaques notables, par exemple, les attaques par force brute. Ce champ n'est pas disponible si l'option de profil par défaut est activée.

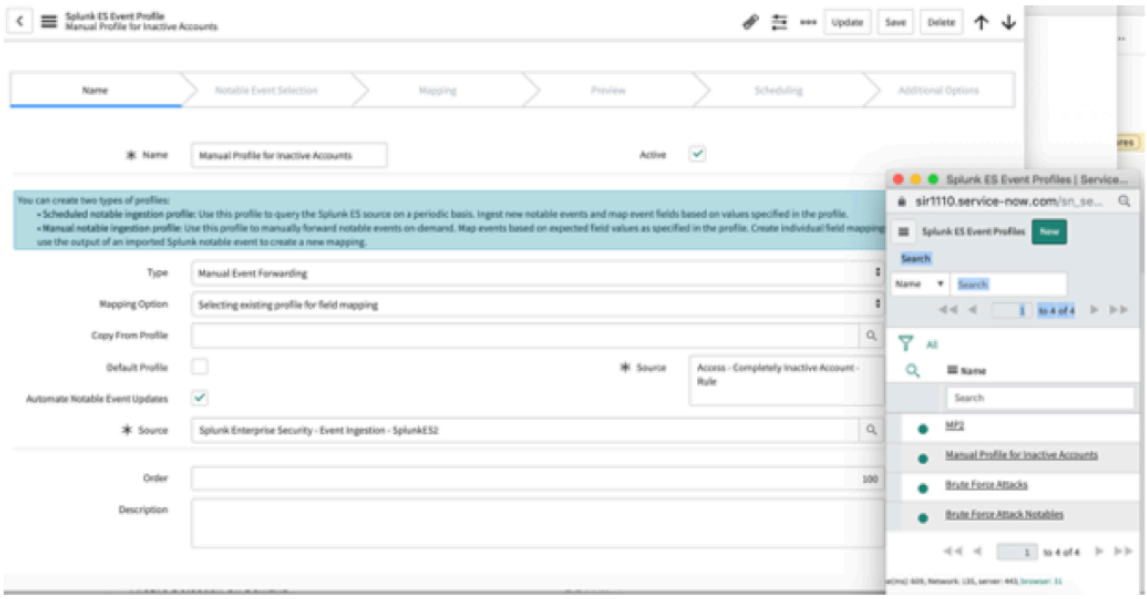
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	S'il est disponible, ce champ autorise le mappage de champs d'événements uniques avec les champs d'incidents de sécurité en fonction de la règle de corrélation Splunk qui est généralement différente pour différents types d'événements. Si vous souhaitez gérer différentes règles de corrélation séparément, vous pouvez créer différents profils d'événements de profil basés sur la règle de corrélation pour satisfaire à cette condition.
Automatiser les mises à jour des événements notables	Cochez cette case si vous souhaitez mettre à jour le statut de l'événement notable et ajouter des commentaires supplémentaires lorsqu'un incident SIR est créé à partir de l'événement notable et/ou lorsque l'incident SIR est fermé. Cela se produit à la fois pour les événements notables déclencheurs initiaux qui créent l'incident SIR et pour les événements agrégés.
Source (Splunk serveur)	Serveur Splunk que vous avez configuré comme source pour les événements notables. Si vous avez configuré plusieurs Splunk serveurs, sélectionnez le serveur approprié pour les types d'événements notables qui seront mis à jour pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Laissez ce paramètre sur la valeur par défaut. Si vous avez créé un grand nombre de profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow du profil dont le numéro est le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

Pour un profil avec un nouveau mappage de champ, vérifiez que vous avez saisi une valeur dans le champ Type de source et cliquez sur **Continuer** pour passer à l'étape de mappage de la configuration.

Pour un profil avec un mappage de champ existant, reportez-vous à la figure et au tableau suivants pour plus d'informations.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Sélectionner un profil existant pour l'option de mappage de champ

Option ou champ	Description
Sélectionner un profil existant pour le mappage de champs	Réutilisez un mappage de champs existant pour votre nouveau profil d'événement notable. Le champ Copier à partir du profil s'affiche. Procédez comme suit pour copier un mappage de champ existant pour ce profil. **i.** À gauche du champ Copier à partir du profil qui s'affiche, cliquez sur l'icône de recherche. **ii.** Dans la liste des profils d'événements Splunk ES qui s'affiche, cliquez sur le nom du profil qui contient la carte que vous souhaitez copier. Le nom du profil s'affiche dans le champ Copier à partir du profil.
Profil par défaut	Profil de transfert d'événement par défaut pour tous les événements notables dont la Splunk source n'a pas de correspondance. Désactivé par défaut. Lorsque cette option est activée, ce profil devient le profil par défaut pour le transfert manuel d'événements. Le champ Source n'est pas disponible si l'option de profil par défaut est activée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
Source (champ d'événement notable)	Il s'agit d'un champ qui définit généralement la règle de corrélation qui a déclenché les attaques notables, par exemple, les attaques par force brute. Ce champ n'est pas disponible si l'option de profil par défaut est activée. S'il est disponible, ce champ autorise le mappage de champs d'événements uniques avec les champs d'incidents de sécurité en fonction de la règle de corrélation Splunk qui est généralement différente pour différents types d'événements. Si vous souhaitez gérer différentes règles de corrélation séparément, vous pouvez créer différents profils d'événements de profil basés sur la règle de corrélation pour satisfaire à cette condition.
Automatiser les événements notables	Cochez cette case si vous souhaitez mettre à jour le statut de l'événement notable et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir de l'événement notable ou lorsque l'incident de sécurité est fermé. Cela se produit à la fois pour les événements notables déclencheurs initiaux qui créent l'incident de sécurité et pour les événements agrégés.
Source (Splunk serveur)	Splunk Fin de serveur ou de recherche que vous avez configurée comme source pour les événements notables. Si vous avez configuré plusieurs Splunk serveurs, sélectionnez le serveur approprié pour les types d'événements notables qui seront mis à jour pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Laissez ce paramètre sur la valeur par défaut. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow du profil dont le numéro est le plus bas a la priorité la plus élevée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

Au bas du formulaire de sélection d'un mappage existant pour votre profil, cliquez sur **Terminer** pour finaliser la configuration du profil.

Créer des mappages pour Splunk ES l'événement notable, l'examen des incidents et la contribution aux détails de l'événement (transfert manuel)

Au cours de l'étape de mappage des champs d'événements notables, vous mappez les champs d'événements individuels des événements notables aux champs d'un Now Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Mappez jusqu'à cinq événements notables de la colonne Ingestion d'échantillons d'événements notables à gauche du formulaire aux champs d'incident de sécurité dans la colonne Mappage de champs d'incidents SIR à droite.

Créez des mappages personnalisés en ajoutant ou en supprimant les champs de la grille de mappage sur le côté droit du formulaire. Les champs par défaut qui sont généralement des champs importants à renseigner sur le formulaire d'incident SIR s'affichent. Toutefois, ces champs peuvent être supprimés et tous les champs supplémentaires peuvent être affichés à l'aide des boutons + et -. Créez des cartes personnalisées en ajoutant ou en supprimant les champs de la grille de mappage sur le côté droit du formulaire. La personnalisation des champs vous permet de mapper Splunk des champs qui ne sont pas affichés sur la grille de mappage par défaut sur l'incident SIR de sécurité.

Procédure
1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Suivez ces étapes pour charger les données de pièce jointe dans votre Now Platform® instance.

   a. Si vous n'êtes pas déjà connecté, connectez-vous à votre Splunk Enterprise console.

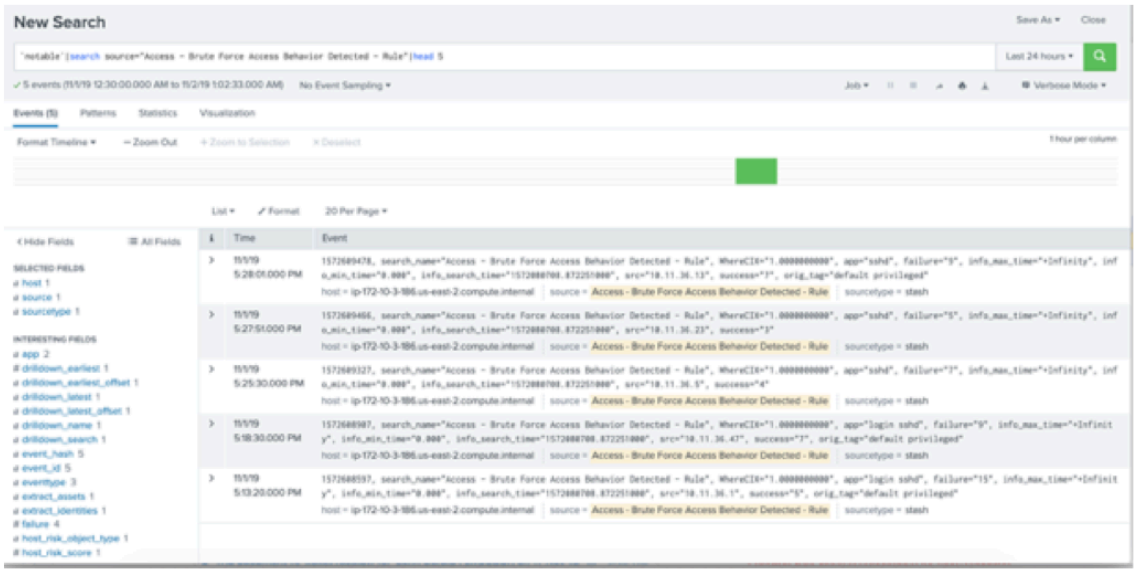
   b. Accédez à l'onglet Rechercher et entrez un nom pour une recherche contenant les données d'événements notables que vous souhaitez exporter.
   Un exemple de format de recherche permettant de récupérer des événements notables pour la règle de corrélation Comportement d'accès par force brute serait le suivant : 'notable' | search source="Access - Comportement d'accès par force brute détecté - Règle ».

   c. Développez l'événement notable et, dans la colonne Champ, sélectionnez les champs que vous souhaitez importer.

   Ces champs correspondent aux paires champ-valeur qui sont exportées et affichées sur la page de mappage de votre Now Platform® instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

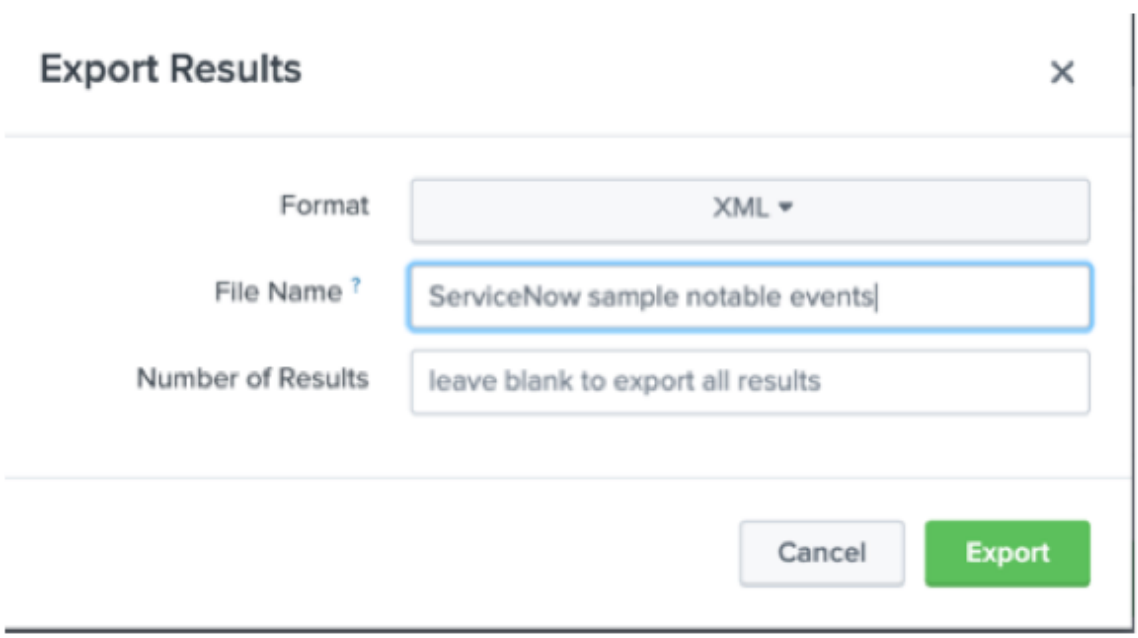


d. Dans votre Splunk Enterprise console, en haut à droite de la page de recherche, cliquez sur l'icône **Exporter** .

e. Dans la liste de choix du champ Format de la boîte de dialogue qui s'affiche, cliquez sur **Format XML**.

f. Facultatif : Entrez un nouveau nom de fichier.

g. Cliquez sur **Exporter**.



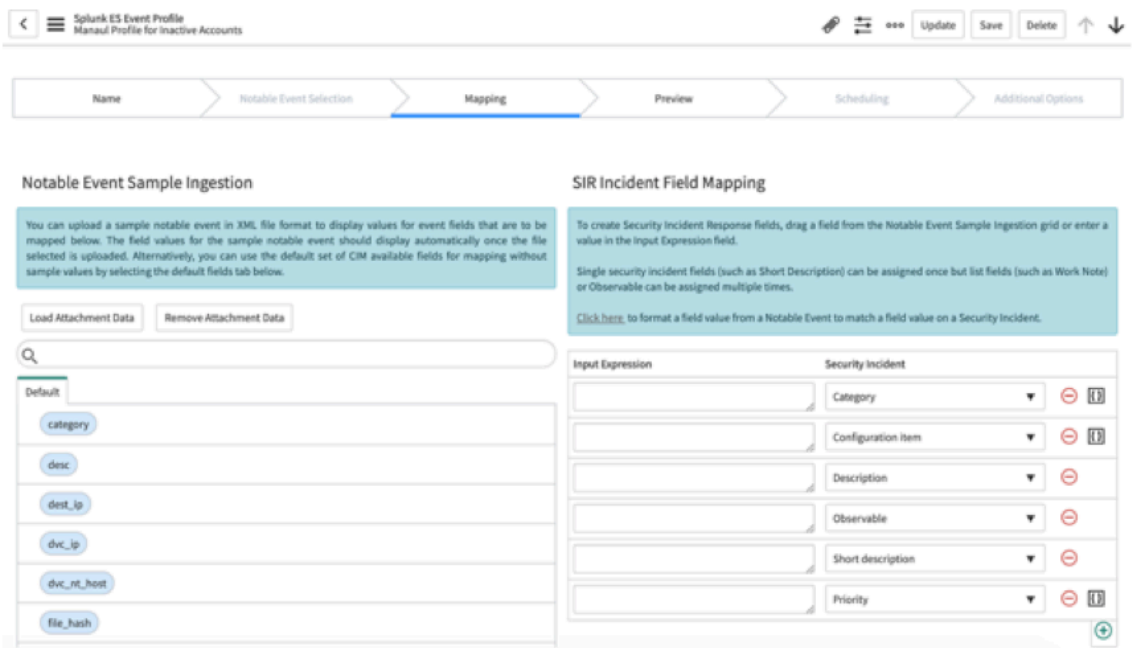
Le fichier XML de l'événement notable exporté Splunk doit maintenant être téléchargé sur votre Now Platform® instance.

h. Si la page de mappage n'est pas déjà affichée dans votre Now Platform® instance, cliquez sur **Mappage** dans la barre de progression.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Dans la colonne Ingestion d'échantillons d'événements notables, cliquez sur **Charger les données de la pièce jointe**.



j. Dans la boîte de dialogue qui s'affiche, cliquez sur **Choisir des fichiers** et accédez au `fichier .xml` que vous avez exporté, puis cliquez sur **Ouvrir**.
Une fois que vous avez cliqué pour charger les données de pièce jointe pour les événements transférés manuellement, les champs d'événements Splunk ES notables sont renseignés sur le côté gauche du formulaire. Ces valeurs correspondent aux valeurs de champ que vous mappez aux champs d'incident de sécurité du côté du formulaire Mappage de champs d'incident SIR.
Les paires de valeurs des champs que vous avez exportés pour l'événement s'affichent sur le côté gauche du formulaire de mappage.

3. Suivez les étapes 5 à 10 de la Créer des mappages pour Splunk ES la revue des incidents d'événements notables et la contribution aux détails de l'événement (ingestion planifiée) section.

Configurez votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise Security notables

Installez et configurez le ServiceNow module complémentaire Security Operations Event Ingestion pour l'application dans Splunk Enterprise Security votre Splunk console d'entreprise ou votre instance Splunk Cloud si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise Security console pour cette intégration.

Avant de commencer

L'installation et la configuration du ServiceNow module complémentaire Security Operations Event Ingestion pour l'application dans Splunk Enterprise Security votre console d'entreprise ou dans votre Splunk instance Splunk Cloud sont facultatives.

Vérifiez que vous avez installé l'application pour cette intégration ServiceNow Store avant d'installer le module d'extension Splunkbase requis pour l'ingestion manuelle d'événements. Si vous n'avez pas installé l'application pour l'intégration à partir de , consultez ServiceNow StoreInstallez et configurez l'application ServiceNow pour l'intégration

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'ingestion d'événements Splunk Enterprise Security notables et suivez les instructions pour l'installer.

Rôle requis : Splunk Enterprise Security administrateur

Pourquoi et quand exécuter cette tâche

Si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise console pour l'intégration, téléchargez, installez et configurez le ServiceNow module complémentaire Security Operations Event Ingestion pour Splunkbase dans Splunk Enterprise Security votre Splunk Enterprise Security console. Ce ServiceNow module complémentaire d'extension est requis pour que les incidents de sécurité puissent être créés à partir d'événements exportés manuellement dans votre Now Platform instance. Ce ServiceNow module complémentaire d'ingestion d'événements de Security Operations pour Splunk Enterprise Security l'application est disponible sur splunkbase .

Pour le transfert manuel d'événements, vous pouvez identifier jusqu'à deux points de terminaison (instances) différents Now Platform dans votre Splunk Enterprise Security console. Vous transférez manuellement les événements au ou aux points de terminaison pour créer des incidents de sécurité. Par exemple, vous pouvez spécifier à la fois une instance de stockage intermédiaire (développement) et une instance de production. En spécifiant des instances distinctes et en nommant des workflows primaires et secondaires pour chaque instance, vous pouvez choisir où vous souhaitez transférer les différents événements.

Procédure

1. Si vous n'avez pas encore installé le ServiceNow module complémentaire Security Operations Event Ingestion pour Splunk Enterprise Security, procédez comme suit pour l'installer et le configurer.

   a. Accédez à splunkbase .

   b. Recherchez le module complémentaire ServiceNow Opérations de sécurité Security Operations Event Ingestion for Splunk Enterprise Security.

      Remarque : Vérifiez que vous avez sélectionné ServiceNow Opérations de sécurité le module complémentaire d'ingestion d'événements pour Splunk Enterprise Security. Il existe d'autres ServiceNow addons qui sont affichés dans cette liste. Ces modules complémentaires sont destinés à différentes ServiceNow Splunk intégrations et ne sont pas requis pour cette intégration.

   c. Téléchargez l'application.

   d. Ouvrez votre Splunk Enterprise Security compte.

   e. Sur la page Applications, cliquez sur l'icône d'engrenage ou sur le raccourci **Gérer les applications** dans la liste déroulante du menu.

   f. Dans le coin supérieur gauche de la page Applications qui s'affiche, cliquez sur **Installer l'application à partir d'un fichier**.

   g. Cliquez sur **Choisir un fichier**, sélectionnez ServiceNow Security Operations Event Ingestion Addon pour Splunk Enterprise Security, puis cliquez sur **Télécharger**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

h. Si vous y êtes invité, redémarrez Splunk Enterprise.
Le module complémentaire Splunk Enterprise Security d'ingestion ServiceNow d'événements pour Security Operations est installé dans votre Splunk Enterprise Security console. L'étape suivante pour configurer l'Addon.

2. Pour configurer le complément, procédez comme suit.

a. Dans Splunk Enterprise Security, cliquez sur l'icône **d'engrenage Applications** ou sur **Gérer les applications** dans la liste déroulante du menu.

b. Dans la liste des applications qui s'affiche, dans la colonne **Actions** , cliquez sur **Configurer** pour ServiceNow Opérations de sécurité le complément d'ingestion d'événements pour Splunk Enterprise Security.

c. Remplissez le formulaire.

La figure suivante est un exemple de formulaire rempli dans votre Splunk Enterprise Security console.



Champ dans la section Spécifier l'instance primaire ServiceNow	Description
Étiquette de l'action de workflow	Nom du workflow pour votre Now Platform instance de production (principale). Ce nom est le nom d'une Now Platform ins-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ dans la section Spécifier l'instance primaire ServiceNow	Description
	tance que les utilisateurs qui surveillent les Splunk événements identifient comme instance principale, par exemple, Servicenow Event Ingestion (Production). La valeur par défaut pour ce champ est Ingestion d'événements ServiceNow (production). Dans votre Splunk Enterprise Security console, ce nom de workflow s'affiche pour l'instance de production (principale) dans la liste déroulante `Actions d'événement` développée d'une recherche. Ce nom est le nom de votre instance de production. Vous pouvez modifier le nom.
URL	URL de l'instance Now Platform que vous avez saisie dans le champ Étiquette de l'action de workflow précédent. Copiez l'URL dans votre navigateur et collez-la dans ce champ du formulaire.
Point de terminaison	Chemin de l'API de base. Pour plus d'informations, reportez-vous à la figure qui suit le tableau. Si vous n'avez pas de valeur pour le point de terminaison de votre Now Platform instance de production, procédez comme suit. **a.** Connectez-vous à votre Now Platform instance de production en tant qu'utilisateur disposant du rôle d'administrateur système (admin). **b.** `Entrez les API REST basées sur un script` dans le panneau de navigation. **c.** Une fois le panneau de navigation actualisé, sélectionnez le module **API REST scripté** qui s'affiche. **d.** Si l'ingestion d'événement n'est pas répertoriée dans la colonne Nom de la liste API `REST scriptées` qui s'affiche, dans le champ de recherche en haut, saisissez `l'ingestion d'événement`. **e.** Dans la colonne Chemin d'accès de l'API de base sur la page actualisée, copiez cette valeur et collez-la dans le champ Point de terminaison du formulaire. Un

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

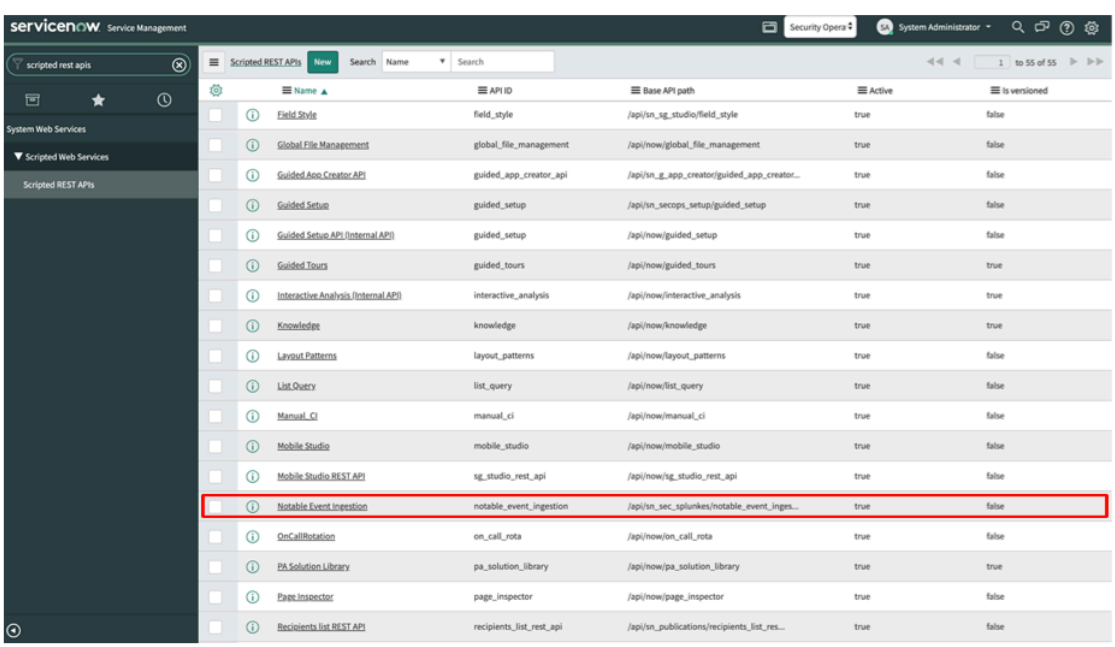
Champ dans la section Spécifier l'instance primaire ServiceNow	Description
	exemple de chemin d'accès de l'API de base est `/api/sn_sec_splunk_-v2/event_ingestion`.
Nom d'utilisateur	Nom d'utilisateur de votre Now Platform instance. Ce nom est le nom d'utilisateur de l'instance Now Platform dans laquelle vous avez affecté un utilisateur avec le rôle (sn_-sec_splunk_v2.api_account_access) pour le transfert manuel d'événements. Pour en savoir plus sur l'affectation de ce rôle, reportez-vous à Configurer votre Now Platform instance pour l'intégration Splunk Enterprise Event Ingestion.
Mot de passe	Mot de passe de votre Now Platform instance. Ce mot de passe est le mot de passe de l'instance Now Platform dans laquelle vous avez affecté un utilisateur avec le rôle (sn_-sec_splunk_v2.api_account_access) pour le transfert manuel d'événements.
(Facultatif) Champs dans la section Spécifier l'instance secondaire ServiceNow	Description Ces champs sont facultatifs. Vous n'êtes pas obligé de spécifier une instance secondaire.
Étiquette de l'action de workflow	Nom du workflow pour votre Now Platform instance secondaire (intermédiaire). Ce nom correspond au nom d'une Now Platform instance que les utilisateurs qui surveillent les Splunk événements identifient comme instance secondaire, par exemple, ServiceNow Ingestion d'événements (intermédiaire). Dans votre Splunk Enterprise Security console, ce nom de workflow s'affiche pour l'instance intermédiaire (secondaire) dans la liste déroulante Actions d'événement développée d'une recherche. Cette Now Platform instance est votre instance intermédiaire. Vous pouvez modifier le nom.
URL	URL de l'instance Now Platform que vous avez saisie dans le champ Étiquette de l'action de workflow précédent pour l'instance secondaire Now Platform . Copiez l'URL dans votre navigateur et collez-la dans ce champ du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ dans la section Spécifier l'instance primaire ServiceNow	Description
Point de terminaison	Chemin de l'API de base. Cette valeur du chemin d'accès de l'API de base pour votre instance secondaire est la même que celle du chemin de l'API de base pour votre instance primaire. Consultez la figure précédente du formulaire pour plus d'informations.
Nom d'utilisateur	Nom d'utilisateur de votre Now Platform instance de stockage intermédiaire. L'utilisateur doit disposer du rôle (sn_sec_splunk_-v2.api_account_access).
Mot de passe	Mot de passe de votre Now Platform instance de stockage intermédiaire. L'utilisateur doit disposer du rôle (sn_sec_s-plunkes.api_account_access).

La figure suivante est un exemple de la liste des API REST scriptées dans votre Now Platform. La liste affiche l'emplacement de la valeur de point de terminaison d'une Now Platform instance que vous entrez dans le formulaire dans le cadre de la configuration ServiceNow du module complémentaire Security Operations Event Ingestion pour extension dans Splunk Enterprise Security votre Splunk Enterprise Security console.



3. Dans le formulaire de configuration de votre Splunk Enterprise Security console, cliquez sur **Enregistrer** pour enregistrer vos modifications.

   Après quelques instants, en haut à gauche du formulaire de votre Splunk Enterprise Security console, un message s'affiche indiquant que l'enregistrement a été mis à jour.

   Une fois le formulaire enregistré, les noms (étiquettes d'action de workflow) de votre Now Platform ou vos instances que vous avez créées dans le formulaire sont disponibles dans la liste de choix Actions d'événement sur un événement sélectionné d'une recherche dans votre Splunk Enterprise Security console.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Si vous n'avez pas encore enregistré les recherches dans votre Splunk Enterprise Security console, l'étape suivante consiste à enregistrer les recherches en tant qu'alertes dans votre Splunk Enterprise Security console.

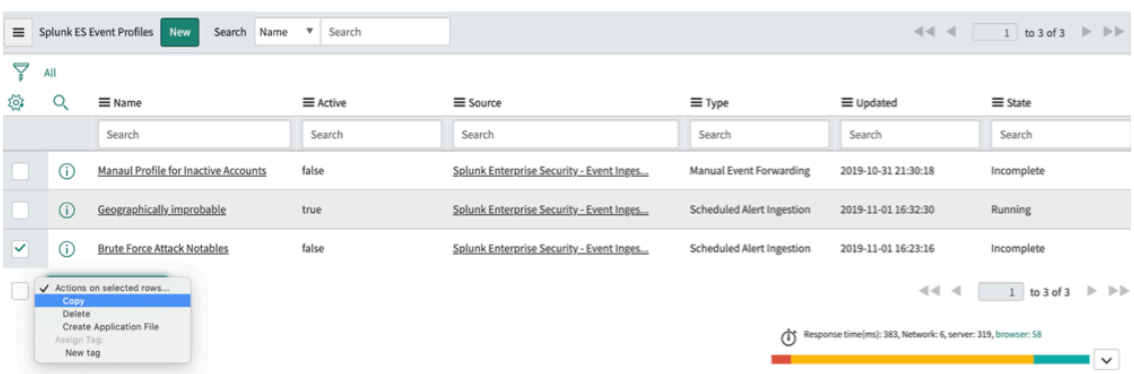
Copier un profil d'événement pour l'intégration de l'ingestion d'événements Splunk Enterprise Security

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils d'alarme pour gagner du temps.

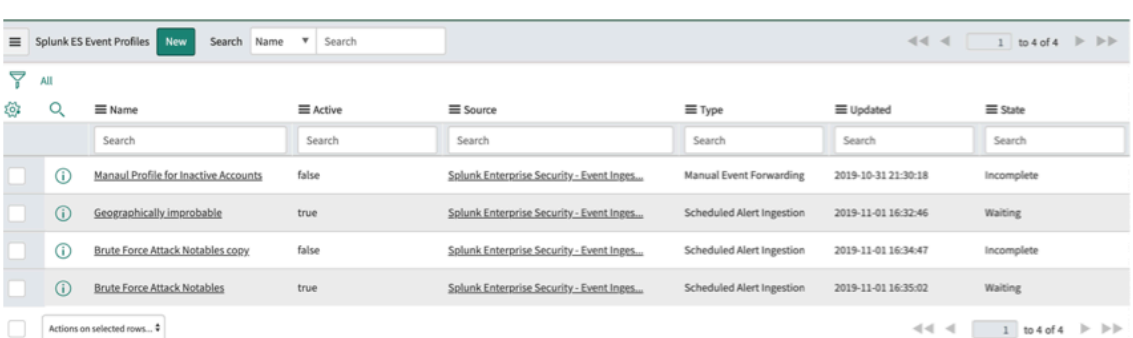
Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Si vous copiez un profil, le nom du profil est d'abord modifié pour éviter les doublons. En outre, le profil copié est désactivé (faux) afin qu'il ne soit pas activé accidentellement avant la fin de la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure
1. Accédez à la **Tout** > **Splunk Integration** > **Profil d'événement Splunk**.
2. Dans la liste Profils d'événements Splunk qui s'affiche, sélectionnez un profil que vous souhaitez copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier**.



Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (`vrai`), la copie est désactivée à ce stade (`faux`). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Vous êtes invité à activer le nouveau profil une fois que vous avez terminé l'étape de configuration.

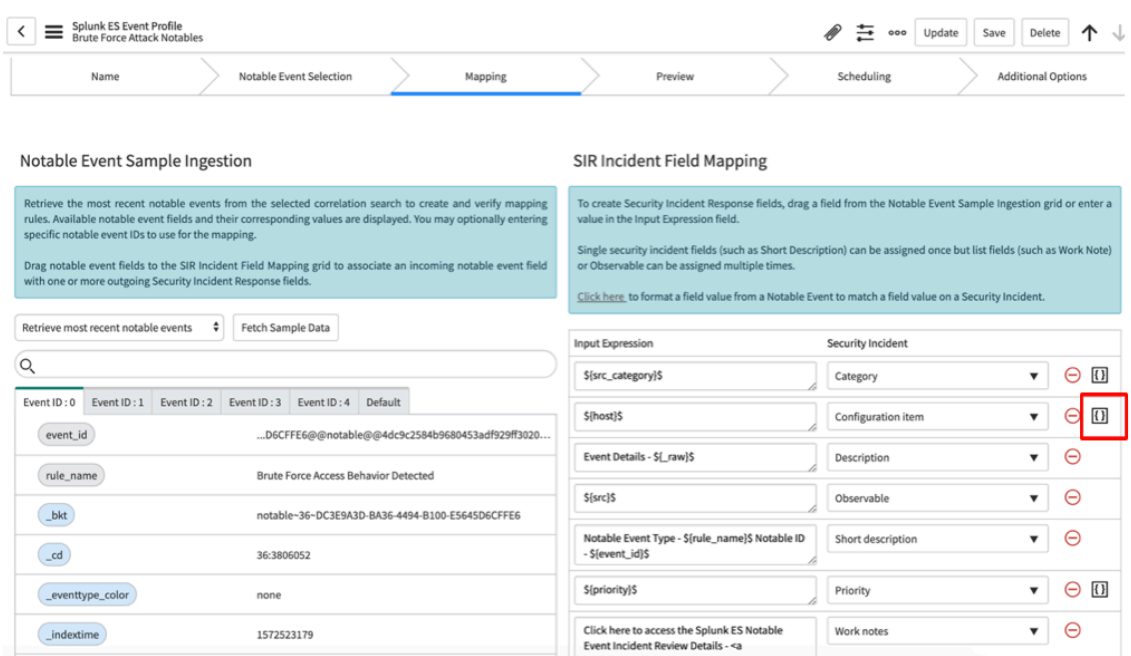
Utiliser l'éditeur de script pour formater les valeurs d'alerte pour l'intégration de l'ingestion d'événements Splunk Enterprise Security

En plus des champs directement mappés à partir des valeurs d'événements notables ingérées et des valeurs que vous saisissez manuellement, utilisez l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Dans certains cas, Splunk Enterprise Security les valeurs d'événements notables sont mappées aux champs Catégorie, Élément de configuration (CI) et Observables de l'incident SIR ne sont pas prises en charge. Vous préférez peut-être modifier les valeurs mappées. Si vous souhaitez convertir la valeur d'un Splunk Enterprise Security événement notable en une valeur prise en charge par ces champs sur l'incident SIR de sécurité, utilisez l'éditeur de script.

Procédure
1. Une fois le formulaire de mappage affiché, cliquez sur le lien pour ouvrir l'éditeur de script.



2. Dans la liste de choix, sélectionnez un champ de destination pour la valeur que vous souhaitez modifier.
3. Dans la section Mappage de champs d'incidents SIR, vous pouvez également cliquer sur l'icône de crochet `[{}]` en regard d'un champ pour ouvrir l'éditeur de script relatif à ce champ.

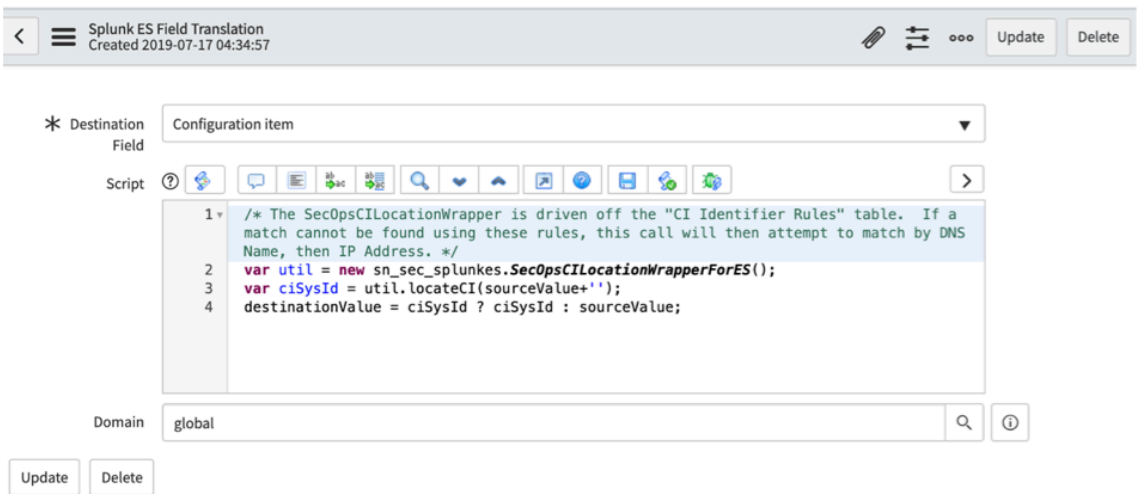
   Dans certains cas, un include de script peut être approprié pour le champ Élément de configuration. Pour un événement notable, par exemple, une valeur pour l'élément de configuration peut ne pas correspondre.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comme le montre la figure suivante, si une correspondance de nom d'hôte est introuvable dans la Now Platform® CMDB pour le champ Élément de configuration, vous pouvez modifier la règle de sorte que, si une adresse IP est trouvée, elle remplisse le champ Élément de configuration. S'il n'y a pas de valeur pour l'alarme, le champ de l'incident de sécurité est défini sur null.

L'éditeur s'ouvre avec le champ affiché dans Champ de destination. L'image suivante montre l'éditeur avec le champ `Élément de configuration` comme champ de destination.



4. Entrez toutes les modifications dans le script, puis cliquez sur **Mettre à jour** pour enregistrer vos modifications.
   La Splunk table Traductions de champ s'affiche.
5. Fermez la table pour revenir au formulaire de mappage.

Copier Splunk Enterprise Security les profils d'une instance à l'autre à l'aide de la fonctionnalité d'exportation/importation

Vous pouvez exporter et importer Splunk Enterprise Security les paramètres des profils d'une Now Platform instance à une autre Now Platform .

Avant de commencer

Les paramètres que vous pouvez exporter et importer incluent le nom du profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les exemples de données extraits, la planification et les informations sur la source des vignettes de configuration.

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Cette fonctionnalité permet à l'administrateur de sécurité de copier des profils qui ont été testés et vérifiés sur une instance, par exemple en non-production, vers une Now Platform autre Now Platform instance, par exemple en production, sans avoir à refaire tous les paramètres de configuration. Les paramètres exportés et importés comprennent le nom du profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les données d'échantillon extraites, la planification et les informations sur la source des vignettes de configuration.

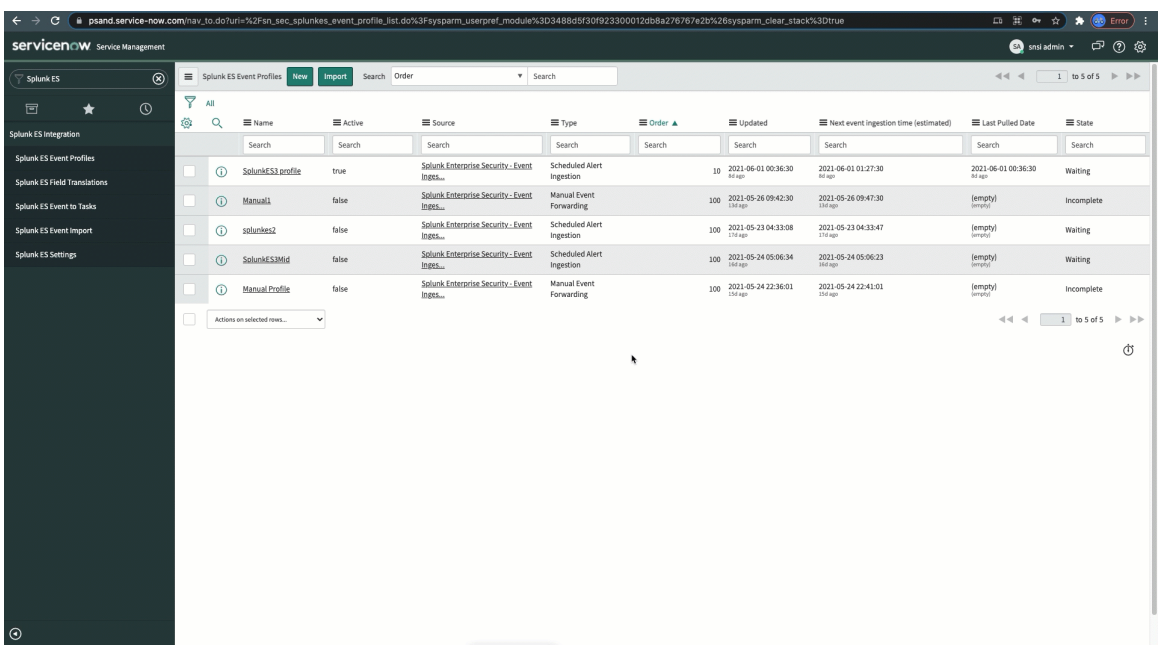
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous exportez un type de profil de transfert d'événements manuel, les données de pièce jointe utilisées pour l'exemple de mappage de champ sont copiées, mais le fichier de pièce jointe lui-même n'est pas exporté.

Procédure

1. Accédez à la **Tout** > **Intégration de Splunk ES** > **Profils d'événements Splunk ES**.
2. Sélectionnez un profil que vous souhaitez exporter vers une autre Now Platform instance. Vous pouvez sélectionner plusieurs profils pour l'exportation.
3. Dans le menu Actions, cliquez sur **Exporter**.
4. Une fois que le message « Exportation terminée » s'affiche, cliquez sur **Télécharger**.

   L'illustration suivante montre l'exportation d'un profil (SplunkES3profile) à partir de l'instance Now Platform (psand.service-now.com).



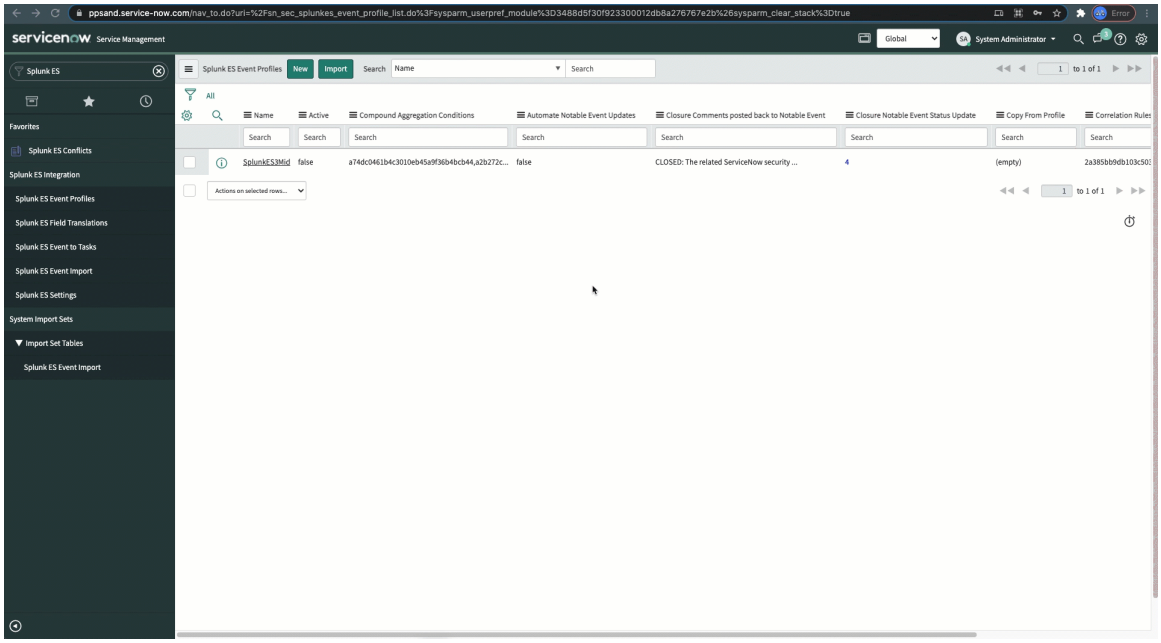
   Le fichier payload.xml exporté est téléchargé sur votre ordinateur. Le fichier contient le nom du profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les exemples de données récupérées, la planification et les informations sur la source des vignettes de configuration. Lorsque vous sélectionnez et téléchargez plusieurs profils, ils apparaissent dans le même fichier payload.xml.

   Vous pouvez maintenant procéder à l'importation du profil dans une autre Now Platform instance.

5. Accédez à la **Intégration de Splunk ES** > **Profils d'événements Splunk ES**.
6. Cliquez sur **Importer**.
7. Cliquez sur **Choisir un fichier** et sélectionnez le fichier xml sur votre ordinateur.
8. Cliquez sur **Charger**.
9. Cliquez sur **Fermer et recharger les profils**.

   L'illustration suivante montre l'importation d'un profil (SplunkES3profile) de l'instance Now Platform (psand.service-now.com) vers l'instance Now Platform (ppsand.service-now.com).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous avez importé le profil avec succès à partir d'une autre Now Platform instance.

Vérifiez que les paramètres de configuration de la source exportée (Splunk compte API et Splunk URL du serveur) et du serveur MID sont valides et disponibles dans l'instance importée Now Platform . Mettez à jour votre Splunk Enterprise Security configuration si nécessaire.

10. Facultatif : Vérifiez les paramètres du Serveur MID après l'importation d'un profil.
11. Facultatif : Accédez à la **Security Operations** > **Configurations d'intégration**.
12. Facultatif : Sélectionnez la vignette de Splunk Enterprise Security configuration, puis cliquez sur **Mettre à jour**.
13. Facultatif : Examinez et mettez à jour les détails de la source et du serveur MID selon les besoins.

Liste de vérification pour l'intégration de l'ingestion d'événements Splunk Enterprise Security notables

Utilisez cette liste de vérification pour vous guider dans toutes les tâches de l'intégration. La liste de vérification suivante comprend les tâches de configuration et d'installation, ainsi que des exemples de cas d'utilisation incluant les résultats attendus pour l'intégration.

Avant de commencer
Rôles requis : admin, sn_si.admin, sn_si.analyst, Splunk Enterprise Security administrator

Pourquoi et quand exécuter cette tâche
Suivez la progression de l'installation, de l'installation et de la configuration de l'intégration à l'aide de la table suivante. Terminez toutes les tâches d'une étape avant de passer à l'étape suivante. Chaque ligne du tableau répertorie les tâches et identifie les rôles requis pour effectuer les tâches. Les rubriques numérotées du guide d'installation et de configuration sont également référencées.

Les rôles requis pour chaque tâche sont répertoriés à chaque étape dans la table suivante.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Suivez la progression de l'installation, de l'installation et de la configuration de l'intégration. Terminez toutes les tâches d'une étape avant de passer à l'étape suivante.
2. Suivez les étapes du tableau dans l'ordre dans lequel elles sont présentées.

Liste de vérification

☐	En tant qu'utilisateur disposant du Now Platform rôle administrateur, configurez votre Now Platform instance. ◦ Affectez des utilisateurs ayant les rôles sn_si.admin et sn_si.analyst, selon les besoins. ◦ Installez et configurez un serveur MID si le Splunk serveur est déployé au sein de votre réseau d'entreprise. ◦ Vérifiez que les modules d'extension ServiceNow Réponse aux incidents de sécurité sont activés pour votre version du Now Platformfichier . ◦ (Facultatif) Si vous souhaitez transférer manuellement des événements de votre Splunk Enterprise Security console vers votre Now Platform instance, vérifiez que vous avez affecté le rôle (sn_sec_splunkes.api_account_access) à un utilisateur disposant de l'autorisation d'administrateur Splunk Enterprise Security . Pour plus d'informations, consultez #unique_1734.
☐	En tant qu'utilisateur disposant du Now Platform rôle administrateur, installez et configurez l'application Splunk Enterprise Security à partir du ServiceNow Store. **a.** Téléchargez et installez l'application sur votre Now Platform instance. **b.** Configurez l'application et connectez-vous à votre Splunk Enterprise Security console. Pour plus d'informations, consultez Installez et configurez l'application ServiceNow pour l'intégration d'ingestion d'événements Splunk Enterprise Security notables.
☐	(Facultatif) Si vous avez l'intention d'exporter manuellement des événements de votre Splunk Enterprise Security console vers votre Now Platform instance, effectuez les tâches suivantes : ◦ En tant qu'administrateur Splunk Enterprise Security , installez, configurez et activez le ServiceNow module complémentaire Security Operations Event Ingestion pour Splunk Enterprise Security à partir de splunkbase dans votre Splunk Enterprise Security console. ◦ En tant qu'administrateur Splunk Enterprise Security , si ce n'est pas déjà fait, enregistrez les recherches en tant qu'événements notables dans votre Splunk Enterprise Security console. Pour plus d'informations, consultez Configurez votre Splunk environnement pour l'ingestion manuelle d'événements pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	l'intégration de l'ingestion d'événements Splunk Enterprise Security notables.
☐	En tant qu'utilisateur disposant du Now Platform rôle sn_si.admin, créez et nommez un profil d'événement. Sélectionnez le type de profil dans la liste de choix. Les options sont un profil d'alerte planifiée que vous utilisez pour ingérer des exemples de données ou un profil d'événement que vous utilisez pour exporter manuellement des données de pièce jointe à partir de votre Splunk Enterprise Security console. ◦ Pour une alerte planifiée, sélectionnez une alerte disponible. ◦ Pour le profil des données exportées manuellement, créez une nouvelle carte ou copiez une carte existante. Pour plus d'informations, consultez Créer et nommer un profil d'événement pour l'intégration d'ingestion d'événements Splunk Enterprise Security.
☐	En tant qu'utilisateur disposant du Now Platform rôle sn_si.admin, mappez les valeurs ingérées ou les données de pièce jointe exportées Splunk Enterprise Security vers Now Platform les incidents de sécurité. **a.** Extrayez des exemples de données pour une alerte planifiée. **b.** (Facultatif) Exporter manuellement des données de pièce jointe à partir d'un Splunk Enterprise Security événement. **c.** Modifiez la configuration de mappage par défaut. **d.** Vous pouvez également ajouter des critères de filtrage, ajouter une alerte à un incident de sécurité existant et utiliser l'éditeur de script. Pour plus d'informations, consultez Mapper les champs d'événements notables pour l'intégration Splunk Enterprise Security et Créer des mappages pour Splunk ES la revue des incidents d'événements notables et la contribution aux détails de l'événement (ingestion planifiée).
☐	◦ En tant qu'utilisateur disposant du Now Platform rôle sn_si.admin, prévisualisez les données qui Splunk Enterprise s'affichent sur un Now Platform incident de sécurité. ◦ Corrigez les erreurs ou ajoutez des données manquantes afin qu'aucun message d'erreur ne s'affiche. Pour plus d'informations, consultez Prévisualiser l'incident de sécurité pour l'intégration de l'ingestion d'événements Splunk Enterprise Security.
☐	En tant qu'utilisateur disposant du Now Platform rôle sn_si.admin, planifiez la récupération d'alerte pour un profil avec une alerte planifiée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	Pour plus d'informations, consultez Planifiez et récupérez les événements notables nouveaux ou mis à jour pour l'intégration de l'ingestion d'événements Splunk Enterprise Security.

Vous avez terminé avec succès les étapes de configuration et vérifié les résultats attendus pour l'intégration.

Splunk - Intégration de l'enrichissement pour les incidents

L'intégration Splunk d'enrichissement d'incident recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer	Configuration
Intégrations de Réponse aux incidents de sécurité	Premiers pas avec l'intégration de recherche Splunk pour Opérations de sécurité
Utiliser • Exécuter une recherche d'observations • Security Operations Integration - Workflow de recherche de perceptions • Security Operations Integration : workflow de recherche d'observations Splunk • Afficher les détails de la recherche d'observations • Afficher les résultats de recherche d'observations	Développer • ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et Informations supplémentaires • Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service et assistance client	

Premiers pas avec l'intégration de recherche Splunk pour Opérations de sécurité

Splunk Le logiciel recherche, surveille et analyse les données volumineuses générées par la machine et s'intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l'intégration Splunk d'enrichissement d'incident, vous devez la télécharger à ServiceNow Store partir du et ajouter l'URL de base API et les informations d'identification de connexion appropriées.

Avant de commencer

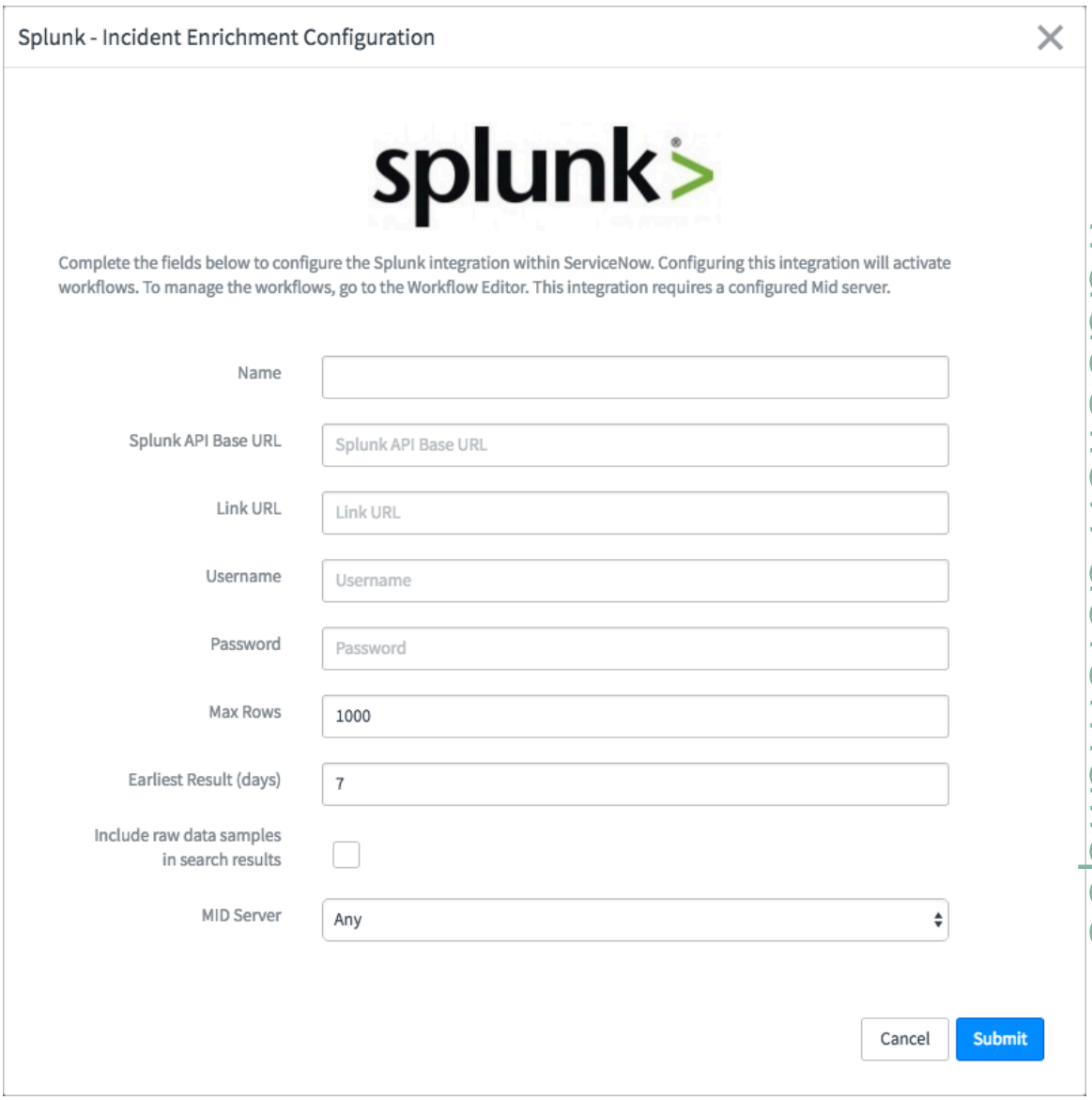
Rôle requis : sn_si_admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à Splunk la clé API et à l'ID API sous votre profil, et obtenez-les.
3. Dans votre instance, accédez à **Security Operations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la fiche Splunk - Enrichissement d'incident, cliquez sur **Nouveau**.



5. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
URL de Base de l'API Splunk	L'URL de base que vous avez acquise à partir du Splunk site.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL de lien	[Facultatif] URL du lien qui renvoie à l'interface Web, lorsqu'elle Splunk est disponible.
Nom d'utilisateur	Votre nom d'utilisateur Splunk.
Mot de passe	Votre mot de passe Splunk.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend du paramètre que vous définissez sur le **nombre de lignes de la propriété de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	Sélectionnez **N'importe lequel** pour utiliser n'importe quel Serveur MID actif ou sélectionnez un nom de Serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

6. Cliquez sur **Envoyer**.
   La carte de configuration de l'intégration s'affiche.
7. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
8. Pour revenir à la liste initiale des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Expérience mobile pour Réponse aux incidents de sécurité

Utilisez votre équipement mobile Android ou iOS pour gérer vos tâches du centre des opérations de sécurité (SOC).

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Réponse aux incidents de sécurité

Si vous n'êtes pas familier avec les concepts de base du Réponse aux incidents de sécurité produit (SIR) sur votre Now Platform® instance, consultez la rubrique Réponse aux incidents de sécurité Vue d'ensemble pour en savoir plus sur Threat Intelligence et sur la manière dont ce produit peut vous aider à hiérarchiser et à résoudre les cybermenaces qui pèsent sur votre organisation.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble

En tant que responsable du centre des opérations de sécurité (SOC) ou utilisateur ayant le rôle d'analyste Now Platform de la sécurité (sn_si.analyst), vous pouvez vous connecter à une Now Platform instance directement à partir de votre équipement mobile. Avec le Application mobile Réponse aux incidents de sécurité, vous pouvez afficher, modifier et affecter vos incidents de sécurité et tâches de réponse les plus récents et les plus critiques SIR . Les notifications vous informent lorsque des incidents de sécurité critiques qui vous sont affectés arrivent.

Avec le Application mobile Réponse aux incidents de sécurité, vous pouvez effectuer les tâches suivantes SIR à partir de votre équipement mobile :

- Affichez une liste des incidents de sécurité critiques et des tâches de réponse.
- Recevez des notifications détaillées pour les incidents de sécurité et les tâches qui répondent aux critères de notification prédéfinis.
- Affichez les regroupements d'incidents ou de tâches de sécurité basés sur un ensemble prédéfini de requêtes ou de filtres.
- Affichez les notes de travail et les listes connexes des incidents de sécurité.
- Mettre à jour les incidents de sécurité et ajouter des notes de travail ou des pièces jointes.
- Modifier les champs sur les incidents de sécurité.
- Affecter des incidents de sécurité à vous-même ou à d'autres membres de votre équipe de sécurité.

Lorsqu'elles sont renseignées, vous pouvez afficher les listes connexes suivantes sur SIR les incidents de sécurité avec :Application mobile Réponse aux incidents de sécurité

- ID d'élément de configuration
- Utilisateur affecté
- Services affectés
- Incidents de sécurité enfants
- Incidents de sécurité similaires (non pris en charge par la Now Platform)
- Observables
- Tâches de réponse
- Tâches
- SLA de tâche
- Pièces jointes (non prises en charge par Now Platform)

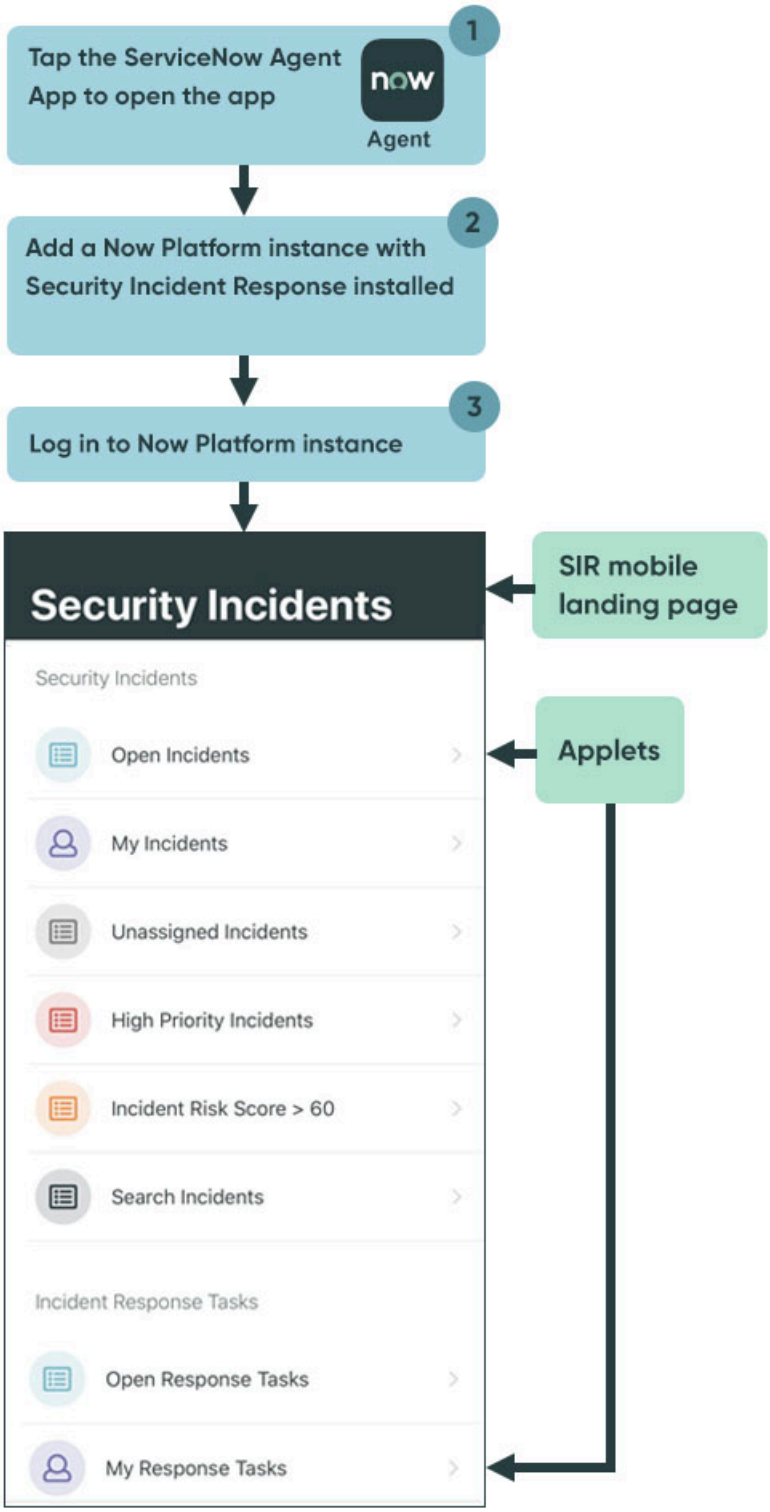
La figure suivante illustre la façon dont vous vous connectez à votre Now Platform instance à partir de votre équipement mobile et la structure de l'écran d'accueil qui est joué après la Application mobile Réponse aux incidents de sécurité connexion.

Pour obtenir des instructions détaillées sur la configuration de votre instance et l'installation de , Now PlatformApplication mobile Réponse aux incidents de sécuritéreportez-vous à la section Configurer une liste de vérification pour le Application mobile Réponse aux incidents de sécurité. Pour obtenir des instructions sur la façon de se connecter, reportez-vous à la section Connectez-vous au Application mobile Réponse aux incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application mobile Réponse aux incidents de sécurité



Applications

Les applications sont les ServiceNow® composants logiciels tels que Réponse aux incidents de sécurité (SIR), Réponse aux vulnérabilités (VR), Gouvernance, risque et conformité (GRC) qui fournissent des fonctionnalités spécifiques au sein de votre Now Platform instance. Une fois que vous avez installé l'application Application mobile Réponse aux incidents de sécurité principale et sur Réponse aux incidents de sécurité votre Now Platform instance, l'icône de l'application principale s'affiche au bas de votre Android appareil mobile après iOS votre connexion.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application mobile Réponse aux incidents de sécurité (Incidents de sécurité) icône

Dossiers

Chaque ServiceNow® Mobile application contient des dossiers qui séparent les applets par catégorie. Dans l'image précédente de la page de destination, **les incidents de sécurité** et **les tâches de réponse aux incidents** sont des dossiers.

Applets

Les applets sont les différentes options au sein de l'application. Les icônes sous les sections **Incidents de sécurité** et **Tâches de réponse aux incidents** sont les applets disponibles du Application mobile Réponse aux incidents de sécurité.

Configurer une liste de vérification pour le Application mobile Réponse aux incidents de sécurité

La liste de vérification suivante répertorie les tâches de configuration que vous devez effectuer dans votre Now Platform® instance et sur votre équipement mobile avant d'utiliser le Application mobile Réponse aux incidents de sécurité.

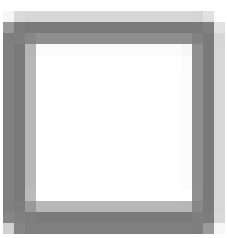
Avant de commencer

En option, imprimez cette liste de vérification et utilisez-la pour vous guider dans les tâches de configuration requises pour le Application mobile Réponse aux incidents de sécurité. Vérifiez que chaque élément de la liste est terminé afin de pouvoir afficher et modifier SIR les incidents de sécurité sur votre équipement mobile.

Les éléments de la liste de vérification sont affichés en surbrillance. Plus d'informations suivent chaque élément dans la colonne de droite. Temps estimé pour accomplir cette tâche : 15 à 20 minutes.

Rôles requis : admin, sn_si.analyst

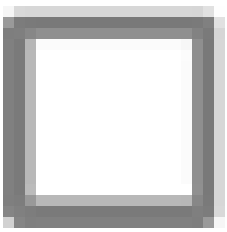
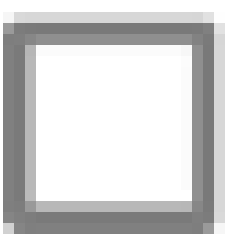
Liste de vérification mobile

Élément	Description
	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que l'application Réponse aux incidents de sécurité Core est installée sur une Now Platform instance. Il s'agit de l'instance Now Platform que vous affichez sur votre appareil mobile. **Remarque :** L'application Réponse aux incidents de sécurité principale et l'instance Now Platform doivent provenir de la même version de famille. 1. Pour vérifier que l'application principale est installée sur votre instance, accédez à **Modules d'extension** et recherchez Réponse aux incidents de sécurité. 2. Si l'application principale n'est Réponse aux incidents de sécurité pas déjà installée, cliquez sur **Installer** pour l'installer. Pour en savoir plus sur l'installation de l'application principale, reportez-vous Réponse aux incidents de sécurité à la section Installer et configurer Réponse aux incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification mobile (suite)

Élément	Description
	Si l'application principale n'est pas visible dans Modules d'extension, pour plus d'informations sur l'installation Réponse aux incidents de sécurité d'applications principales et les autorisations d'accès aux applications, reportez-vous à la section .
	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que vous avez installé Now Platform l'instance Application mobile Réponse aux incidents de sécurité que vous souhaitez afficher sur votre équipement mobile. **Remarque :** L'instance et doivent Application mobile Réponse aux incidents de sécuritéNow Platform provenir de la même version de famille. Téléchargez et installez le Application mobile Réponse aux incidents de sécurité à partir de sur ServiceNow Store votre Now Platform instance. Lorsque vous installez , ses Application mobile Réponse aux incidents de sécuritédépendances, com.glide.sg et com.glide.sg.agent_native_client, sont également installées. Pour vérifier que ces dépendances sont installées : **1.** Accédez à **Modules d'extension.** **2.** Recherchez les ID des modules d'extension (com.glide.sg et com.glide.sg.agent_native_client). **3.** S'ils ne sont pas activés, activez ces modules d'extension. Ces modules d'extension sont requis pour le Application mobile Réponse aux incidents de sécuritéfichier . Pour plus d'informations sur l'installation d'applications et les autorisations d'accès aux applications, reportez-vous à la section .
	En tant qu'utilisateur disposant du Now Platform rôle admin, vérifiez que vous avez affecté des utilisateurs mobiles avec les rôles requis dans votre Now Platform instance. **1.** Pour afficher les rôles affectés à un utilisateur, accédez à **Utilisateurs et groupes** > **Utilisateurs**. **2.** Sélectionnez le nom d'utilisateur suivi de la liste connexe des rôles. Tous les rôles affectés à cet utilisateur s'affichent. **3.** Vérifiez qu'un utilisateur est affecté ou affectez à un utilisateur le rôle ITIL (ITIL Bibliothèque d'infrastructures ITIL). Les utilisateurs disposant du rôle itil peuvent créer, ouvrir, mettre à jour et fermer des incidents de sécurité. Seuls les utilisateurs disposant du rôle itil peuvent se voir affecter des tâches. **4.** Vérifiez qu'un utilisateur est affecté ou affectez à un utilisateur le rôle d'analyste de la sécurité (sn_si.analyst). Les utilisateurs disposant du rôle sn_si.analyst peuvent lire et modifier les enregistrements

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification mobile (suite)

Élément	Description
	d'incidents de sécurité. Ce rôle est automatiquement ajouté lorsque vous affectez le rôle itil. **5.** Vérifiez que vous avez créé tous les groupes d'affectation requis et affecté des utilisateurs mobiles à ces groupes. **Remarque :** Si vous disposez d'un grand nombre d'utilisateurs pour l'application mobile, vous pouvez également affecter le rôle sn_si.analyst à un groupe. Chaque utilisateur que vous ajoutez au groupe hérite de ce rôle. Pour en savoir plus sur les analystes de sécurité, reportez-vous à la section Affectation des analystes de sécurité. Pour plus d'informations sur les utilisateurs et l'affectation de rôles aux utilisateurs et aux groupes, consultez Administration utilisateurs .
☐	En tant qu'utilisateur disposant du rôle sn_si.analyst, téléchargez l'application Agent la plus récente ServiceNow® sur votre équipement mobile. La version la plus récente de l'application Agent est disponible sur l'App Store d'Apple iOS et le Google Play Store.
☐	En tant qu'utilisateur disposant du rôle sn_si.analyst, vérifiez que les notifications sont activées sur votre équipement mobile et dans votre Now Platform instance. Les notifications vous informent lorsque des incidents de sécurité critiques vous sont affectés ou sont affectés à votre groupe d'affectation. Pour vous aider à y remédier en temps opportun, après avoir activé les notifications, cliquez sur une notification dans le Application mobile Réponse aux incidents de sécurité pour accéder directement à l'incident de sécurité. Pour activer les notifications dans votre Now Platform instance afin qu'elles s'affichent sur votre équipement mobile, procédez comme suit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification mobile (suite)

Élément	Description
	1. Vérifiez que vous avez téléchargé et installé le Application mobile Réponse aux incidents de sécurité sur votre Now Platform instance. **2.** Dans les paramètres système de votre Now Platform instance, sous Notifications, vérifiez que vous avez activé **l'application mobile ServiceNow**. Pour plus d'informations sur la définition des notifications, consultez Définition des préférences de notification de l'utilisateur dans l'interface utilisateur principale . Now Platform Les notifications sont également affichées sur l'écran Messages de votre appareil mobile. Vérifiez que les notifications sont également activées dans les paramètres de votre équipement mobile.

Vous avez correctement configuré votre équipement mobile et le Now Platform pour le Application mobile Réponse aux incidents de sécurité. L'étape suivante consiste à vous connecter à votre Now Platform instance avec votre équipement mobile.

Connectez-vous au Application mobile Réponse aux incidents de sécurité

Ouvrez l'application mobile Réponse aux incidents de sécurité et ajoutez une Now Platform® instance avec Réponse aux incidents de sécurité à votre appareil mobile.

Avant de commencer

Rôle requis : sn_si.analyst

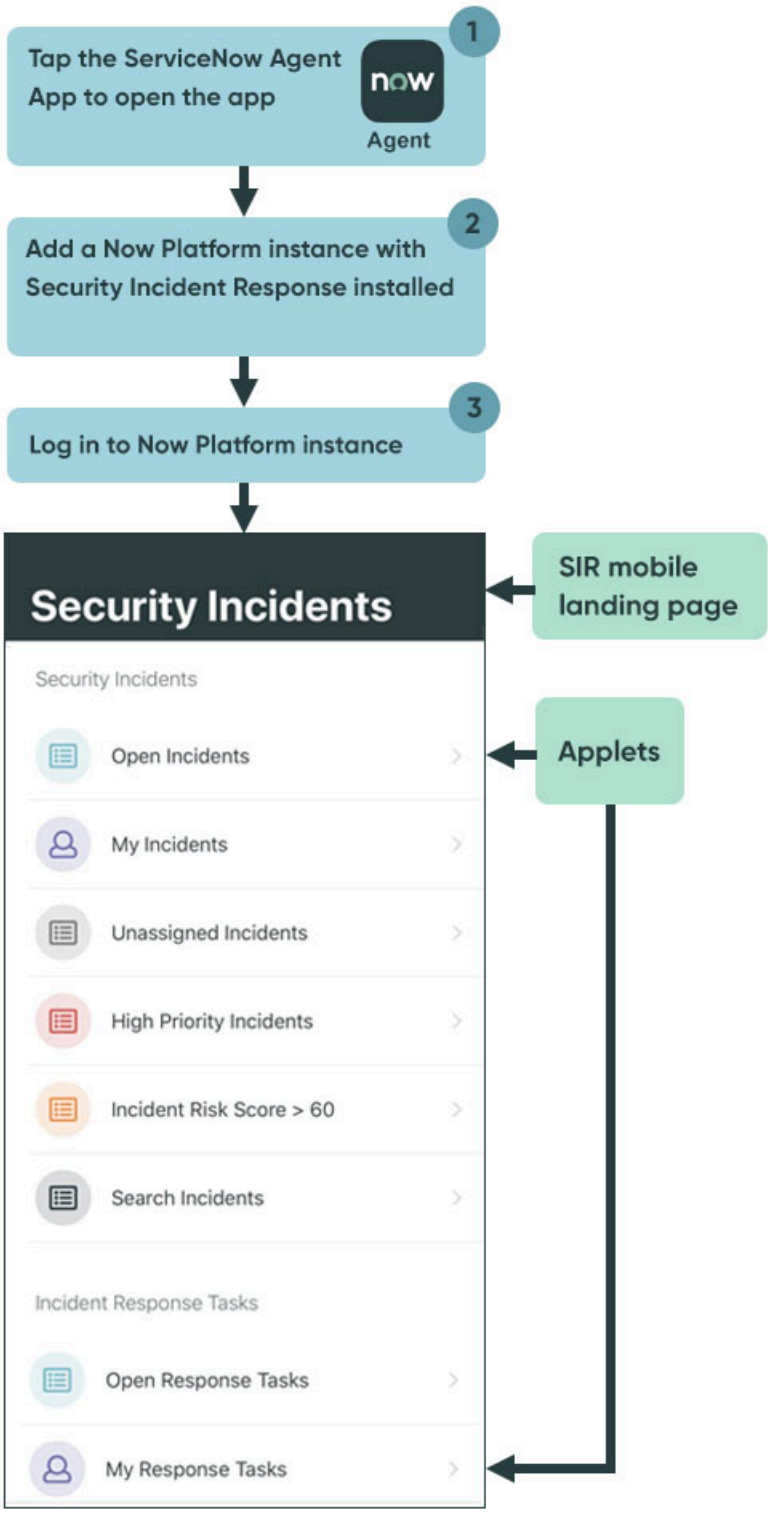
Pourquoi et quand exécuter cette tâche

Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.
Vérifiez que vous avez terminé les étapes de configuration décrites à la section Configurer une liste de vérification pour le Application mobile Réponse aux incidents de sécurité.

Traduction automatique

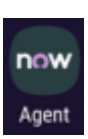
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application mobile Réponse aux incidents de sécurité



Procédure

1. Sur votre équipement mobile, appuyez sur l'application **ServiceNow Agent** pour l'ouvrir.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous n'êtes pas déjà connecté à une Now Platform instance, l'écran Instances s'affiche.

2. Si l'instance Now Platform avec l'application Réponse aux incidents de sécurité principale n'est pas déjà ajoutée à votre appareil mobile, procédez comme suit pour l'ajouter.

   a. Sur l'écran Instances qui s'affiche, appuyez sur 
   Un écran s'affiche et vous invite à saisir et à enregistrer l'adresse d'une Now Platform instance.

   b. Renseignez les champs.

Champ	Description
Entrez l'adresse de l'instance ou scannez un code QR.	Choisissez-en un pour continuer : ▪ Avant le `.service-now.com`, saisissez le nom de votre Now Platform instance, par exemple, `sirmobileny`. ▪ Entrez une adresse. Cette adresse est l'URL de votre Now Platform instance que vous souhaitez afficher sur votre appareil mobile, par exemple https://sirmobileny.service-now.com. ▪ Scannez un code QR.
(Facultatif) Entrez le pseudonyme	entrez un surnom pour cette instance. Si plusieurs instances ont été ajoutées à l'appareil , des surnoms peuvent vous aider à localiser rapidement une instance Now Platform.

   c. Appuyez sur **Enregistrer et se connecter**.

3. Sur l'écran de connexion qui s'affiche ServiceNow , saisissez le nom d'utilisateur et le mot de passe de l'instance Now Platform que vous souhaitez ajouter, puis appuyez sur **Connexion**.
   L'écran d'accueil Incidents de sécurité s'affiche. Vous vous êtes connecté avec succès au Application mobile Réponse aux incidents de sécuritéfichier .
4. Après vous être connecté, vérifiez que les notifications sont activées dans le Application mobile Réponse aux incidents de sécurité.

   a. Sur l'écran d'accueil en bas, appuyez sur **Notification**.

   b. Sur l'écran Notifications, appuyez sur **Activer les notifications** si elles ne sont pas activées.
   Les notifications provenant de s'affichent Now Platform sur l'écran Notifications du Application mobile Réponse aux incidents de sécurité.

5. Une fois que vous êtes connecté à une instance sur votre équipement mobile, il s'agit de l'instance par défaut Now Platform sur l'appareil.
   Si vous souhaitez en afficher une autre Now Platform sur l'appareil, vous devez vous déconnecter de l'instance par défaut. Pour vous déconnecter :

   a. Appuyez sur l'icône des paramètres.

   b. Appuyez sur **Déconnexion**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'écran Instances s'affiche avec toutes les Now Platform instances que vous avez ajoutées à l'équipement mobile.

c. Facultatif : Appuyez sur une autre instance pour vous y connecter ou, à défaut, suivez les étapes précédentes pour ajouter une autre instance.

Si l'écran des instances ne s'affiche Application mobile Réponse aux incidents de sécurité pas après que vous avez appuyé sur l'application **ServiceNow Agent** sur votre appareil, vérifiez que **ServiceNow Agent** est autorisé en tant qu'application approuvée sur votre appareil. Pour autoriser l'accès en tant qu'application approuvée, accédez aux paramètres et à la gestion générale de l'appareil sur votre appareil et appuyez sur l'option (Application de confiance, etc.) pour autoriser l'accès.

Si un message d'erreur s'affiche une fois que vous avez saisi vos informations d'identification dans l'écran de connexion, vérifiez que votre nom d'utilisateur et votre mot de passe pour l'instance Now Platform sont corrects.

Si vous rencontrez des problèmes pour afficher l'écran d'accueil, vérifiez votre connexion réseau.

Si vous ne pouvez pas afficher l'écran des instances après avoir appuyé sur l'application **ServiceNow Agent** , essayez de la désinstaller de votre appareil. Vérifiez que vous disposez de la version la plus récente de l'application de l'App Store d'Apple iOS ou du Google Play Store et essayez de la réinstaller.

Affichez, modifiez et affectez des incidents de sécurité ouverts avec le Application mobile Réponse aux incidents de sécurité

En tant qu'analyste des incidents de sécurité, affichez, modifiez et affectez les incidents de sécurité ouverts Réponse aux incidents de sécurité (SIR) à partir de votre équipement mobile. Consultez les listes connexes et la piste d'audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Dans la liste des enregistrements, affectez-vous un incident de sécurité ouvert ou réaffectez-le. Vous pouvez également afficher les détails et les listes connexes de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

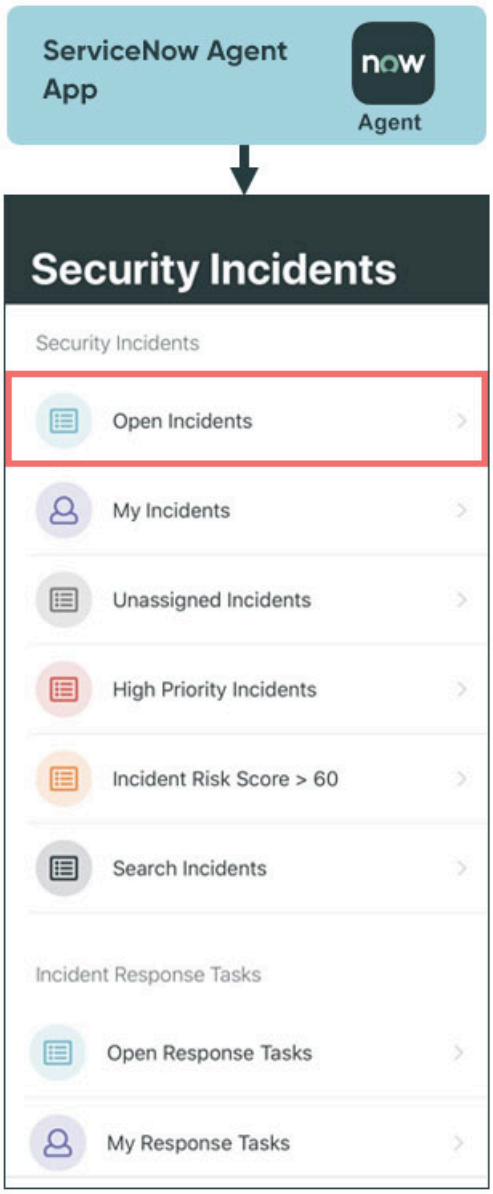
Procédure

1. Si vous n'êtes pas connecté à votre Now Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application mobile Réponse aux incidents de sécurité.
2. Une fois la page de destination Incidents de sécurité affichée, appuyez sur **Incidents ouverts**.

   Si vous quittez l'application Application mobile Réponse aux incidents de sécurité après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous avez affiché.

Traduction automatique

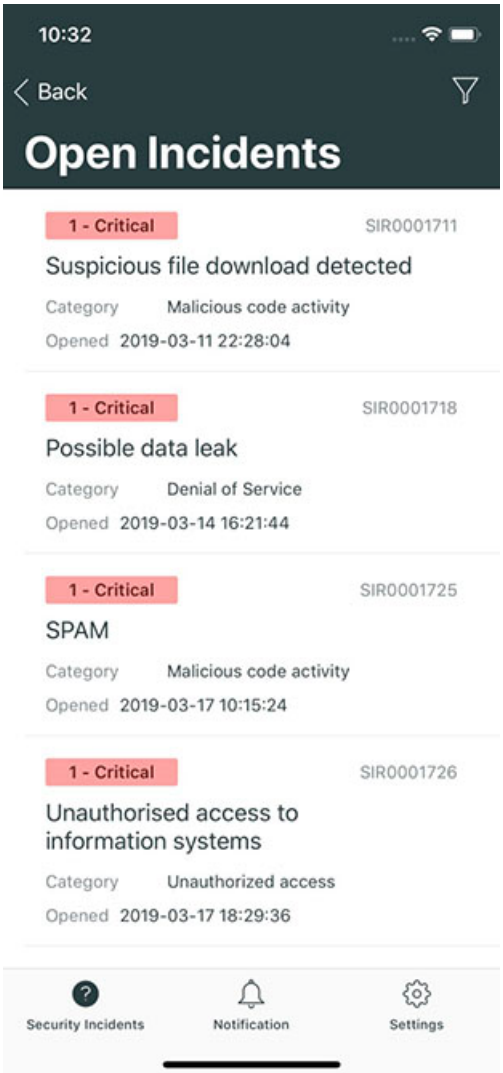
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'écran Incidents ouverts affiche une liste des enregistrements d'incidents de sécurité ouverts.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Facultatif : Reportez-vous à Rechercher des incidents de sécurité avec l'attribut Application mobile Réponse aux incidents de sécurité pour rechercher des incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans dans l'application mobile fonctionne comme avec un générateur de conditions sur Now Platform.

4. Pour vous affecter un incident ou le réaffecter directement à partir de la liste des incidents de sécurité ouverts, faites glisser un enregistrement vers la gauche pour ouvrir le menu.
5. Choisissez-en un dans le menu qui s'affiche pour continuer.

Option	Description
Mes affectations	Vous affecter l'incident de sécurité. Si l'incident de sécurité vous est déjà affecté, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation :

Traduction automatique

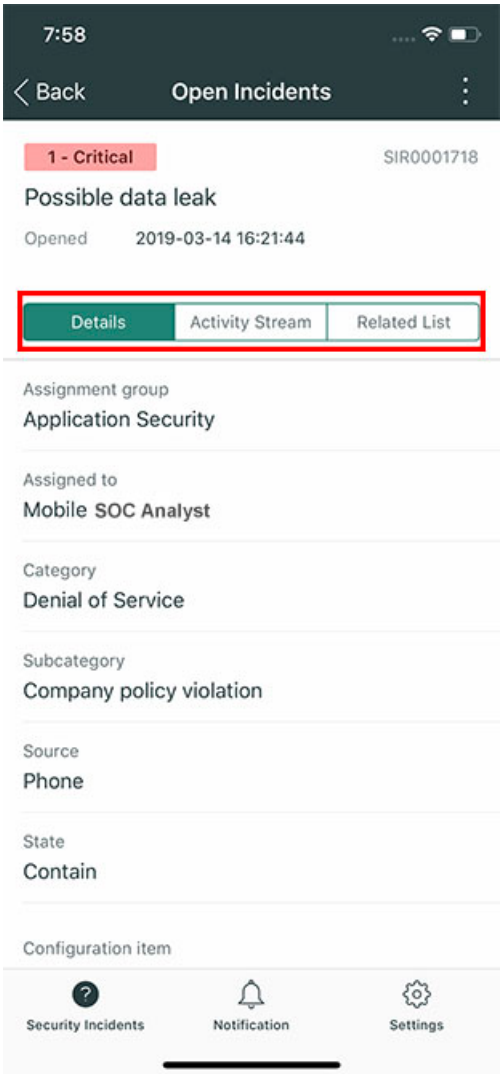
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste affichée ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter l'incident de sécurité à un membre du groupe d'affectation : **a.** Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône d'envoi (ou **sur Soumettre** pour enregistrer et soumettre vos modifications.

6. Pour afficher les détails d'un enregistrement d'incident de sécurité ouvert et afficher plus d'enregistrements associés et de listes connexes, appuyez également sur un enregistrement de la liste avec l'écran Incidents ouverts affiché.
7. Dans l'enregistrement ouvert qui s'affiche, choisissez une option dans la table suivante pour continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Appuyez sur l'icône de menu ( ) en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez l'une des options suivantes. ◦ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et saisir du texte. ◦ Pour réaffecter l'incident, appuyez sur **Réaffecter** ou **Me l'affecter**. Suivez les instructions décrites dans le tableau précédent. Une fois que vous avez terminé vos modifications, appuyez sur l'icône d'envoi ( ) ou **sur Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, examinez la piste d'audit des notes de tra-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	vail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône plus ( pour ajouter une note de travail ou joindre un fichier.
Onglet de liste connexe	Avec l'onglet Liste connexe sélectionné, affichez les éléments de toutes les listes connexes de l'incident de sécurité qui sont remplies. Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments affichées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Icônes de l'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ◦ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ◦ Si elle est affichée, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ◦ Appuyez sur **Notification** pour afficher les notifications du et du Now PlatformApplication mobile Réponse aux incidents de sécurité. ◦ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance Now Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle Now Platform .

Traduction automatique

Afficher, modifier et réaffecter les incidents de sécurité qui vous sont affectés avec le Application mobile Réponse aux incidents de sécurité

En tant qu'analyste des incidents de sécurité, affichez, modifiez et réaffectez Réponse aux incidents de sécurité (SIR) les incidents qui vous sont affectés. Consultez les listes connexes et la piste d'audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer
Rôle requis : sn_si.analyst

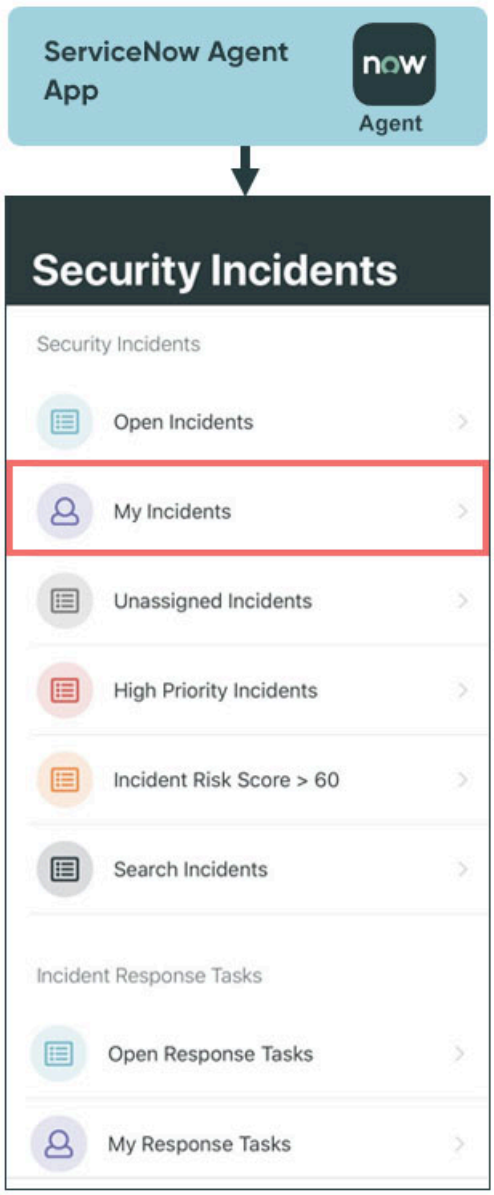
Pourquoi et quand exécuter cette tâche
Réaffectez un incident de sécurité ouvert à un autre analyste de votre groupe à partir de la liste des enregistrements. Vous pouvez également afficher les détails et les listes connexes de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si vous n'êtes pas connecté à votre Now Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application mobile Réponse aux incidents de sécurité.
2. Une fois l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Mes incidents**.

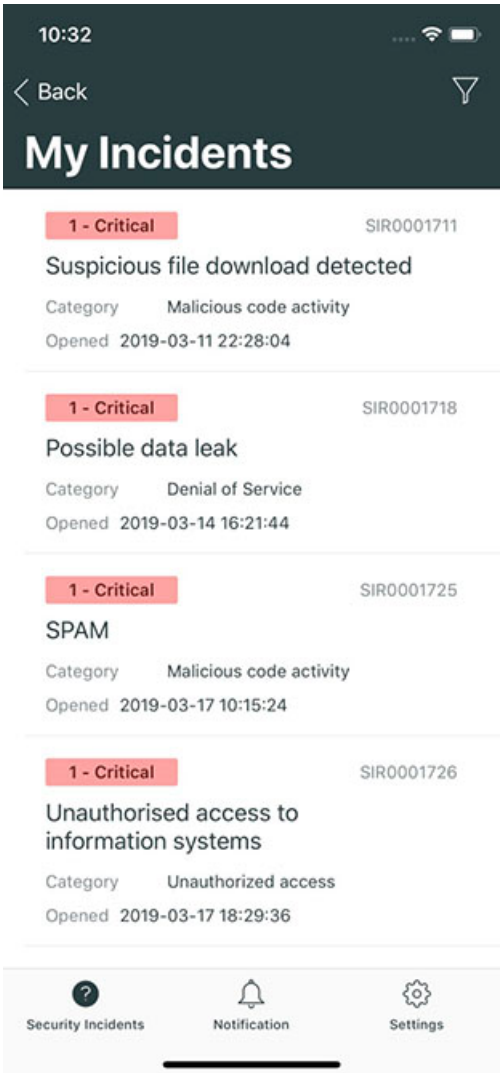
   Si vous quittez l'application Application mobile Réponse aux incidents de sécurité après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous avez affiché.



L'écran Mes incidents affiche une liste des enregistrements d'incidents de sécurité ouverts qui vous sont affectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



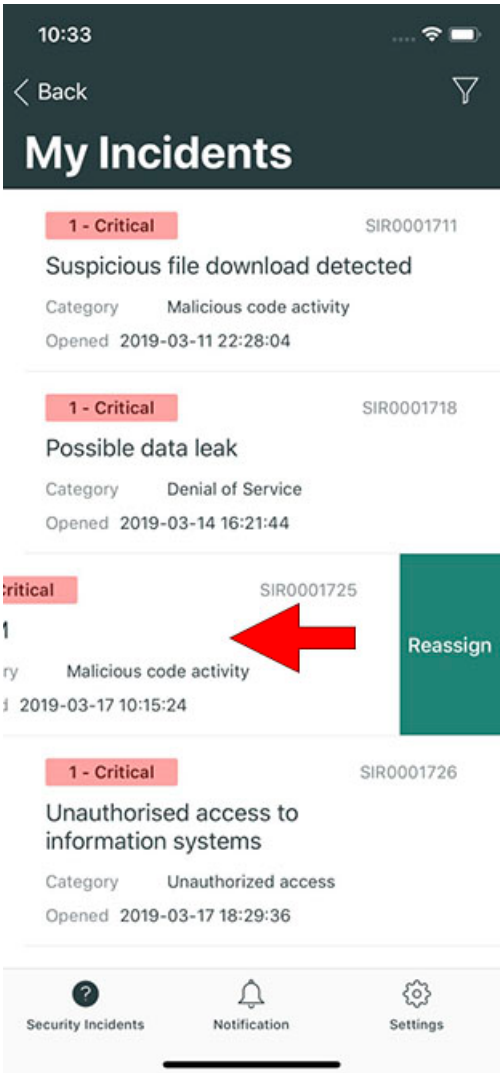
3. Facultatif : Reportez-vous à Rechercher des incidents de sécurité avec l'attribut Application mobile Réponse aux incidents de sécurité pour rechercher des incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans dans l'application mobile fonctionne comme avec un générateur de conditions sur Now Platform.

4. Pour réaffecter un incident directement à partir de la liste, avec la liste des enregistrements d'incidents de sécurité ouverts affichée, faites glisser vers la gauche sur un enregistrement pour ouvrir le menu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

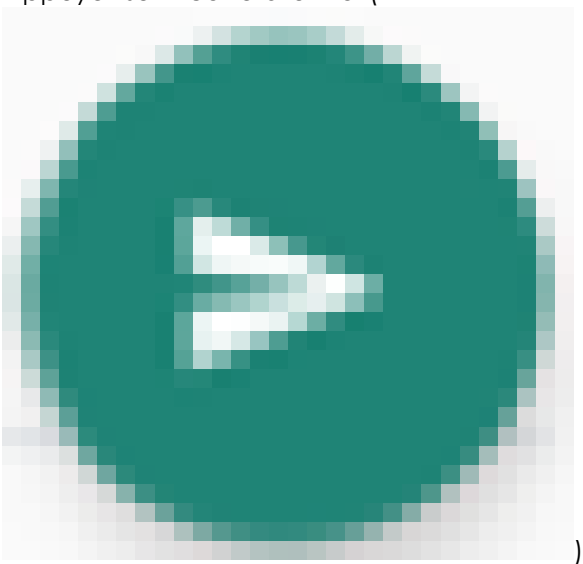


5. Modifiez les champs Groupe d'affectation ou Affecté à à partir du menu qui s'affiche.

Option	Description
Réaffecter	Pour réaffecter le groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste affichée ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter l'incident de sécurité à un membre du groupe d'affectation : **a.** Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche.

Traduction automatique

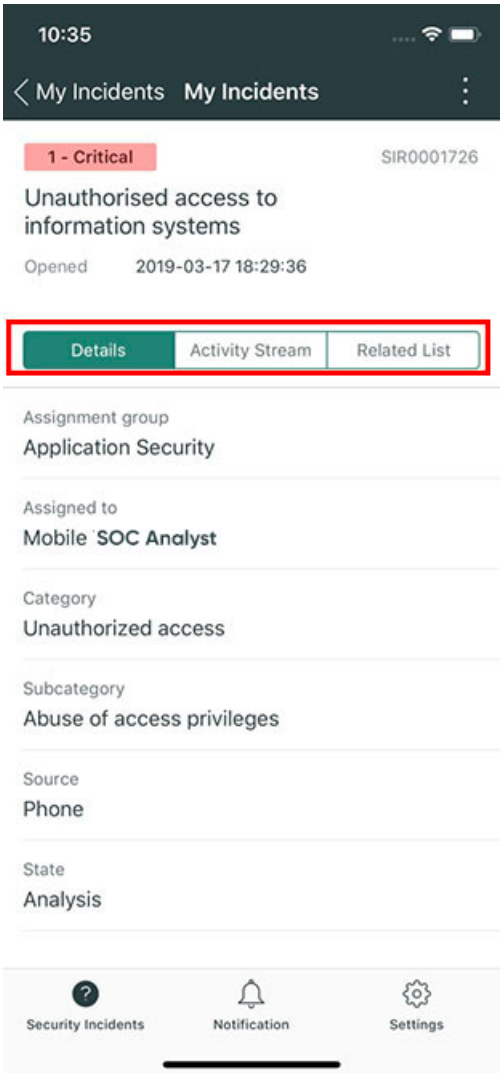
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Appuyez sur l'icône d'envoi () ou **sur Soumettre** pour enregistrer et soumettre vos modifications.

6. Pour afficher les détails de l'enregistrement d'incident de sécurité ouvert, appuyez également sur un enregistrement de la liste avec l'écran Mes incidents affiché.
7. Dans l'enregistrement ouvert qui s'affiche, choisissez une option dans la table suivante pour continuer.

Traduction automatique

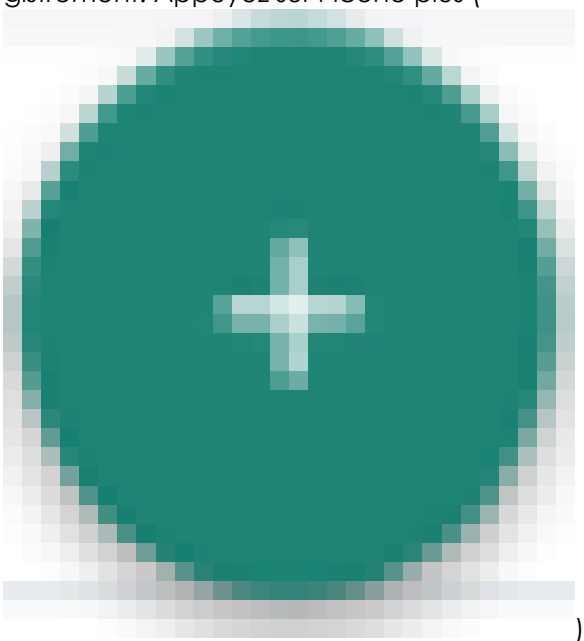
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Appuyez sur l'icône de menu ( ) en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez l'une des options suivantes. ◦ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et saisir du texte. ◦ Pour réaffecter l'incident, appuyez sur **Réaffecter**. Suivez les instructions décrites dans le tableau précédent. Une fois que vous avez terminé vos modifications, appuyez sur l'icône d'envoi (

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	) ou **sur Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, examinez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône plus () pour ajouter une note de travail ou joindre un fichier.
Onglet de liste connexe	Avec l'onglet Liste connexe sélectionné, affichez les éléments sur toutes les listes connexes renseignées sur l'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments affichées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Icônes de l'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ◦ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ◦ Si elle est affichée, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ◦ Appuyez sur **Notification** pour afficher les notifications du et du Now PlatformApplication mobile Réponse aux incidents de sécurité. ◦ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance Now Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle Now Platform .

Affichez, modifiez et affectez des incidents de sécurité non affectés avec le Application mobile Réponse aux incidents de sécurité

À partir de votre équipement mobile, affichez, modifiez et affectez les () incidents non affectésRéponse aux incidents de sécuritéSIR. Consultez les listes connexes et la piste d'audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

À partir de la liste des enregistrements, affectez-vous un incident de sécurité ouvert et non affecté ou affectez-vous à un autre analyste de votre groupe. Vous pouvez également afficher les détails et les listes connexes de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

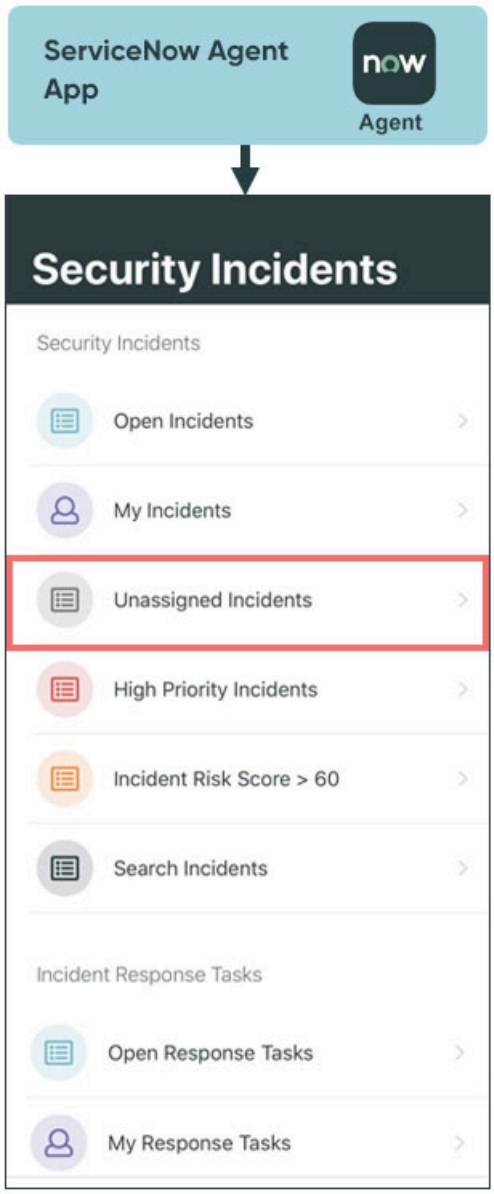
Procédure

1. Si vous n'êtes pas connecté à votre instance Now Platform sur votre équipement mobile, consultez .Connectez-vous au Application mobile Réponse aux incidents de sécurité
2. Une fois l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Incidents non affectés**.

   Si vous quittez l'application Application mobile Réponse aux incidents de sécurité après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous avez affiché.

Traduction automatique

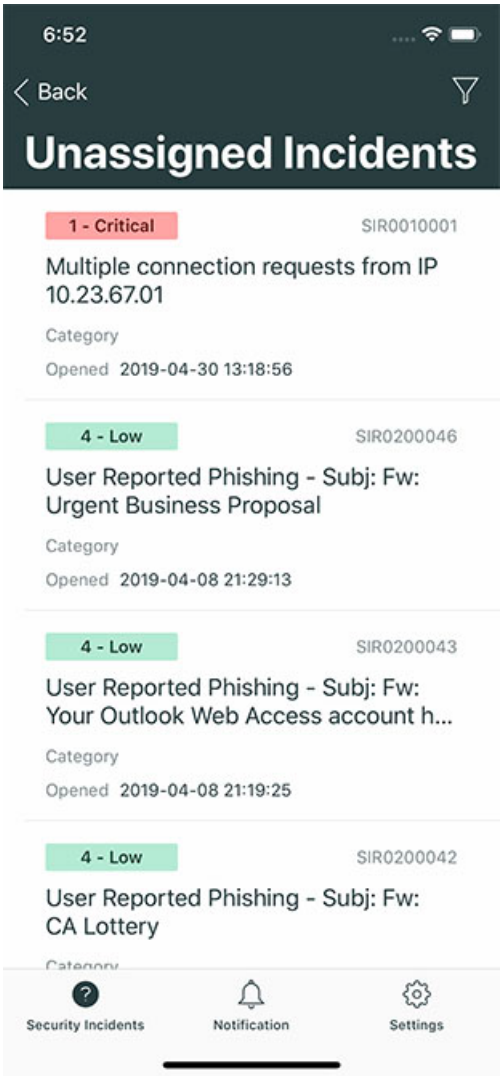
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'écran Incidents non affectés affiche une liste d'enregistrements d'incidents de sécurité non affectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



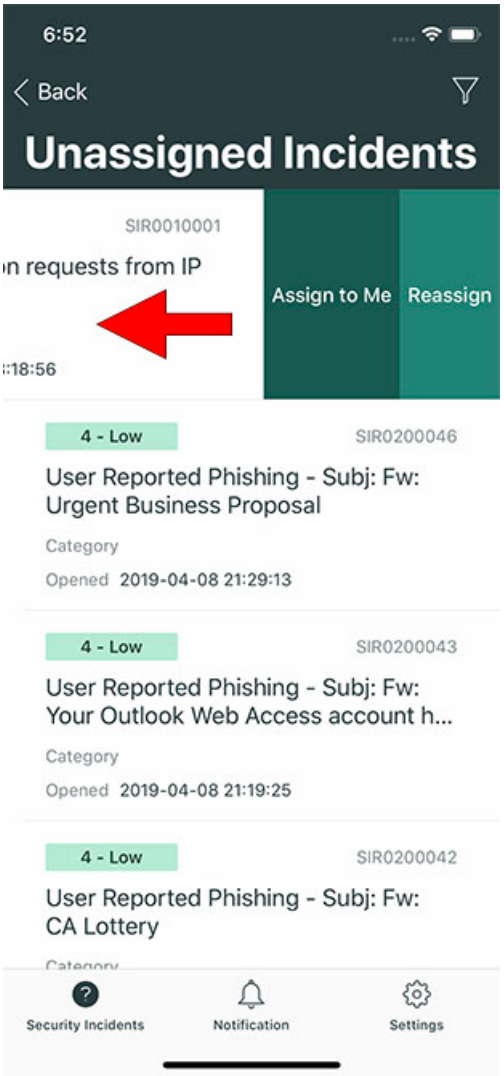
3. Facultatif : Reportez-vous à Rechercher des incidents de sécurité avec l'attribut Application mobile Réponse aux incidents de sécurité pour rechercher des incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans dans l'application mobile fonctionne comme avec un générateur de conditions sur Now Platform.

4. Pour affecter ou réaffecter un enregistrement d'incident de sécurité ouvert directement à partir de la liste, avec la liste des enregistrements d'incidents de sécurité ouverts non affectés affichée, faites glisser vers la gauche sur un enregistrement pour ouvrir le menu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Choisissez-en un dans le menu pour continuer.

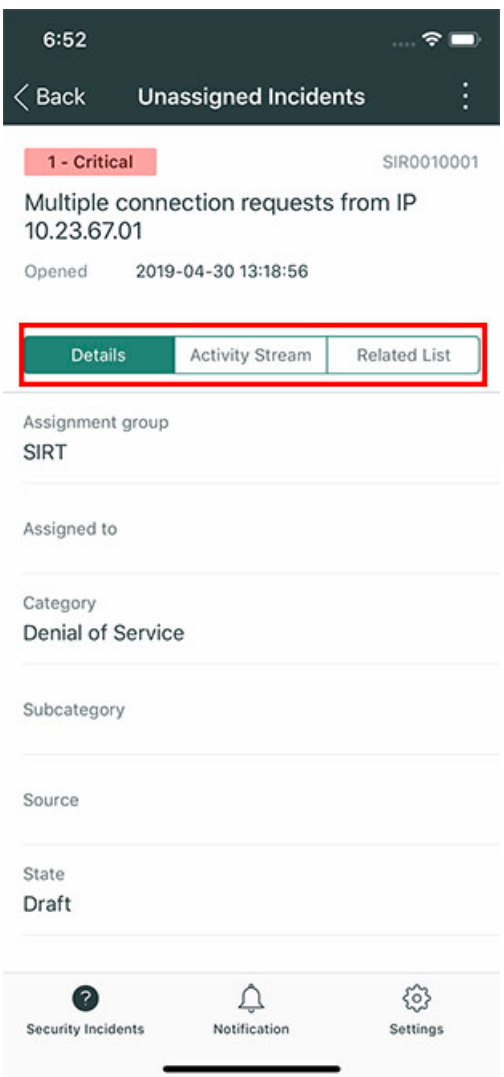
Option	Description
Mes affectations	Vous affecter l'incident de sécurité. Si l'incident de sécurité vous est déjà affecté, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste affichée ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter l'incident de sécurité à un membre du groupe d'affectation :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône d'envoi ( ) ou **sur Soumettre** pour enregistrer et soumettre vos modifications.

6. Alternativement, lorsque l'écran Incidents non affectés s'affiche, appuyez sur un enregistrement de la liste.
7. Dans l'enregistrement ouvert qui s'affiche, choisissez une option dans la table suivante pour continuer.



Option	Description
Appuyez sur l'icône de menu ( ) en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez l'une des options suivantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	◦ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et saisir du texte. ◦ Pour affecter ou réaffecter l'incident, appuyez sur **Réaffecter** ou **Me l'affecter**. Suivez les instructions décrites dans le tableau précédent. Une fois que vous avez terminé vos modifications, appuyez sur l'icône d'envoi (ou **sur Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, examinez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône plus (pour ajouter une note de travail ou joindre un fichier.
Onglet de liste connexe	Avec l'onglet Liste connexe sélectionné, affichez les éléments de l'une des listes connexes renseignées sur l'incident de sécurité. Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments affichées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Icônes de l'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ◦ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ◦ Si elle est affichée, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ◦ Appuyez sur **Notification** pour afficher les notifications du et du Now PlatformApplication mobile Réponse aux incidents de sécurité. ◦ Appuyez sur **Paramètres** et choisissez-en un pour continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	▪ Affichez des informations sur l'instance Now Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle Now Platform .

Affichez, modifiez et affectez des incidents à priorité élevée avec l' Application mobile Réponse aux incidents de sécurité

À partir de votre équipement mobile, affichez, modifiez et affectez des incidents de priorité Réponse aux incidents de sécurité élevée (SIR). Consultez les listes connexes et la piste d'audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

À partir de la liste des enregistrements, affectez-vous un incident de sécurité critique ouvert ou un autre analyste de votre groupe. Vous pouvez également afficher les détails et les listes connexes de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

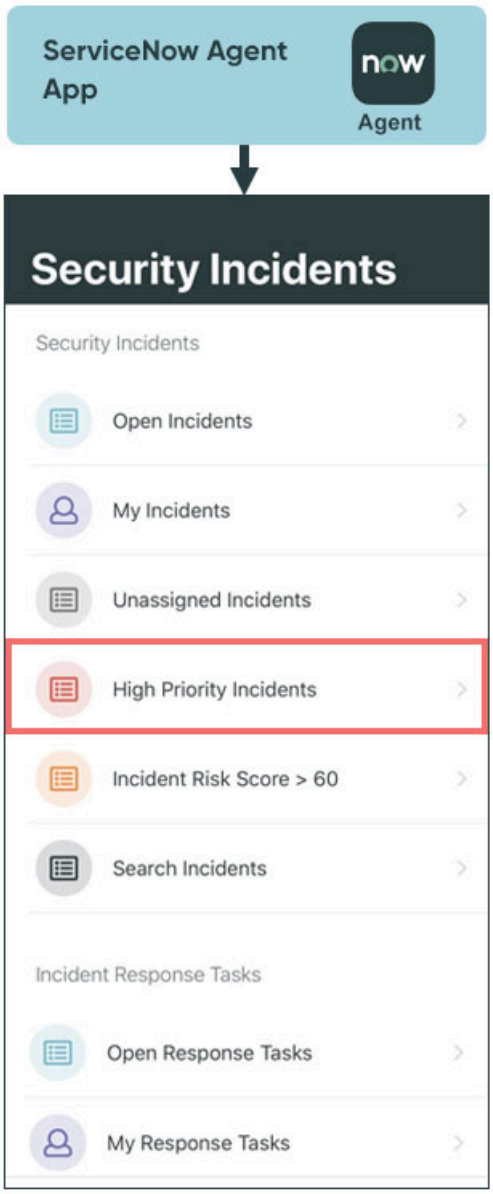
Procédure

1. Si vous n'êtes pas connecté à votre instance Now Platform sur votre équipement mobile, consultez .Connectez-vous au Application mobile Réponse aux incidents de sécurité
2. Une fois l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Incidents avec une priorité élevée**.

   Si vous quittez l'application Application mobile Réponse aux incidents de sécurité après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous avez affiché.

Traduction automatique

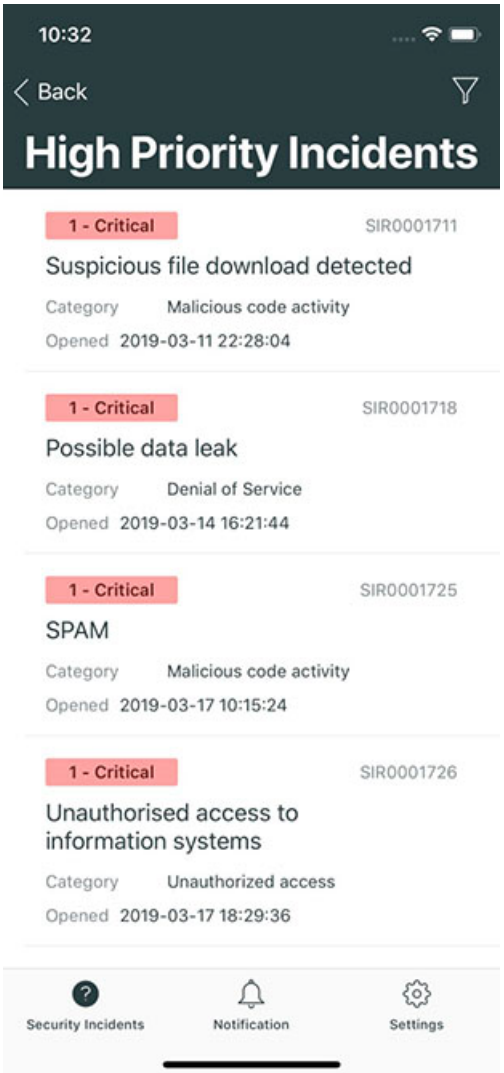
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'écran Incidents de priorité élevée s'affiche avec une liste d'incidents de sécurité critiques (priorité élevée).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



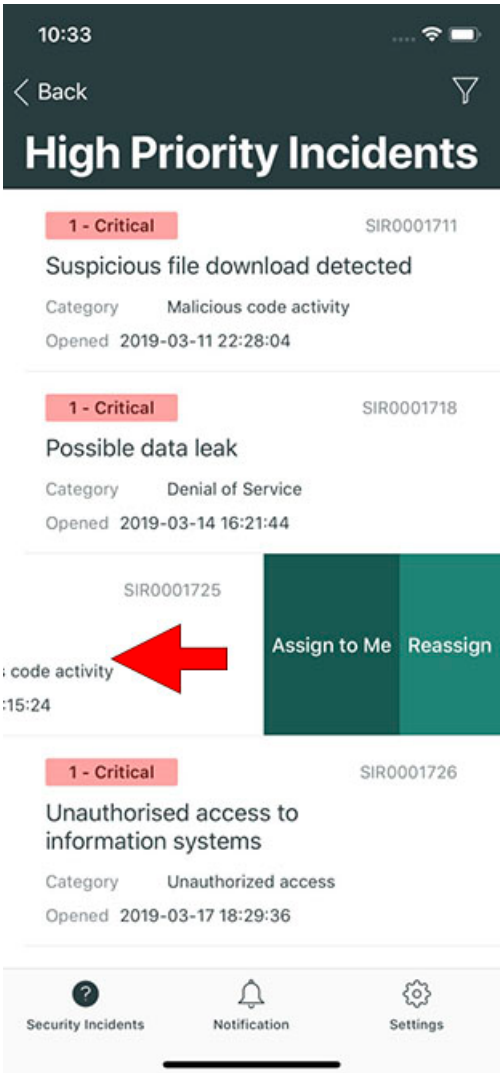
3. Facultatif : Reportez-vous à Rechercher des incidents de sécurité avec l'attribut Application mobile Réponse aux incidents de sécurité pour rechercher des incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans dans l'application mobile fonctionne comme avec un générateur de conditions sur Now Platform.

4. Une fois affichée la liste des enregistrements d'incidents de sécurité de priorité élevée ouverts, faites glisser un enregistrement vers la gauche pour ouvrir le menu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

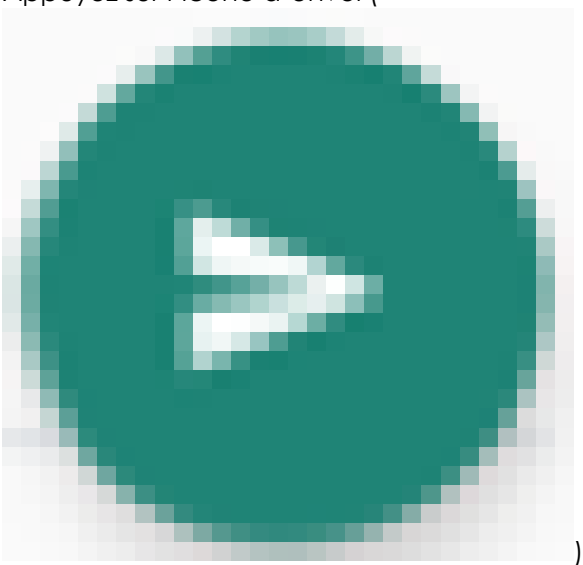


5. Choisissez-en un pour continuer.

Option	Description
Mes affectations	Vous affecter l'incident de sécurité. Si l'incident de sécurité vous est déjà affecté, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation** **b.** Appuyez sur un groupe dans la liste affichée ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter l'incident de sécurité à un membre du groupe d'affectation :

Traduction automatique

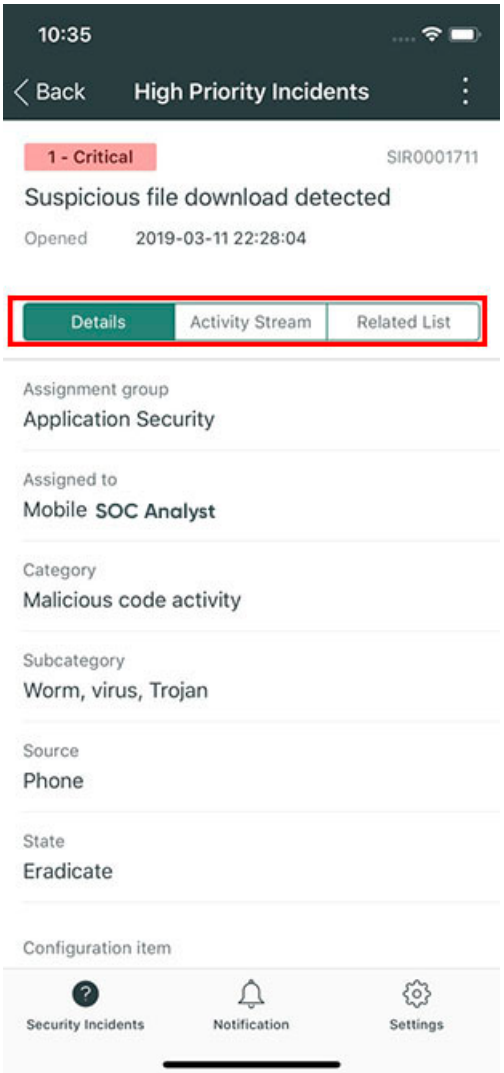
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône d'envoi () ou **sur Soumettre** pour enregistrer et soumettre vos modifications.

6. Pour afficher les détails d'un enregistrement d'incident de sécurité ouvert et pour afficher plus d'enregistrements associés et de listes connexes, avec l'écran Incidents de priorité élevée affiché, appuyez sur un enregistrement de la liste.
7. Dans l'enregistrement ouvert qui s'affiche, choisissez une option dans la table suivante pour continuer.

Traduction automatique

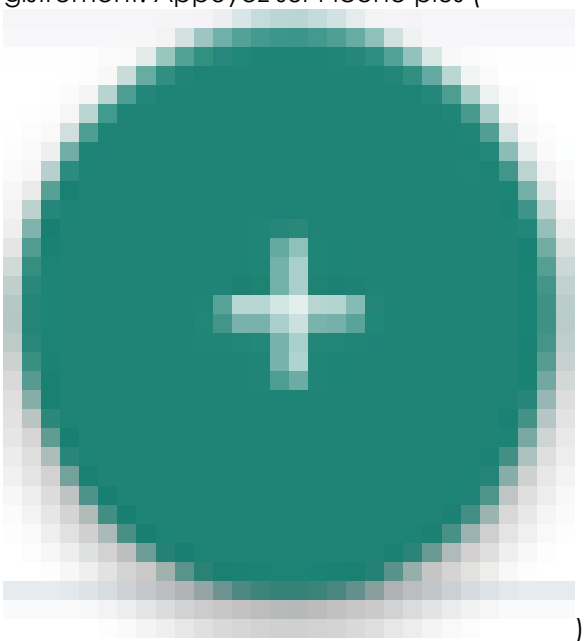
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Appuyez sur l'icône de menu ( ) en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez l'une des options suivantes. ◦ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et saisir du texte. ◦ Pour réaffecter l'incident, appuyez sur **Réaffecter** ou **Me l'affecter**. Suivez les instructions décrites dans le tableau précédent. Une fois que vous avez terminé vos modifications, appuyez sur l'icône d'envoi (

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	) ou **sur Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.
Onglet Flux d'activité	Avec l'onglet Activité sélectionné, examinez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône plus () pour ajouter une note de travail ou joindre un fichier.
Onglet de liste connexe	Avec l'onglet Liste connexe sélectionné, affichez les éléments de l'une des listes connexes renseignées sur l'incident de sécurité. Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments affi-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	chées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Appuyez sur une icône d'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ◦ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ◦ Si elle est affichée, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ◦ Appuyez sur **Notification** pour afficher les notifications du et du Now PlatformApplication mobile Réponse aux incidents de sécurité. ◦ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance Now Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle Now Platform .

Affichez, modifiez et affectez des incidents de sécurité avec un score de risque supérieur à 60 avec l' Application mobile Réponse aux incidents de sécurité

À partir de votre équipement mobile, affichez et modifiez Réponse aux incidents de sécurité (SIR) les incidents dont la valeur dans le champ de score de risque est supérieure à 60. Consultez les listes connexes et la piste d'audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

À partir de la liste des enregistrements, affectez-vous un incident de sécurité ouvert dont le score de risque est supérieur à 60 à vous-même ou à un autre analyste de votre groupe. Vous pouvez également afficher les détails et les listes connexes de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

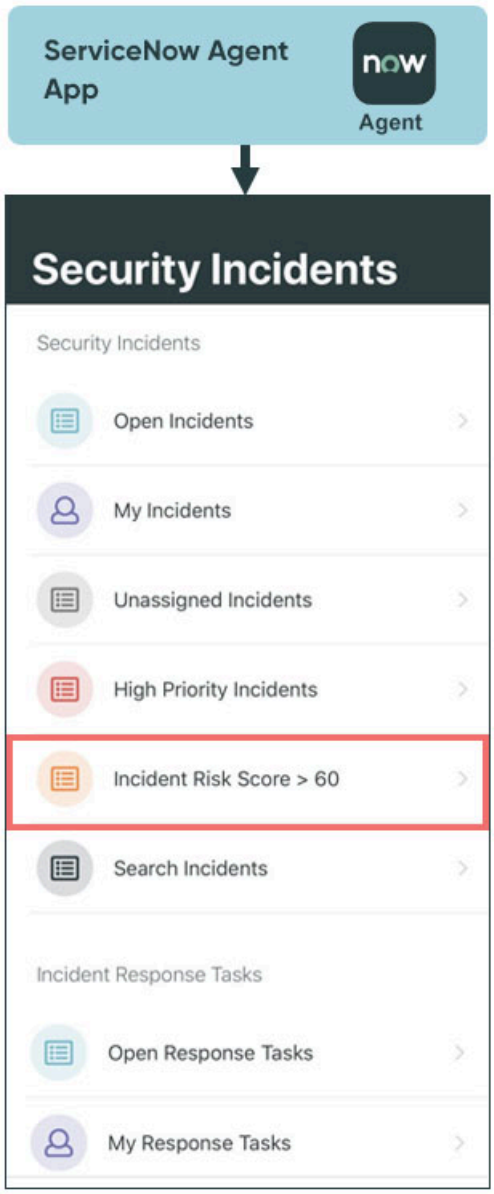
Procédure

1. Si vous n'êtes pas connecté à votre instance Now Platform sur votre équipement mobile, consultez .Connectez-vous au Application mobile Réponse aux incidents de sécurité
2. Avec l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Score de risque > 60**.

   Si vous quittez l'application Application mobile Réponse aux incidents de sécurité après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous avez affiché.

Traduction automatique

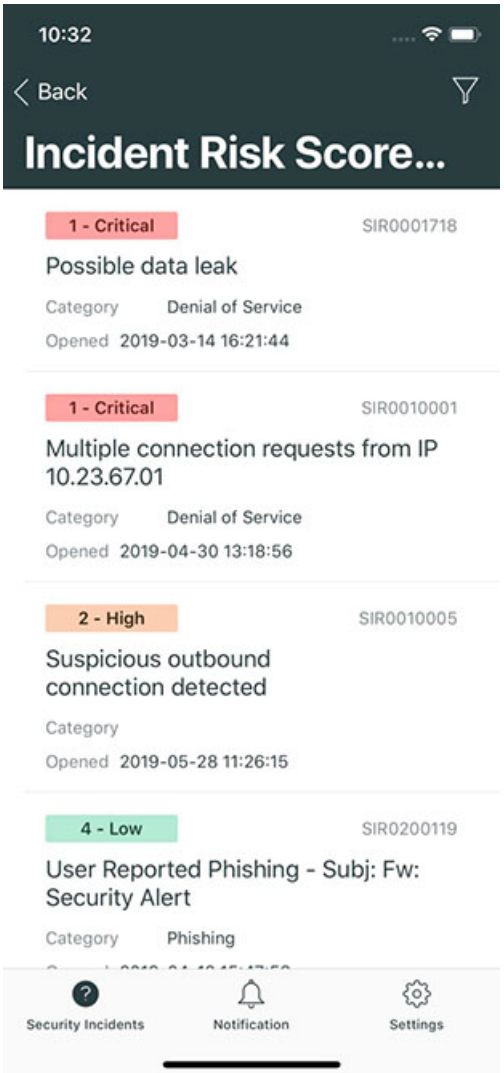
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'écran Score de risque d'incident affiche une liste d'incidents de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



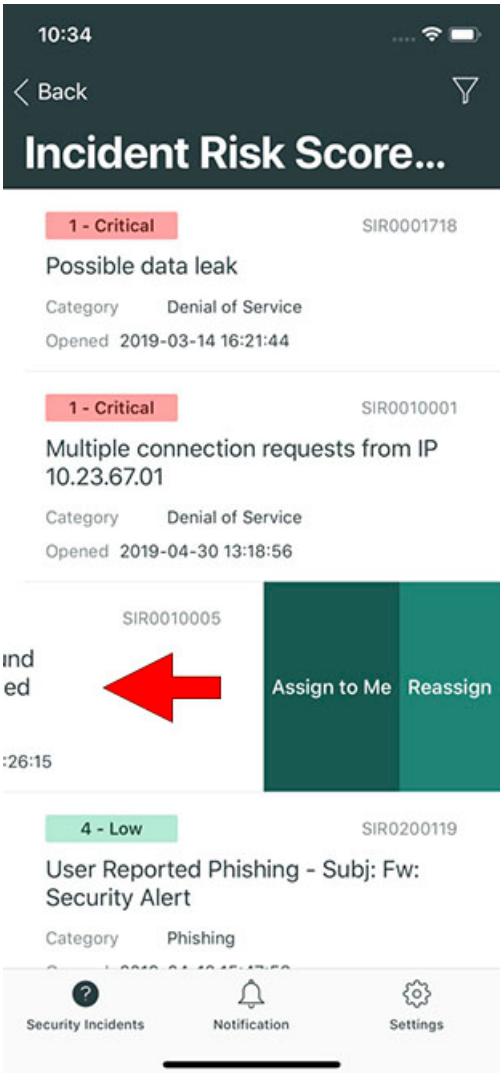
3. Facultatif : Reportez-vous à Rechercher des incidents de sécurité avec l'attribut Application mobile Réponse aux incidents de sécurité pour rechercher des incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans dans l'application mobile fonctionne comme avec un générateur de conditions sur Now Platform.

4. Pour vous affecter un incident de sécurité ou le réaffecter directement à partir de la liste des enregistrements d'incidents de sécurité ouverts affichée, faites glisser un enregistrement vers la gauche pour ouvrir le menu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Choisissez-en un pour continuer.

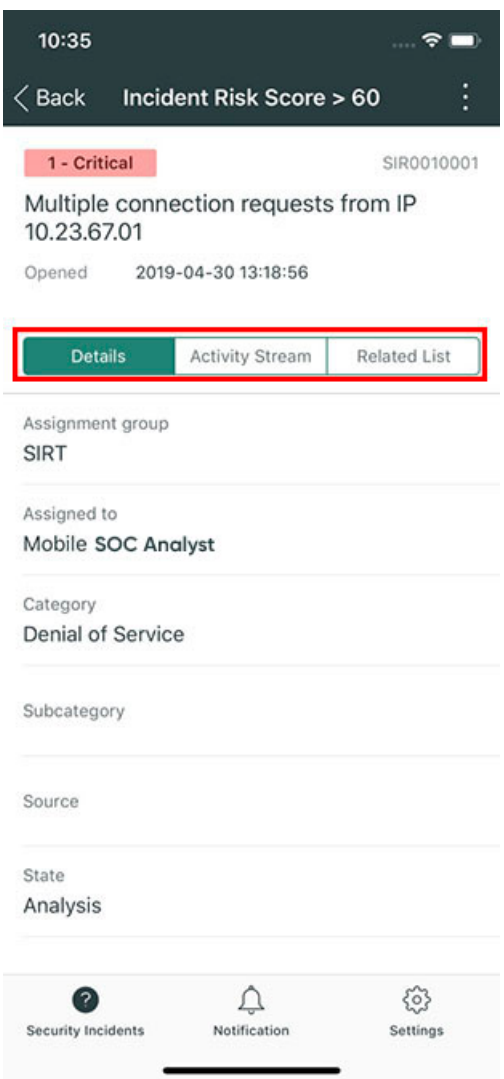
Option	Description
Mes affectations	Vous affecter l'incident de sécurité. Si l'incident de sécurité vous est déjà affecté, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste affichée ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter l'incident de sécurité à un membre du groupe d'affectation :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Affecté à** et **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône d'envoi (ou **sur Soumettre** pour enregistrer et soumettre vos modifications.

6. Pour afficher les détails d'un enregistrement d'incident de sécurité ouvert et afficher plus d'enregistrements associés et de listes connexes, appuyez également sur un enregistrement de la liste avec l'écran de score de risque d'incident affiché.
7. Dans l'enregistrement ouvert qui s'affiche, choisissez une option dans la table suivante pour continuer.



Option	Description
Appuyez sur l'icône de menu en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez l'une des options suivantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	◦ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et saisir du texte. ◦ Pour réaffecter l'incident, appuyez sur **Réaffecter** ou **Me l'affecter**. Suivez les instructions décrites dans le tableau précédent. Une fois que vous avez terminé vos modifications, appuyez sur l'icône d'envoi (ou **sur Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, examinez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône plus (pour ajouter une note de travail ou joindre un fichier.
Onglet de liste connexe	Avec l'onglet Liste connexe sélectionné, affichez les éléments de l'une des listes connexes renseignées sur l'incident de sécurité. Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments affichées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Icônes de l'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ◦ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ◦ Si elle est affichée, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ◦ Appuyez sur **Notification** pour afficher les notifications du et du Now PlatformApplication mobile Réponse aux incidents de sécurité. ◦ Appuyez sur **Paramètres** et choisissez-en un pour continuer.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	▪ Affichez des informations sur l'instance Now Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle Now Platform .

Rechercher des incidents de sécurité avec l'attribut Application mobile Réponse aux incidents de sécurité

Réponse aux incidents de sécurité Recherchez les incidents de sécurité (SIR) sur une Now Platform® instance. Seuls les incidents qui correspondent aux critères de recherche spécifiques que vous entrez sont affichés.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

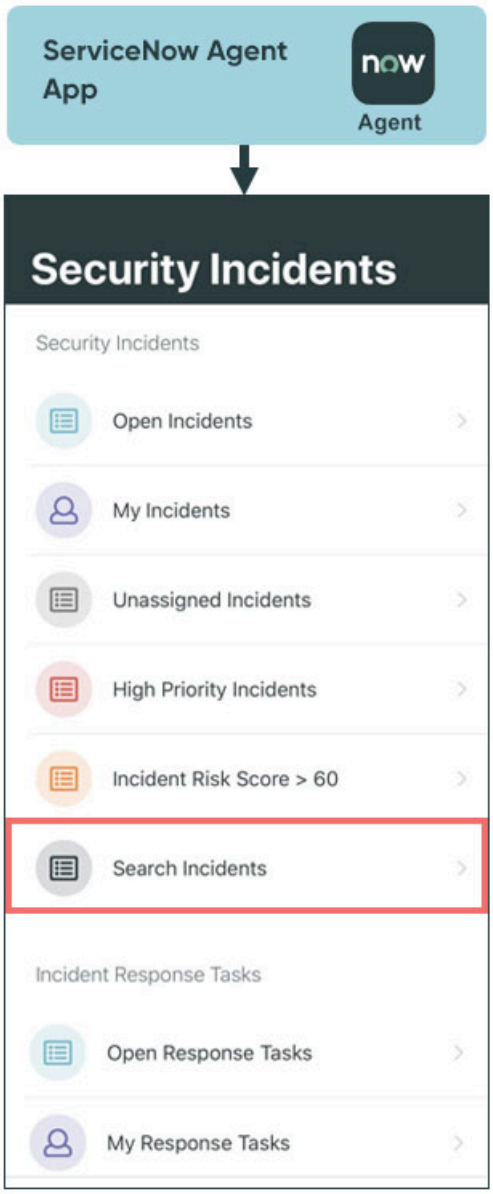
Procédure

1. Si vous n'êtes pas connecté à votre instance Now Platform sur votre équipement mobile, consultez .Connectez-vous au Application mobile Réponse aux incidents de sécurité
2. Une fois l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Rechercher des incidents**.

   Si vous quittez l'écran après vous Application mobile Réponse aux incidents de sécurité être connecté, appuyez à tout moment sur Now Agent pour revenir au dernier écran que vous avez affiché.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour limiter le nombre de résultats de recherche renvoyés, vous pouvez préférer remplir autant de champs que possible sur le formulaire.
Pour ajouter des critères de recherche, reportez-vous au tableau suivant. Suivez les instructions après la table pour modifier les critères de recherche existants, effacer les critères de recherche ou soumettre une recherche.

Appuyez sur ce champ	**Pour ajouter une entrée sur** Android **les appareils**	**À ajouter et à saisir sur** iOS **les appareils**
Numéro	Saisissez une valeur alphanumérique pour un incident de sécurité, par exemple `SIR0010004`. Ce numéro est affiché dans le coin supérieur droit de l'incident de sécurité.	Saisissez une valeur alphanumérique pour un incident de sécurité, par exemple `SIR0010004`. Ce numéro est affiché dans le coin supérieur droit de l'incident de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appuyez sur ce champ	Pour ajouter une entrée sur Android les appareils	À ajouter et à saisir sur iOS les appareils
	La fonctionnalité effectue une recherche sur les chaînes numériques et les chaînes numériques partielles. Pour des recherches plus précises, saisissez plus de chiffres. Les jokers (*) ne sont pas acceptés. Appuyez sur un nouveau champ pour entrer plus de critères ou sur  pour soumettre une recherche.	La fonctionnalité effectue une recherche sur les chaînes numériques et les chaînes numériques partielles. Pour des recherches plus précises, saisissez plus de chiffres. Les jokers (*) ne sont pas acceptés. Appuyez sur un nouveau champ pour saisir d'autres critères ou **sur une recherche** pour soumettre une recherche.
Description brève	Saisissez du texte dans le champ, par exemple, `programme malveillant`. La fonctionnalité effectue une recherche sur les chaînes de texte et les chaînes de texte partielles dans le champ Brève description. Pour des recherches plus précises, saisissez plus de texte. Les jokers (*) ne sont pas acceptés. Appuyez sur un nouveau champ pour entrer plus de critères ou sur  pour soumettre une recherche.	Saisissez du texte dans le champ, par exemple, `programme malveillant`. La fonctionnalité effectue une recherche sur les chaînes de texte et les chaînes de texte partielles dans le champ Brève description. Pour des recherches plus précises, saisissez plus de texte. Les jokers (*) ne sont pas acceptés. Appuyez sur un nouveau champ pour saisir d'autres critères ou **sur une recherche** pour soumettre une recherche.
Priorité	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur l'icône en forme de coche pour revenir à l'écran Rechercher des incidents.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des incidents.
Catégorie	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur l'icône en forme de coche pour	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appuyez sur ce champ	Pour ajouter une entrée sur Android les appareils	À ajouter et à saisir sur iOS les appareils
	revenir à l'écran Rechercher des incidents.	revenir à l'écran Rechercher des incidents.
État	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur l'icône en forme de coche pour revenir à l'écran Rechercher des incidents.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des incidents.
Affecté à	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**.	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**.
Groupe d'affectation	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**.	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**.

Pour Android les appareils, une fois l'écran Rechercher des incidents affiché et tous vos critères entrés, choisissez-en un pour continuer.

Option	Description
Effacer ou modifier les critères de recherche avant d'exécuter une recherche	Pour effacer tous les critères saisis, avec l'écran Rechercher des incidents affiché, appuyez sur la flèche arrière pour effacer tous les champs et revenir à l'écran d'accueil des incidents de sécurité. La recherche n'est pas envoyée et les critères de recherche sont effacés. Vous pouvez également modifier un champ :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	◦ Avec l'écran Rechercher des incidents affiché, appuyez sur un champ avec des critères de recherche pour le développer. ◦ Appuyez sur un élément pour le désélectionner. Appuyez sur **Tout** pour sélectionner tous les éléments. Appuyez à nouveau sur **Tout** pour effacer tous les éléments. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**. ◦ Appuyez sur l'icône en forme de coche pour enregistrer les changements et revenir à l'écran Rechercher des incidents.
Soumettre une recherche	Une fois que l'écran Rechercher des incidents s'affiche avec les critères de recherche que vous avez saisis, appuyez sur l'icône d'envoi (icône ) Les incidents de sécurité qui correspondent à vos critères de recherche s'affichent. Une fois la recherche terminée, les critères de recherche ne sont pas enregistrés.

4. Pour iOS les appareils, une fois l'écran Rechercher des incidents affiché, choisissez-en un pour continuer.

Option	Description
Effacer ou modifier les critères de recherche avant d'exécuter une recherche	Pour effacer tous les critères et revenir à l'écran d'accueil, appuyez sur l'icône de fermeture (X). Les critères de recherche saisis ne sont pas enregistrés. Vous pouvez également modifier un champ : ◦ Avec l'écran Rechercher des incidents affiché, appuyez sur un champ avec des critères de recherche pour le développer. ◦ Appuyez sur un élément de la liste pour le désélectionner ou appuyez sur **Tout effacer**. Pour effacer une valeur pour les champs Groupe d'affectation et Affecté à, pour aucune entrée, sélectionnez **Aucun**. ◦ Appuyez sur **Terminé** pour enregistrer les changements et revenir à l'écran Rechercher des incidents.
Soumettre une recherche	L'écran Rechercher des incidents s'affiche avec les critères de recherche que vous avez saisis, puis appuyez sur **Rechercher**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Les incidents de sécurité qui correspondent à vos critères de recherche s'affichent. Une fois la recherche terminée, les critères de recherche ne sont pas enregistrés.

5. Facultatif : Si votre recherche renvoie plusieurs enregistrements, vous pouvez Filtrer les enregistrements avec l'attribut Application mobile Réponse aux incidents de sécurité affiner les résultats de la recherche.

Affichez, modifiez et affectez des tâches de réponse ouvertes avec l' Application mobile Réponse aux incidents de sécurité

Affichez, modifiez et affectez des tâches de réponse ouvertes. Vos modifications sont enregistrées dans la tâche Réponse aux incidents de sécurité de l'incident de sécurité parent.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

À partir de la liste des enregistrements, affectez-vous une tâche de réponse ouverte et non affectée ou affectez-vous à un autre analyste de votre groupe. Vous pouvez également afficher les détails de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

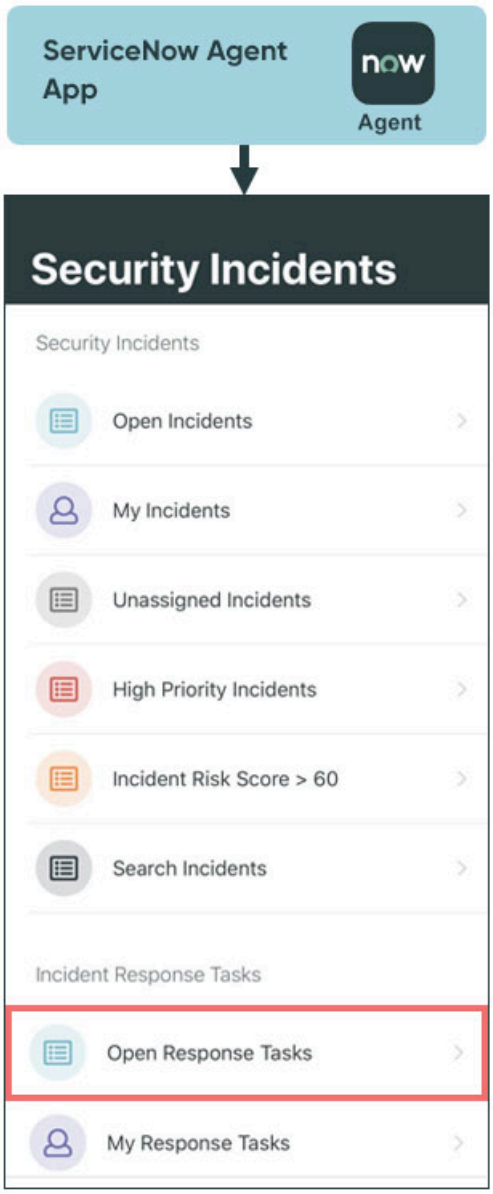
Procédure

1. Si vous n'êtes pas connecté à votre instance Now Platform sur votre équipement mobile, consultez .Connectez-vous au Application mobile Réponse aux incidents de sécurité
2. Une fois l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Tâches de réponse ouvertes**.

   Si vous quittez l'application Application mobile Réponse aux incidents de sécurité après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous avez affiché.

Traduction automatique

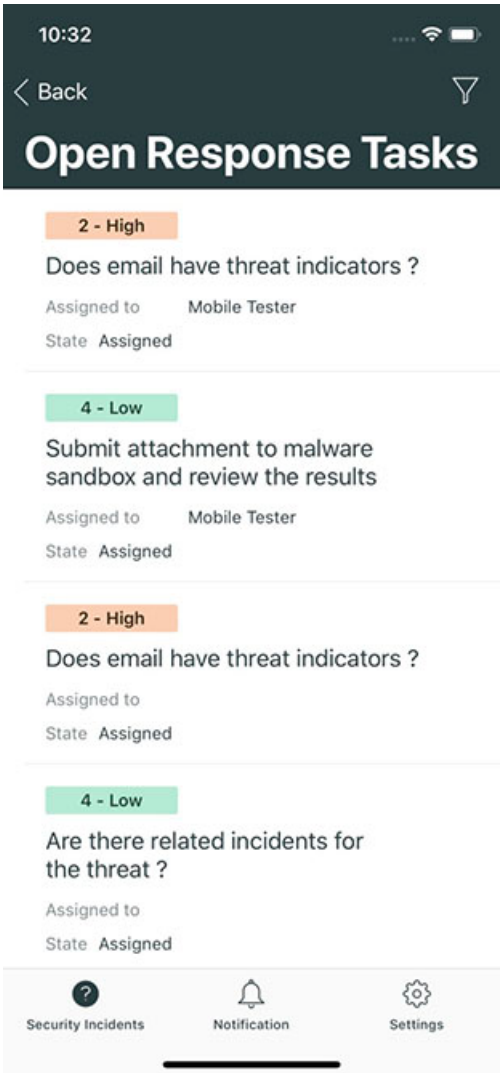
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'écran Tâches de réponse ouvertes s'affiche avec une liste des tâches ouvertes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Facultatif : Reportez-vous à Rechercher des incidents de sécurité avec l'attribut Application mobile Réponse aux incidents de sécurité pour rechercher des tâches qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans dans l'application mobile fonctionne comme avec un générateur de conditions sur Now Platform.

4. Une fois la liste des tâches de réponse ouvertes affichée, pour affecter ou réaffecter directement à partir de la liste, faites glisser vers la gauche sur un enregistrement pour ouvrir le menu.

5. Choisissez-en un pour continuer.

Option	Description
Mes affectations	Affectez-vous la tâche de réponse. Si la tâche vous est déjà affectée, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation :

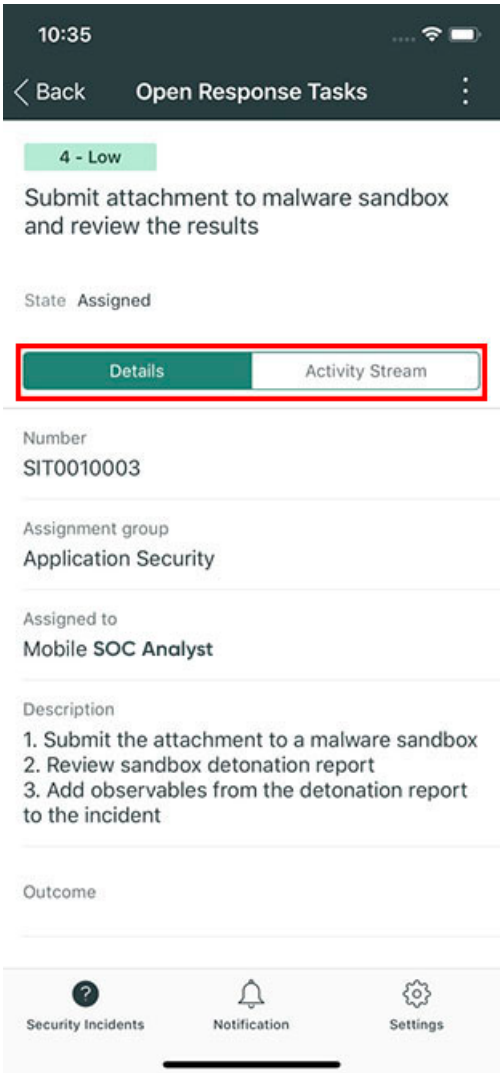
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Groupe d'affectation** **b.** Appuyez sur un groupe dans la liste affichée ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter la tâche à un membre du groupe d'affectation : **a.** Appuyez sur **Affecté à** et **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Un message s'affiche pour confirmer la mise à jour de l'enregistrement. La tâche de l'incident de sécurité parent est affectée à un nouvel utilisateur et mise à jour dans votre Now Platform instance. Appuyez sur l'icône d'envoi ( ou **sur Soumettre** pour enregistrer et soumettre vos modifications.

6. Pour afficher les détails d'un enregistrement de tâche de réponse ouvert, avec l'écran Tâches de réponse ouvertes affiché, appuyez également sur un enregistrement de la liste.
7. Une fois les onglets de l'enregistrement de tâche de réponse affichés, choisissez-en un dans la table suivante pour continuer.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Onglet Détails	Avec l'onglet Détails sélectionné, examinez les champs de la tâche de réponse. Pour modifier des champs ou affecter la tâche, appuyez sur l'icône de menu (icône ⋮ Dans le menu qui s'affiche, choisissez l'une des options suivantes. ◦ Appuyez sur **Modifier**. Avec l'écran Modifier la tâche de réponse affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et saisir du texte. ◦ Pour réaffecter la tâche, appuyez sur **Réaffecter** ou **Me l'affecter**. Une fois que vous avez terminé vos modifications, appuyez sur l'icône d'envoi ( ) ou **sur Soumettre** pour enregistrer vos modifications et mettre à jour l'enregistrement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	La tâche Réponse aux incidents de sécurité sur l'incident de sécurité parent dans votre Now Platform instance est mise à jour.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, choisissez-en un pour continuer. ◦ Affichez la piste d'audit créée par les notes de travail dans l'enregistrement. Pour ajouter une note de travail ou joindre un fichier, appuyez sur l'icône plus ( ) ◦ Appuyez sur l'icône de menu () pour modifier ou réaffecter la tâche.
Icônes de l'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ◦ Si elle est affichée, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ◦ Appuyez sur **Notification** pour afficher les notifications d'incidents de sécurité critiques qui vous sont affectés ou qui sont affectés à votre groupe d'affectation. ◦ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance Now Platform . ▪ Déconnectez-vous de l'instance actuelle. Pour vous déconnecter d'une Now Platform instance sur votre appareil, avec la page de détails affichée, appuyez sur **Déconnexion**.

Traduction automatique

Affichez, modifiez et réaffectez vos tâches de réponse avec le Application mobile Réponse aux incidents de sécurité

Affichez, modifiez et réaffectez les tâches de réponse qui vous sont affectées. Vos modifications sont enregistrées dans la tâche Réponse aux incidents de sécurité de l'incident de sécurité parent.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

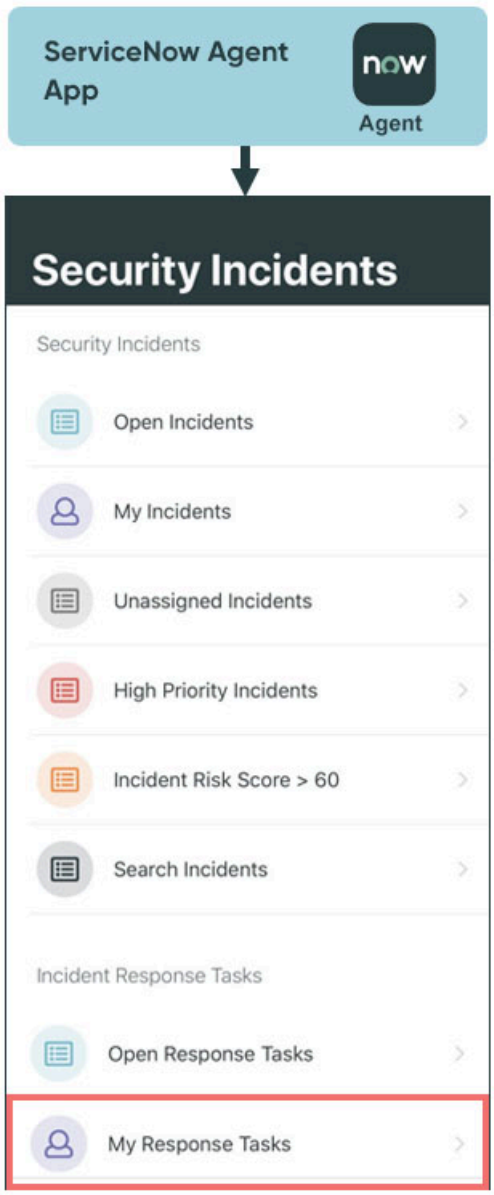
Dans la liste des enregistrements, réaffectez une tâche de réponse ouverte qui vous est affectée à un autre analyste de votre groupe. Vous pouvez également afficher les détails de l'enregistrement ou ajouter une note de travail avant la réaffectation. Temps nécessaire pour accomplir cette tâche : 5 à 10 minutes.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si vous n'êtes pas connecté à votre instance Now Platform sur votre équipement mobile, consultez .Connectez-vous au Application mobile Réponse aux incidents de sécurité
2. Une fois l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Mes tâches de réponse**.

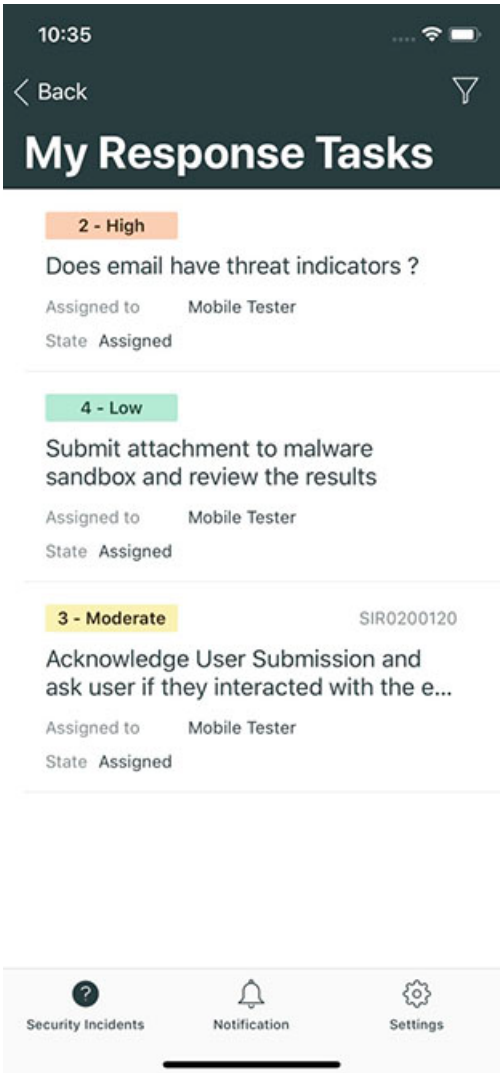
   Si vous quittez l'application Application mobile Réponse aux incidents de sécurité après vous être connecté, appuyez à tout moment sur l'application Now Agent (Prestataire) pour revenir au dernier écran que vous avez affiché.



L'écran Mes tâches de réponse s'affiche avec une liste des tâches de réponse qui vous sont affectées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



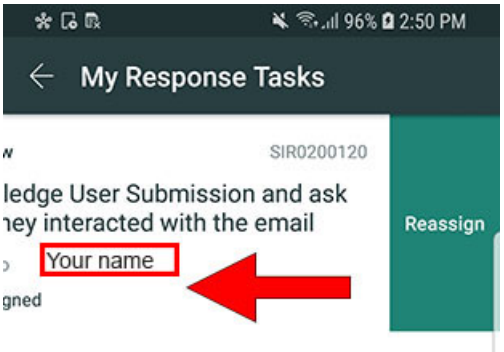
3. Facultatif : Reportez-vous à Rechercher des incidents de sécurité avec l'attribut Application mobile Réponse aux incidents de sécurité pour rechercher des tâches qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans dans l'application mobile fonctionne comme avec un générateur de conditions sur Now Platform.

4. Pour réaffecter une tâche directement à partir de la liste des enregistrements de tâches qui vous sont affectés, faites glisser vers la gauche sur un enregistrement pour ouvrir le menu.

Traduction automatique

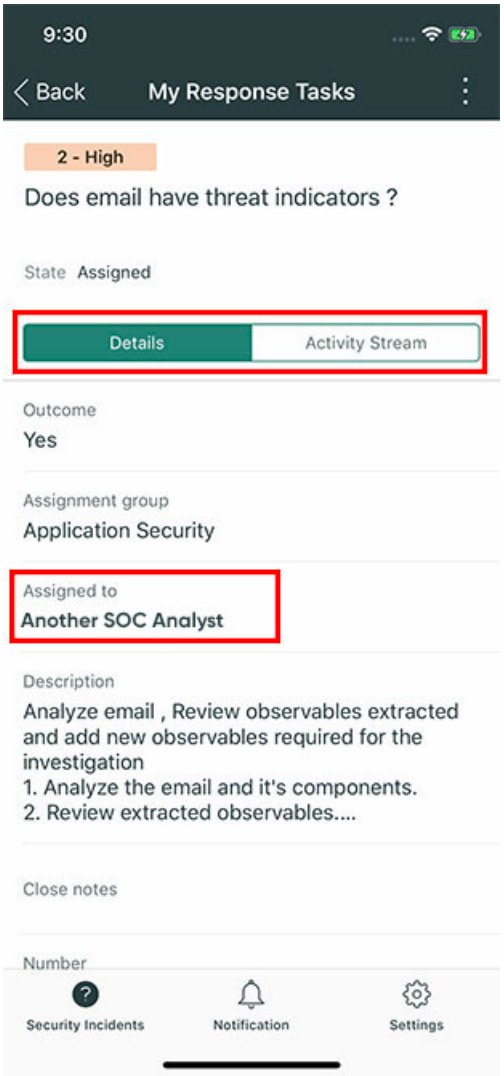
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Appuyez sur **Réaffecter**.
6. Sur l'écran Affecter la tâche de réponse à un autre qui s'affiche, appuyez sur un champ pour le développer et sélectionner un autre groupe ou utilisateur pour la tâche.
7. Appuyez sur l'icône d'envoi ( ) ou sur **Soumettre** pour enregistrer vos modifications et mettre à jour la tâche de réponse.
   Un message s'affiche pour confirmer la mise à jour de l'enregistrement. La tâche est affectée à un nouvel utilisateur sur l'incident de sécurité parent et votre Now Platform instance est mise à jour.
8. Pour afficher les détails d'une tâche de réponse ouverte et afficher les notes de travail, avec l'écran Mes tâches de réponse affiché, appuyez sur un enregistrement de la liste.
9. Une fois les champs de la tâche de réponse affichés, choisissez-en un dans la table suivante pour continuer.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Onglet Détails	Avec l'onglet Détails sélectionné, examinez les champs de la tâche de réponse. Pour modifier des champs ou réaffecter la tâche, appuyez sur l'icône de menu ().

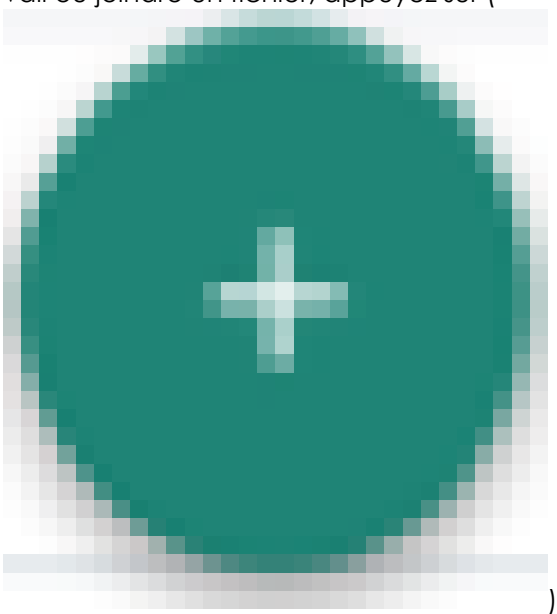
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Dans le menu qui s'affiche, choisissez l'une des options suivantes. ◦ Appuyez sur **Modifier**. Avec l'écran Modifier la tâche de réponse affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et saisir du texte. ◦ Pour réaffecter la tâche, appuyez sur **Affecter à un autre**. Une fois que vous avez terminé vos modifications, appuyez sur l'icône d'envoi () ou **sur Soumettre** pour enregistrer vos modifications et mettre à jour l'enregistrement. La tâche Réponse aux incidents de sécurité sur l'incident de sécurité parent dans votre Now Platform instance est mise à jour.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, choisissez-en un pour continuer. ◦ Affichez la piste d'audit créée par les notes de travail sur l'enregistrement de tâche. Pour ajouter une note de tra-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	vail ou joindre un fichier, appuyez sur (). ◦ Appuyez sur () pour modifier ou réaffecter la tâche.
Appuyez sur une icône d'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ◦ S'il est affiché, appuyez sur une autre icône pour ouvrir une autre ServiceNow® application principale afin de l'ouvrir. ◦ Appuyez sur **Notification** pour afficher les notifications d'incidents de sécurité critiques qui vous sont affectés ou qui sont affectés à votre groupe d'affectation. ◦ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance Now Platform . ▪ Déconnectez-vous de l'instance actuelle. Pour vous déconnecter d'une

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Now Platform instance sur votre appareil, avec la page de détails affichée, appuyez sur **Déconnexion**.

Filtrer les enregistrements avec l'attribut Application mobile Réponse aux incidents de sécurité

Définissez des filtres supplémentaires pour limiter le nombre d'enregistrements qui s'affichent sur un écran. Le filtrage des enregistrements au sein de l'application mobile fonctionne comme avec un créateur de conditions sur Now Platform.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Temps d'exécution de cette tâche : 5 minutes.

Procédure

1. Pour affiner les résultats de votre recherche ou pour entrer des critères de filtrage supplémentaires sur toute liste d'enregistrements affichée, appuyez sur l'icône de filtre (icône 
2. Une fois l'écran Filtres affiché, appuyez sur un champ pour le développer.
3. Dans les options qui s'affichent, cochez la case ou appuyez sur un élément pour votre filtre.
   Pour de nombreux filtres, vous pouvez sélectionner plus d'une option.
4. Appuyez sur la flèche Retour (ou sur **TERMINÉ** pour enregistrer vos modifications dans un champ.
   Les critères que vous avez choisis s'affichent sur l'écran Filtres. Le nombre d'enregistrements qui correspondent à vos critères est également affiché en haut de l'écran. Appuyez sur **RESET** pour supprimer tous les filtres et rétablir le paramètre par défaut.
5. Facultatif : Répétez les étapes 1 à 4 avec l'écran Filtres affiché pour continuer à définir vos critères de filtrage.
6. Appuyez sur l'icône  afin de créer des conditions ET.
   Vous pouvez également appuyer sur l'icône d'intersection afin de créer des conditions OU.
7. Une fois que vous avez ajouté tous les critères que vous souhaitez, avec l'écran Filtres affiché, appuyez sur **TERMINÉ**.
   À l'écran, seuls les enregistrements qui correspondent à vos critères de filtrage s'affichent.

Orchestration de la réponse aux incidents de sécurité

Orchestration de la réponse aux incidents de sécurité Les activités permettent aux utilisateurs d'interagir et de récupérer des données à partir de systèmes et d'environnements Windows ou UNIX à l'aide de l'orchestration de workflow.

Configurer Orchestration de la réponse aux incidents de sécurité

Avant d'utiliser Orchestration de la réponse aux incidents de sécurité, effectuez des étapes de configuration de différentes parties du système, notamment le remplissage de la CMDB, la configuration du MID Server et la configuration des informations d'identification.

Avant de commencer
Rôle requis : administrateur

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Pour utiliser Réponse aux incidents de sécurité, vous avez besoin d'une CMDB entièrement remplie avec des noms de domaine. Pour plus d'informations, consultez Découverte .

Pourquoi et quand exécuter cette tâche

Procédure

1. Activez le Réponse aux incidents de sécurité module d'extension.
2. Configuration des MID Servers .
3. Configurez les informations d'identification du service Windows MID Server .

Comprendre les workflows et les modèles de workflow d'Orchestration de Security Incident Response

Le Réponse aux incidents de sécurité système de base comprend une série de workflows et de modèles de workflow conçus pour fonctionner avec les enregistrements d'incidents de sécurité.

Avant de commencer
Rôle requis : sn_si.basic

Pourquoi et quand exécuter cette tâche
Vous pouvez adapter tous les workflows et modèles de workflow pour mieux répondre à vos besoins, en supposant que vous disposez du rôle approprié : sn_sec_cmn.admin.
Les workflows sont utilisés dans l'ensemble du système Security Operations pour effectuer diverses tâches.
Toutefois, les modèles de workflow sont déclenchés par la sélection d'une valeur dans le champ **Catégorie** d'un incident de sécurité. Lorsque cela se produit, le modèle de workflow associé à la sélection lance un modèle de workflow qui indique aux analystes de sécurité comment gérer un type spécifique de menace.

Par exemple, si vous sélectionnez **Déni de service** dans le champ **Catégorie** d'un incident de sécurité, le **modèle Incident de sécurité - Déni de service - Modèle** est exécuté et l'analyste est chargé de déterminer si la cible du déni de service est critique pour l'entreprise. Si tel est le cas, la tâche suivante entraîne la définition de la priorité de l'incident de sécurité sur **1 - Critique**, puis exécute la tâche suivante. Et ainsi de suite.

Les Réponse aux incidents de sécurité workflows et les modèles de workflow sont donc essentiellement les mêmes, sauf que les modèles sont utilisés pour un ensemble spécifique de fonctions au sein d'un incident de sécurité.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Workflows** > **Voir les workflows de sécurité**.
2. Une liste des workflows et des modèles de workflow expédiés dans le système de base s'affiche.
   Tous les nouveaux workflows que vous avez créés dans la suite d'applications Opérations de sécurité sont également inclus dans la liste.
3. Cliquez sur le nom du workflow ou du modèle de workflow que vous souhaitez afficher.

> **Remarque :** Les workflows peuvent être déclenchés de différentes manières. Sachez que l'association d'un workflow à un déclencheur de workflow ne signifie pas nécessairement que le workflow est actif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Orchestration de la réponse aux incidents de sécurité Workflows et activités

Plusieurs workflows et activités sont inclus avec Orchestration de la réponse aux incidents de sécurité.

seuls les utilisateurs disposant du rôle sn_sec_cmn.admin peuvent Éditeur de workflow .

Créer une demande de recherche pour le workflow des changements IoC

Le flux **Réponse aux incidents de sécurité - Créer une demande de recherche pour les changements IoC** est déclenché par une règle métier pour s'exécuter automatiquement lorsqu'un IoC est ajouté ou changé. Les analyses de logiciels malveillants ne sont déclenchées que lorsque de nouvelles données sont saisies et seules les nouvelles données sont analysées.

Avant de commencer

Rôle requis : sn_si.basic

Pourquoi et quand exécuter cette tâche

Si l'IoC est vide, le workflow ne s'exécute pas. Les analyses historiques sont conservées et consultables dans l'onglet **Demandes d'analyse de sécurité** et dans les notes de travail de l'incident de sécurité. Les incidents de sécurité existants sont automatiquement mis à jour.

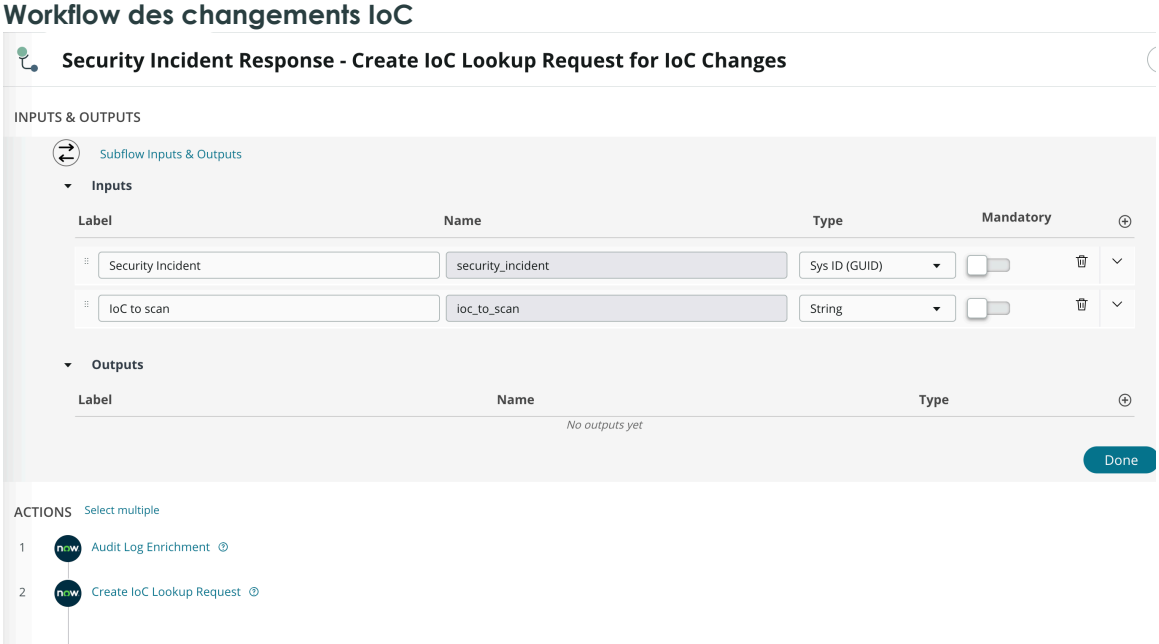
Important :

Le workflow **Réponse aux incidents de sécurité - Créer une demande de recherche pour les changements IoC** est migré vers Flow Designer. Le flux est déclenché uniquement lorsque le sn_ti_scanner a au moins un enregistrement.

Les actions du Concepteur de flux incluent :

- Enrichissement du journal d'audit
- Créer une activité de demande de recherche d'IoC

Workflow des changements IoC



Créer une activité de demande de recherche d'IoC

L'activité Créer une demande de recherche d'IoC peut être utilisée avec n'importe quel workflow pour créer une demande de recherche de programme malveillant pour les champs IoC ajoutés ou modifiés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Demande de recherche créée.
Échec	Demande de recherche non créée.

Variables d'entrée

Variable	Description
iocString	Informations IoC au format JSON. IP, hachage, url.
sild	Identificateur système de l'incident de sécurité

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
scnReqID	Rechercher un identificateur de demande

Workflow Security Incident Response - Obtenir les statistiques réseau

Le champ **Réponse aux incidents de sécurité** > **Obtenir les statistiques réseau** workflow récupère les statistiques réseau d'une ressource Windows affectée lorsqu'elle est ajoutée à un incident de sécurité à l'état **Analyse** .

Avant de commencer

Rôle requis : sn_si.analyst

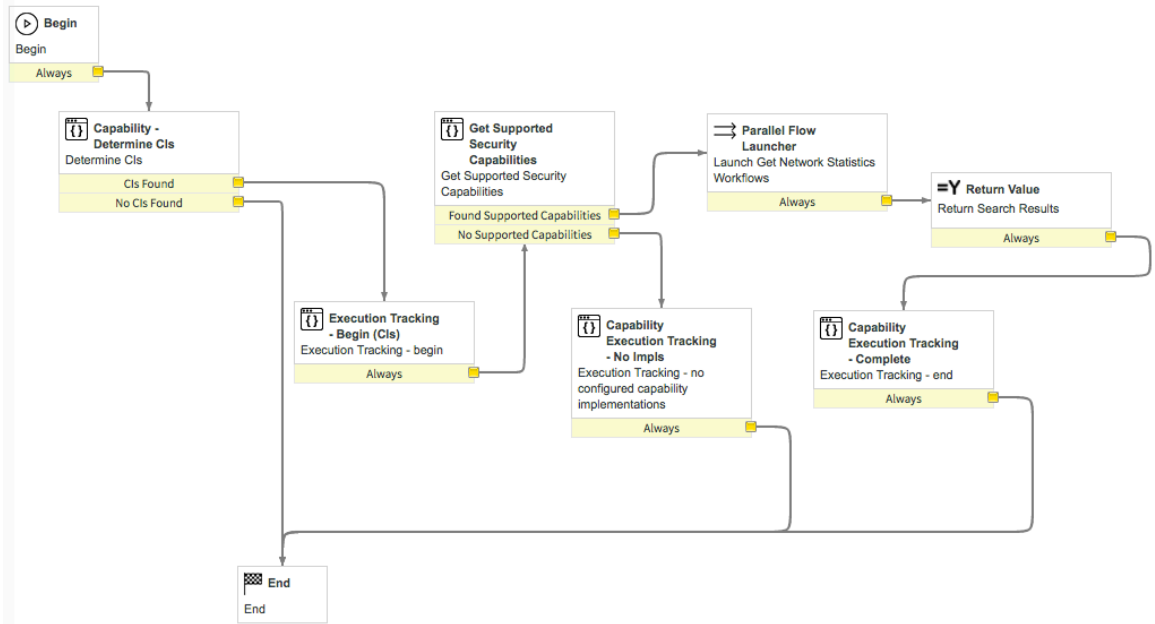
Pourquoi et quand exécuter cette tâche

Pour les nouveaux incidents de sécurité contenant des éléments de configuration, le workflow s'exécute automatiquement lorsque l'état passe à **Analyse**.

Les incidents de sécurité existants sont automatiquement mis à jour lorsque vous êtes dans l'état **Analyse** et que vous ajoutez un nouvel élément de configuration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Obtenir les statistiques réseau



Les activités de processus du workflow comprennent :

- Obtenir l'activité FQDN de l'élément de configuration
- Déterminer le script Shell par système d'exploitation
- Si l'instruction est exécutée par Powershell
- Suivi des exécutions : démarrer l'activité
- Obtenir les statistiques réseau via l'activité netstat
- Suivi d'exécution de l'aptitude : activité d'échec
- Créer une activité d'enregistrements de données d'enrichissement
- Suivi d'exécution de l'aptitude : activité d'échec - Renvoie l'ID d'enrichissement.
- Suivi d'exécution de l'aptitude : terminer l'activité

Procédure

1. Ouvrez un incident de sécurité.
2. Mettez à jour **l'état** sur **Analyse**, si nécessaire.
3. Ajoutez un élément de configuration (ordinateur, serveur ou similaire).
4. Cliquez sur **Mettre à jour**.
   Orchestration de la réponse aux incidents de sécurité fournit des informations statistiques sur le réseau dans le **Liens connexes** > **Enrichissements des incidents de sécurité** onglet. Pour plus d'informations, reportez-vous à la section Opérations de sécurité Mappage des données d'enrichissement.

   Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Réponse aux incidents de sécurité : workflow Obtenir les services d'exécution

Le **workflow Réponse aux incidents de sécurité - Obtenir les services d'exécution** récupère une liste des services en cours d'exécution à partir d'éléments de configuration (CI) basés sur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Windows. ServiceNow Ce workflow est utilisé pour l'enrichissement des incidents au cours des enquêtes.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Le **workflow Réponse aux incidents de sécurité - Obtenir les services d'exécution** s'exécute automatiquement lorsque vous ajoutez un nouvel élément de configuration à un incident de sécurité Windows une fois que l'état est défini sur **Analyse**. Les informations obtenues par ce workflow apparaissent dans les onglets **Afficher les données d'enrichissement** pour l'incident de sécurité.

Remarque : Si l'incident de sécurité reste à l'état **Brouillon** , le **workflow Réponse aux incidents de sécurité - Obtenir les services d'exécution** ne s'exécute pas.

Les activités du workflow comprennent :

Enrichissement du journal d'audit Activité de script

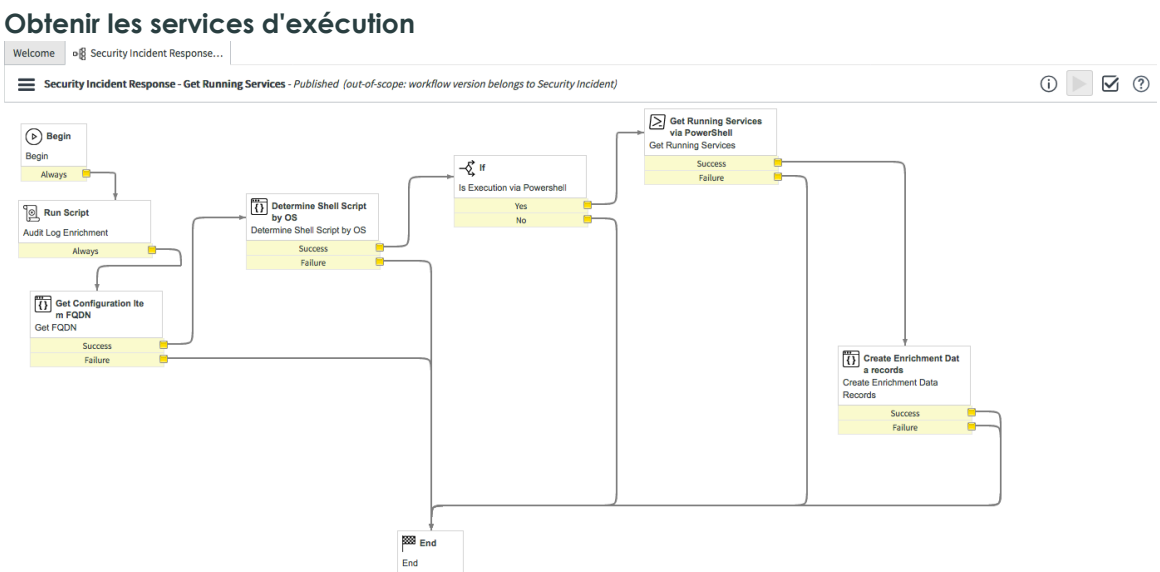
Obtenir l'activité FQDN de l'élément de configuration

Déterminer le script Shell par activité du système d'exploitation

Est une exécution via l'activité PowerShell

Obtenir les services d'exécution : activité d'enrichissement WMI

Créer une activité d'enregistrements de données d'enrichissement



Procédure

1. Ouvrez un incident de sécurité.
2. Mettez à jour **l'état** sur **Analyse**, si nécessaire.
3. Ajoutez un élément de configuration Windows (serveur, ordinateur portable ou similaire).
4. Cliquez sur **Mettre à jour**.
   Réponse aux incidents de sécurité fournit des informations sur les services d'exécution dans le **Liens connexes** > **Enrichissements des incidents de sécurité**onglet. Pour plus d'informations, consultez Opérations de sécurité Mappage des données d'enrichissement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déterminer le script Shell par activité du système d'exploitation

L'activité de workflow Déterminer le script Shell par système d'exploitation détermine le système d'exploitation à utiliser dans le workflow

L'activité Déterminer le script shell par système d'exploitation peut être utilisée avec n'importe quel workflow pour déterminer le script shell à exécuter en fonction du système d'exploitation en cours d'exécution sur le système contenant l'élément de configuration.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Système d'exploitation trouvé.
Échec	Aucun système d'exploitation trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
ciSysId	Identificateur système de l'élément de configuration.
processType	Identificateur interne qui définit le script à extraire de la table.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
processScript (en anglais)	Agent ECC qui rassemble le processus en cours d'exécution.
executionTemplate (modèle d'exécution)	Détermine si le script est exécuté via une sonde ou à l'aide de PowerShell.
enrichmentMappingId	Identificateur système du mappage d'enrichissement utilisé pour transformer les données de réponse.

Obtenir les services d'exécution : enrichissement WMI

Le workflow **Réponse aux incidents de sécurité - Obtenir les services d'exécution** rassemble les services en cours d'exécution sur un élément de configuration ajouté à un incident de sécurité.

L'activité **Obtenir les services en cours d'exécution : enrichissement WMI** est lancée automatiquement pour récupérer les informations sur les services en cours d'exécution pour un hôte Windows.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
cible [chaîne]	Nom de domaine complet (FQDN) du système cible.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
Réponse [chaîne]	Chaîne JSON représentant les services en cours d'exécution sur le système cible. Les données JSON comprennent : name Le nom du service pid Identificateur de processus du service en cours service_type (Facultatif) Type de service en cours d'exécution. start_name Le nom du système pour le service chemin d'accès Chemin d'accès au fichier de l'exécutable du service en cours start_mode Mode de démarrage du service en cours d'exécution. display_name Nom du service en cours d'exécution tel qu'il apparaît à l'utilisateur

Restrictions

Le MID Server doit prendre en charge **PowerShell**.

Le hachage SHA-256 nécessite PowerShell V4.

Exécuter le workflow procdump

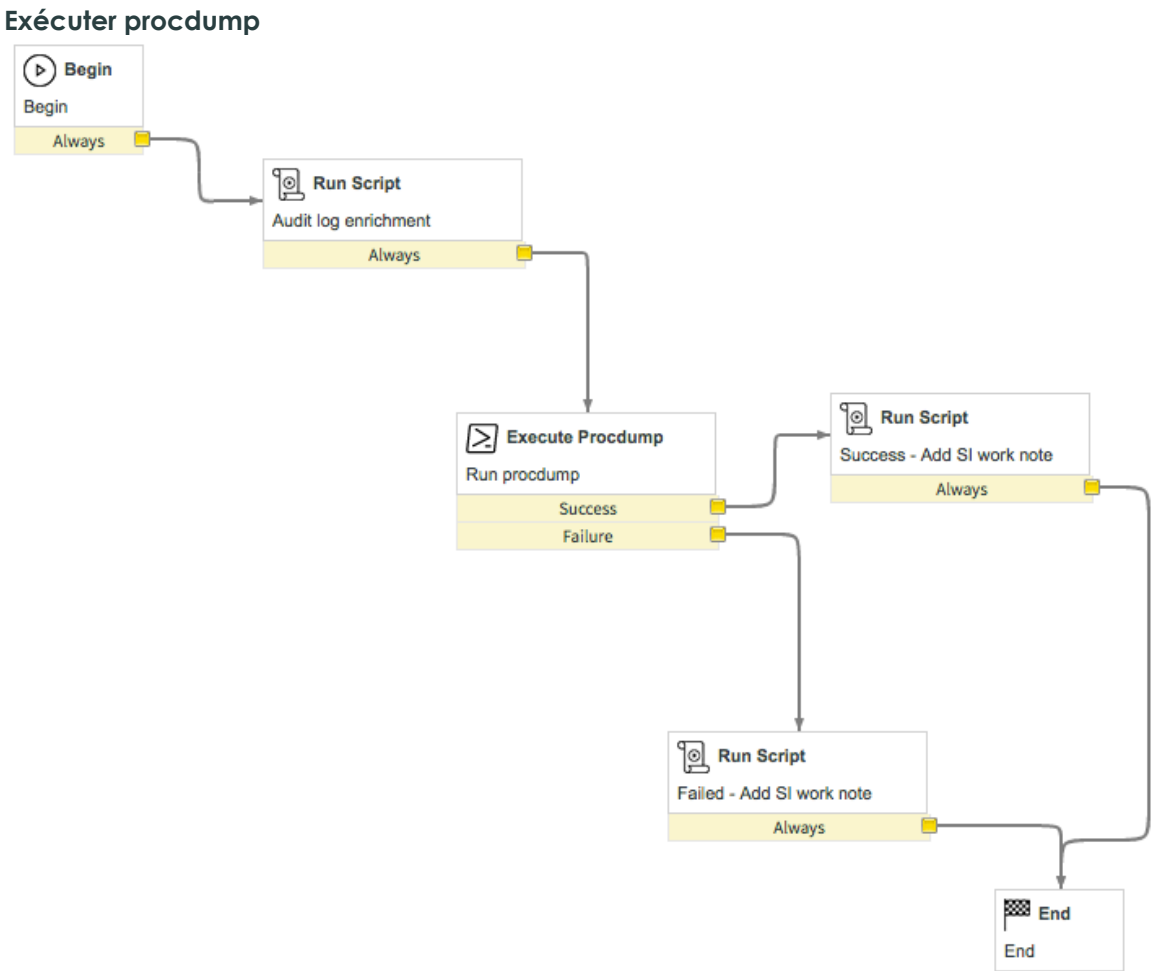
Le workflow **Exécuter procdump** exécute un vidage de processus sur un processus spécifié et l'enregistre dans un fichier qui peut être ciblé par les analystes de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Ce workflow est déclenché lorsque des processus enrichis sont sélectionnés et qu'une action d'interface utilisateur **Exécuter procdump** est exécutée.



Les activités de processus du workflow comprennent :

- Exécuter le script (enrichissement du journal d'audit) : exécute un script pour ajouter un journal d'audit à l'incident de sécurité.
- Exécuter l'activité procdump
- Exécuter le script (Réussite : ajouter une note de travail SI) : exécute un script pour ajouter une note de travail lorsque le procdump réussit.
- Exécuter le script (Échec – Ajouter une note de travail SI) : exécute un script pour ajouter une note de travail lorsque le procdump échoue. Les raisons pour lesquelles le procdump peut échouer sont les suivantes :
  - Chemin de vidage non valide
  - Chemin d'accès du partage de fichier non valide
  - Impossible d'extraire le nom de domaine complet de l'ordinateur Windows sur lequel le procdump s'exécute
  - Le nom du processus n'est pas spécifié

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La variable d'environnement PROCDUMP est introuvable
- Échec de la copie d'une copie du fichier dump à partir du chemin de vidage vers le chemin d'accès du partage de fichiers

Exécuter l'activité procdump

Exécuter procdump est une activité PowerShell qui exécute le procdump sur les processus sélectionnés, vide les données dans un fichier et les publie sur un site partagé sur un réseau interne. Un analyste peut ensuite afficher un processus sur liste de refus, surligné en rouge dans un incident de sécurité, et effectuer une analyse supplémentaire sur le fichier.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Le procdump s'est exécuté avec succès sur le process_name, et les détails sont disponibles dans activityOutput.response.
Échec	Le procdump n'a pas pu s'exécuter sur le process_name, et les détails sont disponibles dans activityOutput.response.

Variables d'entrée

Les variables d'entrée sont utilisées pour créer les sorties demandées.

Variables d'entrée

Variable	Description
targetId	[Obligatoire] ID cible sur lequel exécuter le procdump.
process_name	[Obligatoire] Nom du processus pour le procdump.
dump_path	[Obligatoire] Chemin d'accès du fichier local dans lequel le fichier de vidage généré sera enregistré.
dump_filename	[Obligatoire] Le nom du fichier généré par le procdump. Tous les caractères spéciaux seront remplacés par des traits d'union (-) dans le nom du fichier dump lorsque le fichier est généré.
file_share_path	[Obligatoire] Chemin d'accès du partage de fichiers vers lequel le fichier dump sera copié.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
share_path	Chemin d'accès du partage de fichiers vers lequel le fichier dump a été copié.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
réponse	Représentation JSON du résultat du procdump.
résultat	Résultat du procdump.

Incident de sécurité - Évaluer le workflow des résultats des tâches de réponse

Incident de sécurité - Évaluer le workflow des résultats des tâches de réponse détermine la tâche à utiliser, invoque un workflow choisi et un script d'évaluation basé sur l'enregistrement de l'évaluateur de résultat fourni comme entrée dans le workflow choisi.

Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Ce workflow est destiné à s'exécuter en même temps que l'activité de création de tâche à évaluer. Le script d'évaluation interroge les artefacts (tels que les perceptions, les enregistrements de recherche ou les processus en cours) de l'option configurée à l'aide des informations contextuelles de la tâche de réponse (telles que son incident de sécurité parent) afin de déterminer le résultat approprié pour la tâche de réponse. Le résultat peut potentiellement dépendre de l'activité du workflow, mais est généralement **oui** ou **non**. Lors de la création d'un enregistrement de l'évaluateur de résultat, seules les aptitudes ayant un workflow configuré, avec la case **Est l'aptitude basée sur la tâche** cochée et un jeu de variables d'entrée de tâche peuvent être sélectionnées.

Les activités de processus du workflow comprennent :

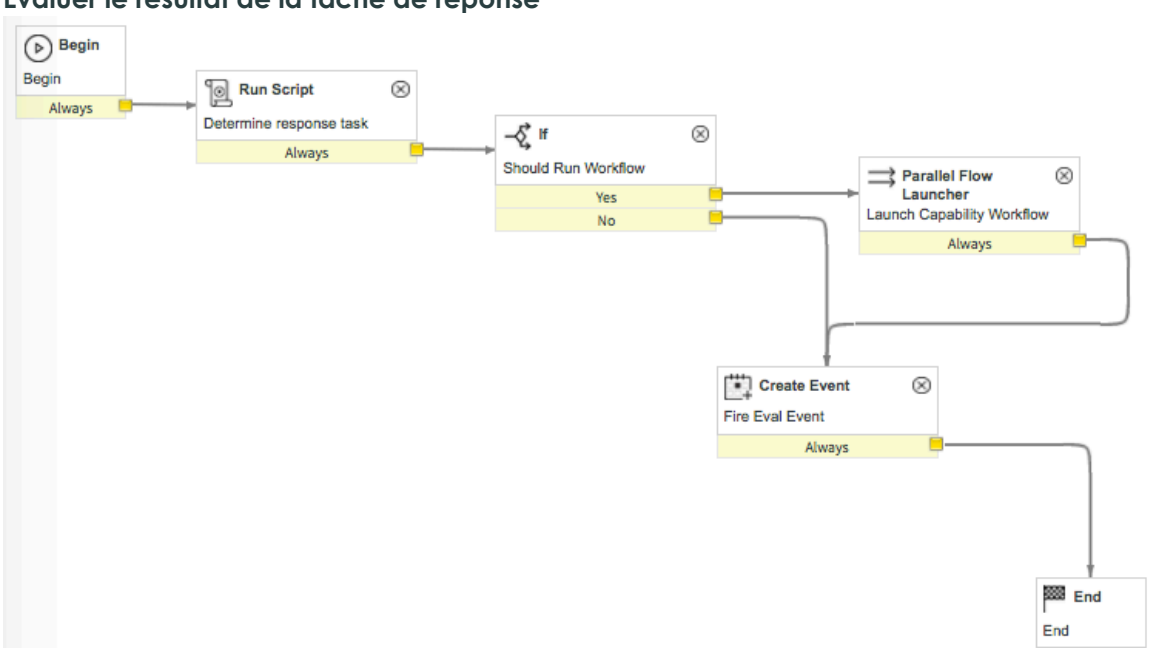
Exécuter le script pour déterminer la tâche de réponse

Doit exécuter le workflow

Workflow d'aptitude de lancement du lanceur de flux parallèle

Créer un événement d'évaluation

Évaluer le résultat de la tâche de réponse



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modèles de workflow Security Incident Response

Des modèles de workflow sont fournis pour Orchestration de la réponse aux incidents de sécurité vous permettre d'exécuter des procédures d'analyse de base liées à l'opération de sécurité. Les modèles peuvent être utilisés tels quels ou vous pouvez les personnaliser pour créer des flux de travail adaptés à vos besoins spécifiques. Les modèles de workflow sont désactivés par défaut.

seuls les utilisateurs disposant du rôle sn_sec_cmn.admin peuvent Éditeur de workflow .

Modèle de workflow d'exposition des données confidentielles des incidents de sécurité

Le modèle Incident de sécurité - Exposition de données confidentielles - vous permet d'effectuer une série de tâches conçues pour gérer l'exposition des données sensibles.

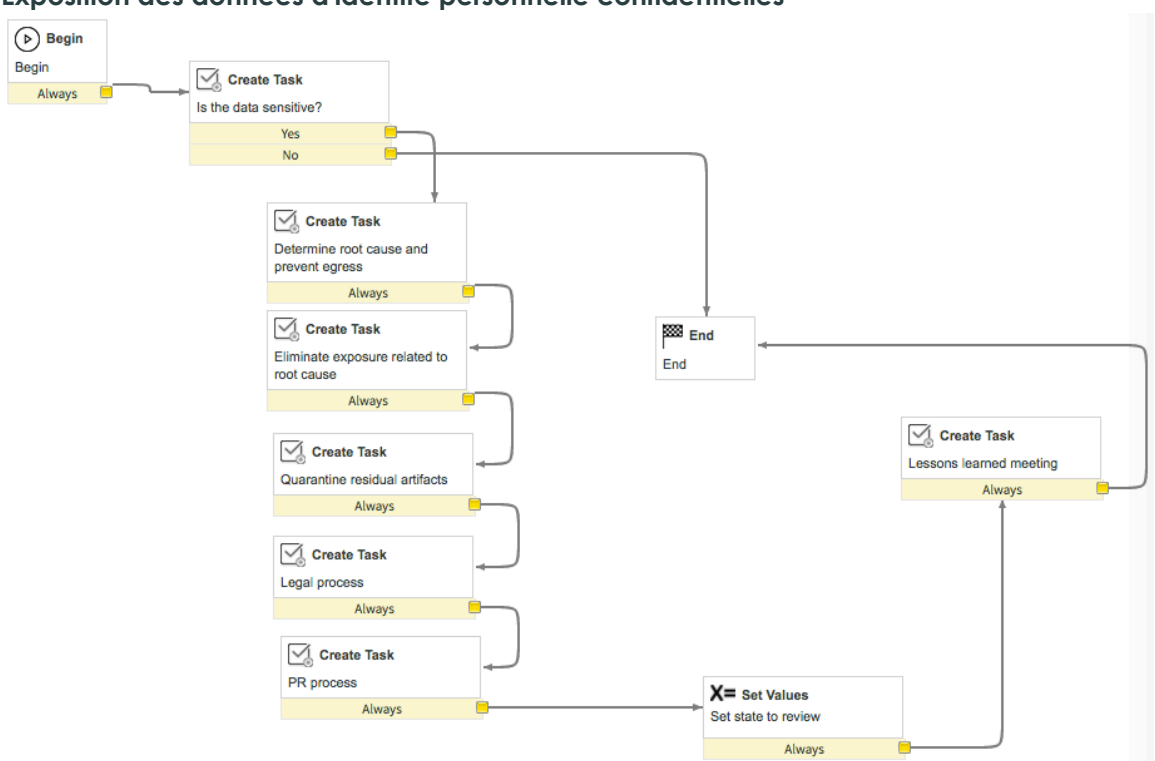
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie ou changée sur **Exposition des données d'identité personnelle confidentielles**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Exposition des données d'identité personnelle confidentielles



Procédure

1. Ouvrez l'incident de sécurité pour lequel vous souhaitez gérer l'exposition aux données sensibles ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Exposition des données d'identité personnelle confidentielles**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du flux.

Tâches de réponse dans le modèle d'exposition des données confidentielles

Tâche de réponse	Description	Résultats
Les données sont-elles sensibles ?	Déterminez si les données associées à cet incident de sécurité sont sensibles ou confidentielles. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous avez sélectionné **Oui**, la tâche de réponse suivante est exécutée. Si vous avez sélectionné **Non**, le flux se termine.
Déterminer la cause première et empêcher la sortie	Déterminez la cause première de l'attaque et ajoutez un filtrage de sortie pour arrêter l'exfiltration, en mettant à jour le champ **État** dans la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Éliminer l'exposition liée à la cause première	En fonction de la cause première, effectuez les étapes pour éliminer l'exposition, en mettant à jour le champ **État** de la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Mettre en quarantaine les artefacts résiduels	Effectuez les étapes de mise en quarantaine de tous les artefacts résiduels, en mettant à jour le champ **État** de la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Processus juridique	Effectuez les étapes pour satisfaire aux exigences juridiques de cette analyse, en mettant à jour le champ **État** de la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Processus de relations publiques	Effectuez les étapes pour satisfaire aux exigences PR de cette analyse, en mettant à jour le champ **État** dans la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**.
Réunion sur les enseignements tirés	Organisez une réunion Enseignements tirés pour trier le travail effectué sur ces données sensibles, en mettant à jour le champ **État** dans la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, l'incident de sécurité reste à l'état **Examiner** jusqu'à ce que vous le fermiez.

Traduction automatique

Modèle de workflow Déni de service d'incident de sécurité

Le modèle Incident de sécurité - Déni de service - vous permet d'effectuer une série de tâches conçues pour gérer les attaques par déni de service (DOS).

Avant de commencer

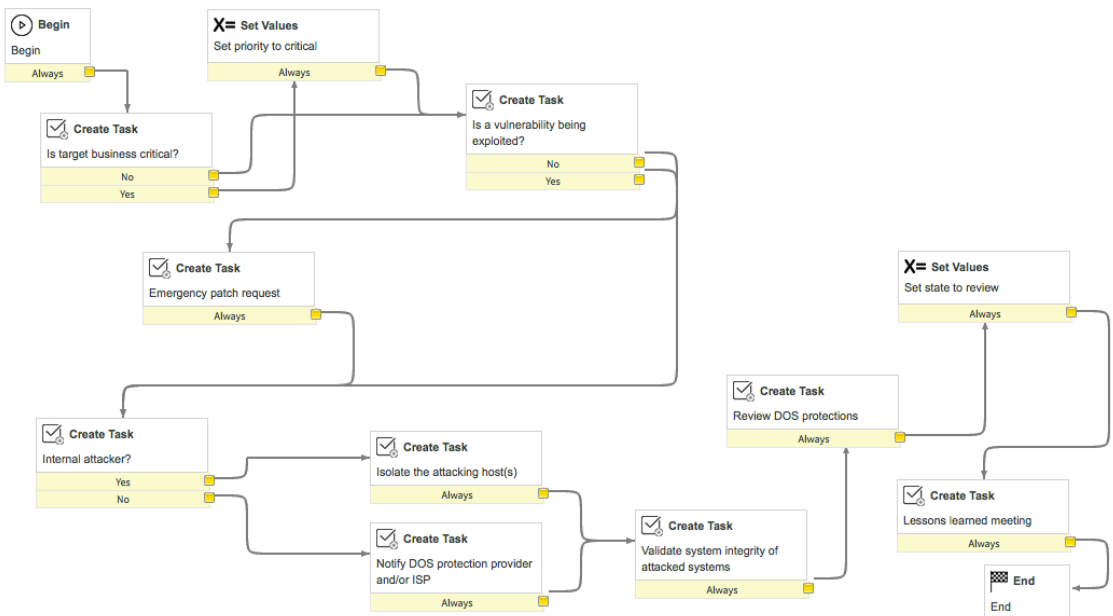
Rôle requis : sn_si.write

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Déni de service**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Déni de service (DOS)



Procédure

1. Ouvrez l'incident de sécurité pour cet événement de déni de service ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Déni de service**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du flux.

Tâches de réponse dans le modèle de déni de service

Tâche de réponse	Action	Résultats
La cible est-elle critique pour l'activité ?	Déterminez si la cible de cette attaque par déni de service est critique pour l'entreprise. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, **l'option Définir la priorité sur la tâche critique** est exécutée. Si vous sélectionnez **Non**, la tâche **Une vulnérabilité est-elle exploitée ?**, est exécutée.
Définir la priorité sur critique	Aucune action n'est requise.	La **priorité** de l'incident de sécurité passe automatiquement à **Critique** et la tâche **Une vulnérabilité**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
		est-elle exploitée ? est exécutée.
Une vulnérabilité est-elle exploitée ?	Déterminez si cette attaque DOS exploite une vulnérabilité logicielle. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **de demande de correctif d'urgence** est exécutée. Si vous sélectionnez **Non**, la tâche **Attaquant interne ?** est exécutée.
Demande de correctif d'urgence	Émettre une demande de correctif d'urgence pour le ou les systèmes attaqués. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez modifié l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Attaquant interne ?	Déterminez si la source de cette attaque DOS est interne à votre organisation. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Isoler le ou les hôtes attaquants** est exécutée. Si vous sélectionnez **Non**, la tâche **Notifier le fournisseur de protection DOS et/ou le FAI** est exécutée.
Isoler le ou les hôtes attaquants	Effectuez les étapes nécessaires pour isoler le ou les hôtes internes responsables de l'attaque. Mettez à jour le champ **État** dans la tâche comme il convient.	Une fois cette étape terminée, la tâche **Valider l'intégrité du système des systèmes attaqués** est exécutée.
Notifier le fournisseur de protection contre le déni de service et/ou le FAI	Effectuez les étapes nécessaires pour contacter votre fournisseur de protection contre le déni de service et/ou votre fournisseur d'accès Internet afin de les informer de l'attaque. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez modifié l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Valider l'intégrité des systèmes attaqués	Effectuez les étapes nécessaires pour évaluer et valider l'intégrité des ordinateurs attaqués. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez modifié l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Examiner les protections DOS	Passez en revue vos protections et procédures DOS existantes. Apportez les modifications nécessaires.	Si vous avez modifié l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
	Mettez à jour le champ **État** dans la tâche comme il convient.	
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**. La tâche **de réunion Enseignements tirés** est exécutée.
Réunion sur les enseignements tirés	Organisez une réunion Enseignements tirés pour trier le travail effectué pour cet incident de déni de service. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé, Terminé** ou **Annulé**, le flux s'arrête.

Modèle de workflow Équipement perdu d'incident de sécurité

Le modèle Incident de sécurité - Équipement perdu - Permet d'effectuer une série de tâches conçues pour gérer les équipements perdus.

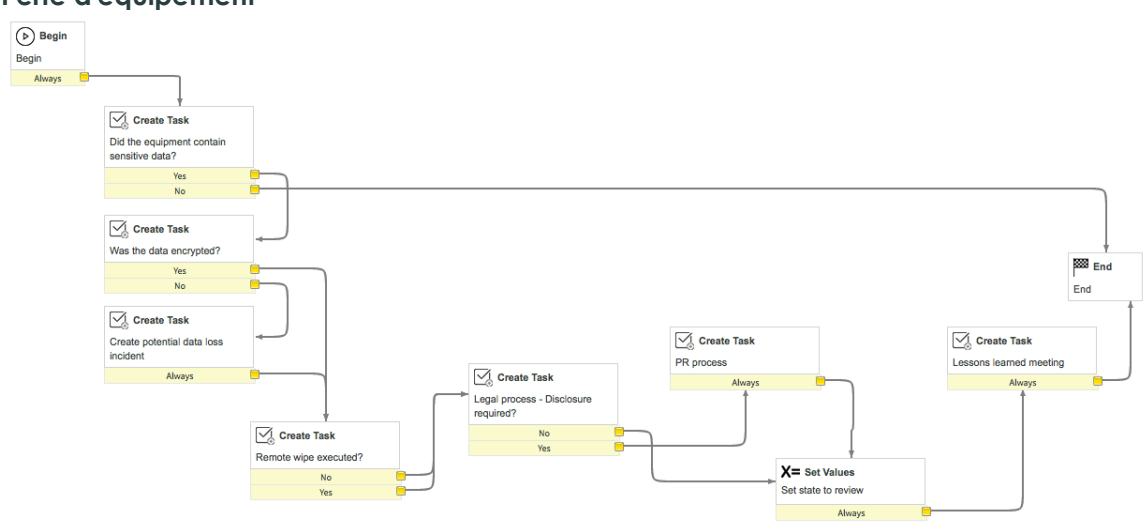
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Perte d'équipement**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Perte d'équipement



Procédure

1. Ouvrez l'incident de sécurité pour la perte d'équipement ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Perte d'équipement**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du flux.

Tâches d'intervention dans le modèle d'équipement perdu

Tâche de réponse	Action	Résultats
L'équipement contenait-il des données sensibles ?	Déterminez si l'équipement associé à cet incident de sécurité contenait des informations sensibles ou confidentielles. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat** , selon le cas.	Si vous sélectionnez **Oui** , la tâche **Les données ont-elles été chiffrées ?,** est exécutée. Si vous sélectionnez **Non**, le flux se termine.
Les données ont-elles été chiffrées ?	Déterminez si les données sensibles de l'appareil perdu ont été chiffrées. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat** , selon le cas.	Si vous sélectionnez **Oui**, la tâche de réponse **Effacement à distance créé ?** est exécutée. Si vous sélectionnez **Non**, la tâche **de réponse Créer un incident de perte de données potentielle**est exécutée.
Créer un incident de perte de données potentielle	Effectuez les étapes nécessaires pour créer un incident de perte de données potentiel. Une fois que vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet** , selon le cas.	La tâche **de réponse Effacement à distance créé ?** est exécutée.
Effacement à distance créé ?	Effectuez les étapes nécessaires pour effectuer un effacement à distance de l'équipement perdu. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat** , selon le cas.	La tâche **Processus juridique - Divulgation requise** est exécutée.
Procédure judiciaire - Divulgation requise ?	Effectuez les étapes pour satisfaire aux exigences juridiques de cette analyse. Sélectionnez **Oui** si une divulgation légale est requise, **Non**si elle ne l'est pas.	La tâche **de réunion Enseignements tirés** est exécutée.
Processus de relations publiques	Effectuez les étapes nécessaires pour satisfaire aux exigences PR de cette analyse.	La tâche **Définir l'état sur révision** est exécutée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
	Une fois que vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet** , selon le cas.	
Définir l'état sur Revue	Aucune action n'est nécessaire.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**.
Réunion sur les enseignements tirés	Organisez une réunion sur les leçons tirées afin de trier le travail effectué pour cet incident de perte d'équipement. Une fois que vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet** , selon le cas.	Le flux se termine.

Modèle de workflow Incident de sécurité Logiciel malveillant

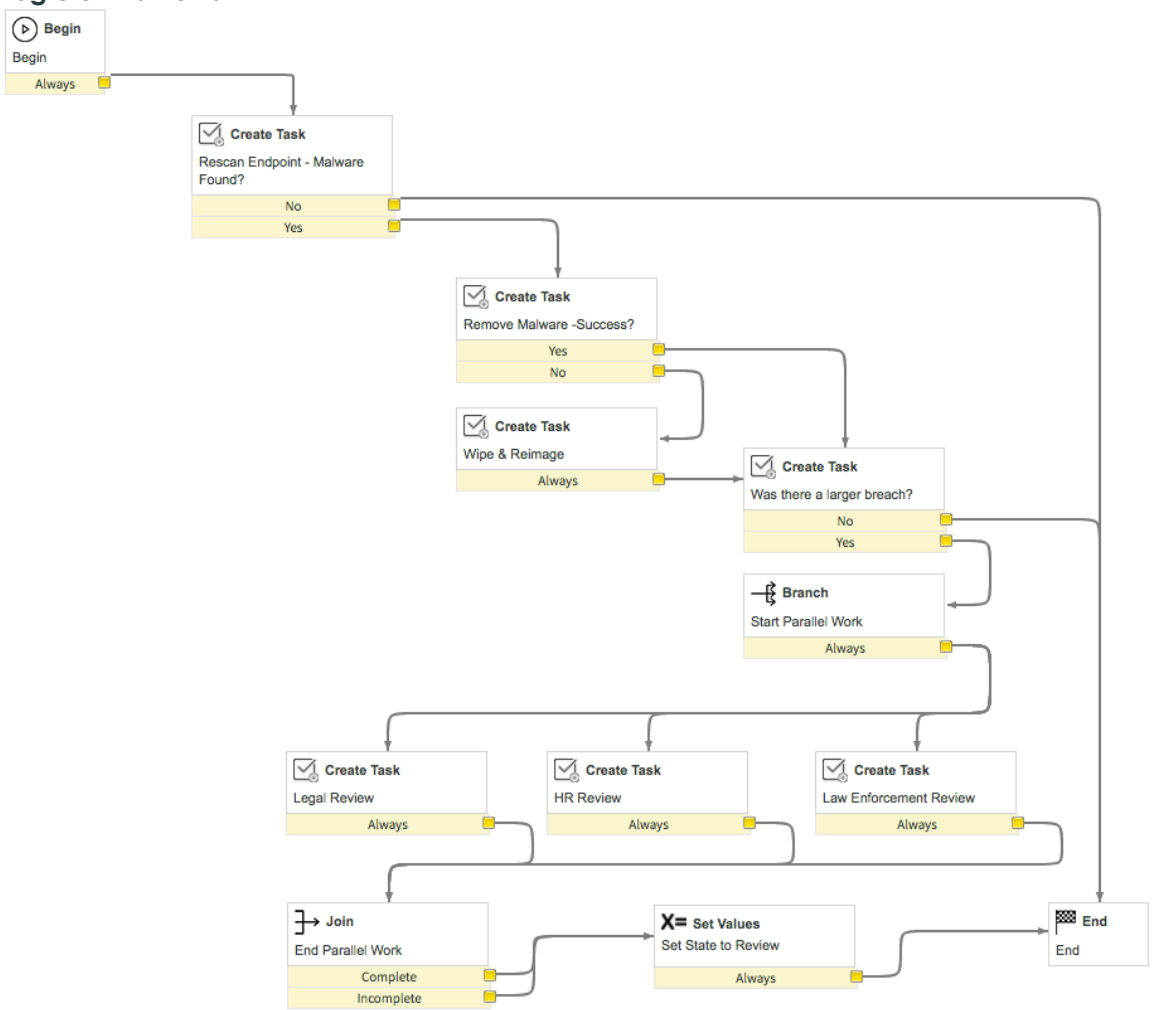
Le modèle Incident de sécurité - Logiciel malveillant - vous permet d'effectuer une série de tâches conçues pour gérer les logiciels malveillants sur votre réseau.

Avant de commencer
Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche
Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Logiciel malveillant**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Logiciel malveillant



Traduction automatique

Procédure

1. Ouvrez l'incident de sécurité de cette attaque potentielle ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Activité du code malveillant**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du workflow.

Tâches de réponse dans Modèle de logiciel malveillant

Tâche de réponse	Action	Résultats
Point de terminaison d'analyse : programme malveillant trouvé ?	Après avoir exécuté une analyse, déterminez si un programme malveillant a été détecté. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Supprimer les logiciels malveillants - Réussite ?** est exécutée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
		Si vous sélectionnez **Non**, le flux se termine.
Supprimer les logiciels malveillants - Succès ?	Déterminez si le programme malveillant a été supprimé avec succès. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Y a-t-il eu une violation plus importante ?** est exécutée. Si vous sélectionnez **Non**, la tâche **Effacer et réimager** est exécutée.
Effacer et réimager	Si vous n'avez pas réussi à supprimer le programme malveillant détecté, cette tâche vous demande d'effectuer un nettoyage et une nouvelle image sur les ordinateurs infectés par le programme malveillant.	Une fois la tâche terminée, la tâche **Définir l'état sur Revue** est exécutée.
Y a-t-il eu une brèche plus importante ?	Déterminez si la violation causée par le logiciel malveillant est plus importante qu'on ne le pensait au départ. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les tâches suivantes sont exécutées en parallèle : ◦ Révision juridique ◦ Revue RH ◦ Examen des applications de la loi Si vous sélectionnez **Non**, le flux se termine.
Révision juridique Revue RH Examen des applications de la loi	Effectuez les étapes nécessaires pour que chacun de ces départements examine le processus que vous avez suivi pour éradiquer le logiciel malveillant.	Lorsque les tâches sont terminées, la tâche **Définir l'état sur Revue** est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examiner** et le flux se termine.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modèle de workflow d'hameçonnage d'incident de sécurité

Le modèle Incident de sécurité - Hameçonnage - vous permet d'effectuer une série de tâches conçues pour gérer les e-mails de harponnage sur votre réseau.

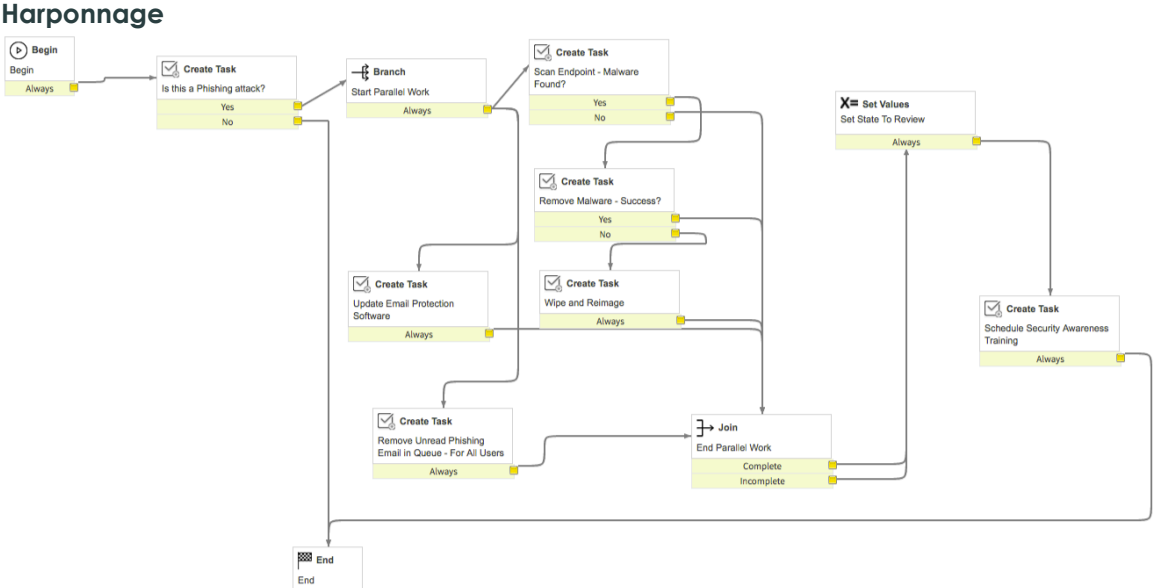
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Harponnage (harponnage)**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Harponnage



Procédure

1. Ouvrez l'incident de sécurité de cette attaque potentielle de spear phishing ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Harponnage (Harponnage)**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du workflow.

Tâches de réponse dans le modèle de harponnage

Tâche de réponse	Action	Résultats
S'agit-il d'une attaque de phishing ?	Déterminez s'il s'agit d'une attaque de hameçonnage. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les tâches suivantes sont exécutées en parallèle : ◦ Point de terminaison d'analyse : programme

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
		malveillant trouvé ? ◦ Mettre à jour le logiciel de protection des e-mails ◦ Supprimer l'e-mail d'hameçonnage non lu dans la file d'attente : pour tous les utilisateurs Si vous sélectionnez **Non**, le flux se termine.
Point de terminaison d'analyse : programme malveillant trouvé ?	Après avoir exécuté une analyse, déterminez si un programme malveillant a été détecté. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Supprimer les logiciels malveillants - Réussite ?** est exécutée. Si vous sélectionnez **Non**, la tâche **Définir l'état sur Revue** est exécutée.
Supprimer les logiciels malveillants - Succès ?	Déterminez si le programme malveillant a été supprimé avec succès. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Définir l'état sur Révision** est exécutée. Si vous sélectionnez **Non**, la tâche **Effacer et réimager** est exécutée.
Effacer et recréer une image	Si vous n'avez pas réussi à supprimer le programme malveillant détecté, cette tâche vous demande d'effectuer un nettoyage et une nouvelle image sur les ordinateurs infectés par le programme malveillant.	Une fois la tâche terminée, la tâche **Définir l'état sur Revue** est exécutée.
Mettre à jour le logiciel de protection des e-mails	S'il s'avère qu'il s'agit d'une attaque de phishing, vous êtes invité à mettre à jour votre logiciel de protection des e-mails en conséquence.	Lorsque la tâche est terminée, la tâche **Définir l'état sur Revue** est exécutée.
Supprimer l'e-mail d'hameçonnage non lu dans la file d'attente : pour tous les utilisateurs	Effectuez les étapes nécessaires pour supprimer l'e-mail d'hameçonnage toujours dans la file d'attente pour tous vos utilisateurs.	Lorsque la tâche est terminée, la tâche **Définir l'état sur Revue** est exécutée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**. La tâche **Planifier la formation de sensibilisation à la sécurité** est exécutée.
Planifier une formation de sensibilisation à la sécurité	Planifiez une formation pour sensibiliser vos employés à la sécurité. Mettez à jour le champ **État** dans la tâche comme il convient.	Lorsque la tâche est terminée, le flux se termine.

Modèle de workflow Violation de la politique en matière d'incidents de sécurité

Le modèle Incident de sécurité - Violation de la politique - Permet d'effectuer une série de tâches conçues pour gérer les violations de la politique de sécurité.

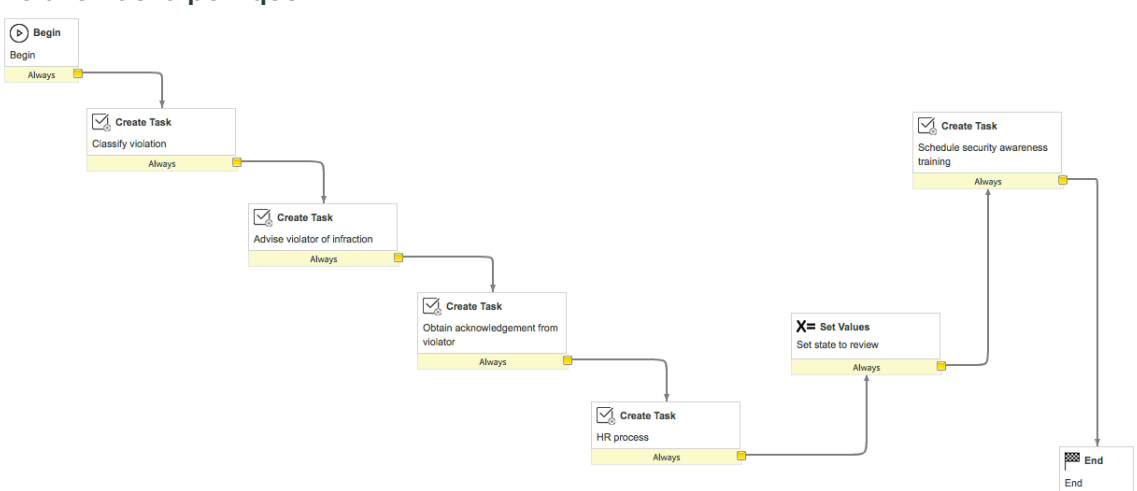
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Violation de la politique**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Violation de la politique



Procédure

1. Ouvrez l'incident de sécurité correspondant à la violation de la politique ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Violation de la politique**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du workflow.

Tâches de réponse dans le modèle de violation de la politique

Tâche de réponse	Action	Résultats
Classifier la violation	Classez en quoi cette infraction enfreint les politiques de sécurité de votre organisation. Mettez à jour le champ **État** dans la tâche une fois que vous l'avez terminée.	La tâche **Aviser le contrevenant de la réponse à l'infraction** est exécutée.
Aviser le contrevenant de l'infraction	Communiquez la nature de l'infraction à l'auteur de l'infraction. Mettez à jour le champ **État** dans la tâche après l'avoir communiqué.	La tâche **de réponse Obtenir la confirmation du contrevenant** est exécutée.
Obtenir la confirmation du contrevenant	Obtenir un accusé de réception de la part de l'auteur de l'infraction. Mettez à jour le champ **État** dans la tâche comme il convient.	La tâche de réponse du **processus RH** est exécutée.
Processus RH	Communiquez toutes les informations nécessaires sur cette violation aux RH. Mettez à jour le champ **État** dans la tâche comme il convient.	La tâche de réponse **Définir l'état sur Revue** est exécutée.
Définir l'état sur Revue	Aucune action n'est nécessaire.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**.
Planifier une formation de sensibilisation à la sécurité	Organisez une formation de sensibilisation à la sécurité pour éduquer le personnel sur la façon de prévenir des violations de sécurité similaires à l'avenir. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé, Terminé** ou **Annulé**, le flux s'arrête.

Traduction automatique

Modèle de workflow d'incident de sécurité Reconnaissance

La reconnaissance est généralement une étape préliminaire vers une nouvelle attaque visant à exploiter un appareil ou un système. Le modèle Incident de sécurité - Reconnaissance - vous permet d'effectuer une série de tâches conçues pour gérer la reconnaissance sur votre réseau.

Avant de commencer

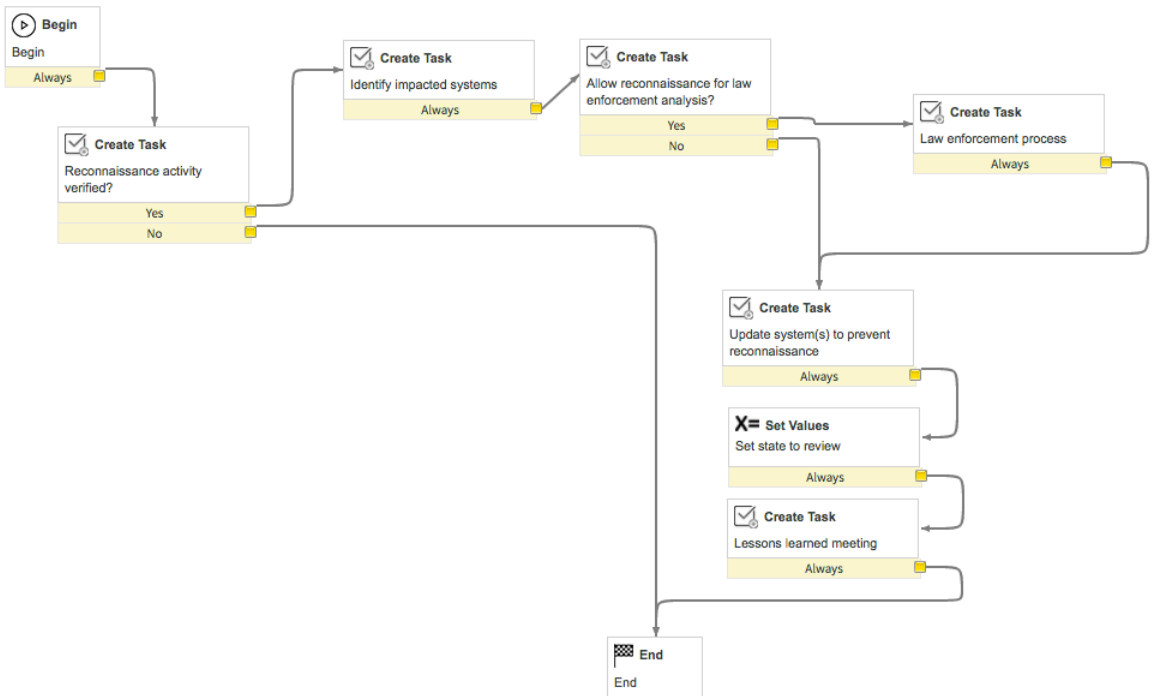
Rôle requis : sn_si.write

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Activité de reconnaissance**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Activité de reconnaissance



Procédure

1. Ouvrez l'incident de sécurité de cette attaque potentielle ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Activité de reconnaissance**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du workflow.

Tâches de réponse dans le modèle de reconnaissance

Tâche de réponse	Action	Résultats
L'activité de reconnaissance a-t-elle été vérifiée ?	Déterminer si toute reconnaissance observée a été vérifiée. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Identifier les systèmes impactés** est exécutée. Si vous sélectionnez **Non**, le flux se termine.
Identifier les systèmes impactés	Déterminer les systèmes impactés par la reconnaissance.	Lorsque cette tâche est terminée, la tâche **Autoriser la reconnaissance pour l'analyse des forces de l'ordre ?** est exécutée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
Autoriser la reconnaissance pour l'analyse des forces de l'ordre ?	Déterminez si vous souhaitez que la reconnaissance soit analysée par les forces de l'ordre. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche Processus **d'application** de la loi est exécutée. Si vous sélectionnez **Non**, la tâche Mettre **à jour le(s) système(s) pour empêcher la reconnaissance** est exécutée.
Processus d'application de la loi	Appliquez le processus d'application de la loi tel que défini par votre société.	Lorsque cette tâche est terminée, le **(s) système(s) de mise à jour pour empêcher** la tâche de reconnaissance est exécuté(s).
Mettre à jour le(s) système(s) pour empêcher la reconnaissance	Effectuez les étapes nécessaires pour mettre à jour les systèmes affectés par la reconnaissance.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur révision** est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examiner** et la tâche de **réunion Enseignements tirés** est exécutée.
Réunion sur les enseignements tirés	Organisez une réunion sur les leçons tirées afin de trier le travail effectué dans le cadre de cet incident de reconnaissance. Mettez à jour le champ **État** dans la tâche comme il convient.	Lorsque cette tâche est terminée, le flux se termine.

Incident de sécurité : serveur ou service non autorisé Modèle de workflow

Le modèle Incident de sécurité - Serveur ou service non autorisé - vous permet d'effectuer une série de tâches conçues pour gérer l'activité des serveurs ou des services non autorisés affectant votre réseau.

Avant de commencer

Rôle requis : sn_si.write

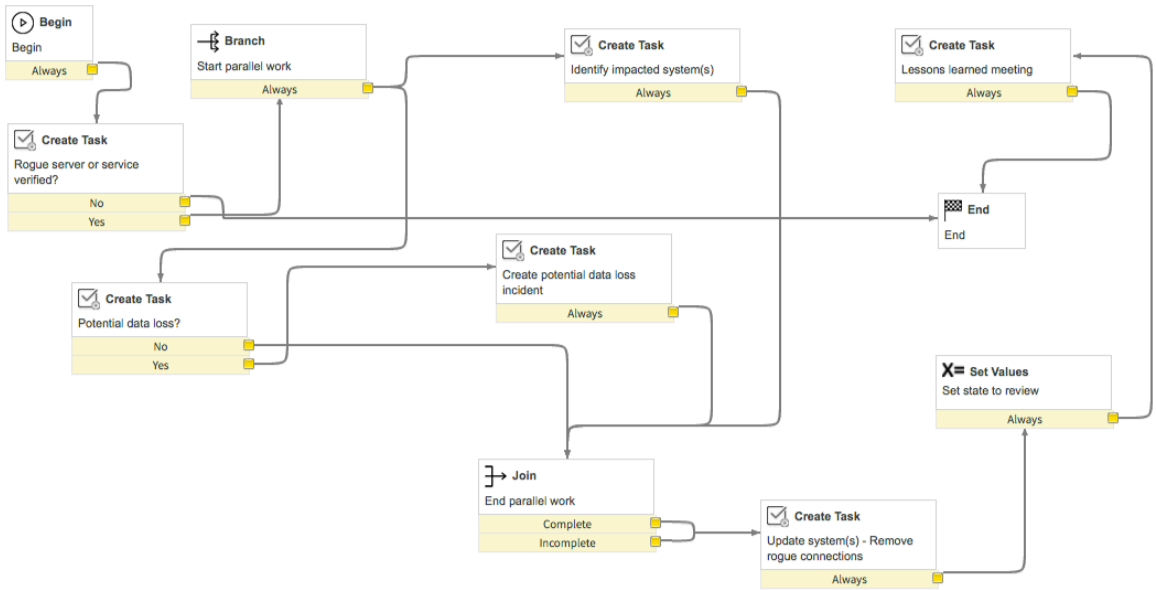
Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Serveur ou service non autorisé**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Serveur ou service non autorisé



Procédure

1. Ouvrez l'incident de sécurité de cette attaque potentielle ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Activité du serveur ou du service non autorisé**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du workflow.

Tâches de réponse dans un serveur ou un modèle de service non autorisé

Tâche de réponse	Action	Résultats
Serveur ou service non autorisé vérifié ?	Déterminez si une connexion avec un serveur ou un service non autorisé a été vérifiée sur votre réseau. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les deux tâches suivantes sont exécutées en parallèle : ◦ **Identifier le(s) système(s) impacté(s)** ◦ **Perte potentielle de données ?** Si vous sélectionnez **Non**, le flux se termine.
Identifier le(s) système(s) impacté(s)	Déterminez les systèmes impactés par le contact avec le serveur ou le service non autorisé.	Lorsque cette tâche est terminée, la tâche **Mettre à jour le(s) système(s) : supprimer les connexions non autorisées** est exécutée.
Perte potentielle de données ?	Déterminez si la connexion au serveur ou au service non autorisé a causé une perte de données potentielle.	Si vous sélectionnez **Oui**, la tâche **Créer un incident de perte potentielle de données** est exécutée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
	Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Non**, la tâche **Mettre à jour le(s) système(s) : supprimer les connexions non autorisées** est exécutée.
Créer un incident de perte de données potentielle	Effectuez les étapes nécessaires pour créer un incident de sécurité en raison de la perte potentielle de données.	Lorsque cette tâche est terminée, la tâche **Mettre à jour le(s) système(s) : supprimer les connexions non autorisées** est exécutée.
Mettre à jour le(s) système(s) : supprimer les connexions non autorisées	Effectuez les étapes nécessaires pour supprimer les connexions non autorisées.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur révision** est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examiner** et la tâche de **réunion Enseignements tirés** est exécutée.
Réunion sur les enseignements tirés	Organisez une réunion des leçons tirées pour trier le travail effectué pour cet incident de service ou de serveur non autorisé. Mettez à jour le champ **État** dans la tâche comme il convient.	Lorsque cette tâche est terminée, le flux se termine.

Modèle de workflow d'incident de sécurité Courrier indésirable

Le modèle Incident de sécurité - Courrier indésirable - vous permet d'effectuer une série de tâches conçues pour gérer le courrier indésirable sur votre réseau.

Avant de commencer

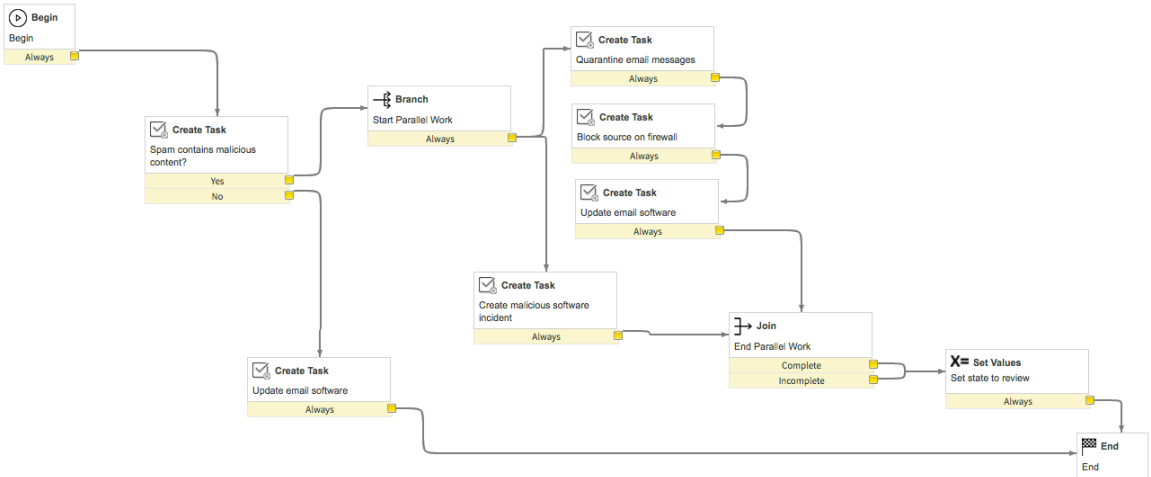
Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie ou changée en **Source de courrier indésirable**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Source du courrier indésirable



Procédure

1. Ouvrez l'incident de sécurité pour lequel vous souhaitez gérer le courrier indésirable ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Source du courrier indésirable**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du workflow.

Tâches de réponse dans le modèle de courrier indésirable

Tâche de réponse	Action	Résultats
Le spam contient-il du contenu malveillant ?	Déterminez si le spam contient un logiciel malveillant. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous avez sélectionné **Oui**, les tâches de réponse suivantes sont exécutées : ◦ **Mettre en quarantaine l'e-mail** ◦ **Créer un incident de logiciel malveillant** Si vous avez sélectionné **Non**, la **mise à jour du logiciel de messagerie** est exécutée.
Créer un incident de logiciel malveillant	Effectuez les étapes pour créer un incident de sécurité, en mettant à jour le champ **État** de la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, cette tâche de réponse attend que les trois tâches de réponse suivantes soient terminées. L'état de l'incident de sécurité passe alors à **l'état Réviser**.
Mettre en quarantaine l'e-mail	Effectuez les étapes de mise en quarantaine du courrier indésirable, en mettant à jour le champ **État** de la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
Source de bloc sur le pare-feu	Effectuez les étapes pour bloquer l'adresse e-mail sur le pare-feu, en mettant à jour le champ **État** de la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Mettre à jour le logiciel de messagerie	Ajoutez l'adresse e-mail à votre liste de blocage, en mettant à jour le champ **État** de la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée. **Remarque :** Cette tâche de réponse est également exécutée si vous avez répondu **Non** à la tâche **de réponse Le spam contient-il du contenu malveillant ?** .
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**.

Modèle de workflow d'incident de sécurité à accès non autorisé

Le modèle Incident de sécurité - Accès non autorisé - vous permet d'effectuer une série de tâches conçues pour gérer les accès non autorisés à votre réseau.

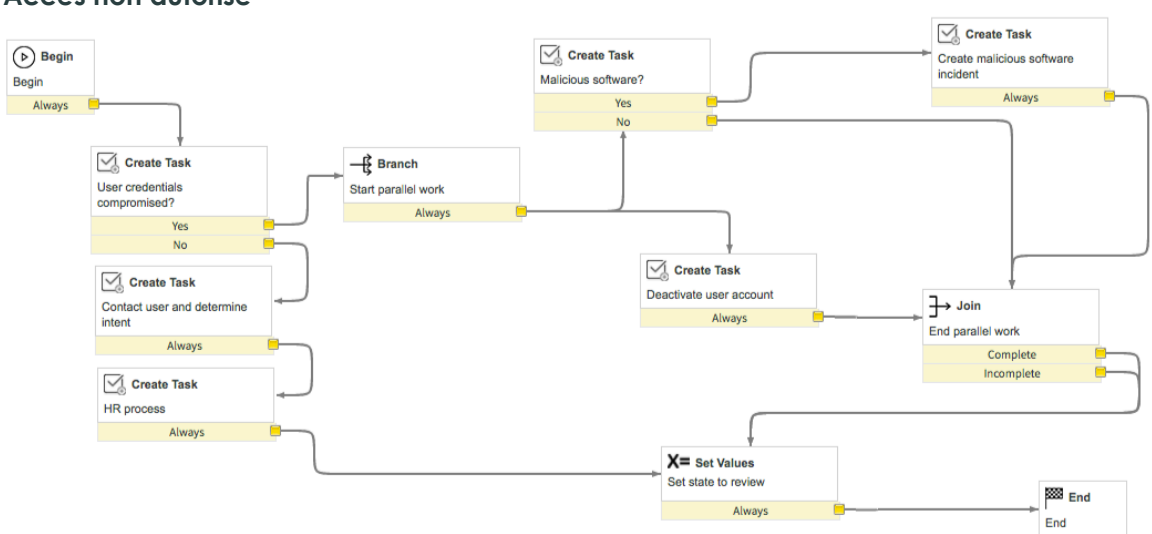
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Accès non autorisé**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Accès non autorisé



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez l'incident de sécurité de cette attaque potentielle ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Accès non autorisé**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du workflow.

Tâches de réponse dans le modèle d'accès non autorisé

Tâche de réponse	Action	Résultats
Les informations d'identification de l'utilisateur compromises ?	Déterminez si les informations d'identification de l'utilisateur ont été compromises. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les deux tâches suivantes sont exécutées en parallèle : ◦ **Un logiciel malveillant ?** ◦ **Désactiver un compte d'utilisateur** Si vous sélectionnez **Non**, la tâche **Contacter l'utilisateur et déterminer l'intention** est exécutée.
Un logiciel malveillant ?	Déterminez si l'accès non autorisé a entraîné l'introduction d'un logiciel malveillant. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Créer un incident de logiciel malveillant** est exécutée. Si vous sélectionnez **Non**, la tâche **Définir l'état sur révision** est exécutée.
Créer un incident de logiciel malveillant	Effectuez les étapes nécessaires pour créer un incident de sécurité pour l'accès non autorisé.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur révision** est exécutée.
Désactiver un compte d'utilisateur	Effectuez les étapes nécessaires pour désactiver le compte utilisateur compromis.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur révision** est exécutée.
Contacter l'utilisateur et déterminer l'intention	Effectuez les étapes nécessaires pour contacter l'utilisateur responsable de l'accès non autorisé et déterminer la raison de la tentative d'accès.	Lorsque cette tâche est terminée, la tâche de **processus RH** est exécutée.
Processus RH	Effectuer les démarches nécessaires pour contacter les ressources humaines afin de mettre en place des mesures disciplinaires si nécessaire.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur révision** est exécutée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examiner** et le flux se termine.

Modèle de workflow de défiguration Web/BBS d'incident de sécurité

Le modèle Incident de sécurité - Altération de site web/BBS - vous permet d'effectuer une série de tâches conçues pour gérer le vandalisme dirigé contre l'un des sites BBS ou Web de votre organisation.

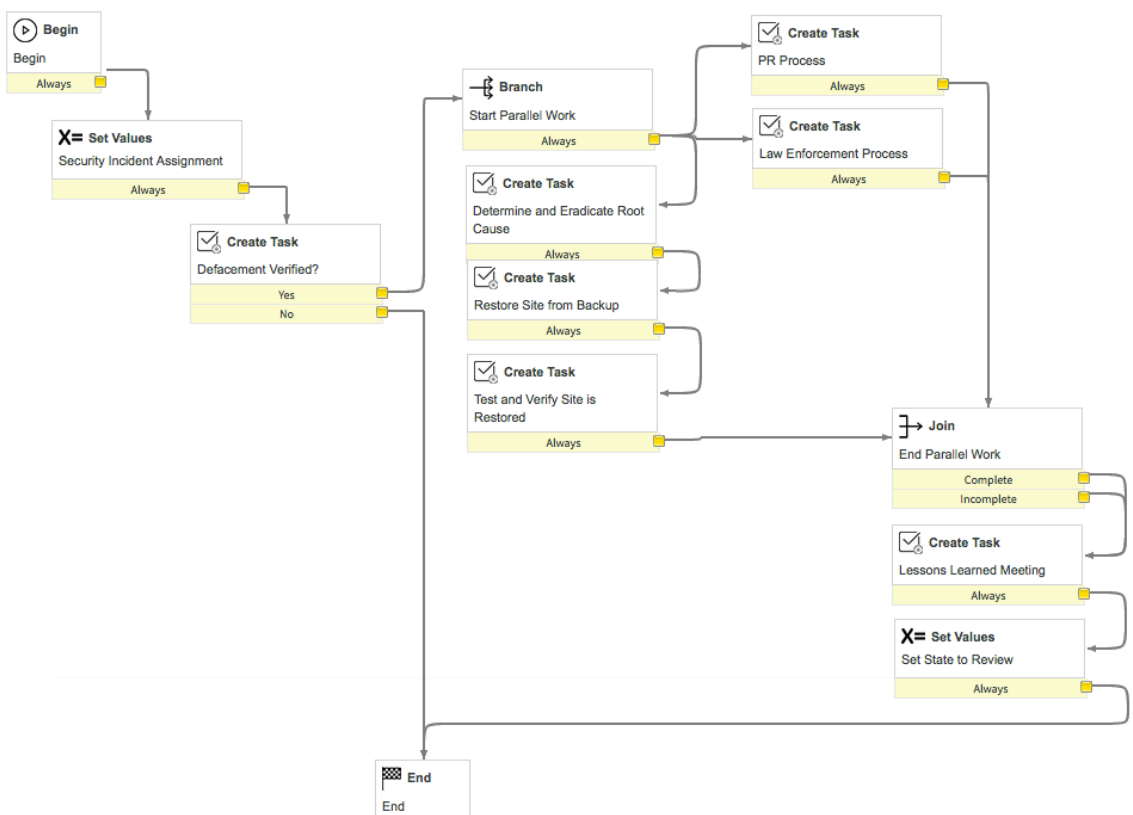
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Altération de site web/BBS**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Altération de site web/BBS



Procédure

1. Ouvrez l'incident de sécurité pour cette occurrence de défiguration de Web ou BBS, ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Altération de site web/BBS**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La première d'une série de tâches de réponse s'affiche. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne soit la création de la tâche de réponse suivante, soit la fin du workflow.

Tâches de réponse dans le modèle de défiguration Web/BBS

Tâche de réponse	Action	Résultats
Affectation d'incident de sécurité	Créez un incident de sécurité pour chaque incident signalé de défiguration de site Web ou de BBS.	La tâche de réponse suivante est exécutée.
Altération vérifiée ?	Déterminez si le site Web ou le BBS a effectivement été défiguré. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les tâches de réponse suivantes sont exécutées : ◦ **Processus de relations publiques** ◦ **Processus d'application de la loi** ◦ **Déterminer et éradiquer la cause première** Si vous sélectionnez **Non**, le flux se termine.
Processus de relations publiques	Effectuez les étapes nécessaires pour aviser le public que le site Web ou le BBS a été dégradé. Lorsque vous avez terminé le processus de PR, définissez l'état de la tâche sur **Terminé** ou **Incomplet** , selon le cas.	La tâche **de réunion Enseignements tirés** est exécutée.
Processus d'application de la loi	Effectuez les étapes nécessaires pour engager les forces de l'ordre appropriées au sujet de l'attaque. Lorsque vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet** , selon le cas.	La tâche **de réunion Enseignements tirés** est exécutée.
Déterminer et éradiquer la cause première	Effectuez les étapes nécessaires pour découvrir et éliminer la cause première de la dégradation. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez modifié l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Restaurer le site à partir d'une copie de sauvegarde	Effectuez les étapes requises pour sauvegarder et restaurer le site Web ou BBS. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez modifié l'état de la tâche sur **Fermé, terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Tester et vérifier que le site est restauré	Vérifiez que le site est restauré.	La tâche **de réunion Enseignements tirés** est exécutée.

Traduction automatique

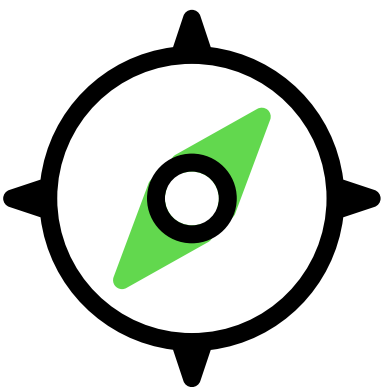
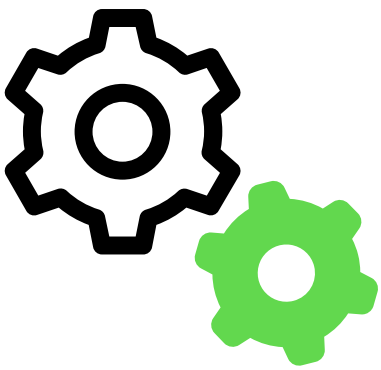
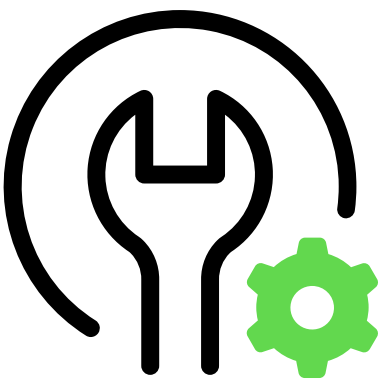
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
	Lorsque vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet** , selon le cas.	
Réunion sur les enseignements tirés	Tenir une réunion sur les leçons tirées afin de trier le travail effectué pour cet incident de défiguration de site Web/BBS. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé**, **Terminé** ou **Annulé**, la tâche **Définir l'état sur Révision** est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**. Le flux se termine.

Renseignements sur les menaces

L'application ServiceNow® Renseignements sur les menaces vous permet de trouver des indicateurs de compromission (IoC) et d'enrichir les incidents de sécurité avec des données de renseignements sur les menaces.

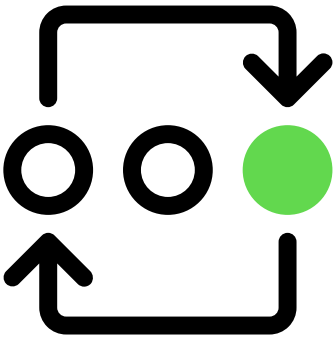
Premiers pas

Explorer	Configurer	Administrer
		
Découvrez les concepts de Threat Intelligence et ses principales fonctionnalités.	Configurez, découvrez les composants installés et les rôles d'utilisateur requis pour répondre aux besoins de votre entreprise.	Définissez les propriétés de Threat Intelligence.

Traduction automatique

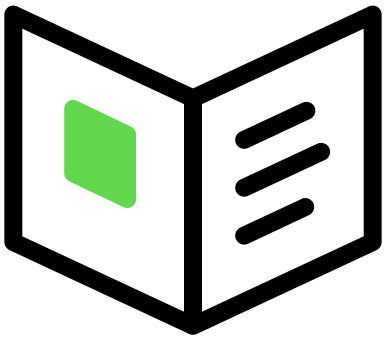
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrer



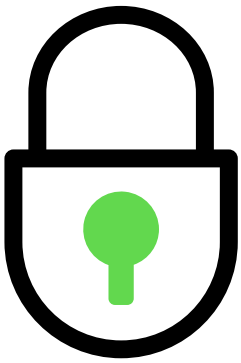
Étendez les options de Threat Intelligence en l'intégrant à ServiceNow et à des applications tierces.

Utiliser



Gérer les indicateurs de compromission (IoC) et divers artefacts.

Cadre de travail MITRE ATT&CK



Gérez le cadre MITRE-ATT&CK, identifiez rapidement les menaces et coordonnez les réponses aux cyberattaques.

Security Case Management



Gérez la gestion des tickets de sécurité en recueillant des informations sur les activités suspectes.

Traduction automatique

Ressources d'apprentissage

- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage et demande d'aide

- Poser des questions et explorer d'autres ressources pour Renseignements sur les menaces dans ServiceNow Community
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Présentation de Renseignements sur les menaces

L'application Renseignements sur les menaces vous permet d'accéder aux données STIX (Structured™ Threat Information Expression) de votre entreprise et de leur fournir un point de référence. L'application est incluse dans Renseignements sur les menaces l'application Gestion des tickets de sécurité , qui fournit un moyen d'analyser les menaces posées à votre organisation par des campagnes ciblées ou des acteurs étatiques.

STIX est un langage permettant de décrire les informations sur les cybermenaces de manière standardisée et structurée. À l'aide des données STIX et des profils TAXII (Trusted™ Automated Exchange of Indicator Information), les professionnels des menaces peuvent utiliser les informations partagées sur les cybermenaces pour isoler les menaces qui ont déjà été identifiées par votre entreprise et provenant d'autres sources. TAXII rend possible l'échange automatisé et généralisé d'informations sur les cybermenaces.

Renseignements sur les menaces prend en charge les versions 1.1, 2.0 et 2.1 de STIX.

STIX™ et TAXII™ sont des marques commerciales de The MITRE Corporation.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Séparation de domaine et Renseignements sur les menaces

L'application Séparation de domaine est prise en charge dans le module disponible dans le Renseignements sur les menaces cadre de Réponse aux incidents de sécurité. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : basique

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Vue d'ensemble

Dans le module Threat Intelligence (dans le cadre de l'application Security Incident Response), Séparation de domaine permet aux fournisseurs de service (SP) de créer et de gérer le référentiel de Threat Intelligence comme suit :

- Sources de menace et profils TAXII (Trusted Automated Exchange of Indicator Information)
- Observables
- Indicateurs de compromis
- Modes / méthodes d'attaque par menace et gestion des tickets dans l'ensemble de la clientèle qu'ils servent avec des coûts opérationnels réduits et une meilleure qualité de service

Le fait de disposer d'espaces de travail client distincts pour les workflows, les tableaux de bord, les rapports, etc., garantit que les données des clients sont séparées et ne sont jamais exposées à d'autres clients.

Prise en charge de Domain Separation dans Renseignements sur les menaces par version

Séparation de domaine pour le module Threat Intelligence (dans le cadre de l'application Réponse aux incidents de sécurité) couvre les fonctionnalités du produit suivantes :

- Les observables d'incident de sécurité sont dirigés vers le domaine approprié de l'utilisateur dont l'ID/les informations d'identification/le champ d'application génère l'incident. Les observables extraits de l'incident sont stockés dans le domaine de l'incident de sécurité.
- Mise en place de profils de service TAXII pour télécharger une ou plusieurs collections TAXII qui offrent des flux d'informations sur les cybermenaces. La configuration est stockée dans le domaine sous lequel le profil est défini.
- Configurer le téléchargement des flux de menaces dans le référentiel IOC dans le domaine sous lequel la configuration est effectuée.
- Création de modes/méthodes d'attaque dans le domaine de la source de renseignements sur les menaces qui fournit automatiquement les informations ou dans le domaine sous lequel un nouveau mode/méthode d'attaque est ajouté manuellement par l'utilisateur
- Création de tickets pour une enquête à long terme sur les incidents, les observables, les CI, les utilisateurs et les indicateurs de compromission (IOC) associés au ticket. Le ticket est stocké dans le domaine créé par l'utilisateur.

Remarque : Dans tous les cas ci-dessus, les principes fondamentaux de visibilité dans des domaines distincts de la NOW Platform s'appliquent. Comme toujours, un incident dans le domaine parent peut faire référence à des artefacts dans le domaine enfant, mais pas l'inverse.

Comment fonctionne Séparation de domaine dans Renseignements sur les menaces (dans le cadre de Réponse aux incidents de sécurité)

Threat Intelligence fait partie de Security Incident Response aux niveaux Professional et Enterprise, mais pas avec le niveau Standard. Par conséquent, un plugin séparé est

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

nécessaire. Le module Threat Intelligence (dans le cadre de l'application Réponse aux incidents de sécurité) crée et gère les informations de Threat Intelligence associées aux incidents de sécurité dans une organisation. Les cas d'utilisation suivants prennent en charge la séparation par domaine :

- Création des observables d'incident de sécurité au moment de la création de l'incident
  - À partir d'analyseurs d'e-mails (basé sur la plateforme, hameçonnage signalé par les utilisateurs, personnalisé)
  - À partir d'applications dans des magasins tiers Gestion des informations et des événements et de sécurité (SIEM)
  - Saisie manuelle par l'analyste SOC
- Collecte d'observables à partir de sources de flux de menaces - Sources de renseignements sur les menaces à partir de collectes TAXII
- Gérer les observables d'incident de sécurité
  - Associer des observables à des indicateurs connexes
  - Associer des observables à des incidents de sécurité
  - Associer des observables à des observables enfants
  - Associer l'observable à la source du flux de menaces
  - Ajouter des annotations de sécurité aux observables
- Gérer les indicateurs de compromission
  - Associer des indicateurs à des observables connexes
  - Associer les indicateurs au mode/méthode d'attaque
  - Associer des indicateurs à des types d'indicateurs
  - Associer des indicateurs à une source de flux de menaces
  - Ajouter des annotations de sécurité aux indicateurs
- Gérer les tickets
  - Créer un ticket (manuellement ou à partir d'un incident)
  - Modifier un nouveau ticket pour ajouter des détails (choisir le type et la gravité du ticket, ajouter des incidents, des observables, des éléments de configuration, des utilisateurs, des indicateurs)
  - Supprimer un ticket

Traduction automatique

Configuration de Domain Separation

La configuration de Séparation de domaine pour Threat Intelligence ne nécessite aucune étape supplémentaire. Toutes les tables Threat Intelligence acquièrent la colonne Domaine une fois que l'instance est séparée par domaine.

Données séparées par domaine

Les données peuvent être séparées par domaine, ce qui signifie :

- Les observables d'un incident de sécurité dans un domaine ne peuvent pas être affichés à partir du champ d'application d'autres domaines.
- Les indicateurs de compromission dans un domaine ne peuvent pas être visualisés à partir du champ d'application d'autres domaines.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les modes/méthodes d'attaque associés à un domaine ne peuvent pas être affichés dans le champ d'application d'autres domaines.
- Les profils de service TAXII associés à un domaine ne peuvent pas être affichés à partir du champ d'application d'autres domaines.
- Les sources de renseignements sur les menaces associées à un domaine ne peuvent pas être affichées dans le champ d'application d'autres domaines.
- Les tickets associés à un domaine ne peuvent pas être affichés dans le champ d'application d'autres domaines.

Les propriétés de Threat Intelligence sont définies au niveau global et ne sont donc pas séparées par domaine. Les paramètres sont les suivants :

- Nom du domaine pour récupérer des informations supplémentaires pour les adresses IP/URL
- Clé API à utiliser pour la récupération
- Recherche des tables IoC locales avant l'envoi au scanner distant
- Nombre de jours durant lesquels les observables locaux sont pris en compte
- Marquer un mode/une méthode d'attaque comme inactif lorsqu'il n'est pas reçu de sources de renseignements sur les menaces
- Marquer un indicateur comme inactif lorsqu'il n'est reçu d'aucune source pendant un nombre de jours spécifié

Configuration

Tous les aspects de la configuration de la fonctionnalité Threat Intelligence sont autonomes dans un environnement séparé par domaine.

Les tâches suivantes peuvent être configurées par domaine :

1. Création de profils de service TAXII
   - Choisir une configuration du service Discovery
   - Choisir une configuration de service de collecte : affecter des rôles à des utilisateurs et à des groupes d'utilisateurs
2. Création de sources de renseignements sur les menaces
   - Configurer le service REST qui fournit les informations de renseignement sur les menaces
   - Planifier le téléchargement des informations de Threat Intelligence
   - Choisir les informations sur les détails de la menace à affecter à la source
3. Création de modes/méthodes d'attaque (manuel)
   - Source, type de programme malveillant, mécanisme d'attaque, type d'acteur de menace, description, traitement, effet escompté, premier observé, dernier observé
   - Indicateurs associés, mode/méthode d'attaque enfant, incidents de sécurité associés

   Remarque : Les modes/méthodes d'attaque sont également créés automatiquement à partir des sources de flux de menaces.

4. Définition de listes par défaut pour les catégories d'informations sur les menaces suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Mécanismes d'attaque
- Méthodes de Détection
- Actualise
- Types des indicateurs
- Effets souhaités
- Notifications
- Types des observables
- Définitions de limite d'évaluation
- Types d'acteurs de menace
- Motivations de l'attaque
- Types d'infrastructure
- Options de logiciel malveillant
- Types de malware
- Types de rapport
- Rôles d'acteur de menace
- Types d'outil

Comment les domaines de locataire gèrent-ils leurs propres données d'application ?

- Les propriétaires de domaines locataires peuvent créer leurs propres profils de service TAXII.
- Les propriétaires de domaines locataires peuvent créer leurs propres sources de renseignements sur les menaces.
- Les propriétaires de domaines locataires peuvent créer leurs propres modes/méthodes d'attaque.
- Les propriétaires de domaines locataires peuvent créer leurs propres listes par défaut pour les catégories d'informations sur les menaces.

Remarque : La logique métier et les processus permettent de séparer les calendriers de téléchargement des sources de renseignements sur les menaces par domaine propriétaire de l'instance.

Information associée

Séparation de domaine pour les fournisseurs de services

Configurer Renseignements sur les menaces

Avant de l'exécuter Renseignements sur les menaces dans votre instance, vous devez la télécharger à ServiceNow Storepartir du fichier . Vous pouvez également configurer des propriétés et définir une source de menace.

Installer Renseignements sur les menaces

Avant de l'exécuter Renseignements sur les menaces dans votre instance, vous devez la télécharger à ServiceNow Storepartir du fichier .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Remplissez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâches de configuration	Description
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte le rôle d'administrateur de menace [sn_ti.admin]. • L'administrateur de menace [sn_ti.admin] supervise la configuration et vérifie les résultats attendus.

Rôle requis : administrateur

Procédure

Suivez les instructions pour le téléchargement d'une application à partir de ServiceNow Store.

Que faire ensuite

Définir les Renseignements sur les menaces propriétés.

Composants installés avec Renseignements sur les menaces

Plusieurs types de composants sont installés avec l'activation du module d'extension Renseignements sur les menaces, y compris les tables et les rôles d'utilisateur.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
Administrateur de menace [sn_ti.admin]	Dispose d'un contrôle total sur toutes les propriétés, SLA et notifications de menace.	sn_ti.write
Lecteur de menace [sn_ti.read]	Dispose d'un accès en lecture aux informations sur les menaces.	sn.sec_cmn.int_read

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
Rédacteur de menace [sn_ti.write]	Dispose d'un accès en écriture aux informations sur les menaces. Impossible de supprimer les modes d'attaque, les indicateurs ou les observables. Seul un administrateur de menaces peut les supprimer.	• sn_sec_cmn.int_write • sn_ti.read
Analyste MITRE [sn_ti.mitre_analyst]	Ce rôle permet d'accéder en lecture aux MITRE-ATT&CK modules contenus Renseignements sur les menaces et au SIR module.	• sn_ti.read • sn_si.read

Tables installées

Table	Description
Mécanisme d'attaque [sn_ti_attack_mechanism]	Organise les modèles d'attaque de manière hiérarchique en fonction des mécanismes fréquemment utilisés lors de l'exploitation d'une vulnérabilité. Les catégories membres de cette vue représentent les différentes techniques utilisées pour attaquer un système.
Mode/méthode d'attaque [sn_ti_attack_mode]	Les modes et méthodes d'attaque sont des représentations du comportement des cyberadversaires. Ils caractérisent ce que fait un adversaire et comment il le fait avec des niveaux de détail croissants.
Méthode de détection [sn_ti_discovery_method]	Expression de la façon dont un incident a été détecté.
Flux [sn_ti_feed]	Utilisé pour configurer le flux de menaces (RSS) dans la vue d'ensemble des menaces.
Mode/méthode d'attaque de l'indicateur [sn_ti_m2m_indicator_attack_mode]	Utilisé pour mapper les modes/méthodes d'attaque aux indicateurs.
Indicateur de compromis [sn_ti_indicator]	Utilisé pour transmettre des modèles observables spécifiques combinés à des informations contextuelles destinées à représenter des artefacts et/ou des comportements d'intérêt dans un contexte de cybersécurité.
Indicateur de métadonnées compromises [sn_ti_indicator_metadata]	Utilisé pour remplir les enregistrements TAXII.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Source de l'indicateur [sn_ti_m2m_indicator_source]	Utilisé pour collecter toutes les sources rapportant l'indicateur spécifique.
Type d'indicateur [sn_ti_indicator_type]	Caractérise un indicateur de cybermenace composé d'un modèle identifiant certaines conditions observables, ainsi que d'informations contextuelles sur la signification des modèles, la manière et le moment où ils sont traités, etc.
Type d'indicateur connexe [sn_ti_m2m_indicator_indicator_type]	Relie les indicateurs à leurs types applicables
Nombre d'incidents [sn_ti_observable]	Nombre d'incidents de sécurité associés à un observable.
Effet souhaité [sn_ti_intended_effect]	Utilisé pour exprimer l'effet escompté d'un acteur de menace.
Résultat de l'analyse IP [sn_ti_ip_result]	Utilisé pour afficher les résultats d'une recherche d'adresses IP.
Programme malveillant Limite du taux [sn_ti_rate_limit]	Définit une limite de taux à utiliser sur une source de recherche.
Analyse anti-programme malveillant [sn_ti_scan]	Une recherche. Contient les éléments à rechercher, la source de recherche et un résumé des résultats de la recherche.
Entrée de la file d'attente de l'analyse de programme malveillant [sn_ti_scan_q_entry]	Enregistrement de recherche mis en file d'attente pour recherche ou traitement. Facilite les demandes dans les limites de taux indiquées.
Résultat de l'analyse anti-programme malveillant [sn_ti_scan_result]	Affiche le résultat d'une recherche.
Analyseur de programme malveillant [sn_ti_scanner]	Définit les sources de recherche tierces à utiliser pour effectuer les recherches.
Limite de taux du scanner de programme malveillant [sn_ti_scanner_rate_limit]	Associe une source de recherche à une limite de taux.
Type de programme malveillant [sn_ti_malware_type]	Utilisé pour exprimer les types d'instances de programme malveillant.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Observable [sn_ti_observable]	Les observables dans STIX représentent des propriétés avec état ou des événements mesurables pertinents pour le fonctionnement des ordinateurs et des réseaux.
Type de contexte de l'observable [sn_ti_observable_context_type]	Stocke le contexte (source, destination d'une adresse IP, etc.) d'un observable.
Indicateur d'observable [sn_ti_m2m_observable_indicator]	Utilisé pour relier les observables aux indicateurs.
Source d'observable [sn_ti_observable_source]	Utilisé pour relier les observables aux sources de menace.
Type d'observable [sn_ti_observable_type]	Répertorie les différents types d'observables, tels que les adresses IP.
Catégorie de type de l'observable [sn_ti_observable_type_category]	Stocke la première catégorisation des observables (par exemple, les adresses IP et les URL). Il est utilisé pour déterminer plus précisément les types des observables.
Mode/méthode d'attaque associé [sn_ti_m2m_attack_mode_attack_mode]	Utilisé pour relier les modes d'attaque les uns aux autres.
Observables associés [sn_ti_m2m_observables]	Utilisé pour relier les observables les uns aux autres.
Type d'analyse [sn_ti_scan_type]	La définition d'un type de recherche, avec des enregistrements initiaux pour le fichier, l'URL et l'adresse IP.
Ticket de sécurité [sn_ti_case]	Stocke les enregistrements de tickets de sécurité créés à l'aide de la gestion des tickets.
IoC de ticket de sécurité [sn_ti_case_ioc]	Utilisé pour gérer la relation entre les observables et les tickets.
Tâche associée au ticket de sécurité [sn_ti_m2m_case_task]	Utilisé pour gérer la relation entre les tâches (incidents de sécurité, demandes de changement, etc.) et les tickets de sécurité.
Exclusion de la relation de ticket de sécurité [sn_ti_case_relationship_exclusion]	Fournit la définition de l'inclusion et de l'exclusion des enregistrements connexes dans les tickets de sécurité.
Perception	Le lien m2m entre l'observable et le résultat de détail de recherche de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_ti_sighting]	perceptions utilisé dans l'exécution d'une demande de recherche de perception.
Éléments de configuration de perception [sn_ti_m2m_sighting_ci]	Mappe les éléments de configuration à une recherche de perceptions.
Détails de la recherche de perception [sn_ti_sighting_search_detail]	Détails d'une recherche de perception, par exemple, le nombre d'éléments internes externes trouvés.
Résultat de recherche de perception [sn_ti_sighting_search]	L'en-tête d'une exécution de recherche de perceptions.
Types d'observables pris en charge [sn_ti_m2m_ind_type_obs_type]	Associe les types d'indicateurs aux types d'observables valides.
Type d'analyse pris en charge [sn_ti_supported_scan_type]	Mappe le type de recherche à une implémentation spécifique à la source/ au fournisseur de recherche. Indique qu'une source de recherche spécifique prend en charge le type.
Mode/méthode d'attaque de la tâche [sn_ti_m2m_task_attack_mode]	Associe les modes d'attaque aux tâches.
Indicateur de tâche [sn_ti_m2m_task_indicator]	Relie les indicateurs aux tâches.
Observable de tâche [sn_ti_m2m_task_observable]	Associe les observables aux tâches.
Détection de tâches [sn_ti_m2m_task_sighting]	Stocke les enregistrements de tâches (incidents de sécurité et tickets) liés à un enregistrement de perception.
Collecte TAXII [sn_ti_taxii_collection]	Définit un flux de renseignements sur les cyber-risques qui peut être importé par un serveur TAXII.
Profil TAXII [sn_ti_taxii_profile]	Définit un référentiel pour le partage de renseignements sur les cyber-risques. Contient les collections TAXII.
Type d'acteur de menace [sn_ti_threat_actor_type]	Fournit des caractérisations d'acteurs malveillants (ou d'adversaires) représentant une menace de cyberattaque, y compris l'intention présumée et le comportement historiquement observé.
Threat Intelligence Source	Définit une source pour l'importation de données sur les menaces.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_ti_source]	
Motivation de l'attaque associée [sn_ti_stix2_m2m_object_attack_motivation]	Collecte toutes les motivations d'attaque associées à un objet STIX.
Type d'infrastructure connexe [sn_ti_stix2_m2m_infra_type]	Relie l'infrastructure avec leurs types.
Phase de kill chain associée [sn_ti_stix2_m2m_indicator_kill_chain_phase]	Relie les phases de kill chain aux indicateurs.
Phase de kill chain associée [sn_ti_stix2_m2m_object_kill_chain_phase]	Relie les phases de kill chain aux objets STIX.
Aptitude de logiciel malveillant associée [sn_ti_stix2_m2m_malware_capability]	Relie les programmes malveillants à leurs capacités.
Type de programme malveillant associé [sn_ti_stix2_m2m_malware_malware_type]	Relie les programmes malveillants à leurs types.
Observable associé [sn_ti_stix2_m2m_malware_observable]	Collecte tous les observables associés à un programme malveillant.
Observable associé [sn_ti_stix2_m2m_observed_data_observable]	Collecte tous les observables associés à une donnée observée.
Type de rapport associé [sn_ti_stix2_m2m_report_report_type]	Relie les rapports de menace à leurs types.
Rôle d'acteur de menace associé [sn_ti_stix2_m2m_threat_actor_threat_actor_role]	Relie les acteurs de menace à leurs rôles.
Type d'acteur de menace associé [sn_ti_stix2_m2m_threat_actor_threat_actor_type]	Relie les acteurs de menace à leurs types.
Type d'outil associé [sn_ti_stix2_m2m_tool_tool_type]	Liez les outils avec leurs types.
Motivation de l'attaque [sn_ti_stix2_attack_motivation]	La motivation de l'attaque façonne l'intensité et la persistance d'une attaque. Les acteurs de menace et les ensembles d'intrusion agissent généralement d'une manière qui reflète leur émotion ou leur situation sous-

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	jacente, ce qui informe les défenseurs de la manière dont ils ont attaqué.
Modèle d'attaque [sn_ti_stix2_attack_pattern]	Type de TTP qui décrit les méthodes utilisées par les adversaires pour tenter de compromettre les cibles.
Campagne [sn_ti_stix2_campaign]	Un groupe de comportements antagonistes qui décrivent un ensemble d'activités ou d'attaques malveillantes (parfois appelées vagues) qui se produisent sur une période donnée contre un ensemble spécifique de cibles.
Déroulement de l'action [sn_ti_stix2_course_of_action]	Recommandation d'un producteur de renseignements à un consommateur sur les mesures qu'il pourrait prendre en réponse à ces renseignements.
Référence externe [sn_ti_stix2_external_reference]	Pointeurs vers des informations représentées en dehors de STIX.
Perception de l'identité [sn_ti_stix2_m2m_sighting_identity]	Collecte toutes les identités associées à une observation.
Identité [sn_ti_stix2_identity]	Personnes, organisations ou groupes réels (par exemple, ACME, Inc.) ainsi que catégories de personnes, d'organisations, de systèmes ou de groupes (par exemple, le secteur financier).
Référence externe de l'indicateur [sn_ti_stix2_indicator_external_reference]	Représente les références externes associées aux indicateurs.
Perception d'indicateur [sn_ti_stix2_indicator_sighting]	Représente les observations d'indicateurs.
Type d'infrastructure [sn_ti_stix2_infrastructure_type]	Représente les différents types d'infrastructures.
Infrastructure [sn_ti_stix2_infrastructure]	Type TTP qui décrit les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées, destinés à soutenir un objectif spécifique (par exemple, les serveurs C2 utilisés dans le cadre d'une attaque, les périphériques ou les serveurs qui font partie de la défense, les serveurs de base de données ciblés par une attaque, entre autres).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Logiciel installé [sn_ti_stix2_m2m_malware_analysis_sw]	Collecte tous les logiciels (types de logiciels SCO) associés à une analyse de programme malveillant.
Ensemble d'intrusion [sn_ti_stix2_intrusion_set]	Ensemble groupé de comportements et de ressources antagonistes ayant des propriétés communes qui est censé être orchestré par une seule organisation.
Phase de kill chain [sn_ti_stix2_kill_chain_phase]	Représente les phases de kill chain associées à une kill chain.
Chaîne de frappe [sn_ti_stix2_kill_chain]	Représente différentes chaînes de frappe.
Emplacement [sn_ti_stix2_location]	Représente un emplacement géographique fourni par STIX.
Analyse de programme malveillant [sn_ti_stix2_malware_analysis]	Les métadonnées et les résultats d'une analyse statique ou dynamique particulière effectuée sur une instance ou une famille de logiciels malveillants.
Aptitude de logiciel malveillant [sn_ti_stix2_malware_capability]	Représente les options communes qu'une famille ou une instance de logiciel malveillant présente.
Programme malveillant Système d'exploitation [sn_ti_stix2_m2m_malware_operating_system]	Collecte tous les systèmes d'exploitation (types de logiciels SCO) associés aux programmes malveillants.
Programme malveillant [sn_ti_stix2_malware]	Un type TTP qui représente un code malveillant.
Définition de marquage [sn_ti_stix2_marking_definition]	Représente les besoins de gestion ou de partage pour les objets STIX.
Perception d'objets [sn_ti_stix2_object_sighting]	Représente les observations d'objets STIX.
Relation objet-indicateur [sn_ti_stix2_m2m_object_indicator]	Collecte toutes les relations entre les objets STIX et les indicateurs STIX.
Relation objet-objet [sn_ti_stix2_m2m_object]	Collecte toutes les relations entre les objets STIX et d'autres objets STIX, à l'exception des indicateurs.
Relation objet-observable [sn_ti_stix2_m2m_object_observable]	Collecte toutes les relations entre les observables STIX et les objets STIX.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Observation de données observées [sn_ti_stix2_m2m_sighting_observed_data]	Collecte tous les objets de données observés associés à une observation.
Données observées [sn_ti_stix2_observed_data]	Transmet des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX.
Type de rapport [sn_ti_stix2_report_type]	Représente l'objectif ou l'objet primaire des rapports de menace.
Observable signalé [sn_ti_stix2_m2m_malware_analysis_observable]	Collecte tous les observables associés à l'analyse de programme malveillant.
Objet STIX V2 [sn_ti_stix2_object]	Table parente commune pour l'objet STIX.
Observation STIX V2 [sn_ti_stix2_sighting]	Table parente commune pour les tables de perception STIX.
Rôle d'acteur de menace [sn_ti_stix2_threat_actor_role]	Représente les rôles qui peuvent être joués par les acteurs de menace.
Acteur de menace [sn_ti_stix2_threat_actor]	Les auteurs de menace sont des personnes, des groupes ou des organisations qui sont soupçonnés d'agir avec des intentions malveillantes.
Regroupement des menaces [sn_ti_stix2_threat_grouping]	Regroupe tous les objets STIX qui partagent un contexte commun.
Note de menace [sn_ti_stix2_threat_note]	Fournit un contexte et une analyse supplémentaire qui ne sont pas contenus dans l'objet STIX correspondant.
Opinion sur la menace [sn_ti_stix2_threat_opinion]	Fournit une évaluation de l'exactitude des informations contenues dans un objet STIX produit par une entité différente.
Rapport de menace [sn_ti_stix2_threat_report]	Les rapports sont des ensembles de renseignements sur les menaces axés sur un ou plusieurs sujets, tels qu'une description d'un acteur de menace, d'un programme malveillant ou d'une technique d'attaque, y compris le contexte et les détails connexes. Ils sont utilisés pour regrouper des renseignements sur les menaces

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	connexes afin de les publier sous la forme d'une histoire complète sur les cybermenaces.
Type d'outil [sn_ti_stix2_tool_type]	Catégories d'outils qui peuvent être utilisés pour effectuer des attaques.
Outil [sn_ti_stix2_tool]	Les outils sont des logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques.
Vulnérabilité [sn_ti_stix2_vulnerability]	Représente une faiblesse ou un défaut dans les exigences, les conceptions ou les implémentations de la logique de calcul (exemple de code) que l'on trouve dans le logiciel et certains composants matériels (exemple de microprogramme). Ils peuvent être directement exploités pour avoir un impact négatif sur la confidentialité, l'intégrité ou la disponibilité de ce système.

Définir les Renseignements sur les menaces propriétés

Renseignements sur les menaces Les propriétés vous permettent de contrôler le fonctionnement de différents aspects du système, y compris la définition des clés API.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration** > **Propriétés**.
2. Définissez les propriétés suivantes comme il convient.

Propriétés pour Threat Intelligence

Propriété	Description
Nom du domaine pour récupérer des informations supplémentaires pour les adresses IP/URL sn_ti.ip_lookup.web_site	Le nom de domaine à utiliser pour récupérer des informations supplémentaires dans votre base de données IoC. Cette propriété est utilisée par le Script `Include ThreatAdditionalInfo` pour renseigner des informations supplémentaires sur le formulaire Observables. Valeur par défaut : http://api.ipinfodb.com/v3/ip-country/

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Remarque : L'API tierce pinfodb.com est disponible sans frais supplémentaires et utilisée dans de nombreux logiciels commerciaux. Si vous le remplacez par un autre nom de domaine, vous devez également fournir la clé API dans le champ suivant.
Clé API à utiliser pour le domaine, le cas échéant sn_ti.ip_lookup.api_key	Clé API à utiliser pour récupérer des informations supplémentaires dans votre base de données IoC. Cette propriété est utilisée (avec la propriété sn_ti.ip_lookup.web_site) par l'include de script `ThreatAdditionalInfo` pour renseigner des informations supplémentaires sur le formulaire Observables.
N'exécutez pas une recherche automatisée de menace sur un observable lorsque l'observable est associé à un IoC ou s'avère malveillant. sn_ti.scan_ioc_avant_envoi **Remarque :** Vous devez définir la durée dans la propriété suivante (sn_ti.scan_ioc_num_days).	Option permettant d'arrêter l'exécution de la recherche automatisée de menace sur un observable lorsque l'observable s'avère malveillant ou associé à un IoC pour la durée configurée (en jours). Si vous devez toujours exécuter la recherche de menace pour l'observable, vous pouvez le faire manuellement. Valeur par défaut : oui
Durée (en jours) sn_ti.scan_ioc_num_days	Option permettant de définir la durée pendant laquelle la recherche automatisée de menace de l'observable est ignorée. Valeur par défaut (en jours) : 30
N'exécutez pas la recherche automatisée de menaces sur un observable si elle a déjà été exécutée. sn_ti.enable_threat_lookup_bypass	Si un résultat de la recherche de menace pour un observable est déjà disponible, vous pouvez ignorer la nouvelle exécution de la recherche de menace

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Remarque : Vous devez définir la durée dans la propriété suivante (sn_ti.threat_lookup_bypass_times).	automatisée pour le même observable jusqu'à ce que la durée configurée soit écoulée. Valeur par défaut : non **Remarque :** Si vous activez cette propriété, assurez-vous d'ajouter une valeur appropriée.
Durée (en minutes) sn_ti.délai_de_contournement_recherche_de_menace	Option permettant de définir la durée après laquelle la recherche automatisée des menaces pour l'observable peut être réexécutée. Valeur par défaut (en minutes) : 0
Définissez une durée de validité pour les remplacements d'utilisateur sur le résultat des observables. sn_ti.enable_observable_finding_system_override **Remarque :** Vous devez définir la validité dans la propriété suivante (sn_ti.observable_finding_override_expiry).	Option permettant de définir une durée de validité pour les remplacements utilisateur sur les résultats observables. Le résultat de la recherche de menaces pour l'observable ne sera pas modifié par le système de base pendant cette durée de validité. Valeur par défaut : Non. **Remarque :** Si vous activez cette propriété, assurez-vous d'ajouter une valeur appropriée.
Validité (en minutes) sn_ti.observable_finding_override_expiry	Option permettant de définir la période de validité du résultat de l'observable. Valeur par défaut (en minutes) : aucune
Lorsqu'un mode/méthode d'attaque n'a été reçu d'aucune source pendant le nombre de jours spécifié, marquez-le comme inactif sn_ti.attack_mode_inactivate_days	Nombre de jours à partir de la dernière réception d'un mode/méthode d'attaque pour que l'enregistrement soit marqué comme inactif. Valeur par défaut : 360

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Remarque : La case à cocher **Actif** n'est pas visible sur le formulaire **Mode/méthode d'attaque** par défaut. Cependant, vous pouvez l'ajouter. Lorsque les modes/méthodes d'attaque sont inactifs, ils ne peuvent pas être sélectionnés sur d'autres formulaires.
Lorsqu'aucun indicateur n'a été reçu d'aucune source pendant le nombre spécifié de jours, marquez-le comme inactif sn_ti.indicator_inactivate_days	Nombre de jours à partir de la dernière réception d'un indicateur pour que l'enregistrement soit marqué comme inactif. Valeur par défaut : 180 **Remarque :** Par défaut, la case à cocher **Actif** n'est pas visible sur le formulaire **d'indicateur** . Cependant, vous pouvez l'ajouter. Lorsque les indicateurs sont inactifs, ils ne peuvent pas être sélectionnés sur d'autres formulaires.
Taille maximale de la charge utile (en Mo) d'une pièce jointe STIX pouvant être analysée. sn_ti.stix.max_payload_size	Spécifie la taille maximale de la charge utile pour la pièce jointe STIX que vous pouvez analyser. Valeur par défaut : aucune Valeur maximale autorisée : aucune limite.
Délai maximal, en secondes, pendant lequel une connexion HTTP sortante attend pour récupérer les données de collecte TAXII sn_ti.taxii.http.max_timeout	Spécifie la durée maximale d'attente d'une connexion HTTP sortante avant d'extraire le paquet suivant de données de collecte TAXII. Valeur par défaut : 300
Nombre maximal d'objets récupérés dans un seul appel REST à partir d'un serveur TAXII (applicable uniquement pour les versions 2.0 et 2.1 de TAXII) sn_ti.taxii.max_page_size	Spécifie le nombre maximal d'objets récupérés dans un seul appel REST à partir du serveur TAXII pour une page.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Valeur par défaut : 5000 Valeur maximale autorisée : 50000
Nombre maximal de nouvelles tentatives pour un échec d'appel REST TAXII 2.X sn_ti.taxii2.retry_count	Spécifie le nombre maximal de nouvelles tentatives pour un échec de l'appel REST TAXII. Valeur par défaut : 3

3. Cliquez sur **Enregistrer**.

Définir une source de menace

Vous pouvez tenir à jour une liste des sources de Renseignements sur les menaces menace. Chaque source inclut la possibilité de définir la fréquence à laquelle une source est interrogée. Vous pouvez également exécuter une source de menace à la demande pour importer les données STIX (Structured Threat Information eXpression) nécessaires.

Avant de commencer

Rôle requis : sn_ti.admin

Pourquoi et quand exécuter cette tâche

Renseignements sur les menaces utilise deux technologies pour importer des informations relatives aux menaces : STIX et TAXII (Trusted Automated Exchange of Indicator Information).

STIX fournit un langage normalisé et structuré pour représenter un vaste ensemble d'informations sur les cybermenaces qui comprend des indicateurs d'activité de compromission (IoC) (par exemple, les adresses IP et les hachages de fichiers), ainsi que des informations contextuelles concernant les menaces, telles que les modes/méthodes d'attaque, qui, ensemble, caractérisent plus complètement les motivations, les capacités et les activités d'un cyberadversaire. En tant que telles, les données STIX fournissent des informations précieuses sur la meilleure façon dont votre organisation peut se défendre contre les cybermenaces.

L'échange automatisé d'informations sur les indicateurs (TAXII) est utilisé pour faciliter l'échange automatisé d'informations sur les cybermenaces. TAXII définit un ensemble de services et d'échanges de messages qui permettent le partage d'informations exploitables sur les cybermenaces au-delà des frontières de l'organisation et des produits/services pour la détection, la prévention et l'atténuation des cybermenaces. Les profils TAXII peuvent être configurés en tant que référentiels pour le partage d'informations au format STIX. Chaque profil contient une ou plusieurs collections ou flux TAXII.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Sources** > **Sources de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Le nom de la source de menace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	L'application qui contient l'enregistrement.
Actif	Cochez cette case pour activer la source de menace.
Avancés	Cochez cette case pour afficher les scripts dans les champs **Script de l'instanciateur d'intégration** et **Processeur de rapports** .
Description	Description de cette source de menace.

4. Renseignez les champs de la section **Calendrier** , selon vos besoins.

Champ	Description
Exécuter	Fréquence à laquelle vous souhaitez que l'intégration s'exécute : Quotidienne, Hebdomadaire, Périodique, et ainsi de suite. Comme indiqué, les champs suivants sont affichés en fonction du paramètre de ce champ.
Jour	Le jour où vous souhaitez que l'intégration s'exécute. ◦ Si vous avez sélectionné **Hebdomadaire** dans le champ **Exécuter** , ce champ affiche les jours de la semaine. ◦ Si vous avez sélectionné **Mensuel** dans le champ **Exécuter** , ce champ affiche les jours du mois.
Heure	Heure à laquelle vous souhaitez que l'intégration démarre.
Intervalle de répétition	Si vous avez sélectionné **Périodiquement** dans le champ **Exécuter** , ce champ affiche le nombre de jours et d'heures avant que l'intégration ne s'exécute à nouveau.
En cours de démarrage	Si vous avez sélectionné **Périodiquement** dans le champ **Exécuter** , ce champ affiche les dates et l'heure à utiliser comme point de départ pour les mises à jour périodiques.
Conditionnel	Sélectionnez ce champ si vous souhaitez ajouter des paramètres conditionnels.
Condition	Si vous avez coché la case **Conditionnel** , entrez les conditions ici.

5. Renseignez les champs de la section Détails de la **menace** comme il convient.

Champ	Description
Indicateur	Indicateur à utiliser lorsque les données n'en fournissent pas explicitement. Pour les listes de blocs, si elles sont vides, un nouvel indicateur est créé pour chaque observable.
Type d'indicateur	Type d'indicateur à utiliser pour les indicateurs qui sont créés lorsque les données ne fournissent pas explicitement un type d'indicateur.
Mode/méthode d'attaque	Mode/méthode d'attaque à utiliser lorsque les données n'en fournissent pas explicitement un.
Type d'observable	Type d'observable à utiliser pour les observables qui sont créés et dont les données ne fournissent pas explicitement un type d'observable.[SI1]

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Poids	Entrez une valeur de poids pour cette source à utiliser dans le calcul de confiance.

Remarque : L'utilisation des champs **Indicateur**, **Type d'indicateur**, **Mode/Méthode d'attaque** et **Type d'observable** est propre à l'implémentation. Le processeur par défaut, SimpleBlocklistProcessor, se comporte comme le montrent les info-bulles. Cependant, une source de menace TAXII est entièrement pilotée par les données. N'importe quel processeur de source de menace personnalisé serait en mesure d'utiliser sa propre stratégie. Ces champs sont essentiellement des éléments à exposer à l'intégration/au processeur et l'implémentation décide de la manière de les utiliser.

6. Renseignez les champs de la section Détails de la **source** , comme il convient.

Champ	Description
Point de terminaison	Entrez l'URL du point de terminaison du service Web où la source de menace est accessible par Renseignements sur les menaces. Cliquez sur l'icône de verrou pour verrouiller l'URL.
Utiliser le message REST	Si vous avez besoin d'un message REST pour accéder à la source de menace, cochez cette case. Les champs **Message REST** et **Méthode REST** deviennent obligatoires.
Message REST	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cliquez sur **Nouveau** pour définir un nouveau message REST .
Méthode REST	Cliquez sur l'icône de recherche, puis sélectionnez la méthode REST dans la liste ou cliquez sur **Nouveau** pour définir une nouvelle méthode REST.
Script d'intégration	Le script d'intégration par défaut est **SimpleRESTSecurityDataIntegration**. Il exécute un simple appel REST, enregistre la réponse en tant que pièce jointe, puis renvoie la pièce jointe au processeur. Ce script répond aux besoins de la plupart des organisations. Mais si vous le souhaitez, vous pouvez cliquer sur l'icône de recherche et sélectionner un autre script d'intégration ou en définir un nouveau.
Script de l'instanciateur d'intégration	Si la case à cocher **Avancé** est activée, ce champ affiche le script réel pour la construction du script d'intégration. Vous pouvez modifier le script selon vos besoins. Cette capacité est utile pour les implémentations personnalisées. Les intégrations dans le système de base n'ont généralement pas besoin d'une logique de constructeur personnalisée.
Script de processeur de rapport	Le script d'intégration par défaut est **SimpleBlocklistProcessor**. Ce script est un processeur simple qui accepte une liste de blocs simple (simple, c'est-à-dire un document à colonne unique avec des observables tels que des URL ou des adresses IP) et crée des observables. Il utilise les différents champs Détails de la **menace** pour déterminer les champs à définir lors de la création des observables.
Script de l'instanciateur de processeur	Si la case **Advanced (Avancé**) est cochée, ce champ affiche le script réel de construction du processeur. Vous pouvez modifier le script selon vos besoins. Ce script est généralement utile pour les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	implémentations personnalisées. Les intégrations dans le système de base n'ont généralement pas besoin d'une logique de constructeur personnalisée.

7. Cliquez sur **Envoyer**.

Remarque : Pour en savoir plus sur la configuration de la pagination de la source de menace, consultez KB1213825 article.

Créer un profil TAXII

Vous pouvez gérer les profils TAXII pour partager des informations au format STIX. Chaque profil contient une ou plusieurs collections ou flux TAXII.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Sources** > **Profils TAXII**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs suivants, le cas échéant.

Champ	Description
Nom	Nom du profil TAXII
Application	L'application qui contient l'enregistrement.
Utiliser les messages REST comme modèle	Si vous avez besoin d'un message REST pour accéder au profil TAXII, cochez cette case.
Version TAXII	Spécifiez la version TAXII. Les versions STIX prises en charge sont 1.1, 2.0 et 2.1.
Description	Description de ce profil TAXII.

4. Renseignez les champs de la section **Configuration du service Discovery** comme il convient.

Champ	Description
Point de terminaison de service de découverte	Le point de terminaison de détection autorise les clients à obtenir des informations sur un serveur TAXII et à obtenir une liste des racines d'API.
Utiliser le message REST	Sélectionnez cette option si vous avez besoin d'un message REST pour accéder au profil TAXII. Les champs Message **REST du service** de **découverte et Méthode REST du service de découverte** deviennent obligatoires.
Message REST du service de découverte	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cli-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	quez sur **Nouveau** pour définir un nouveau message REST.
Méthode REST du service de découverte	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cliquez sur **Nouveau** pour définir une nouvelle méthode REST.

5. Renseignez les champs de la section **Configuration du service de collecte** , selon vos besoins.

Champ	Description
Informations sur la collection Point de terminaison de service	Une collection TAXII est une interface vers un référentiel logique d'objets CTI fourni par un serveur TAXII et est utilisée par les clients TAXII pour envoyer des informations au serveur TAXII ou demander des informations au serveur TAXII. Un serveur TAXII peut héberger plusieurs collections par racine d'API, et les collections sont utilisées pour échanger des informations sous la forme d'une requête et d'une réponse.
Utiliser le message REST	Sélectionnez cette option si vous avez besoin d'un message REST pour accéder au profil TAXII. Les champs **Message REST Service d'informations sur la collecte** et **Méthode REST Service d'informations sur la collecte** deviennent requis.
Service d'informations sur la collecte Message REST	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cliquez sur **Nouveau** pour définir un nouveau message REST.
Service d'informations sur la collecte Méthode REST	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cliquez sur **Nouveau** pour définir une nouvelle méthode REST.

6. Cliquez sur **Envoyer**.

Référentiel IoC

Le référentiel IoC contient des objets STIX, chacun de ces objets contient une information spécifique.

Lorsque vous combinez des objets STIX par le biais de relations, vous permettez des représentations faciles ou complexes de Cyber Threat Intelligence (CTI).

Renseignements sur les menaces prend en charge les versions 1.1, 2.0 et 2.1 de STIX.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modes et méthodes d'attaque

Les modes et méthodes d'attaque, parfois appelés tactiques, techniques et procédures (TTP), sont des représentations du comportement des cyberadversaires. Ils caractérisent ce que font ces adversaires et comment ils le font, avec des niveaux de détail croissants. Les modes et méthodes d'attaque s'appliquent à la STIX version 1.1.

Par exemple, un mode/méthode d'attaque peut consister à utiliser un logiciel malveillant pour voler les informations d'identification d'une carte de crédit. Ou une autre tactique connexe (à un niveau de détail inférieur) pourrait être d'envoyer des e-mails ciblés avec des pièces jointes contenant un code malveillant, qui s'exécute à l'ouverture, capture les informations de carte de crédit à partir des frappes au clavier et utilise http pour communiquer avec un serveur de commande et de contrôle afin de transférer des informations.

Les modes et méthodes d'attaque s'appliquent à la STIX version 1.1.

Définir un mode/méthode d'attaque

Les modes et méthodes d'attaque sont importés avec les données STIX, mais vous pouvez ajouter de nouveaux modes/méthodes, si nécessaire.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Mode/méthode d'attaque**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Sélectionner une balise de classification	Si vous configurez et activez des balises de classification pour ajouter des métadonnées à l'enregistrement, vous pouvez sélectionner une ou plusieurs balises pour spécifier le degré de sensibilité du mode/méthode d'attaque. Si vous n'avez pas configuré ou activé les balises de classification, cette liste déroulante ne s'affiche pas.
Titre	Entrez un nom descriptif pour ce mode/méthode d'attaque.
Type de programme malveillant	Sélectionnez le type de logiciel malveillant pour ce mode/méthode d'attaque. Les types de logiciels malveillants disponibles sont récupérés à partir du serveur du fournisseur sous forme de données STIX.
Source	Sélectionnez la source de données de menace pour ce mode/méthode d'attaque. Certaines sources de données sont incluses dans le système de base. Vous pouvez créer de nouvelles sources de données selon vos besoins.
Mécanisme d'attaque	Sélectionnez le mécanisme d'attaque pour ce mode/méthode d'attaque. Les mécanismes d'attaque représentent les différentes techniques utilisées pour attaquer un système. Les mécanismes d'attaque disponibles sont récupérés sur le serveur du fournisseur sous forme de données STIX.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Premier vu	Cette date est récupérée sur le serveur du fournisseur sous forme de données STIX.
Dernier observé	Cette date est récupérée sur le serveur du fournisseur sous forme de données STIX.
Type d'acteur de menace	Sélectionnez le type d'acteur de menace pour ce mode/méthode d'attaque. Les types d'acteurs de menace caractérisent les acteurs malveillants (ou les adversaires) représentant une menace de cyberattaque, y compris l'intention présumée et le comportement historiquement observé. Les types d'acteurs de menace disponibles sont récupérés à partir du serveur du fournisseur sous forme de données STIX.
Description	Entrez une description du mode/de la méthode d'attaque.
Manutention	Entrez des instructions sur la façon de gérer ce mode/méthode d'attaque.
Effet souhaité	Entrez l'effet escompté de ce type d'attaque.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
   Vous pouvez consulter l'une des listes connexes suivantes pour afficher des informations supplémentaires.

Liste connexe	Description
Indicateurs connexes	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace.
Mode/méthode d'attaque enfant	Répertorie les modes/méthodes d'attaque qui sont des enfants du mode/de la méthode d'attaque parent.
Tâches associées	Répertorie les changements associés au mode/méthode d'attaque parent.

Ajouter un IoC à un mode/méthode d'attaque

En plus d'importer des indicateurs sous forme de données STIX, vous pouvez ajouter manuellement des IoC à un mode/méthode d'attaque.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Mode/méthode d'attaque**.
2. Cliquez sur le mode d'attaque auquel vous souhaitez ajouter un IoC.
3. Cliquez sur la liste **connexe Indicateurs connexes** .
4. Cliquez sur **Modifier**.
5. Au besoin, utilisez les filtres pour localiser l'IoC que vous souhaitez ajouter.
6. À l'aide de la zone de liste double, ajoutez l'IoC à la liste **des indicateurs connexes** .
7. Cliquez sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter une méthode de mode d'attaque connexe

En plus d'importer des modes/méthodes d'attaque sous forme de données STIX, vous pouvez ajouter manuellement des modes/méthodes d'attaque associés.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Mode/méthode d'attaque**.
2. Cliquez sur le mode d'attaque auquel vous souhaitez ajouter un mode/méthode d'attaque associé.
3. Cliquez sur la liste **connexe Mode/méthode d'attaque enfant** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser le mode/méthode d'attaque que vous souhaitez associer au mode/méthode actuel.
6. À l'aide de la zone de liste double, ajoutez le mode/la méthode d'attaque à la liste **des modes/méthodes d'attaque enfant** .
7. Cliquez sur **Enregistrer**.

Ajouter une tâche associée à un mode/méthode d'attaque

En plus d'importer les tâches associées (telles que les changements et les incidents) sous forme de données STIX, vous pouvez les ajouter manuellement à un mode/méthode d'attaque.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Mode/méthode d'attaque**.
2. Cliquez sur le mode d'attaque auquel vous souhaitez ajouter une tâche associée.
3. Cliquez sur la liste **connexe Tâches associées** .
4. Cliquez sur **Modifier**.
5. Au besoin, utilisez les filtres pour localiser les tâches que vous souhaitez associer au mode/méthode d'attaque.
6. À l'aide de la zone de liste double, ajoutez la tâche à la liste **des tâches associées** .
7. Cliquez sur **Enregistrer**.

Indicateurs de compromis

Les indicateurs de compromission (IoC) sont des artefacts observés sur un réseau ou un système d'exploitation susceptibles d'indiquer une intrusion. Les IoC typiques sont les signatures de virus et les adresses IP, les hachages MD5 de fichiers ou d'URL de logiciels malveillants ou les noms de domaine. IoC s'applique pour STIX 1.1 et 2.x.

Un IoC peut être un observable unique ou une collection d'observables (par exemple, une seule URL incorrecte connue ou la présence d'un fichier spécifique et de quelques valeurs de clé de registre spécifiques).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois que les IoC ont été identifiés dans le cadre d'un processus de réponse aux incidents et d'expertise informatique, ils peuvent être utilisés pour la détection précoce de futures tentatives d'attaque à l'aide de systèmes de détection d'intrusion et de logiciels antivirus.

IoC s'applique pour STIX 1.1 et 2.x.

Afficher un IoC

Les IoC, parfois appelés indicateurs, sont le plus souvent récupérés à partir d'une source de données de menace en tant que données STIX. Si nécessaire, vous pouvez également créer des IoC.

Avant de commencer

Rôle requis : sn_ti.write

Procédure

1. Une fois que la tâche planifiée a récupéré les données IoC à partir de la source de données définie, naviguez vers **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
   Les IoC récupérés sont répertoriés.
2. Cliquez sur l'IoC que vous souhaitez afficher.
3. Les informations suivantes s'affichent.

Champ	Description
Sélectionner une balise de classification	Si vous avez configuré et activé des balises de sécurité pour ajouter des métadonnées à l'enregistrement, vous pouvez sélectionner une ou plusieurs balises pour spécifier le degré de sensibilité de l'IoC. Si vous n'avez pas configuré ou activé les balises de sécurité, cette liste déroulante ne s'affiche pas.
Titre	Nom descriptif pour cet indicateur.
Premier vu	Date à laquelle cet indicateur a été observé pour la première fois dans le système.
Dernier observé	La date la plus récente à laquelle cet indicateur a été observé dans le système.
Nombre rencontré	Nombre de fois que l'indicateur a été rencontré.
Nombre approvisionné	Nombre de fois où l'indicateur a été importé à partir de sources de menace définies.
Notes	Toute remarque supplémentaire sur l'indicateur. Ce champ peut également contenir des paires clé/valeur JSON.

4. Vous pouvez cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Observables associés	Répertorie les observables liés à l'indicateur actuel.
Mode/ méthode d'attaque connexe	Répertorie les modes/méthodes d'attaque connexes qui ont été identifiés comme associés à cet indicateur.
Type associé	Répertorie les autres types d'indicateurs associés à cet IoC.
Sources d'indicateurs	Répertorie les sources de cet indicateur, ainsi que le niveau de fiabilité de la source.
Tâches associées	Répertorie l'ensemble des tâches, des changements et des incidents associés à l'IoC.
Métadonnées de l'indicateur	Si le champ **Notes** contient des paires clé/valeur JSON valides, elles sont analysées et affichées. Si aucune paire clé/valeur JSON n'est présente, ou si le JSON n'est pas valide, cette liste connexe n'est pas affichée.
Annotations de sécurité	
Références externes de l'indicateur	
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.

Ajouter un observable connexe à un IoC

En plus d'importer des observables sous forme de données STIX, vous pouvez ajouter manuellement des observables connexes à un IoC.

Avant de commencer

Rôle requis : sn_ti.write

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'indicateur auquel vous souhaitez ajouter un observable associé.
3. Cliquez sur la liste connexe **Observables associés** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser l'observable que vous souhaitez associer à l'IoC.
6. À l'aide de la zone de liste double, ajoutez l'observable à la liste **Observables connexes** .
7. Cliquez sur **Enregistrer**.

Ajouter un mode/une méthode d'attaque connexe à un IoC

En plus d'importer les modes/méthodes d'attaque associés sous forme de données STIX, vous pouvez ajouter manuellement des modes/méthodes d'attaque associés à un IoC.

Avant de commencer

Rôle requis : sn_ti.write

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'indicateur auquel vous souhaitez ajouter un mode/méthode d'attaque associé.
3. Cliquez sur la liste **connexe Mode/méthode d'attaque connexe** .
4. Cliquez sur **Modifier**.
5. Au besoin, utilisez les filtres pour localiser le mode/la méthode d'attaque que vous souhaitez associer à l'IoC.
6. À l'aide de la zone de liste double, ajoutez le mode/la méthode d'attaque à la liste des **modes/méthodes d'attaque associés** .
7. Cliquez sur **Enregistrer**.

Identifier les types d'indicateurs associés

Si aucun type d'indicateur associé à un IoC n'est défini, il suit tous les types d'observables. Toutefois, si vous associez un ou plusieurs types d'indicateurs à un IoC, cela limite les types d'observables qui peuvent être associés à l'IoC.

Avant de commencer

Rôle requis : sn_ti.write

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'indicateur auquel vous souhaitez associer un type d'indicateur.
3. Cliquez sur la liste connexe **Type associé** .
4. Cliquez sur **Modifier**.
5. Au besoin, utilisez les filtres pour localiser le type d'indicateur que vous souhaitez associer à l'IoC.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. À l'aide de la zone de liste double, ajoutez le type d'indicateur à la liste **Type associé** .
7. Cliquez sur **Enregistrer**.

Identifier les sources d'indicateurs

Les sources d'indicateurs sont normalement suivies automatiquement dans le cadre du processus d'importation des menaces, mais d'autres sources peuvent être ajoutées manuellement.

Avant de commencer

Rôle requis : sn_ti.write

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'indicateur auquel vous souhaitez ajouter des sources d'indicateurs.
3. Cliquez sur la liste connexe **Sources d'indicateurs** .
4. Cliquez sur **Modifier**.
5. Au besoin, utilisez les filtres pour localiser la source d'indicateur que vous souhaitez associer à l'IoC.
6. À l'aide de la zone de liste double, ajoutez la source d'indicateur à la liste **Sources d'indicateur** .
7. Cliquez sur **Enregistrer**.

Ajouter des tâches associées à un IoC

En plus d'importer les tâches associées (telles que les changements et les incidents) sous forme de données STIX, vous pouvez les ajouter manuellement à un IoC.

Avant de commencer

Rôle requis : sn_ti.write

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'IoC auquel vous souhaitez ajouter une tâche associée.
3. Cliquez sur la liste **connexe Tâches associées** .
4. Cliquez sur **Modifier**.
5. Au besoin, utilisez les filtres pour localiser les tâches que vous souhaitez associer à l'IoC.
6. À l'aide de la zone de liste double, ajoutez la tâche à la liste **des tâches associées** .
7. Cliquez sur **Enregistrer**.

Observables

Les observables représentent des propriétés avec état (telles que le hachage MD5 d'un fichier ou la valeur d'une clé de Registre) ou des événements mesurables (tels que la création d'une clé de registre ou la suppression d'un fichier) qui sont pertinents pour le fonctionnement des ordinateurs et des réseaux. Les observables s'appliquent pour STIX 1.1 et 2.x.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les ensembles d'observables cybernétiques sont utiles pour identifier les indicateurs de compromission lorsqu'ils sont combinés à des informations contextuelles qui représentent les comportements des cybermenaces.

Les observables s'appliquent pour STIX 1.1 et 2.x.

Définir un observable

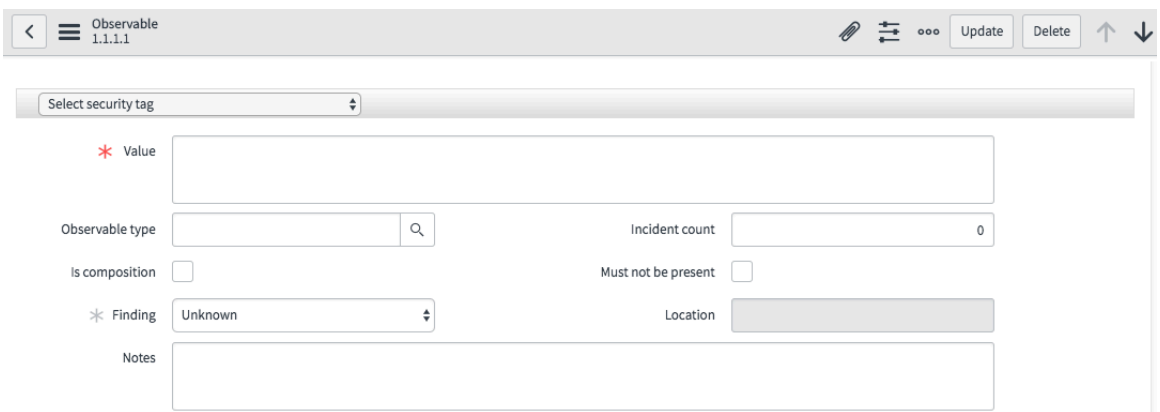
Les observables sont récupérés sur le serveur fournisseur en tant que données STIX. Toutefois, vous pouvez créer des observables selon vos besoins.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur **Nouveau**.



3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Sélectionner une balise de classification	Si vous avez configuré et activé des balises de sécurité pour ajouter des métadonnées à l'enregistrement, vous pouvez sélectionner une ou plusieurs balises pour spécifier le degré de sensibilité de l'observable. Si vous n'avez pas configuré ou activé les balises de sécurité, cette liste déroulante ne s'affiche pas.
Valeur	Valeur (par exemple, adresse IP ou hachage) associée à l'observable. **Remarque :** Si une analyse de menace porte sur une adresse IP ou un hachage, un programme malveillant renvoyé ou une autre défaillance, l'adresse IP ou la valeur de hachage est automatiquement ajoutée à la table Observable [sn_ti_observable]. En tant que tel, il peut être recherché à partir du formulaire Observables.
Type d'observable	Sélectionnez la classification de l'observable, telle qu'une adresse IP ou un hachage de fichier. Ces types d'observables sont définis dans le module **Types d'observables** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nombre d'incidents	Nombre de fois où la valeur observable a été rencontrée.
Est une composition	Ce champ s'affiche uniquement une fois l'enregistrement de l'observable enregistré. Si le **type d'observable** est défini sur autre chose que **la composition de l'observable** et que ce nouvel observable est une composition, cochez cette case. Si le **type d'observable** est déjà défini sur **Composition de l'observable**, la case est cochée et en lecture seule. Une composition observable est un observable qui contient des observables enfants.
Résultat	Sélectionnez l'une des options suivantes : ◦ **malveillant** : indique que l'observable est préjudiciable à l'organisation. ◦ **Suspect** : indique que l'observable pourrait nuire à l'organisation. ◦ **Nettoyer** : indique que l'observable n'est pas nuisible pour l'organisation. ◦ **Inconnu** : indique que nous n'avons pas encore déterminé le résultat de l'observable. ◦ Valeur par défaut : inconnue. Pour plus d'informations, consultez Calculateurs de résultats de la recherche de menace. **Remarque :** Après une mise à niveau, les observables existants sont marqués malveillants.
Opérateur	Ce champ s'affiche uniquement lorsque la case **Est une composition** est cochée. En fonction du paramètre que vous avez défini dans ce champ, les observables et leurs enfants sont pris en compte pour décider si un indicateur associé est présent. Définissez ce champ sur **ET** si tous les observables enfants doivent être présents pour qu'un indicateur associé soit considéré comme présent. Affectez-lui la valeur **OU** si l'un des observables enfants est présent pour qu'un indicateur associé soit considéré comme présent.
Ne doit pas être présent	Ce champ s'affiche uniquement une fois l'enregistrement de l'observable enregistré. S'il est sélectionné, ce champ signifie que l'absence de l'observable est le problème potentiel (par exemple, une clé de registre manquante).
Emplacement	À l'aide des paramètres de deux propriétés et d'une définition de script include, vous pouvez effectuer un chargement Charger plus de données IoC dans ce champ.
Notes	Entrez toutes les notes supplémentaires sur l'observable.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires.

Liste connexe	Description
Indicateurs connexes	Répertorie les indicateurs qui ont été identifiés par la source de menace.
Tâches associées	Répertorie les changements associés à l'observable.
Observables enfants	Répertorie les observables associés qui ont été identifiés par la source de menace.
Ressources correspondantes pour IP	Si l'observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante.
Sources des observables	Répertorie les sources de cet observable, ainsi que le niveau de fiabilité de la source.
Annotations de sécurité	Répertorie les annotations de sécurité ajoutées à cet observable.

Ajouter un IoC connexe à un observable

En plus d'importer des observables sous forme de données STIX, vous pouvez ajouter manuellement des observables connexes à un IoC.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'observable auquel vous souhaitez ajouter un IoC associé.
3. Cliquez sur la liste **connexe Indicateurs connexes** .
4. Cliquez sur **Modifier**.
5. Selon les besoins, utilisez les filtres pour localiser l'indicateur que vous souhaitez associer à l'observable.
6. À l'aide de la zone de liste double, ajoutez l'indicateur à la liste **Indicateurs connexes** .
7. Cliquez sur **Enregistrer**.

Ajouter des tâches associées à un observable

En plus d'importer les tâches associées (telles que les changements et les incidents) en tant que données STIX, vous pouvez les ajouter manuellement à un observable.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'observable auquel vous souhaitez ajouter une tâche associée.
3. Cliquez sur la liste **connexe Tâches associées** .
4. Cliquez sur **Modifier**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Selon vos besoins, utilisez les filtres pour localiser les tâches que vous souhaitez associer à l'observable.
6. À l'aide de la zone de liste double, ajoutez la tâche à la liste **des tâches associées** .
7. Cliquez sur **Enregistrer**.

Ajouter un observable connexe

En plus d'importer des observables sous forme de données STIX, vous pouvez ajouter manuellement des observables associés.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'observable auquel vous souhaitez ajouter un observable associé.
3. Cliquez sur la liste **connexe Observables enfants** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser l'observable que vous souhaitez associer à l'observable actuel.
6. À l'aide de la zone de liste double, ajoutez l'observable à la liste **des observables enfants** .
7. Cliquez sur **Enregistrer**.

Charger plus de données IoC

En fonction des paramètres de deux propriétés et d'une définition de l'include de script, vous pouvez charger des informations de géolocalisation pour les adresses IP et les sites Web dans le formulaire Observables. Avec une personnalisation plus poussée, vous pouvez également ajouter d'autres informations, telles que les codes des pays, les noms des villes.

Avant de commencer

Les deux propriétés suivantes doivent être définies :

- **Nom du domaine pour récupérer des informations supplémentaires pour les adresses/URL IP** [sn_ti.ip_lookup.web_site]
- **Clé API à utiliser pour le domaine ci-dessus, le cas échéant** [sn_ti.ip_lookup.api_key]

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'adresse IP ou l'URL de l'observable pour lequel vous souhaitez afficher plus de données IoC.
   Le champ **Emplacement** affiche la géolocalisation de l'IoC.
3. Cliquez sur le bouton **Enrichir les données** pour charger les données IoC supplémentaires.
4. Vous pouvez également configurer le formulaire Observable pour ajouter d'autres champs liés à l'emplacement, tels que le code du pays et le code de la ville.

> **Remarque :** Pour charger plus d'informations liées à l'emplacement, modifiez l'include de script **ThreatAdditionalInfo** et fournissez la clé API appropriée à partir du site Web qui fournit les informations supplémentaires.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Identifier les sources des observables

Si un observable n'a pas de sources définies, il utilise tous les types de sources. Toutefois, si vous ajoutez une ou plusieurs sources de menace à un observable, cela limite les sources utilisées.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'observable auquel vous souhaitez ajouter des sources d'observables.
3. Cliquez sur la liste connexe **Sources des observables** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser la source que vous souhaitez associer à l'observable.
6. À l'aide de la zone de liste double, ajoutez la source observable à la liste **Sources des observables** .
7. Cliquez sur **Enregistrer**.

Effectuer des recherches sur les observables

Vous pouvez effectuer des recherches de renseignements sur les menaces sur un ou plusieurs observables pour déterminer s'ils sont associés à des menaces de sécurité connues. Les implémentations d'analyse qui s'exécutent dépendent de celles que vous avez activées.

Avant de commencer
Avant de pouvoir effectuer des recherches, vous devez activer le module d'extension Threat Intelligence. Vous devez également installer le module d'extension pour une ou plusieurs des implémentations d'analyse :

- Intégration de CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Opérations de sécurité : Ai-je été victime d'une attaque ?
- VirusTotal

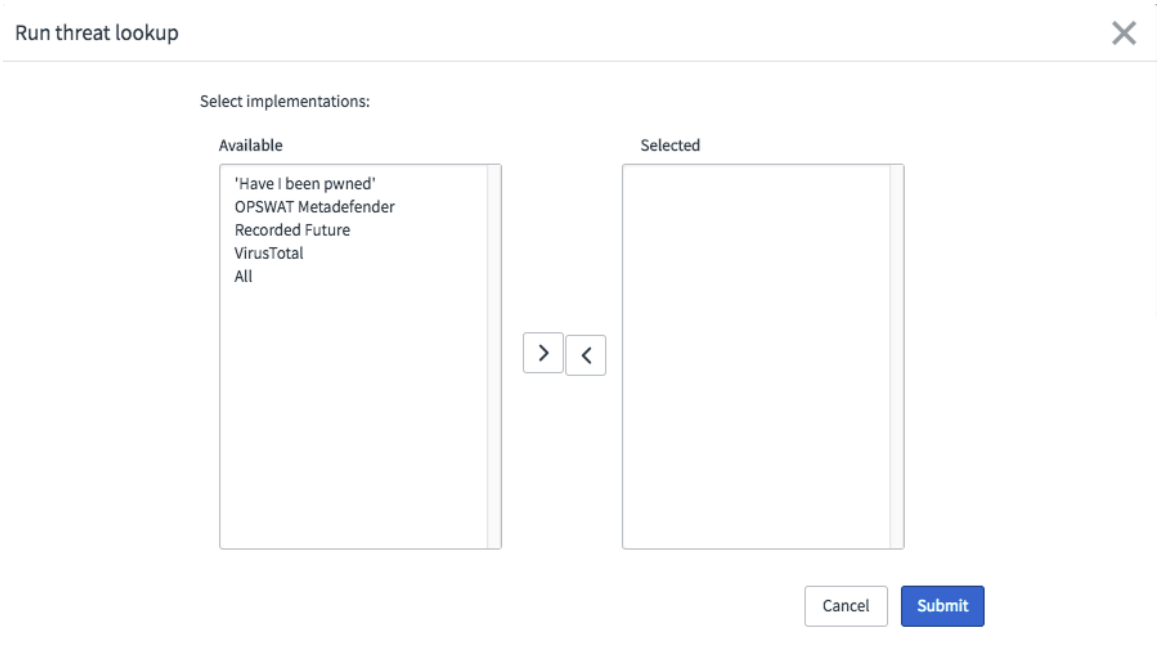
Rôle requis : sn_ti.write

Procédure

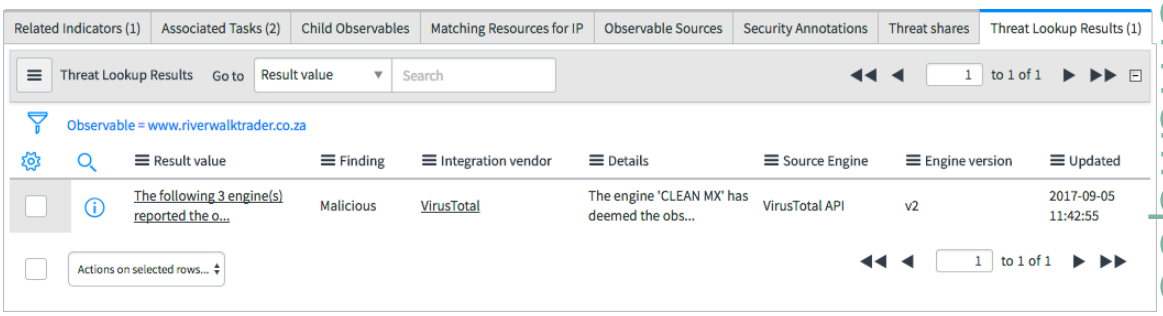
1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Effectuez l'une des actions suivantes :
   - Pour effectuer une recherche sur plusieurs observables, sélectionnez-les, cliquez sur **Actions sur les lignes sélectionnées**, puis sélectionnez Exécuter la **recherche de menace**.
   - Pour effectuer une recherche sur un seul observable, ouvrez l'enregistrement de l'observable et cliquez sur le lien connexe **Exécuter la recherche de menace** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Sélectionnez les implémentations de recherche de menaces que vous souhaitez utiliser ou sélectionnez **Tout** pour effectuer des recherches à l'aide de toutes les implémentations actives, puis cliquez sur **Soumettre**.
   Un message indique que les recherches de menaces ont commencé. Le Workflow de recherche de menaces - Intégration des opérations de sécurité exécute également les workflows d'implémentation pour les implémentations de recherche de menaces que vous avez sélectionnées. Les recherches sont effectuées et les résultats sont générés.
4. Lorsque les recherches sont terminées, vous pouvez cliquer sur l'onglet **Résultats de la recherche de menace** pour afficher les résultats.



Résultat de la recherche de menace récente : vous pouvez également voir les résultats de recherche de menaces récents ou récents de chaque fournisseur d'intégration lorsque vous cliquez sur l'onglet Résultat de la **recherche de menace récente** .

Remarque : L'onglet Résultat de la recherche de menaces récente ne fait pas partie du système de base.

Pour activer cet onglet, procédez comme suit :

a. Cliquez avec le bouton droit sur l'en-tête du formulaire.

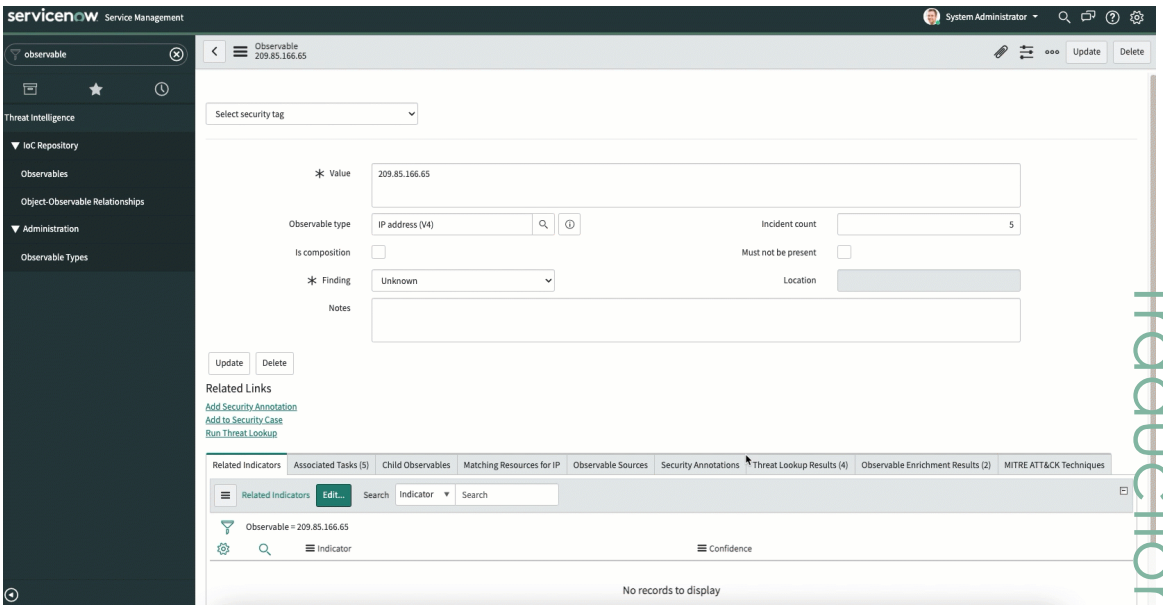
b. Accédez à la **Configurer** > **Listes connexes**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

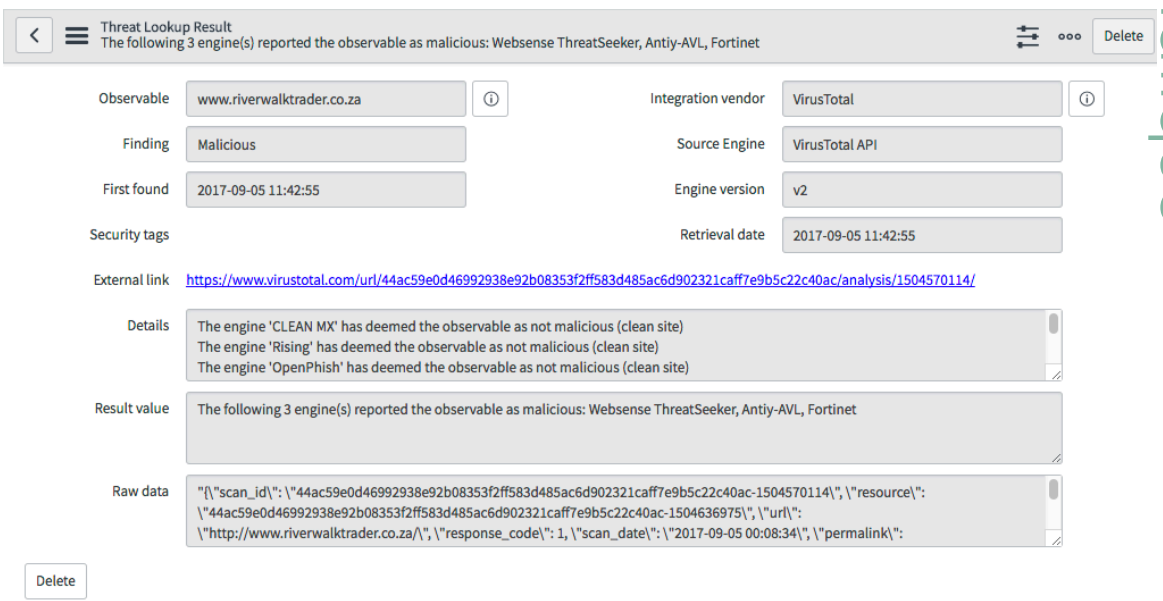
c. Localisez **les résultats de recherche de menaces récents** sur la liste Disponible et déplacez-les vers la liste Sélectionné.

d. Cliquez sur **Enregistrer**.
Vous pouvez maintenant afficher les résultats de la recherche de menaces récente de chaque fournisseur d'intégration dans l'onglet Résultat de la **recherche de menaces récente.**



5. Pour afficher des détails supplémentaires, y compris les résultats bruts d'une recherche spécifique, cliquez sur la **valeur Résultat**.

Remarque : Lorsque les implémentations VirusTotal ou OPSWAT Metadefender sont utilisées, les détails sont consolidés, comme indiqué ci-dessous.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procéder à un enrichissement des menaces sur les observables

Vous pouvez enrichir la connaissance des menaces sur un ou plusieurs observables pour déterminer s'ils sont associés à des menaces de sécurité connues. Les implémentations qui s'exécutent dépendent de celles que vous avez activées.

Avant de commencer

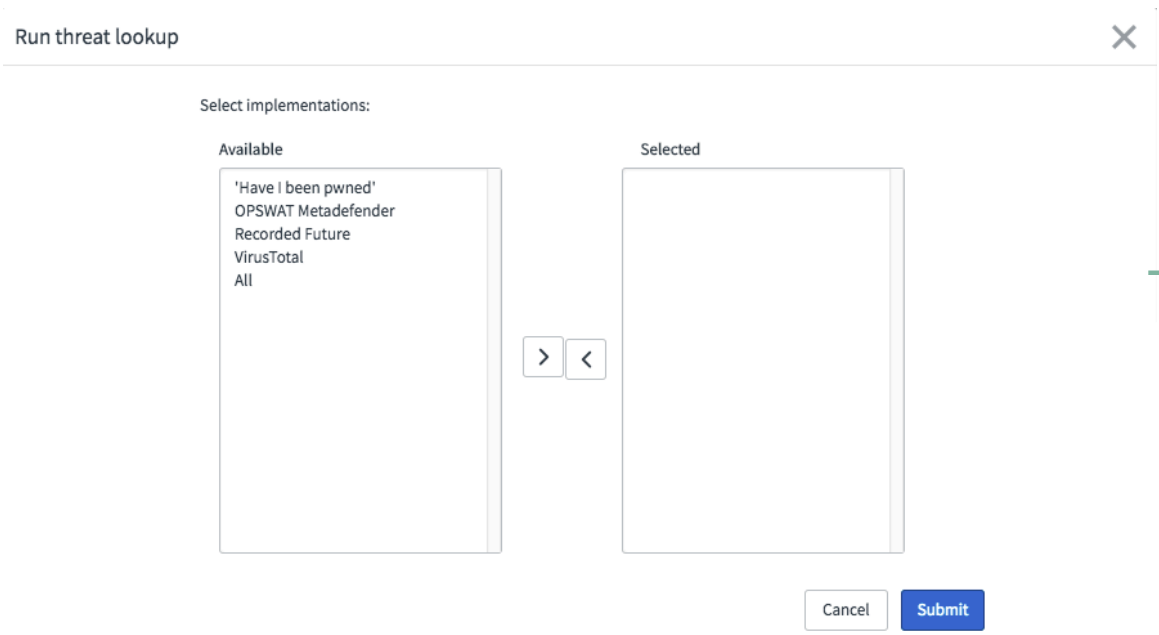
Avant de pouvoir procéder à l'enrichissement, vous devez activer le module d'extension Threat Intelligence. Vous devez également installer le module d'extension pour une ou plusieurs des implémentations d'enrichissement :

- Intégration de CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Opérations de sécurité : Ai-je été victime d'une attaque ?
- VirusTotal
- Qui est ?

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Effectuez l'une des actions suivantes :
   - Pour effectuer une recherche sur plusieurs observables, sélectionnez-les, cliquez sur **Actions sur les lignes sélectionnées**, puis sélectionnez Exécuter la **recherche de menace**.
   - Pour effectuer une recherche sur un seul observable, ouvrez l'enregistrement de l'observable et cliquez sur le lien connexe **Exécuter la recherche de menace** .



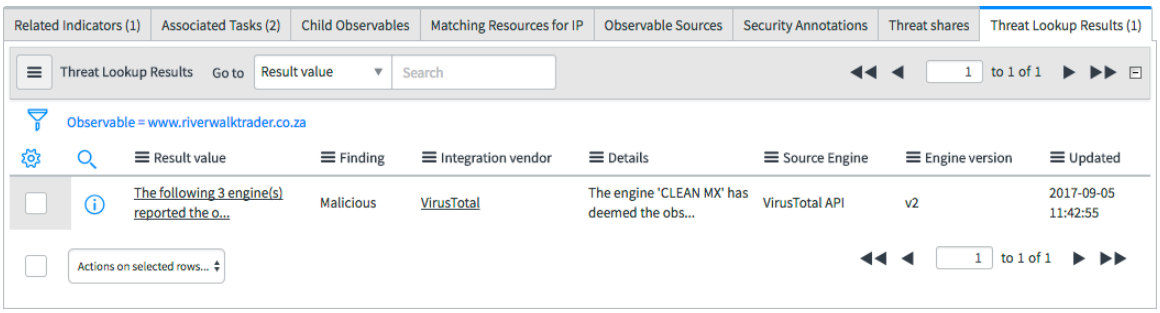
3. Sélectionnez les implémentations de recherche de menaces que vous souhaitez utiliser ou sélectionnez **Tout** pour effectuer des recherches à l'aide de toutes les implémentations actives, puis cliquez sur **Soumettre**.
   Un message indique que les recherches de menaces ont commencé. Le Workflow de recherche de menaces - Intégration des opérations de sécurité exécute également les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

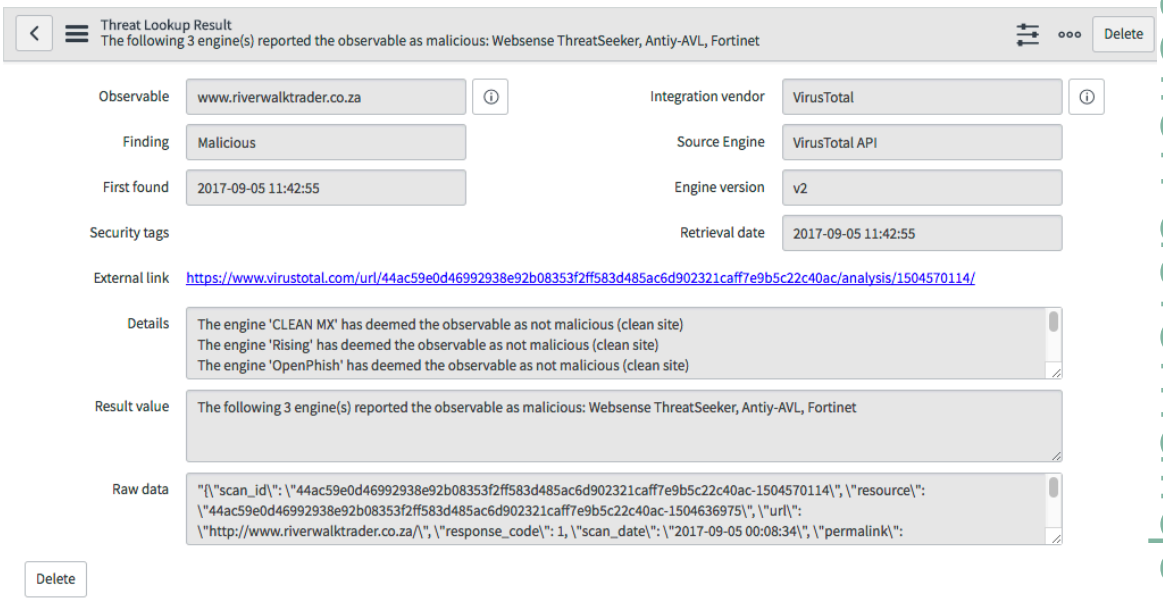
workflows d'implémentation pour les implémentations de recherche de menaces que vous avez sélectionnées. Les recherches sont effectuées et les résultats sont générés.

4. Lorsque les recherches sont terminées, vous pouvez cliquer sur l'onglet **Résultats de la recherche de menace** pour afficher les résultats.



5. Pour afficher des détails supplémentaires, y compris les résultats bruts d'une recherche spécifique, cliquez sur la **valeur Résultat**.

Remarque : Lorsque les implémentations VirusTotal ou OPSWAT Metadefender sont utilisées, les détails sont consolidés, comme indiqué ci-dessous.



Traduction automatique

Schémas d'attaque

Les schémas d'attaque sont un type de tactiques, techniques et procédures (TTP) qui décrivent les méthodes par lesquelles les adversaires tentent de compromettre les cibles. Les schémas d'attaque s'appliquent à STIX 2.x.

Les schémas d'attaque sont utilisés pour faciliter la catégorisation des attaques. Ils généralisent des attaques spécifiques aux modèles qu'ils suivent et fournissent des informations détaillées sur la façon dont les attaques sont exécutées.

Par exemple, le spear phishing est un type d'attaque courant qui consiste pour un attaquant à envoyer un e-mail soigneusement conçu à une partie dans le but de l'inciter à cliquer sur un lien ou à ouvrir une pièce jointe pour diffuser un logiciel malveillant. Les schémas d'attaque sont plus spécifiques, comme le spear phishing par un acteur de menace particulier (par exemple, le fait que la cible a gagné un concours) peuvent également être des schémas d'attaque.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir un modèle d'attaque

Définissez un modèle d'attaque pour faciliter la catégorisation des attaques.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Schémas d'attaque**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Entrez une description du modèle d'attaque.
Alias	Noms alternatifs permettant d'identifier ce modèle d'attaque.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au modèle d'attaque.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Déroulement des actions	Répertorie le plan d'actions associé à cet objet qui sont des réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu) pour prévenir une attaque.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

Campagnes

Une campagne est un regroupement de comportements antagonistes. Ces comportements décrivent un ensemble d'activités malveillantes ou d'attaques qui se produisent au fil du temps contre un ensemble spécifique de cibles. Les campagnes s'appliquent à STIX 2.x.

Les campagnes ont généralement des objectifs bien définis et peuvent faire partie d'un ensemble d'intrusions.

Les campagnes sont souvent attribuées à un ensemble d'intrusions et à des acteurs de la menace. Les auteurs de menace peuvent réutiliser l'infrastructure connue de l'ensemble d'intrusions ou mettre en place une nouvelle infrastructure spécifique à la conduite de cette campagne.

Les campagnes ont un objectif commun dans les incidents qu'elles provoquent, sur les personnes, sur les ressources qu'elles ciblent et les ressources qu'elles utilisent.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, un syndicat du crime attaque les dirigeants de la banque ACME. Ils attaquent en utilisant une variante spécifique de logiciel malveillant et de nouveaux serveurs pour obtenir des informations secrètes sur une fusion à venir avec une autre banque.

Définir une campagne

Définissez une campagne pour regrouper les comportements antagonistes.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Campagnes**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom descriptif pour cette campagne.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur la campagne. Il s'agit notamment de son objectif et de ses caractéristiques clés.
Alias	Noms alternatifs pour identifier cette campagne.
Objectif	L'objectif principal, l'objectif, le résultat souhaité ou l'effet escompté de la campagne. Ce que l'auteur de la menace ou l'ensemble d'intrusion espère accomplir avec cette campagne.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la campagne.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

Déroulement des actions

Un plan d'action est une action entreprise soit pour empêcher une attaque, soit pour répondre à une attaque en cours. Des plans d'action s'appliquent pour STIX 2.x.

Le plan d'action décrit les réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu). Il peut également décrire des actions de niveau supérieur telles que la formation des employés ou des changements de politique.

Par exemple, un plan d'action pour atténuer une vulnérabilité pourrait consister à appliquer le correctif qui la corrige.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir un plan d'action

Définissez un plan d'action pour prévenir une attaque ou pour répondre à une attaque en cours.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Déroulement des actions**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour ce plan d'action.
Action	Pour capturer des plans d'action structurés ou automatisés.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Description qui fournit plus de détails et de contexte sur le plan d'action, y compris potentiellement son objectif et ses caractéristiques clés.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au plan d'action.

Liens connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes	Description
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Identités

Les identités représentent des individus, des organisations ou des groupes réels (ACME, Inc.) et des catégories d'individus, de systèmes ou de groupes (le secteur financier). Les identités s'appliquent pour STIX 2.x.

Le SDO de l'identité peut capturer des informations d'identification de base, des informations de contact et les secteurs auxquels l'identité appartient. L'identité représente les cibles des attaques, les sources d'information, les créateurs d'objets et les identités des acteurs de menace.

Définir les identités

Définissez les identités qui représentent des individus, des organisations ou des groupes réels.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Identités**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour cette identité. Lorsqu'il s'agit d'une entité spécifique (un individu ou une organisation), cette propriété doit contenir le nom canonique de l'entité spécifique.
Classe d'identité	Type d'entité que cette identité décrit. Par exemple, personne ou organisation.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Description qui fournit plus de détails et de contexte sur l'identité, y compris éventuellement son objectif et ses caractéristiques clés.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'identité.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Infrastructure

Le SDO d'infrastructure représente un type de tactiques, de techniques et de procédures (TTP). Ils décrivent les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées destinés à soutenir un objectif d'une attaque. L'infrastructure s'applique pour STIX 2.x.

Les éléments d'une attaque sont représentés par d'autres SDO ou SCO. Toutefois, le SDO d'infrastructure représente un groupe nommé de données qui constitue l'infrastructure.

Des exemples d'infrastructure incluent les serveurs C2 utilisés dans une attaque, un appareil ou un serveur faisant partie d'une défense, ou les serveurs de base de données ciblés par une attaque.

Définir l'infrastructure

Définissez une infrastructure qui regroupe les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées destinés à soutenir un objectif d'une attaque.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Infrastructure**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour identifier l'infrastructure.
Premier vu	Heure à laquelle cette infrastructure a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette infrastructure a été vue pour la dernière fois en train d'effectuer des activités malveillantes.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Description qui fournit plus de détails et de contexte sur l'infrastructure, y compris potentiellement son objectif, la façon dont elle est utilisée, son lien avec d'autres activités de renseignement capturées dans des objets connexes et ses principales caractéristiques.
Alias	Noms alternatifs permettant d'identifier cette infrastructure.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires. Vous pouvez également associer d'autres objets à l'infrastructure.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Observables associés	Répertorie les observables associés à cet objet.
Infrastructure associée	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Ensemble d'intrusions

Un ensemble d'intrusions est un ensemble groupé de comportements et de ressources antagonistes ayant des propriétés communes. Un ensemble d'intrusions implique généralement une seule organisation. L'ensemble d'intrusions s'applique à STIX 2.x.

Un ensemble d'intrusions peut capturer plusieurs campagnes ou autres activités. Ces activités partagent des attributs indiquant un acteur de menace connu ou inconnu.

Une nouvelle activité peut être attribuée à un ensemble d'intrusions, même si les auteurs de menace à l'origine de l'attaque ne sont pas connus. Les auteurs de menace peuvent passer de la prise en charge d'un ensemble d'intrusion à la prise en charge d'un autre, ou ils peuvent prendre en charge plusieurs ensembles d'intrusion.

Un ensemble d'intrusion est l'ensemble de l'attaque et peut être utilisé sur une longue période dans plusieurs campagnes pour atteindre des objectifs potentiellement multiples.

Définir un ensemble d'intrusions

Définissez un ensemble d'intrusions, c'est-à-dire un ensemble groupé de comportements et de ressources antagonistes ayant des propriétés communes.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Ensemble d'intrustions**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom descriptif pour identifier l'ensemble d'intrusions.
Premier vu	Heure à laquelle cet ensemble d'intrusion a été observé pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cet ensemble d'intrusion a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Motivation principale	La raison, la motivation ou l'objectif principal derrière cet ensemble d'intrusions. La motivation est la raison pour laquelle l'ensemble d'intrusion veut atteindre l'objectif (ce qu'il essaie d'atteindre).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par exemple, une intrusion dans le but de perturber le secteur financier d'un pays peut être motivée par une haine idéologique du capitalisme.
Niveau de ressource	Cette propriété spécifie le niveau organisationnel auquel cet ensemble d'intrusion fonctionne généralement, qui à son tour détermine les ressources disponibles pour une utilisation dans une attaque.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Description qui fournit plus de détails et de contexte sur l'ensemble d'intrusions, incluant éventuellement son objectif et ses caractéristiques clés.
Alias	Noms alternatifs permettant d'identifier cet ensemble d'intrusions.
Objectifs	Les objectifs de haut niveau de cette intrusion ont été fixés, à savoir ce qu'ils essaient de faire. Par exemple, ils peuvent être motivés par un gain personnel, mais leur objectif est de voler des numéros de carte de crédit. Pour ce faire, ils peuvent exécuter des campagnes spécifiques qui ont des objectifs détaillés, comme compromettre les systèmes de point de vente d'un grand détaillant.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

Traduction automatique

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au jeu d'intrusion.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Motivations de l'attaque associée	Répertorie toutes les motivations secondaires pour lesquelles cet ensemble d'intrusion veut atteindre.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

Emplacements

Un emplacement représente un emplacement géographique. Les emplacements sont principalement utilisés pour donner un contexte à d'autres SDO. Les emplacements s'appliquent à STIX 2.x.

L'emplacement peut contenir tout ou partie des éléments suivants : région (Amérique du Nord), adresse municipale (New York, États-Unis), latitude et longitude.

Le SDO d'emplacement peut se rapporter à un ensemble d'identité ou d'intrusion pour indiquer que l'ensemble d'identité ou d'intrusion se trouve à cet emplacement. Il peut également s'agir d'un logiciel malveillant ou d'un modèle d'attaque pour indiquer que la victime cible se trouve dans un endroit particulier.

Par exemple, un emplacement pourrait être utilisé dans une relation pour décrire que l'ensemble d'intrusion Bourgeois Swallow est originaire d'Europe de l'Est.

Au moins une des propriétés ou ensembles de propriétés suivants doit être fourni :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- région
- pays
- Latitude et longitude

Définir l'emplacement

Définissez un emplacement géographique pour fournir plus de contexte aux autres SDO.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Emplacements**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour identifier l'emplacement.
Adresse (rue)	Adresse postale que cet emplacement décrit. Cette propriété comprend tous les aspects ou parties de l'adresse postale.
Ville	Ville dans laquelle se trouve cet emplacement.
Code postal	Code postal dans lequel se trouve cet emplacement.
Région	Région dans laquelle se trouve cet emplacement.
Pays	Pays dans lequel se trouve cet emplacement.
Latitude	Latitude de l'emplacement en degrés décimaux. Les nombres positifs décrivent les latitudes au nord de l'équateur et les nombres négatifs décrivent les latitudes au sud de l'équateur. La valeur de cette propriété doit être comprise entre -90,0 et 90,0 respectivement.
Longitude	Longitude de l'emplacement en degrés décimaux. Les nombres positifs décrivent les longitudes à l'est du méridien d'origine et les nombres négatifs les longitudes à l'ouest du méridien d'origine. La valeur de cette propriété doit être comprise entre -180,0 et 180,0 inclus.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Description qui fournit plus de détails et de contexte sur l'ensemble d'intrusions, incluant éventuellement son objectif et ses caractéristiques clés.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'emplacement.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Programme malveillant

Un programme malveillant est un type de TTP qui représente un code malveillant. Il s'agit d'un programme qui est inséré secrètement dans un système. Les logiciels malveillants s'appliquent à STIX 2.x.

L'intention d'un programme malveillant est de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation (OS) de la victime.

Malware SDO caractérise, identifie et catégorise les instances et les familles de logiciels malveillants à partir de données dérivées de l'analyse. Ce SDO capture des informations détaillées sur le fonctionnement du logiciel malveillant et ce qu'il fait.

Définir un programme malveillant

Définissez un programme malveillant qui représente un code malveillant.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Programme malveillant**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom pour identifier l'instance ou la famille de logiciels malveillants, tel que spécifié par le créateur du SDO. Pour une famille de logiciels malveillants, le nom doit être défini.
Premier vu	Heure à laquelle cette instance ou famille de logiciels malveillants a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette instance ou famille de programme malveillant a été vue pour la dernière fois en train d'effectuer des activités malveillantes.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur l'instance ou la famille de logiciels malveillants, y compris potentiellement son but et ses caractéristiques clés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Alias	Noms alternatifs pour identifier cette instance ou famille de logiciels malveillants.
ID source	Identificateur unique de cet objet dans la source de menace.
Est la famille	Spécifie si l'objet représente une famille de programmes malveillants ou une instance de programme malveillant.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au programme malveillant.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Options associées	Répertorie les options identifiées et associées à cet objet.
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Observables associés	Répertorie les observables associés à cet objet.
Programme malveillant associé	Répertorie les programmes malveillants associés identifiés à cet objet.
Systèmes d'exploitation associés	Systèmes d'exploitation sur lesquels l'objet est exécutable. Cela s'applique aussi bien aux systèmes d'exploitation virtualisés qu'à ceux fonctionnant sur du bare metal.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Campagnes	Répertorie les campagnes associées à cet objet.
Déroulement des actions	Répertorie le plan d'actions associé à cet objet qui sont des réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu) pour prévenir une attaque.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Analyse de programme malveillant	Répertorie les enregistrements d'analyse de programme malveillant associés à cet objet.
Observables rapportés	Répertorie les observables signalés dans le cadre de cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

Analyse de programme malveillant

Malware Analysis capture les métadonnées et les résultats d'un malware. L'analyse des logiciels malveillants s'applique à STIX 2.x.

L'analyse de programme malveillant comprend une analyse statique ou dynamique effectuée sur une instance ou une famille de logiciels malveillants.

Définir l'analyse de programme malveillant

Définissez une analyse de programme malveillant qui capture les métadonnées et les résultats d'une analyse statique ou dynamique particulière effectuée sur une instance ou une famille de programmes malveillants.

Avant de commencer

Rôle requis : sn_ti.admin

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Analyse de programme malveillant**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom descriptif pour identifier l'ensemble d'intrusions.
Version du moteur d'analyse	Version du moteur ou du produit d'analyse (y compris les moteurs antivirus) qui a été utilisée pour effectuer l'analyse.
Version de la définition de l'analyse	Version des définitions d'analyse utilisée par l'outil d'analyse (y compris les outils antivirus).
Analyse démarrée	La date et l'heure auxquelles l'analyse de programme malveillant a été lancée.
Analyse terminée	Date et heure auxquelles l'analyse de programme malveillant a été terminée.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Résultat	Le résultat de la classification tel que déterminé par le processus d'analyse du scanner ou de l'outil.
Nom des résultats	Le résultat de classification ou le nom affecté à l'instance de programme malveillant par l'outil de scanner.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'analyse de programme malveillant.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Programme malveillant associé	Répertorie les programmes malveillants associés identifiés à cet objet.
Observables rapportés	Répertorie les observables signalés dans le cadre de cet objet.
Logiciel installé	Répertorie tous les logiciels non standard installés sur le système d'exploitation utilisés pour l'analyse dynamique de l'instance ou de la famille de programmes malveillants.

Données observées

Les données observées transmettent des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX. Les données observées s'appliquent à STIX 2.x.

Les données observées capturent à la fois une observation unique d'une seule entité (fichier, connexion réseau) ainsi que l'agrégation de plusieurs observations d'une entité.

Vous pouvez utiliser les données observées seules (sans relations) pour transmettre des données brutes collectées à partir de n'importe quelle source. Les sources comprennent les rapports d'analyste, les bacs à sable et les outils de détection basés sur le réseau et l'hôte.

Par exemple, les données observées peuvent capturer des informations sur une adresse IP, une connexion réseau, un fichier ou une clé de registre. Les données observées ne sont pas une affirmation de renseignement, ce sont simplement des informations brutes sans aucun contexte pour ce qu'elles signifient.

Définir les données observées

Définissez les données observées qui transmettent des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Données observées**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Premier observé	Heure à laquelle les données ont été vues initialement.
Derniers observés	La dernière fois que les données ont été vues.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nombre observé	Le nombre de fois où chaque objet cyber-observable a été vu. La valeur doit être un entier compris entre 1 et 999 999 999.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux données observées.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Observables associés	Répertorie les observables associés à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.

Acteurs de menace

Les auteurs de menace sont des individus, des groupes ou des organisations qui agissent avec des intentions malveillantes. Les acteurs de menace postulent pour STIX 2.x.

Un acteur de menace n'est pas un ensemble d'intrusion, mais il peut soutenir ou être affilié à divers ensembles d'intrusion, groupes ou organisations au fil du temps.

Les acteurs de menace utilisent leurs ressources, ainsi que les ressources d'un ensemble d'intrusions, pour mener des attaques et mener des campagnes contre des cibles.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez identifier les acteurs de menace en fonction de leurs motivations, de leurs capacités, de leurs objectifs, de leur niveau de sophistication, de leurs activités passées, des ressources auxquelles ils ont accès et de leur rôle au sein de l'organisation.

Définir les acteurs de menace

Définissez les acteurs de menace comme étant des individus, des groupes ou des organisations qui agissent avec des intentions malveillantes.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Acteurs de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom pour identifier l'instance ou la famille de logiciels malveillants, tel que spécifié par le créateur du SDO. Pour une famille de logiciels malveillants, le nom doit être défini.
Premier vu	Heure à laquelle cette instance ou famille de logiciels malveillants a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette instance ou famille de programme malveillant a été vue pour la dernière fois en train d'effectuer des activités malveillantes.
Motivation principale	La raison, la motivation ou l'objectif principal de cet auteur de menace. La motivation est la raison pour laquelle l'auteur de la menace veut atteindre l'objectif (ce qu'il essaie d'atteindre). Par exemple, un acteur de menace dont l'objectif est de perturber le secteur financier d'un pays peut être motivé par une haine idéologique du capitalisme.
Niveau de ressource	Le niveau organisationnel auquel cet acteur de menace travaille habituellement, qui à son tour détermine les ressources dont il dispose pour une utilisation dans une attaque.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur l'acteur de menace, y

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	compris potentiellement son objectif et ses principales caractéristiques.
Alias	Une liste d'autres noms permettant d'identifier cet acteur de menace.
Objectifs	Les objectifs de haut niveau de cet acteur de la menace, c'est-à-dire ce qu'il essaie de faire. Par exemple, ils peuvent être motivés par un gain personnel, mais leur objectif est de voler des numéros de carte de crédit.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'acteur de menace.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Rôles associés	Répertorie les rôles associés à l'acteur de menace.
Motivations de l'attaque associée	Répertorie les motivations de l'attaque associées avec l'acteur de menace.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Regroupements des menaces

Un objet Regroupements de menaces déclare explicitement que les objets STIX référencés ont un contexte partagé. Le regroupement des menaces s'applique à STIX 2.x.

Un objet Regroupements de menaces représente un ensemble de données qui, si elles sont suffisamment analysées, arrivent à maturité pour transmettre un rapport d'incident ou de menace en tant qu'objet de rapport STIX. Par exemple, un regroupement peut être utilisé pour caractériser une enquête en cours sur un événement ou un incident de sécurité.

Un objet Groupes de menaces peut également être utilisé pour affirmer que les objets STIX référencés sont liés à un processus d'analyse en cours. Par exemple, un analyste des menaces peut collaborer avec d'autres membres de sa communauté de confiance pour examiner une série de campagnes et d'indicateurs.

Le SDO de regroupement de menaces contient une liste de références aux SDO, SCO et SRO, ainsi qu'une déclaration explicite du contexte partagé par le contenu, une description textuelle et le nom du groupement.

Définir les regroupements de menaces

Définissez les regroupements de menaces comme des objets qui ont un contexte partagé.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Regroupements des menaces**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Entrez un nom pour identifier le regroupement de menaces.
Contexte	Description du contexte particulier partagé par le contenu référencé par le regroupement.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Description brève qui fournit des détails et un contexte sur le regroupement. Il s'agit notamment de son objectif et de ses caractéristiques clés.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au regroupement de menaces.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Objets groupés	Répertorie les objets regroupés dans le cadre du regroupement de menaces.
Indicateurs groupés	Répertorie les indicateurs regroupés dans le cadre du regroupement de menaces.
Observables groupés	Répertorie les observables regroupés dans le cadre du regroupement de menaces.

Définitions de marquage

L'objet de définitions de marquage représente un marquage spécifique.

Les marques de données représentent les restrictions, autorisations et autres conseils sur la façon dont les données peuvent être utilisées et partagées.

Par exemple, les données peuvent être partagées avec la restriction qu'elles ne doivent pas être repartagées ou qu'elles doivent être chiffrées au repos.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans STIX, les marquages de données sont spécifiés à l'aide de l'objet de définition de marquage. Ces définitions sont appliquées aux objets STIX à l'aide de marquages d'objets et aux propriétés individuelles des objets STIX à l'aide de marquages granulaires.

Définir des définitions de marquage

Définissez des définitions de marquage qui représentent un marquage de données spécifique.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Définitions de marquage**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Définition	Spécifiez l'objet de marquage (exemple, TLP) ou une autre définition de marquage qui a été définie.
Type de définition	Identifie le type de définition de marquage : instruction ou TLP (Traffic Light Protocol).
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la définition de marquage.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Objets marqués	Listes des objets marqués avec la définition de marquage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Indicateurs marqués	Listes d'indicateurs marqués avec la définition de marquage.

Notes de menace

Une note de menace transmet un texte informatif pour fournir une analyse supplémentaire qui n'est pas contenue dans les objets STIX, les objets de définition de marquage ou les objets de contenu linguistique auxquels la note se rapporte. Les notes de menace s'appliquent à STIX 2.x.

Par exemple, un analyste peut ajouter une note à un objet Campaign créé par une autre organisation. La note peut indiquer qu'ils ont vu des messages liés à cette campagne sur un forum de hackers.

Les notes sont généralement créées par des analystes humains et sont composées de texte orienté humain, elles contiennent une propriété supplémentaire pour capturer l'auteur qui a créé la note.

Définir les notes de menace

Définissez les notes de menace qui transmettent des informations pour fournir un contexte ou une analyse supplémentaire qui n'est pas disponible dans les objets existants.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Notes de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Abstrait	Spécifiez un bref résumé du contenu de la note.
Contenu	Spécifie le contenu de la note.
Auteurs	Spécifie le nom de l'auteur (par exemple, un analyste).
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux notes de menace.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Objets associés	Listes des objets auxquels les notes de menace s'appliquent.
Indicateurs associés	Listes d'indicateurs auxquels les notes de menace s'appliquent.
Observables associés	Répertorie les observables associés à cet objet.

Opinions sur la menace

Une opinion est une évaluation de l'exactitude des informations contenues dans un objet STIX produit par une entité différente. Les avis sur les menaces s'appliquent pour STIX 2.x.

La propriété opinion capture le niveau d'accord ou de désaccord à l'aide d'une échelle fixe. L'échelle fixe prend également en charge un mappage numérique pour permettre des opérations statistiques cohérentes entre les opinions.

Par exemple, un analyste d'une organisation consommatrice peut dire qu'il est « fortement en désaccord » avec un objet de campagne et expliquer pourquoi.

Les opinions sont subjectives et le cahier des charges n'aborde pas la meilleure façon de les interpréter.

Les analystes humains créent des opinions et sont composés de texte orienté vers l'humain, ils contiennent une propriété supplémentaire pour capturer l'auteur qui a créé l'opinion.

Définir les opinions sur la menace

Définissez les opinions sur les menaces comme une évaluation de l'exactitude des informations contenues dans un objet STIX.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Opinions sur la menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Avis	L'avis du producteur sur l'objet STIX.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Explication	L'explication du producteur sur l'opinion.
Auteurs	Spécifie le nom de l'auteur (par exemple, un analyste).
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'opinion sur la menace.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Objets associés	Liste des objets auxquels l'opinion de menace s'applique.
Indicateurs associés	Liste des indicateurs auxquels l'opinion sur la menace s'applique.
Observables associés	Répertorie les observables associés à cet objet.

Rapports de menace

Les rapports de menace sont des collections de renseignements sur les menaces axées sur un ou plusieurs sujets. Les rapports de menace s'appliquent pour STIX 2.x.

Les rapports de menace comprennent une description d'un acteur de menace, d'un programme malveillant, d'une technique d'attaque, y compris le contexte et des détails connexes. Ils sont utilisés pour regrouper les renseignements sur les menaces connexes afin qu'ils puissent être publiés sous la forme d'une histoire complète sur les cybermenaces.

Le SDO de rapport de menace contient une liste de références aux objets STIX ainsi qu'une description textuelle et le nom du rapport.

Définir les rapports de menace

Définissez des rapports de menace qui décrivent un acteur de menace, un programme malveillant ou une technique d'attaque, y compris le contexte et les détails connexes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure
1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Rapports de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Spécifiez un nom pour identifier le rapport de menace.
Publié	Date à laquelle ce rapport a été officiellement publié par l'auteur du rapport.
Description	Une description qui fournit des informations et un contexte supplémentaires sur le rapport.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite
Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux rapports de menace.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Objets signalés	Liste des objets signalés dans le rapport de menace.
Indicateurs signalés	Listes des indicateurs signalés dans le rapport sur les menaces.
Observables rapportés	Listes des observables signalés dans le rapport de menace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Perceptions

Les perceptions indiquent qu'un indicateur ou un objet a été vu. Les objets peuvent être un logiciel malveillant, un outil, un acteur de menace, etc.

Les perceptions permettent de suivre qui et quoi est la cible, comment les attaques sont menées et de suivre les tendances du comportement d'attaque.

L'objet de relation de perception contient des propriétés supplémentaires qui ne sont pas présentes dans les objets de relation génériques. Ces propriétés supplémentaires représentent des données spécifiques aux relations de perception.

Par exemple, un décompte ou représenter le nombre de fois que quelque chose a été vu.

L'observation est capturée en tant que relation parce que vous ne pouvez pas avoir une observation à moins que vous n'ayez quelque chose qui a été vu.

- Ce qui a été vu, tel qu'un programme malveillant, une campagne ou un autre SDO
- Qui l'a vu et/ou où il a été vu, représenté comme une identité
- Ce qui a été vu sur les systèmes et les réseaux, représenté comme des données observées

Définir les perceptions d'indicateurs

Définissez les perceptions qui indiquent qu'un indicateur a été vu.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Détections d'indicateurs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Indicateur	Identifie l'indicateur. Recherchez et sélectionnez l'indicateur.
Nombre	Le nombre de fois où l'objet a été vu.
Premier vu	Heure à laquelle cet objet a été vu pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cet objet a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur la perception de l'indicateur, y compris potentiellement son but et ses caractéristiques clés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID source	Identificateur unique de cet objet dans la source de menace.
Est une synthèse	
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la perception d'indicateur.

Listes connexes	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Identités	Liste des identités associées à cet objet.
Données observées	Répertorie les données observées associées à cet objet.

Définir les perceptions d'objets

Définissez la perception d'objet qui décrit qu'un objet (programme malveillant, outil, acteur de menace, entre autres) a été vu.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Détections d'objets**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Objet	Identifie l'objet. Recherchez et sélectionnez l'objet.
Nombre	Le nombre de fois où l'objet a été vu.
Premier vu	Heure à laquelle cet objet a été vu pour la première fois en train d'effectuer des activités malveillantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Dernier observé	Heure à laquelle cet objet a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur l'observation de l'objet, y compris potentiellement son but et ses caractéristiques clés.
ID source	Identificateur unique de cet objet dans la source de menace.
Est une synthèse	
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la perception d'objets.

Listes connexes	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Identités	Liste des identités associées à cet objet.
Données observées	Répertorie les données observées associées à cet objet.

Traduction automatique

Outils

Les outils sont des logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques. Les outils s'appliquent à STIX 2.x.

Les outils vous permettent de savoir comment et quand les auteurs de menace les utilisent pour exécuter des campagnes. Contrairement aux logiciels malveillants, ces outils ou progiciels se trouvent souvent sur un système et ont des objectifs légitimes pour les utilisateurs avancés, les administrateurs, les administrateurs réseau ou même les utilisateurs normaux.

Par exemple, les outils d'accès à distance (RDP) et les outils d'analyse du réseau (Nmap) sont des outils qu'un auteur de menace utilise lors d'une attaque.

Définir des outils

Définissez les outils comme des logiciels légitimes utilisés pour effectuer des attaques.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure
1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Outils**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom descriptif pour identifier l'outil.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur l'outil, y compris éventuellement son objectif et ses caractéristiques clés.
Alias	Noms alternatifs permettant d'identifier cet outil.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite
Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'objet outil.

Liens connexes et listes connexes	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Déroulement des actions	Répertorie le plan d'actions associé à cet objet qui sont des réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu) pour prévenir une attaque.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.

Traduction automatique

Vulnérabilités

Une vulnérabilité est une faiblesse ou un défaut d'un composant logiciel ou matériel que les attaquants exploitent. Les vulnérabilités s'appliquent à STIX 2.x.

La faiblesse ou le défaut réside dans les exigences, les conceptions ou les implémentations du code que l'on trouve dans un composant logiciel ou matériel. Cette faiblesse est directement exploitée pour avoir un impact négatif sur la confidentialité, l'intégrité ou la disponibilité de ce système.

CVE est une liste des vulnérabilités et des expositions liées à la sécurité de l'information qui fournit des noms communs pour les problèmes connus du public [CVE].

Par exemple, si un programme malveillant exploite CVE-2015-12345, un objet malveillant peut être lié à un objet de vulnérabilité qui fait référence à CVE-2015-12345.

Définir les vulnérabilités

Définissez la vulnérabilité comme une faiblesse ou un défaut dans un composant logiciel ou matériel que les attaquants exploitent.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure
1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Vulnérabilités**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom descriptif pour identifier la vulnérabilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur la vulnérabilité, y compris potentiellement son objectif et ses caractéristiques clés.
Alias	Noms alternatifs permettant d'identifier cet outil.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite
Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'objet de vulnérabilité.

Liens connexes et listes connexes	Description
Afficher les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. Afficher les relations n'apparaît que lorsque l'objet a un objet associé.
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Déroulement des actions	Répertorie le plan d'actions associé à cet objet qui sont des réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu) pour prévenir une attaque.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Relations

Utilisez les objets de relation pour relier deux SDO ou objets cyber-observables (SCO) STIX afin de décrire leurs relations l'un avec l'autre.

Les objets de relation STIX (SRO) représentent les types de relations entre divers objets STIX. Les objets de relation suivants sont disponibles :

- **Relation objet-objet** : cet objet définit les relations entre les SDO, à l'exception de l'objet indicateur. Un exemple de relation définie objet-objet est qu'un modèle d'attaque délivre un programme malveillant.
- **Relation objet-indicateur** : cet objet définit les relations entre l'objet indicateur et d'autres SDO. Un exemple de relation objet - indicateur est qu'un indicateur détecte des preuves d'une campagne.
- **Relation objet-observable** : cet objet définit les relations entre les SDO et l'objet observable (SCO). Un exemple de relation définie objet-observable est qu'une infrastructure est constituée d'objets cyber-observables qui fournissent des informations sur une attaque potentielle.

Relations d'objet STIX

Objet de relation	Source de l'exemple	Exemple de cible	Exemple de description
Relations objet-objet	Modèle d'attaque	Programme malveillant	Cette relation décrit que ce modèle d'attaque est utilisé pour diffuser cette instance (ou famille) de programme malveillant.
Relations objet-indicateur	Indicateur	Modèle d'attaque, Campagne,	Cette relation décrit le fait que

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Relations d'objet STIX (suite)

Objet de relation	Source de l'exemple	Exemple de cible	Exemple de description
		Infrastructure, Ensemble d'intrusions, Programme malveillant, Acteur de menace, Outil	l'indicateur peut détecter des preuves du modèle d'attaque, de la campagne, de l'infrastructure, de l'ensemble d'intrusions, du programme malveillant, de l'acteur de menace ou de l'outil associé. Il se peut que la preuve ne soit pas directe. Par exemple, l'indicateur peut détecter des preuves secondaires de la campagne, telles que des programmes malveillants couramment utilisés par cette campagne particulière.
Relations objet-observable	Infrastructure	Données observées	Cette relation décrit que l'indicateur est créé en fonction des informations provenant d'un objet de données observé. Un exemple de relation définie objet-observable est qu'une infrastructure est constituée d'objets cyber-observables qui fournissent des informations sur une attaque potentielle.

Traduction automatique

Définir des relations objet-objet

Définissez les relations entre les SDO, à l'exception de l'objet d'indicateur.

Avant de commencer

Rôle requis : sn_ti.admin

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Objet-Objet-Relations**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Objet source	Sélectionnez et définissez l'objet source.
Type de l'objet source	Définit le type d'objet source.
Objet cible	Sélectionnez et définissez l'objet cible.
Type de l'objet cible	Définit le type d'objet cible.
Type de relation	Une description qui fournit plus de détails et de contexte sur le type de relation.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identifie de manière unique l'objet source.

4. Cliquez sur **Envoyer**.

Définir des relations objet-indicateur

Définissez les relations entre l'objet de l'indicateur et d'autres SDO.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Objet-Indicateur-Relations**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Objet	Sélectionnez et définissez l'objet.
Type	Spécifie le type d'objet en fonction de l'objet que vous avez sélectionné.
Indicateur	Sélectionnez les indicateurs de compromission.
Sens de la relation	Définissez le sens de la relation, qu'il soit direct ou inverse.
Type de relation	Une description qui fournit plus de détails et de contexte sur le type de relation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identifie de manière unique l'objet source.

4. Cliquez sur **Envoyer**.

Définir des relations objet-observable

Définissez les relations entre les SDO et l'objet observable (SCO).

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel IoC** > **Relations objet-observable**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Objet	Sélectionnez et définissez l'objet source.
Type	Entrez un nom descriptif pour identifier le type d'objet.
Observable	Sélectionnez et définissez l'observable.
Type de relation	Une description qui fournit plus de détails et de contexte sur le type de relation.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identifie de manière unique l'objet source.

4. Cliquez sur **Envoyer**.

Visualiseur STIX

Le visualiseur STIX représente visuellement la structure de l'objet STIX et sa relation.

Vous pouvez obtenir plus d'informations sur l'objet ou la relation sélectionné dans le volet de détails.

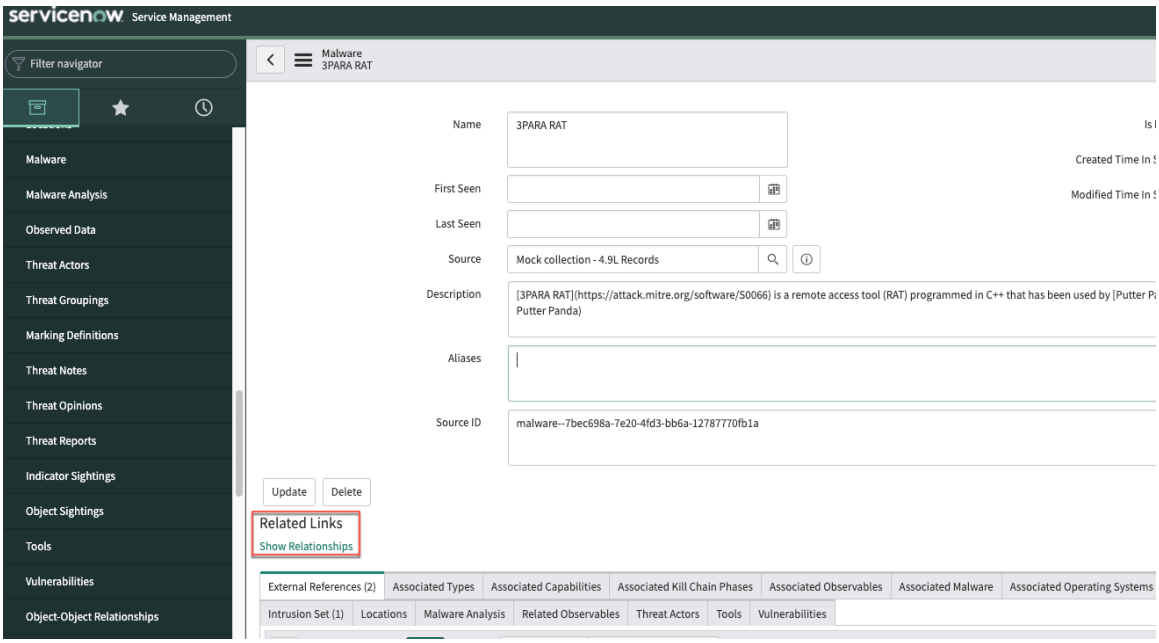
Le graphe des relations montre les relations d'un objet et fournit un contexte pour vous permettre d'examiner la situation. Vous pouvez cliquer sur n'importe quel nœud du graphique pour afficher plus de détails.

Remarque : Le visualiseur STIX est disponible pour tous les SDO, à l'exception des objets Rapport et Données observées.

Traduction automatique

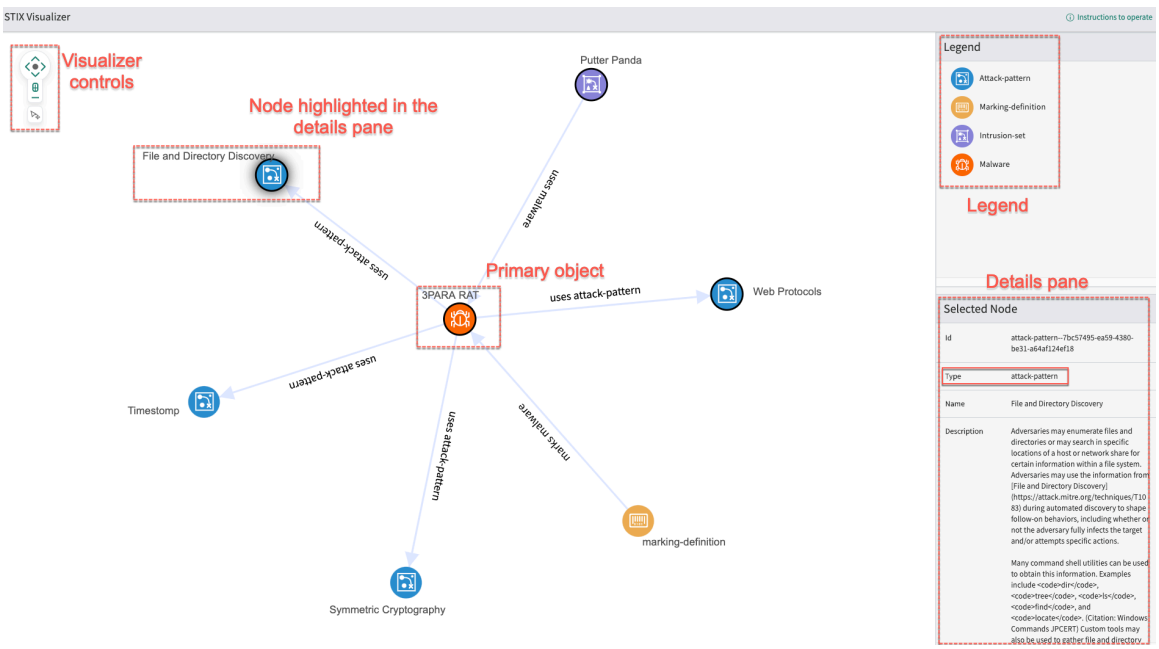
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accéder au visualiseur STIX



Cliquez sur Afficher les relations dans la section Liens connexes pour l'un des SDO afin d'afficher le visualiseur STIX.

Afficher les détails dans STIX Visualizer



Dans le visualiseur, vous pouvez afficher l'objet et sa relation, ce qui vous fournit un contexte vous permettant d'approfondir vos recherches. Le visualiseur utilise des couleurs et des icônes pour illustrer diverses informations sur les objets.

Vous pouvez effectuer un zoom avant sur un objet, faire glisser les nœuds ou les épingler pour mettre en évidence une relation particulière.

Cliquez sur n'importe quel objet pour ouvrir le volet de détails. Dans le volet de détails, vous pouvez obtenir plus d'informations associées à l'objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MITRE-ATT&CK™ Vue d'ensemble du cadre de travail

Le MITRE-ATT&CK cadre de travail est une base de connaissances des tactiques, des techniques et des procédures courantes (TTP) auxquelles votre organisation peut accéder pour développer des modèles de menaces et des méthodologies spécifiques contre les cyberattaques.

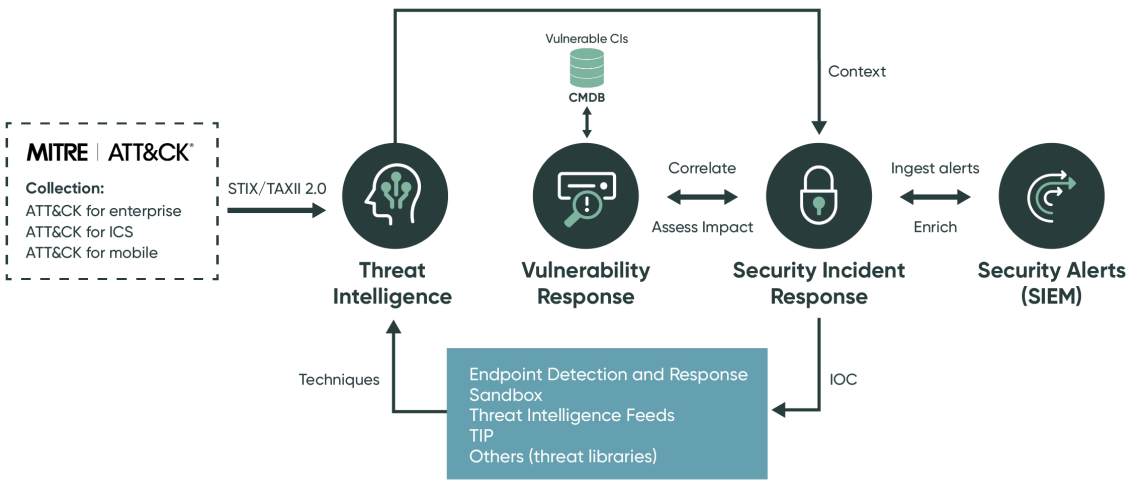
Vue d'ensemble

Le MITRE cadre de travail ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) documente et suit les différentes techniques des adversaires qui sont utilisées au cours des différentes étapes d'une cyberattaque.

En utilisant la MITRE-ATT&CK base de connaissances du cadre, la communauté des renseignements sur les cybermenaces peut rapidement identifier les menaces et coordonner les réponses aux cyberattaques.

MITRE-ATT&CK et Security Operations

Consultez le diagramme suivant pour savoir comment les informations circulent avec Opérations de sécurité les MITRE-ATT&CK applications.



- Le champ préchargé TAXII client se connecte au TAXII serveur pour ingérer les collections de données vers Renseignements sur les menaces.
- Les intégrations SIEM (Security Information and Event Manager) existantes ingèrent leurs données sur les menaces (alertes et événements) avec des TTP pertinents et sont associées à des incidents de sécurité.
- Lorsqu'un IoC est associé à un incident de sécurité, Renseignements sur les menaces recherche automatiquement des informations pertinentes dans les flux de menaces et envoie les IoC à des sources tierces telles que EDR, Sandbox ou TIP pour une analyse supplémentaire.
- Si une source tierce contient l'information MITRE-ATT&CK , Renseignements sur les menaces Extrait les informations sur la technique et enrichit les données du référentiel à des Renseignements sur les menaces fins de corrélation et d'analyse.
- MITRE-ATT&CK partage également des informations de contexte CVE pour chaque technique. Votre équipe de sécurité peut examiner les techniques Réponse aux vulnérabilités exploitées afin de déterminer si vos actifs critiques sont menacés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MITRE-ATT&CK Matrices, tactiques et techniques

Le cœur du MITRE-ATT&CK cadre est une matrice de tactiques et de techniques de l'adversaire. La séquence de la tactique représente ce qu'un adversaire tente d'accomplir au stade d'un incident. Lorsque votre équipe de sécurité comprend cette séquence, vous avez la possibilité d'anticiper le prochain mouvement d'un adversaire et de briser la chaîne de destruction. ATT&CK se compose des matrices suivantes :

- ATT&CK d'entreprise : décrit les comportements et les actions qu'un adversaire adopte pour compromettre et opérer dans un réseau d'entreprise et dans le cloud.

  Remarque : La matrice pré-ATT&CK a été déconseillée par MITRE la matrice Enterprise et a été fusionnée avec elle.

- ICS ATT&CK : décrit les actions qu'un adversaire effectue lorsqu'il opère au sein d'un réseau de systèmes de contrôle industriel (ICS).
- Mobile ATT&CK : décrit les comportements et les actions des adversaires qui se concentrent sur les équipements mobiles.

La tactique représente le pourquoi d'une technique ATT&CK. C'est l'objectif tactique de l'adversaire pour effectuer une action.

Les techniques représentent la façon dont un adversaire atteint un objectif tactique en effectuant une action.

Les techniques peuvent être associées à plus d'une tactique. Par exemple, la manipulation des jetons d'accès est utilisée par un adversaire pour utiliser la tactique d'escalade de privilèges ou d'évasion de défense.

Utilisation d'une approche basée sur l'intention pour les réponses aux incidents

Une réponse basée sur l'intention utilise un cadre de kill chain dynamique et contextuel qui peut aider votre organisation à corréler les incidents de sécurité et à identifier un large éventail d'attaques. Votre équipe de sécurité peut utiliser une réponse basée sur l'intention pour comprendre comment l'organisation est attaquée et ce que l'attaquant pourrait faire ensuite. Ce type de réponse vous permet de prédire le comportement d'un attaquant afin de concentrer efficacement vos ressources.

À l'aide Réponse aux incidents de sécuritéde , votre équipe de sécurité peut gérer le cycle de vie de chaque incident de sécurité, de l'analyse au confinement, en se concentrant sur les indicateurs de compromission (IOC) tels que les adresses IP, les hachages de fichiers et les domaines.

Grâce à leur intégration Réponse aux incidents de sécurité au cadre de travail, les incidents de sécurité sont traités comme des liens dans une attaque plus vaste à l'échelle de l'entreprise MITRE-ATT&CK .

Comment votre organisation peut-elle bénéficier de MITRE-ATT&CK Security Operations ?



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'utilisation du MITRE-ATT&CK cadre de travail peut aider votre organisation à effectuer les opérations suivantes :

- Équipez les analystes de sécurité de MITRE-ATT&CK tactiques, de techniques et de procédures (TTP) pour mieux analyser les incidents de sécurité et y répondre.
- Automatisez les workflows d'incident à l'aide du playbook pour détecter et contenir les menaces dans le MITRE-ATT&CK contexte du cadre de travail.
- Hiérarchisez les indicateurs de compromission et la chasse aux menaces à l'aide MITRE-ATT&CK d'informations.
- Comprenez la posture de sécurité de haut niveau de votre organisation dans le MITRE-ATT&CK contexte du cadre de travail.

Administration MITRE-ATT&CK

Vous pouvez configurer, mapper des sources de données, mapper la couverture globale de détection des techniques et gérer le MITRE-ATT&CK référentiel dans le Now Platformfichier .

Introduction à Framework MITRE-ATT&CK

Passez en revue les informations suivantes avant de commencer à configurer votre MITRE-ATT&CK cadre de travail.

Liste de vérification

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles , Renseignements sur les menaceset Réponse aux incidents de sécurité et requisNow Platform.	Les rôles suivants sont utilisés dans les MITRE-ATT&CK fonctionnalités : • L'administrateur (admin) installe les applications à partir des rôles d'administrateur ServiceNow Store d'incident de sécurité (sn_si.admin) et d'administrateur de Threat Intelligence (sn_ti.admin) et les affecte. • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.read • sn_ti.write • sn_ti.mitre_analyst : le rôle d'analyste MITRE a été introduit pour permettre la navigation croisée pour les MITRE fonctionnalités entre Réponse aux incidents de sécurité et Threat Intelligence Support Common. Avec ce rôle, vous pouvez afficher à la fois le module et le Renseignements sur les menaces MITRERéponse aux incidents de sécurité module en mode lecture seule. • sn_si.read

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	Pour plus d'informations, consultez Configurer Threat Intelligence.
Vérifiez que les ServiceNow applications de base requises pour prendre en charge le MITRE-ATT&CK module sont installées et activées.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. • Prise en charge de Threat Intelligence Composants courants de l'interface utilisateur (sn_ti_seismic) : version 1.0 ou supérieure • Support commun de Threat Intelligence : version 12.0 ou supérieure • Renseignements sur les menaces - Version 12.0 ou ultérieure • Réponse aux incidents de sécurité - Version 12.0 ou ultérieure Pour plus d'informations sur la configuration de votre Now Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une application Security Operations et activer une application ServiceNow Store.
Séparation de domaine	Vérifiez la section Séparation de domaine si vous avez l'intention de séparer les données, les processus et les tâches administratives.

Comprendre le MITRE modèle de données de destination STIX

Passez en revue la terminologie utilisée par MITRE et STIX pour utiliser et comprendre efficacement le MITRE-ATT&CK™ cadre de travail dans le Now Platform.

MITRE Objets à STIX mapper

STIX est un langage permettant de décrire les informations sur les cybermenaces de manière normalisée et structurée. Le modèle de données parent dans le Renseignements sur les menaces module sont les STIX objets. Alors que les MITRE objets sont un sous-ensemble du modèle de données parent STIX . Dans le MITRE-ATT&CK cadre, MITRE fournit des informations similaires STIX avec certaines étiquettes et certains objets.

MITREvers le mappage d'objets STIX

Terminologie de MITRE	Terminologie de STIX
Technique	Modèle d'attaque
Atténuation	Déroulement de l'action

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MITREvers le mappage d'objets STIX (suite)

Terminologie de MITRE	Terminologie de STIX
Groupes	Ensembles d'intrusion
Programme malveillant	Programme malveillant
Outil	Outil

Extension des données dans le Renseignements sur les menaces module

Vous pouvez tenir à jour une liste des sources de Renseignements sur les menaces menace et importer les données nécessaires STIX , y compris un ensemble complet d'informations sur les cybermenaces. Vous pouvez également utiliser les profils pour faciliter l'échange automatisé d'informations sur les TAXII cybermenaces.

Remarque : Pour plus d'informations, consultez Définir une source de menace et créer un profil TAXII.

Extension des données dans le MITRE-ATT&CK module

Vous pouvez étendre les objets Malware, Group, Atténuation et Outil à une technique du MITRE-ATT&CK référentiel.

Vous pouvez créer un objet et établir une relation entre une technique et le nouvel objet dans le module Référentiel MITRE ATT&CK, mais vous ne pouvez pas définir le type de relation dans ce module. Pour définir un type de relation, accédez à l'icône **Renseignements sur les menaces** > **Référentiel IoC** > **Relations objet-objet** module.

Si vous mappez le type de relation entre une technique existante et un objet existant, vous devez définir la technique en tant qu'objet cible et l'objet en tant qu'objet source. Pour ce faire, accédez à l'onglet **Référentiel IoC** > **Relations objet-objet** module.

Vous pouvez créer un groupe et l'associer à un modèle d'attaque, mais dans le référentiel MITRE ATT&CK, vous pouvez uniquement établir la relation entre le groupe et le modèle d'attaque. Pour définir le type de relation objet à objet, vous devez le faire dans le référentiel IoC.

Remarque : Pour plus d'informations, consultez étendre MITRE-ATT&CK données et IoC.

Séparation de domaine et MITRE-ATT&CK

Cette vue d'ensemble de Séparation de MITRE-ATT&CKdomaine concerne . Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Support : basique.

Comment fonctionne Séparation de domaine avec MITRE-ATT&CK

Procédez comme suit pour réaliser Séparation de domaine :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Créez un utilisateur avec les rôles sn_ti.admin requis dans le domaine respectif.
- Répliquez les éléments suivants pour chaque domaine :
  - TAXII Collections

    Remarque :

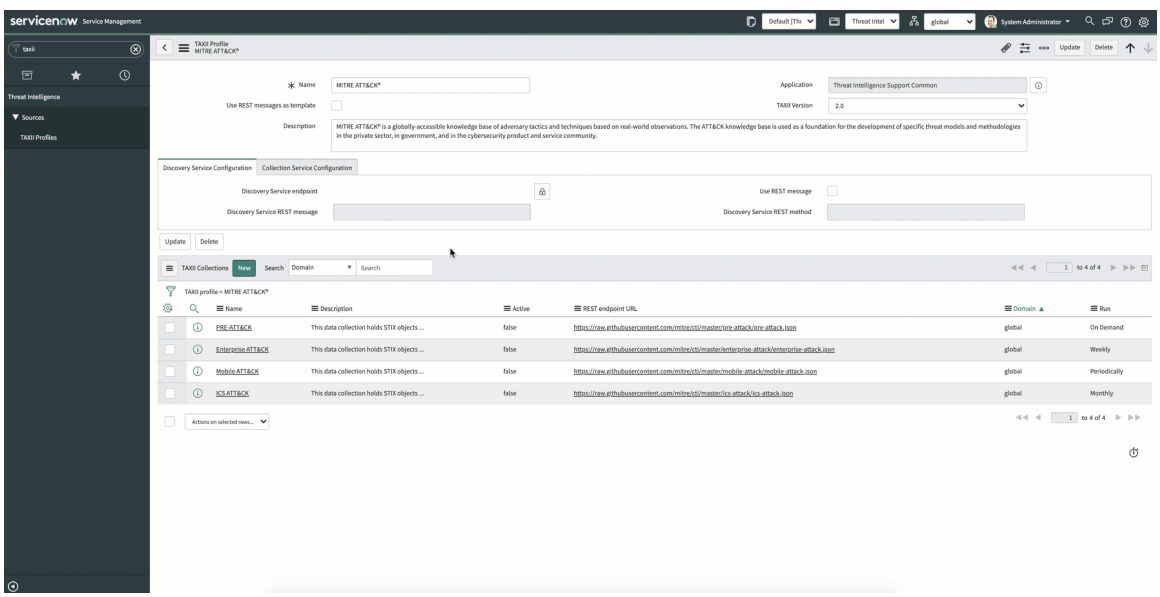
    - N'activez pas les collections dans le domaine global. N'activez que les collections répliquées et disponibles dans votre domaine.
    - Modifiez le champ **Exécuter en tant que** dans les collections sur l'utilisateur ayant le rôle sn_ti.admin dans le domaine respectif.

  - Définition de couverture de la technique
  - Règle d'extraction de la technique
  - Règles de détection : Mappages MITRE ATT&CK
  - Couverture d'atténuation
    - Copiez tous les enregistrements de définition de couverture d'atténuation.
    - Copiez le calculateur d'atténuation de la couverture ou créez un nouveau calculateur pour le domaine concerné.
  - Groupe de menaces : définitions de la carte thermique de la technique

Reproduire la collection TAXII

1. Accédez à la **Renseignements sur les menaces** > **Sources** > **Profils TAXII**.
2. Dans la barre d'en-tête, utilisez le sélecteur de domaine pour sélectionner votre domaine.
3. Sélectionnez la collection TAXII pertinente pour votre organisation (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).
4. Cliquez avec le bouton droit de la souris dans la barre d'en-tête et sélectionnez **Insérer et rester**. La collection TAXII en double est créée sous le domaine sélectionné
5. Revenez au profil TAXII MITRE ATT&CK pour afficher la collection TAXII en double.

L'illustration suivante montre comment sélectionner le domaine TOP/Initech, répliquer la collection TAXII dans le domaine et vérifier la collection TAXII répliquée.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer le MITRE-ATT&CK™ cadre de travail

Activez le MITRE-ATT&CK profil et configurez une tâche planifiée afin de pouvoir configurer MITRE-ATT&CK des collections pour la détection des menaces dans votre organisation.

Avant de commencer

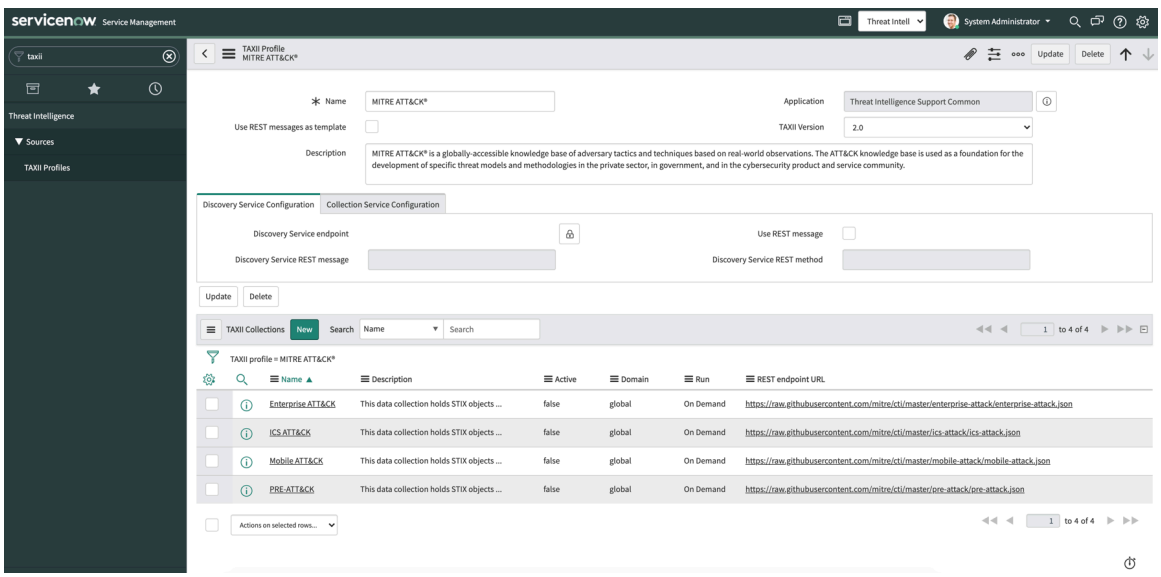
Rôle requis : sn_ti.admin

Pourquoi et quand exécuter cette tâche

L'expression structurée d'information sur les menaces (STIX™ Structured Threat Information Expression) est un langage permettant de décrire les informations sur les cybermenaces de manière standardisée et structurée. À l'aide des données STIX et des profils d'échange automatisé d'informations sur les indicateurs (TAXII™ Trusted Automated Exchange), les équipes de sécurité peuvent utiliser les informations partagées sur les cybermenaces pour isoler les menaces qui ont été précédemment identifiées par votre entreprise et provenant d'autres sources.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Sources** > **Profils TAXII**. Les profils disponibles TAXII s'affichent.
2. Cliquez sur le profil **MITRE ATT&CK** fourni avec le système de base.



3. Pour activer la TAXII collecte, définissez l'option **Actif** sur vrai pour la collection qui est pertinente pour votre TAXII organisation (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).

Collecte TAXII	Description
ATT&CK d'entreprise	Décrit les comportements et les actions qu'un adversaire adopte pour compromettre et opérer dans un réseau d'entreprise et dans le cloud.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Collecte TAXII	Description
	Remarque : La matrice pré-ATT&CK a été déconseillée par MITRE la matrice Enterprise et a été fusionnée avec elle.
Mobile ATT&CK	Décrit les comportements et les actions des adversaires qui se concentrent sur les équipements mobiles.
ICS ATT&CK	Décrit les actions entreprises par un adversaire lorsqu'il opère au sein d'un réseau de systèmes de contrôle industriel (ICS).

4. Pour actualiser périodiquement la collection, définissez l'option **Exécuter** selon les besoins de votre organisation.
Par défaut, cette option est définie sur Sur demande.

Remarque :

a. Les collections sont empaquetées dans le cadre du module d'extension Renseignements sur les menaces Core. L'installation ou la mise à jour de Threat Intelligence Support Common : version 12.0 ou supérieure et de Threat Intelligence : version 12.0 ou supérieure garantit que vos données de collecte sont renseignées automatiquement.

b. Activez la TAXII collection uniquement pour la collection que vous avez l'intention d'utiliser dans votre organisation et désactivez les autres collections. Par exemple, si vous avez l'intention d'utiliser la matrice ATT&CK d'entreprise, activez ATT&CK d'entreprise au niveau de la TAXII collection et au niveau des matrices . Désactivez les autres matrices Mobile ATT&CK et ICS ATT&CK au niveau de la TAXII collection et au niveau des matrices.

c. Dans les TAXII listes connexes Collectes, si vous sélectionnez l'option Exécuter sur Quotidien, une erreur se produit et l'option par défaut est Sur demande. Cette erreur se produit car la planification quotidienne de l'actualisation MITRE-ATT&CK des données est restreinte afin d'optimiser la charge sur les MITRE serveurs. De plus, MITRE les données ATT&CK ne sont mises à jour que deux fois par an.

d. Les TAXII collections ne sont pas actualisées tant que vous ne l'activez pas TAXII .

e. Les mises à jour des collections existantes peuvent être récupérées à partir du MITRE serveur en programmant la fréquence d'exécution dans chaque collection.

f. Les personnalisations que vous apportez aux données du MITRE-ATT&CK référentiel (objets Logiciel malveillant, Groupe, Atténuation et Outil à une technique) sont enregistrées lors des mises à jour planifiées.

g. MITRE Met à jour la base de MITRE-ATT&CK connaissances dans laquelle certains objets sont identifiés comme révoqués ou obsolètes, de nouveaux objets sont ajoutés ou des objets existants sont modifiés. En cas MITRE de révocation d'une tactique ou d'une technique, ces objets sont marqués comme révoqués dans le Now Platformfichier . Les objets révoqués sont conservés dans le référentiel mais ne peuvent pas être utilisés dans le Now Platformfichier .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Une fois la configuration du profil TAXII terminée, les MITRE-ATT&CK données du référentiel sont importées à intervalles réguliers dans le Now Platform®fichier . Vous pouvez afficher ces données en accédant à **Référentiel MITRE ATT&CK** > **Matrices** et **Référentiel MITRE ATT&CK** > **Techniques**.

Gérer les matrices

Gérez les matrices qui ont été importées à partir des MITRE TAXII collections. Les matrices sont un ensemble de tactiques et de techniques. Vous pouvez afficher les matrices à examiner si vos collections sont disponibles dans le MITRE-ATT&CK référentiel.

Avant de commencer

Remarque : Examinez et vérifiez que seule la matrice que vous avez l'intention d'utiliser dans votre organisation est définie sur active et désactivez les autres matrices. Par exemple, si vous avez l'intention d'utiliser la matrice ATT&CK d'entreprise, la matrice ATT&CK d'entreprise est activée au niveau de la collecte TAXII et au niveau des matrices. Désactivez les autres matrices Mobile ATT&CK et ICS ATT&CK au niveau de la TAXII collection et au niveau des matrices.

Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Procédure

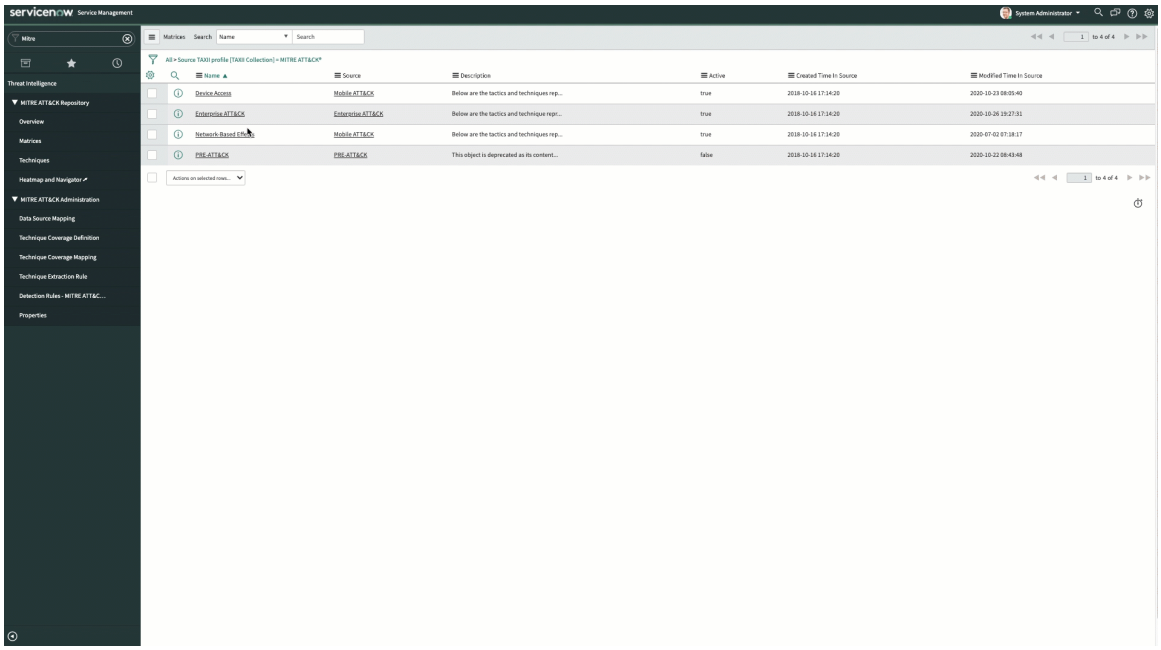
1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Matrices**.
   Toutes les matrices sont désactivées par défaut.
2. Pour activer une matrice, pointez sur **Actif**, double-cliquez et sélectionnez **vrai**.
3. Pour afficher toutes les informations associées, cliquez sur une matrice.
4. Pour afficher toutes les tactiques associées à cette collection, cliquez sur l'onglet **Tactiques MITRE** .
5. Pour afficher des détails supplémentaires et les techniques associées à une tactique sélectionnée, cliquez sur une tactique.
6. Sous l'onglet **Techniques MITRE ATT&CK** , sélectionnez une technique.
7. Dans les listes connexes, affichez les associations disponibles pour la technique que vous avez sélectionnée.

   Dans l'illustration suivante, vous pouvez voir le chemin de navigation de la matrice ATT&CK d'entreprise à la tactique d'accès initial (TA0001), puis à la technique d'hameçonnage (T1566). Sur la page Modèle d'attaque - Technique d'hameçonnage, vous pouvez afficher

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

la liste connexe - Tactique, Sous-technique, Groupe, Atténuation, Références externes, Logiciel malveillant et Outils.



Que faire ensuite

Vous pouvez étendre les informations de certains de ces objets de liste connexes en fonction de la technique que vous avez sélectionnée. Par exemple, vous pouvez ajouter de nouvelles informations pour Groupe, Atténuation, Références externes, Programme malveillant et Outils.

Gérer les techniques

Gérer les techniques qui ont été importées des MITRE TAXII collections. Les techniques contiennent différentes façons dont les attaquants se sont développés pour employer une tactique donnée. Vous pouvez examiner et désactiver les techniques qui ne sont pas pertinentes pour votre organisation. En STIX, les techniques sont connues sous le nom de schémas d'attaque.

Avant de commencer

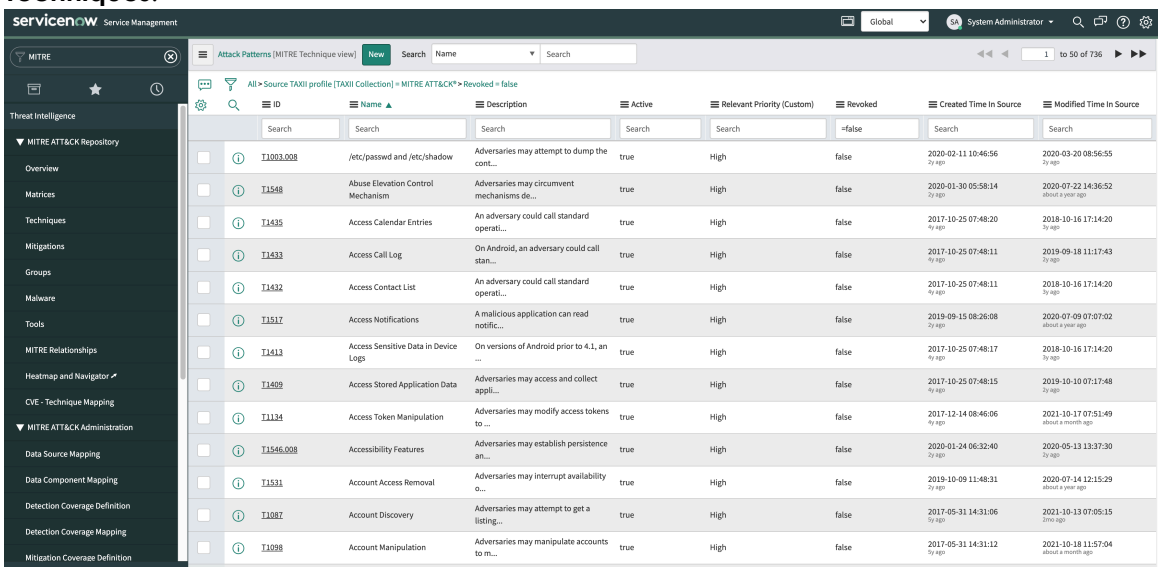
Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Techniques**.



La liste des techniques et sous-techniques est maintenant répertoriée.

2. Pour examiner et désactiver les techniques qui ne sont pas pertinentes pour votre organisation, accédez à la vue de liste pour la technique sélectionnée et, dans la colonne Actif, mettez à jour le paramètre sur **faux** et enregistrez-le.
   Désactivez les techniques qui ne sont pas utilisées par les autres objets du MITRE-ATT&CK référentiel.

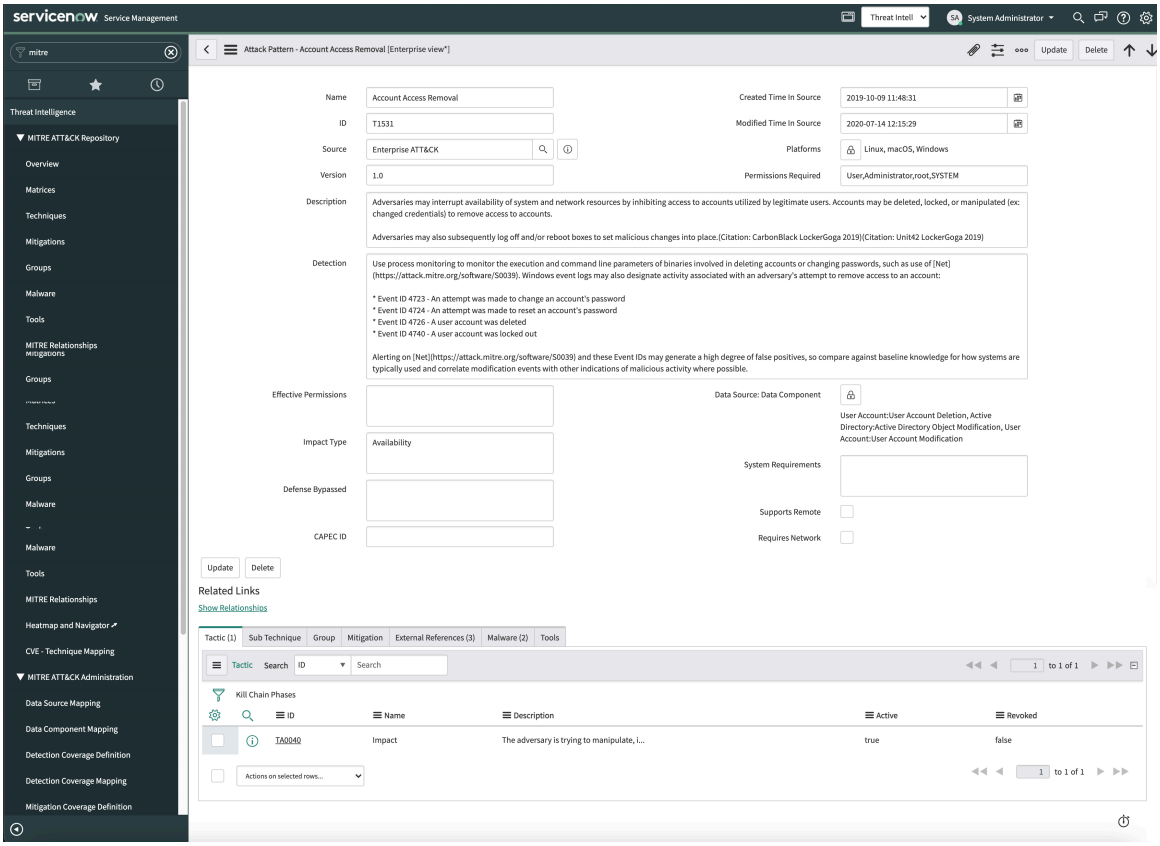
3. Pour prioriser une technique, affectez une priorité dans le champ **Priorité pertinente (personnalisée**).
   La priorité pertinente du système de base est définie sur aucune. Le champ **Priorité pertinente (personnalisé)** n'est MITRE-ATT&CK TAXII pas importé des collections, mais un champ personnalisé introduit dans le Now Platformfichier . Vous pouvez utiliser les informations de priorité pertinentes pour filtrer et hiérarchiser les techniques dans les tableaux de bord, pendant le mappage des sources de données ou lors de l'analyse de la carte thermique.

4. Cliquez sur une technique pour afficher toutes les informations associées à cette technique.

   Dans l'illustration suivante, vous pouvez afficher les détails de chaque technique de suppression d'accès au compte, son ID, sa source et d'autres informations connexes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : L'élément Source de données : composant de données introduit par MITRE remplace le champ Source de données précédent. Le composant de données fournit une sous-couche supplémentaire de contexte aux sources de données. Si votre MITRE-ATT&CK référentiel contient les anciennes TAXII collections, vous pouvez afficher le champ Source de données. Sinon, vous pouvez afficher les sources de données avec le contexte supplémentaire des composants de données dans le champ Source de données : composant de données. Vous pouvez afficher le nouveau champ de composant de données uniquement lorsque la source est Enterprise ATT&CK. Pour plus d'informations, consultez Mappage des composants de données.

5. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Vous pouvez étendre les informations dans certains de ces objets de liste connexes. Par exemple, vous pouvez ajouter de nouvelles informations pour le groupe, l'atténuation et les références externes.

Gérer les atténuations

Gérez les atténuations qui ont été importées à partir des MITRE TAXII collections. Les atténuations vous permettent d'empêcher un adversaire d'exécuter avec succès des techniques ou des sous-techniques contre votre organisation. En STIX, les mesures d'atténuation sont connues sous le nom de plan d'actions.

Avant de commencer

Rôle requis :

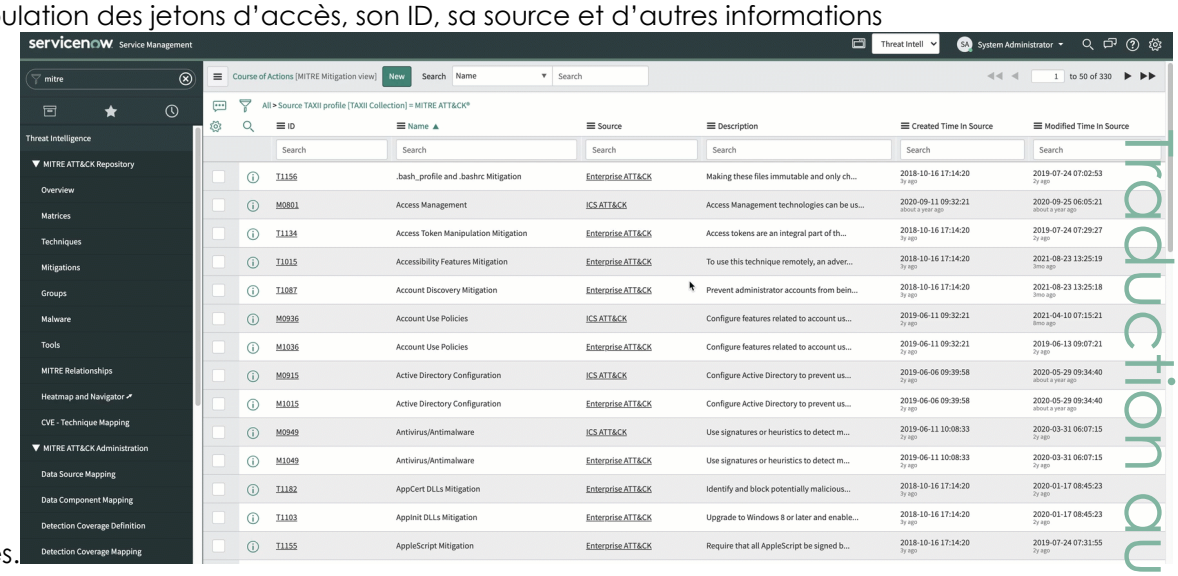
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_ti.admin : supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Atténuations**.
   Les mesures d'atténuation sont maintenant répertoriées.
2. Cliquez sur une atténuation pour afficher toutes les informations associées.
   Dans l'illustration suivante, vous pouvez afficher les détails de l'atténuation de la manipulation des jetons d'accès, son ID, sa source et d'autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Utilisez le module Techniques pour ajouter ou modifier les données d'atténuations.

Gérer les groupes

Gérez les groupes qui ont été importés à partir des MITRE TAXII collections. Les groupes sont des ensembles d'activités d'intrusion connexes qui sont suivis par un nom commun dans la communauté de sécurité. Les analystes suivent les grappes d'activités à l'aide de divers termes tels que groupes de menaces, groupes d'activités, acteurs de menace, ensembles d'intrusion et campagnes. Dans STIX, les groupes sont connus sous le nom d'ensembles d'intrusion.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

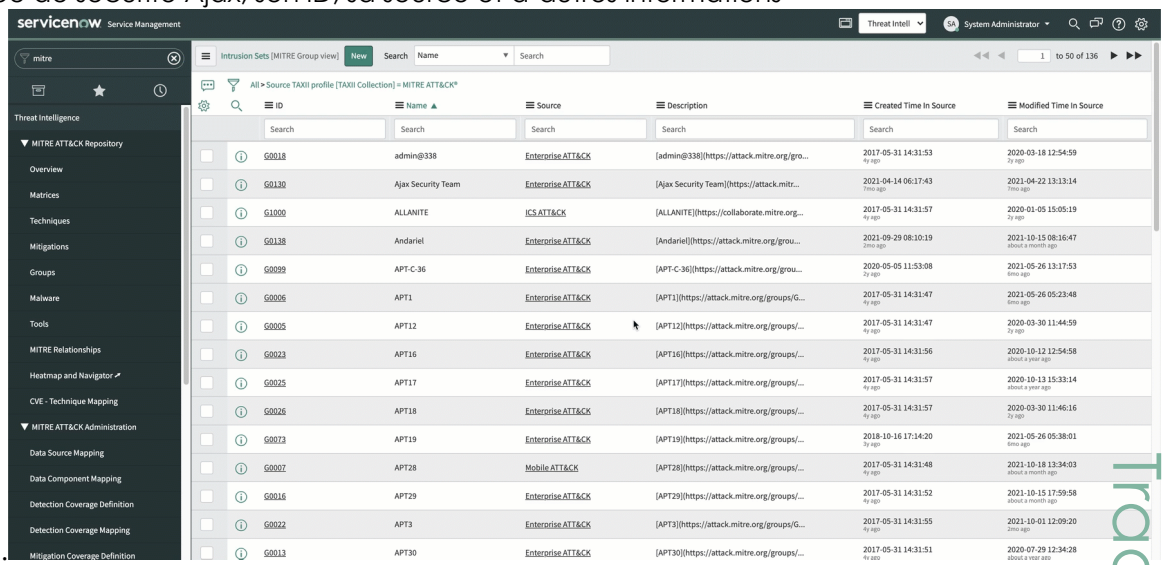
Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Groupes**.
   Vous pouvez afficher les groupes répertoriés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Cliquez sur un groupe pour afficher toutes les informations associées.
   Dans l'illustration suivante, vous pouvez afficher les détails du groupe de l'équipe de sécurité Ajax, son ID, sa source et d'autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

> **Remarque :** Pour associer les groupes de menaces à un ticket de sécurité pour une enquête plus approfondie, cliquez sur **Ajouter au ticket de sécurité**.

Que faire ensuite

Utilisez le module de techniques pour ajouter ou modifier les données des groupes.

Gérer les programmes malveillants

Gérez les informations sur les programmes malveillants que vous avez importées à partir des MITRE TAXII collections. Un programme malveillant est un type de TTP qui représente un code malveillant. Il s'agit d'un programme qui est inséré secrètement dans un système. L'intention d'un programme malveillant est de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation (OS) de la victime.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

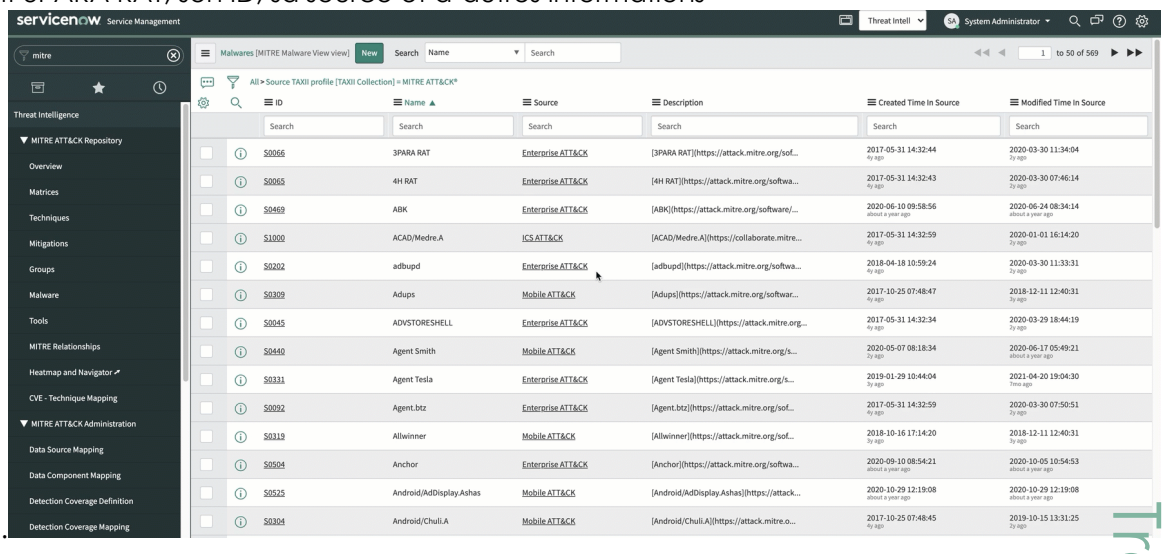
Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Programme malveillant**.
   Vous pouvez afficher les programmes malveillants répertoriés.
2. Cliquez sur un programme malveillant pour afficher toutes les informations associées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'illustration suivante, vous pouvez afficher les détails du programme malveillant 3PARA RAT, son ID, sa source et d'autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Utilisez le module Techniques pour ajouter ou modifier les données de logiciels malveillants.

Gérer les outils

Gérez les informations sur les outils que vous avez importées des MITRE TAXII collections. Les outils sont des logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Pourquoi et quand exécuter cette tâche

Les outils vous permettent de savoir comment et quand les auteurs de menace les utilisent pour exécuter des campagnes. Contrairement aux logiciels malveillants, ces outils ou progiciels se trouvent souvent sur un système et ont des objectifs légitimes pour les utilisateurs avancés, les administrateurs, les administrateurs réseau ou même les utilisateurs normaux.

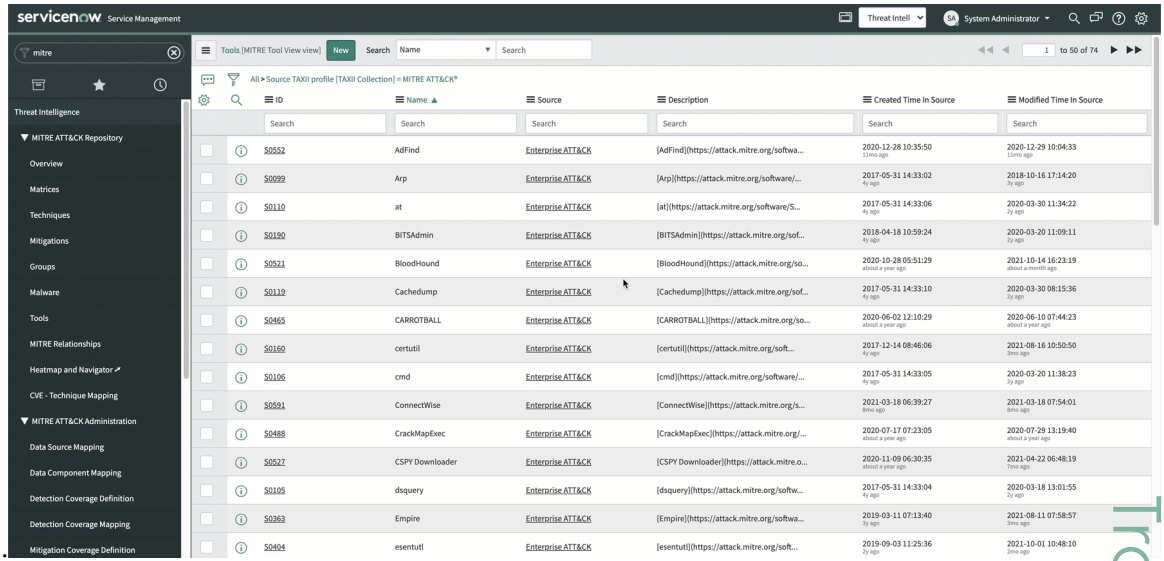
Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Outils**. Vous pouvez afficher les outils répertoriés.
2. Cliquez sur un outil pour afficher toutes les informations associées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'illustration suivante, vous pouvez voir les détails de l'outil CARROTBALL, son ID, sa source et d'autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Utilisez le module Techniques pour ajouter ou modifier les données d'outils.

Gérer les MITRE relations

Gérez les informations de relations MITRE que vous avez importées à partir des MITRE TAXII collections.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

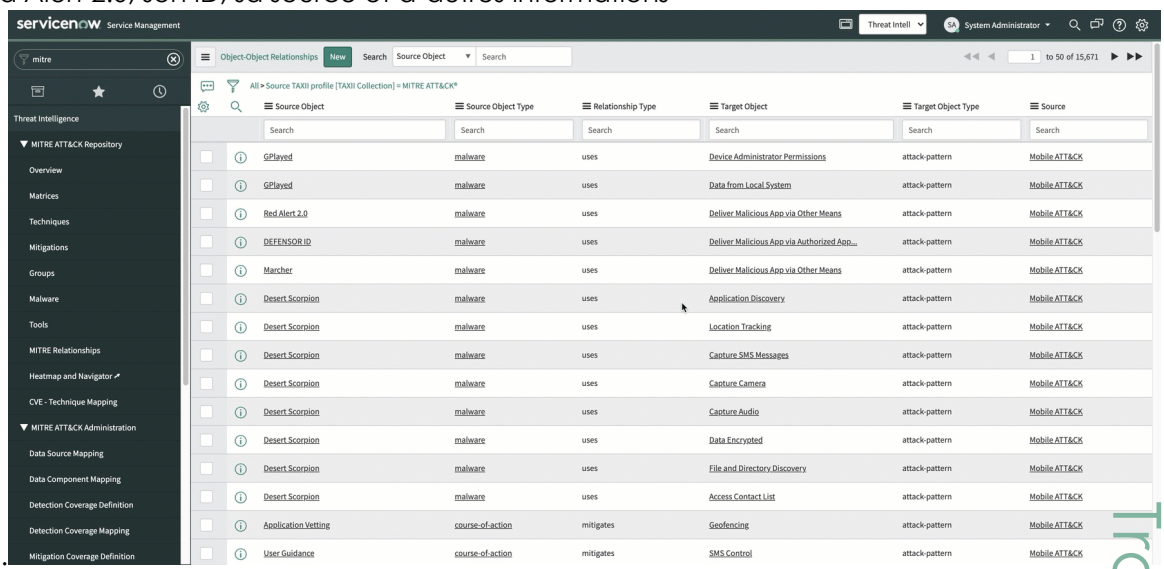
Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Relations MITRE**.
   Vous pouvez afficher les outils répertoriés.
2. Cliquez sur un objet source pour afficher toutes les informations associées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'illustration suivante, vous pouvez voir les détails de l'objet Red Alert 2.0, son ID, sa source et d'autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Utilisez le module Techniques pour ajouter ou modifier les données de relations MITRE.

Gérer les CVE et le mappage des techniques

Gérez les informations CVE et techniques qui sont mappées après l'importation des MITRE TAXII collections.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Remarque : Le module **CVE-Technique Mapping** n'est disponible que lorsque le produit Vulnerability Response est installé dans votre environnement.

Pourquoi et quand exécuter cette tâche

Une fois que vous avez importé les MITRE TAXII collections, vous pouvez visualiser les CVE dans votre environnement et leur relation avec les techniques associées MITRE-ATT&CK . Vous pouvez également créer des associations avec les CVE et les schémas d'attaque.

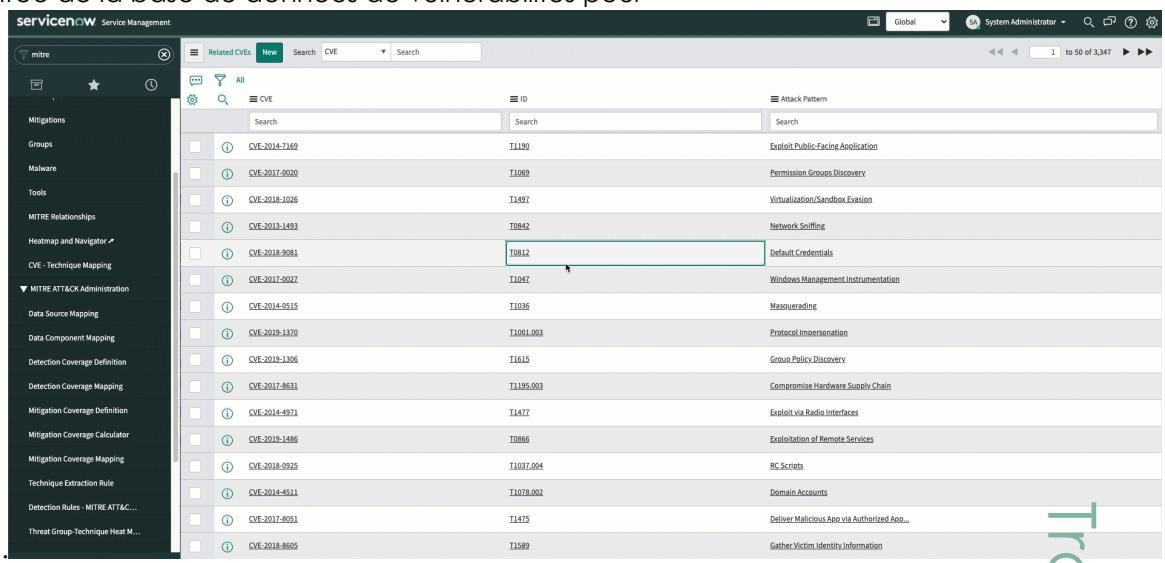
Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **CVE : mappage de technique**.
   Vous pouvez afficher les CVE et les techniques répertoriées.
2. Cliquez sur un CVE pour afficher l'entrée de base de données des vulnérabilités.

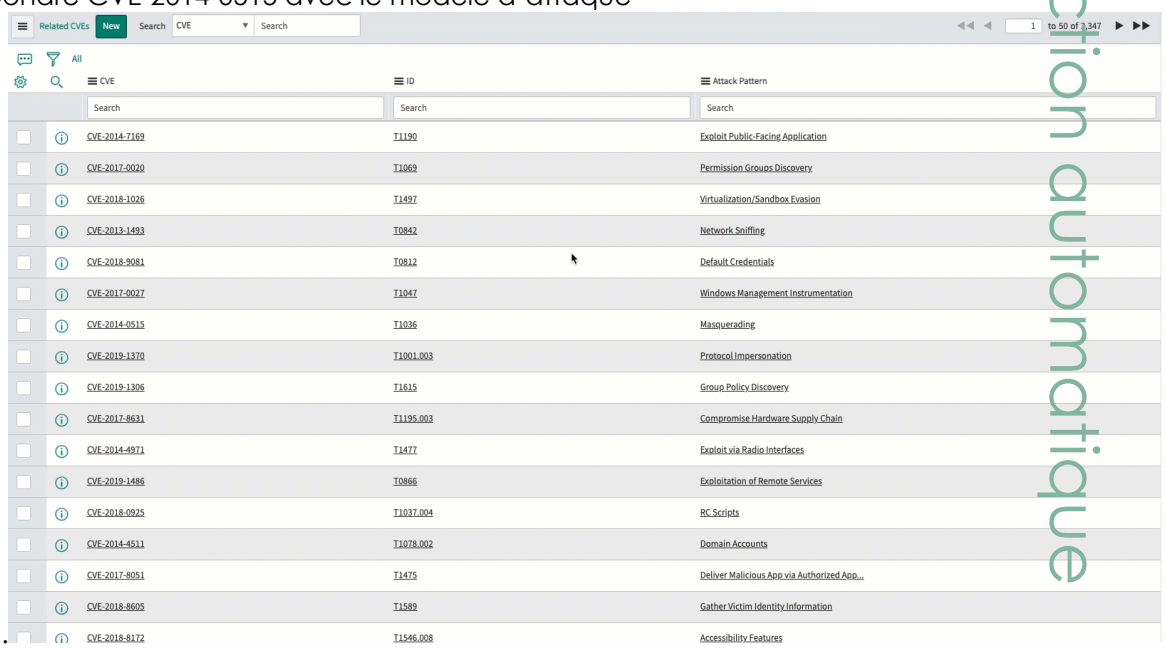
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'illustration suivante, vous pouvez afficher les détails de la liste CVE et de l'entrée de la base de données de vulnérabilités pour CVE-2014-7169.



3. Pour ajouter une entrée, cliquez sur **Nouveau**, mappez les CVE à un modèle d'attaque, puis cliquez sur **Envoyer**.
   Dans l'illustration suivante, une nouvelle entrée est créée en faisant correspondre CVE-2014-0515 avec le modèle d'attaque Masquerading.



Traduction automatique

Agrandir les MITRE-ATT&CK données

Étendre les données du MITRE-ATT&CK référentiel en Now Platform les enrichissant.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Pourquoi et quand exécuter cette tâche

Vous pouvez étendre les objets Malware, Group, Atténuation et Outil à une technique du MITRE-ATT&CK référentiel.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez créer un objet et établir une relation entre une technique et le nouvel objet dans le module Référentiel MITRE ATT&CK, mais vous ne pouvez pas définir le type de relation dans ce module. Pour plus d'informations sur la définition des types de relations, voir Relations d'objet à objet. Pour définir un type de relation, accédez à l'icône **Renseignements sur les menaces** > **Référentiel IoC** > **Relations objet-objet** module.

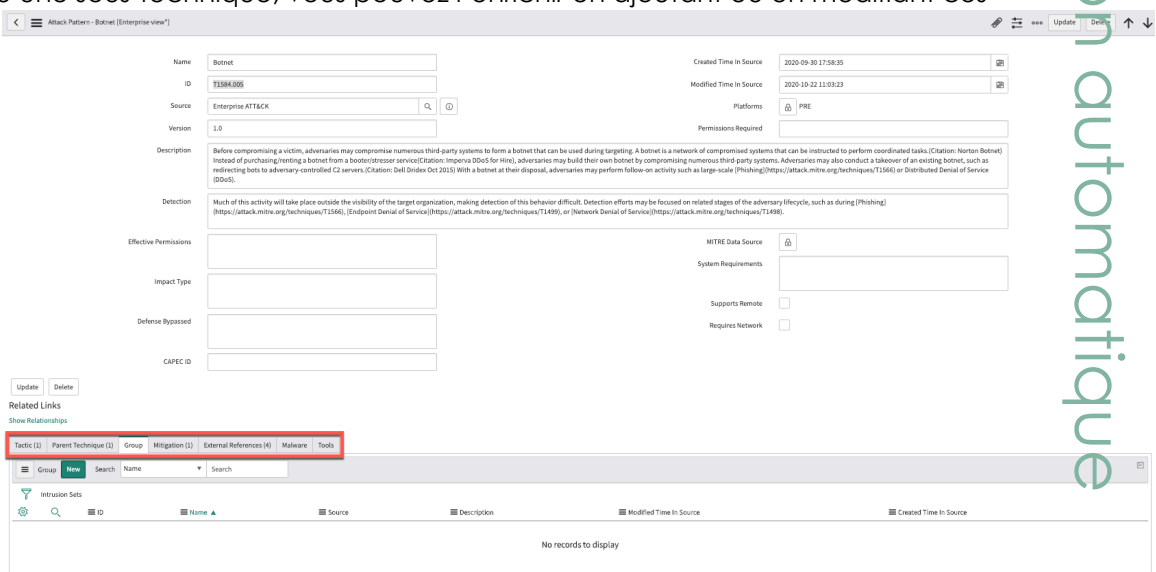
Si vous mappez le type de relation entre une technique existante et un objet existant, vous devez définir la technique en tant qu'objet cible et l'objet en tant qu'objet source. Pour ce faire, accédez à l'onglet **Référentiel IoC** > **Relations objet-objet** module.

Vous pouvez créer un groupe et l'associer à un modèle d'attaque, mais dans le référentiel MITRE ATT&CK, vous pouvez uniquement établir la relation entre le groupe et le modèle d'attaque. Pour définir le type de relation objet à objet, vous devez le faire dans le référentiel IoC.

Remarque : Toutes les personnalisations que vous apportez aux objets sont enregistrées lors des mises à jour planifiées.

Procédure

1. Accédez à la **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Techniques**.
2. Cliquez sur une technique ou une sous-technique pour afficher toutes les informations associées à cette technique.
   Dans l'illustration suivante, vous pouvez voir que la technique Botnet (T1584.005) n'est associée à aucun groupe. Si vous disposez d'informations complémentaires sur une technique ou une sous-technique, vous pouvez l'enrichir en ajoutant ou en modifiant ces informations.

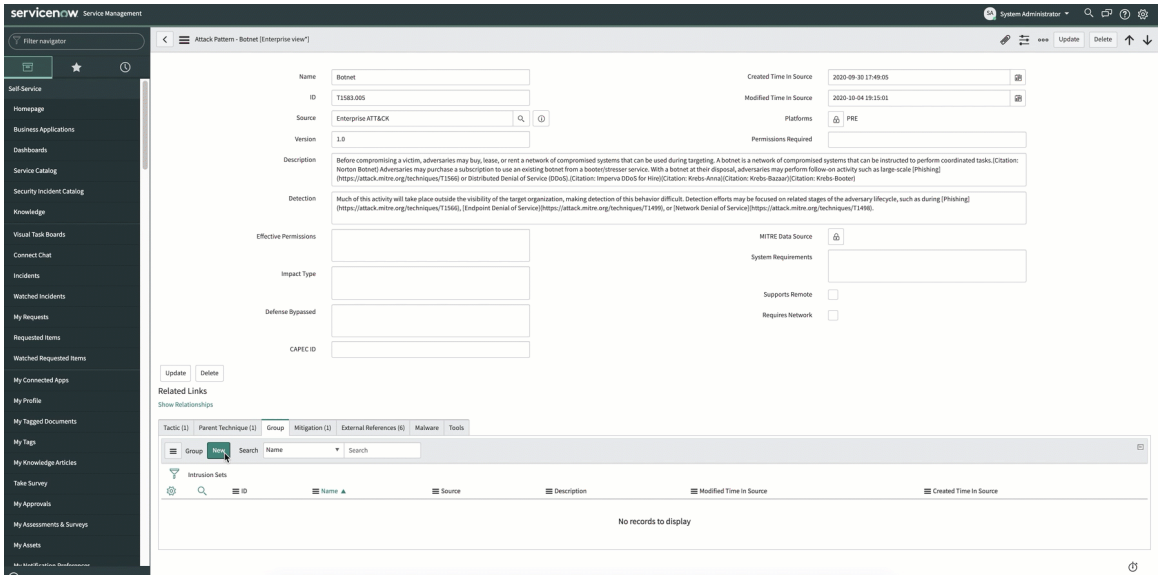


3. Cliquez sur une liste connexe pour enrichir ses données et l'associer à un nouveau groupe.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'illustration suivante, un groupe, Custom1, a été associé à la sous-technique du botnet.



Définir le mappage de la source de données et de l'outil de détection

Définissez le mappage de la source de données et de l'outil de détection pour MITRE-ATT&CK les tactiques et les techniques. Le mappage des sources de données vous donne un aperçu de la pertinence et de la disponibilité des sources de données et des outils de détection pour surveiller les sources de données dans votre environnement.

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : écriture, suppression d'accès
- sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Vous pouvez identifier les sources de données et les outils de détection dont votre organisation a besoin pour détecter efficacement les techniques.

Par exemple, si votre organisation se concentre sur 5 techniques, vous aurez peut-être besoin de 10 sources de données et de 10 outils de détection pour surveiller ces sources. Supposons que vous identifiiez que votre organisation ne dispose pas de deux sources de données et de cinq outils de détection. Cet exercice vous donne une visibilité sur les sources de données, leur pertinence pour votre organisation et vous permet d'identifier les lacunes dans la couverture. Vous pouvez également vous concentrer sur l'amélioration de votre environnement avec les bonnes sources de données et les bons outils de détection.

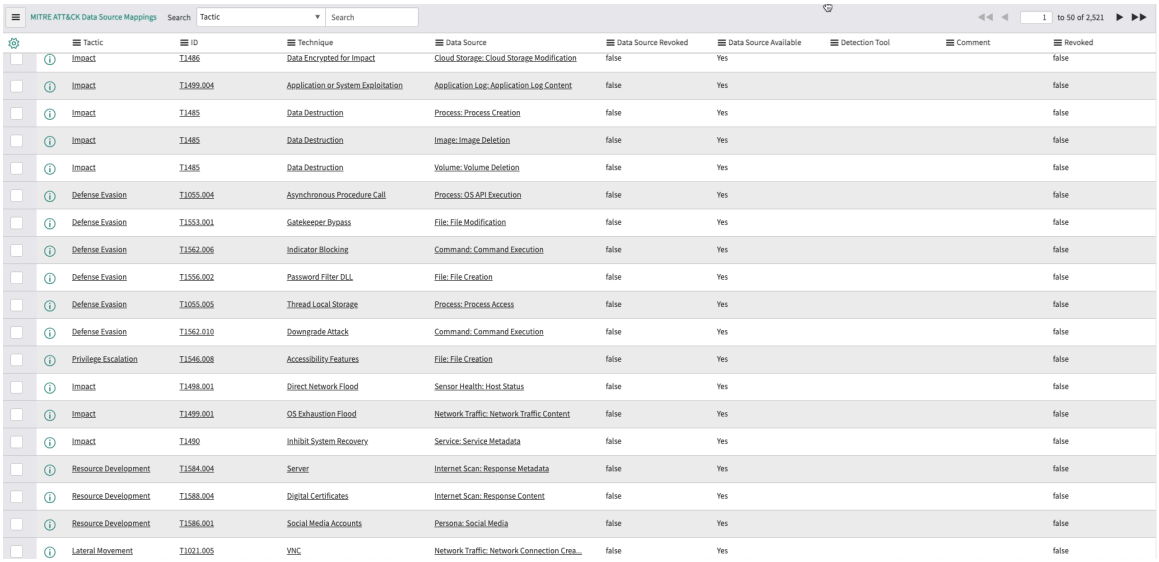
Toutes les tactiques, techniques, ID et sources de données actives sont automatiquement renseignés en fonction de votre TAXII Profil

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Mappage de source de données**.

   L'illustration suivante montre la liste des tactiques, des techniques et de leurs ID qui ont été renseignées en fonction des mises à jour de votre collection.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Tactic	ID	Technique	Data Source	Data Source Revoked	Data Source Available	Detection Tool	Comment	Revoked
Impact	T1486	Data Encrypted for Impact	Cloud Storage: Cloud Storage Modification	false	Yes			false
Impact	T1499.004	Application or System Exploitation	Application Log: Application Log Content	false	Yes			false
Impact	T1485	Data Destruction	Process: Process Creation	false	Yes			false
Impact	T1485	Data Destruction	Image: Image Deletion	false	Yes			false
Impact	T1485	Data Destruction	Volume: Volume Deletion	false	Yes			false
Defense Evasion	T1055.004	Asynchronous Procedure Call	Process: OS API Execution	false	Yes			false
Defense Evasion	T1553.001	Gatekeeper Bypass	File: File Modification	false	Yes			false
Defense Evasion	T1562.006	Indicator Blocking	Command: Command Execution	false	Yes			false
Defense Evasion	T1556.002	Password Filter DLL	File: File Creation	false	Yes			false
Defense Evasion	T1055.005	Thread Local Storage	Process: Process Access	false	Yes			false
Defense Evasion	T1562.010	Downgrade Attack	Command: Command Execution	false	Yes			false
Privilege Escalation	T1546.008	Accessibility Features	File: File Creation	false	Yes			false
Impact	T1498.001	Direct Network Flood	Sensor Health: Host Status	false	Yes			false
Impact	T1499.001	OS Exhaustion Flood	Network Traffic: Network Traffic Content	false	Yes			false
Impact	T1490	Inhibit System Recovery	Service: Service Metadata	false	Yes			false
Resource Development	T1584.004	Server	Internet Scan: Response Metadata	false	Yes			false
Resource Development	T1588.004	Digital Certificates	Internet Scan: Response Content	false	Yes			false
Resource Development	T1586.001	Social Media Accounts	Persona: Social Media	false	Yes			false
Lateral Movement	T1021.005	VNC	Network Traffic: Network Connection Crea...	false	Yes			false

Champ	Description
Tactique	Objectif de l'adversaire ou motif de l'action.
ID	L'identité unique de la technique.
Technique	Comment un adversaire atteint un objectif tactique en effectuant une action.
Source de données	Source de données associée à la technique.
Source de données révoquée	La source de données est révoquée si elle est définie sur vrai, mais le mappage de source de données est toujours conservé. Si la valeur de la source de données est introuvable dans MITRE, la valeur Source de données révoquée est automatiquement marquée comme vraie. Le mappage de source de données pour un enregistrement est révoqué si la technique et les relations de source de données sont manquantes dans les données mises à jour MITRE . Valeur par défaut : false
Source de données disponible	Disponibilité de la source de données.
Outil de détection	Outil qui complète la source de données en détectant les techniques utilisées. L'outil de détection est mappé avec le capteur d'alerte dans SIR.
Révoqué	Le mappage de source de données pour un enregistrement est révoqué si la technique et les relations de source de données sont manquantes dans les données mises à jour MITRE .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Valeur par défaut : false

2. Examinez les sources de données répertoriées et modifiez la valeur dans le champ **Source de données disponible** en fonction de votre environnement.

3. **Remarque :** Vous ne pouvez pas modifier cette entrée à partir de la vue de liste.

   Dans le champ **Outil de détection** , procédez comme suit :

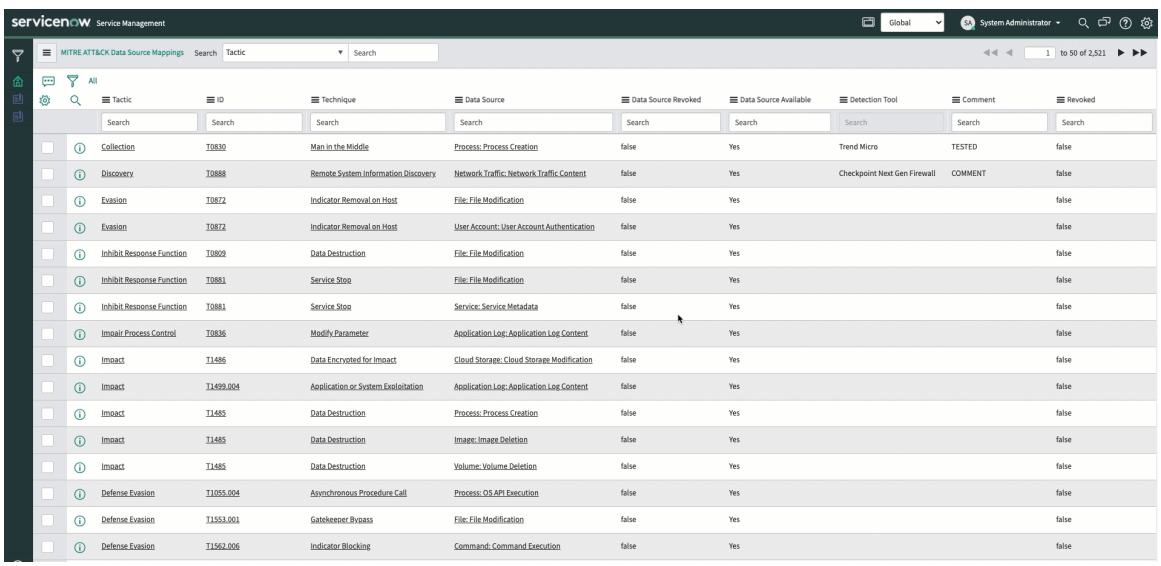
   a. Cliquez sur l'icône d'information, puis cliquez sur **Ouvrir l'enregistrement**.

   b. Déverrouiller l'entrée **de l'outil de détection** .

   c. Utilisez la liste de recherche pour sélectionner un outil de détection. Vous pouvez sélectionner plusieurs outils de détection.

   d. Cliquez sur **Mettre à jour**.

   Dans l'illustration suivante, plusieurs outils de détection sont ajoutés pour surveiller la source de données.



Définir le mappage de la source de données et du composant de données

Utilisez le mappage des composants de données si vous utilisez les dernières TAXII collections et que vous souhaitez conserver une relation entre les sources de données, les composants de données et les différentes techniques. Mappez les sources de données avec le contexte supplémentaire des composants de données, qui fournit une sous-couche supplémentaire de contexte aux sources de données afin de mieux comprendre les comportements des adversaires MITRE-ATT&CK .

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : écriture, suppression d'accès
- sn_ti.read : accès en lecture

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

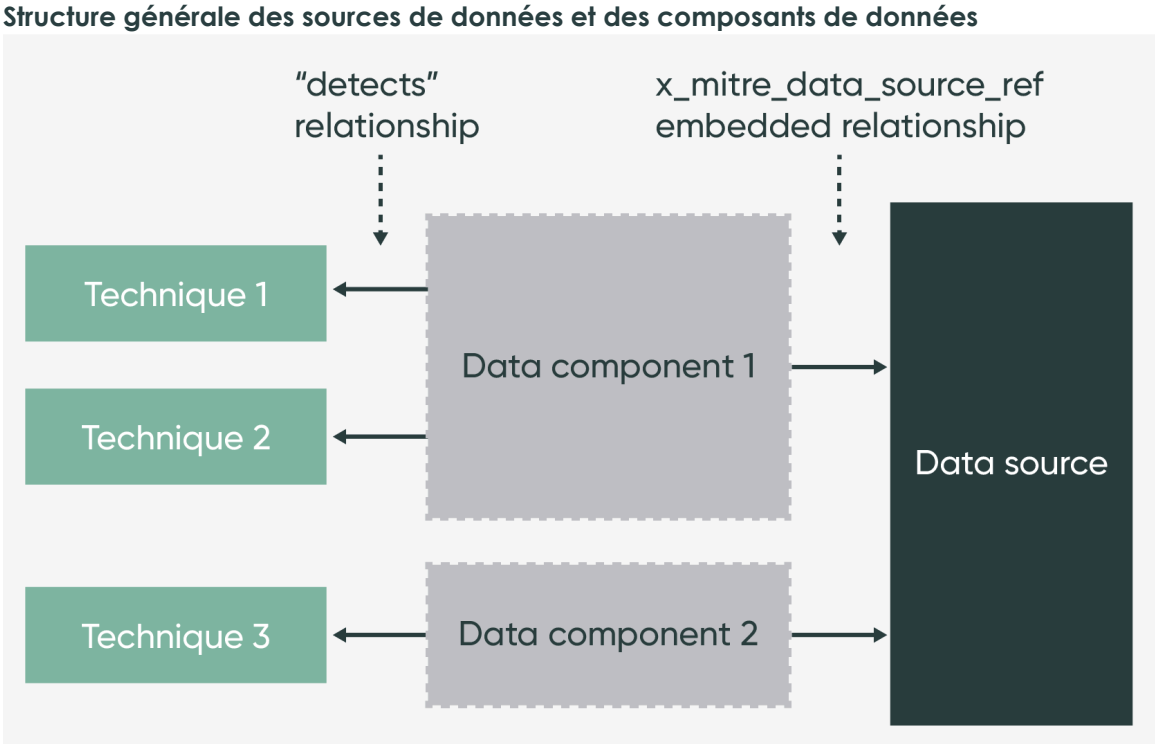
Pourquoi et quand exécuter cette tâche
Le mappage des sources de données et des composants de données offre une visibilité sur les sources de données ou les composants et les techniques pertinentes pour votre organisation.

Par exemple, si votre organisation se concentre sur 7 techniques, vous aurez peut-être besoin de 5 sources de données et de 10 composants de données pour surveiller ces sources. Votre évaluation des outils internes révèle que votre organisation ne dispose pas de deux sources de données et de quatre composants de données. Cet exercice de mappage fournit une visibilité sur les sources de données, les composants et les techniques, leur pertinence pour votre organisation et permet d'identifier les lacunes dans la couverture. Vous pouvez ainsi concentrer votre investissement sur les bonnes sources de données et les bons capteurs d'alerte pour détecter et atténuer les menaces adverses.

Le MITRE-ATT&CK cadre de travail contient une structure mise à jour pour les sources de données - Source de données : composant de données. Cette nouvelle forme de source de données fournit un contexte supplémentaire aux sources de données. L'objet source de données comporte le nom de la source de données ainsi que des détails clés sur les données collectées (fichier, processus, trafic réseau, etc.) et des valeurs ou propriétés spécifiques requises pour détecter les comportements des adversaires.

L'illustration suivante montre la représentation de la structure des sources de données et des MITRE-ATT&CK STIX™ composants de données. Vous pouvez afficher à la fois les sources de données et les composants de données capturés en tant qu'objets personnalisés STIX™. L'illustration montre que chaque source de données contient un ou plusieurs composants de données, et que chaque composant de données détecte une ou plusieurs techniques.

Structure générale des sources de données et des composants de données



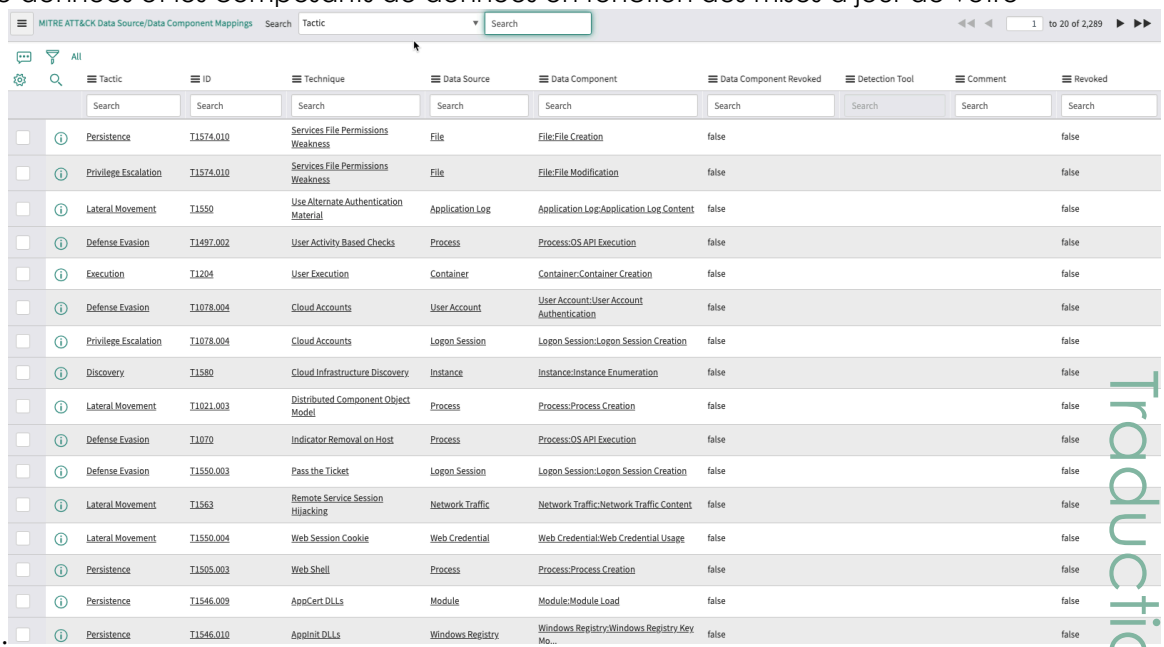
Vous pouvez continuer à utiliser le mappage de source de données si votre MITRE-ATT&CK référentiel contient les anciennes TAXII collections et que vous avez mappé vos sources de données à diverses techniques. Toutefois, utilisez le mappage des composants de données si vous utilisez les dernières TAXII collections et que vous souhaitez conserver une relation entre les sources de données, les composants de données et les différentes techniques.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Mappage des composants de données**.
   L'illustration suivante montre la liste des tactiques, des ID et des techniques, ainsi que les sources de données et les composants de données en fonction des mises à jour de votre collection.



Champ	Description
Tactique	Objectif de l'adversaire ou motif de l'action.
ID	L'identité unique de la technique.
Technique	Comment un adversaire atteint un objectif tactique en effectuant une action.
Source de données	Source de données associée à la technique.
Composant de données	Composant de données associé à la source de données. Un composant de données ne peut avoir qu'une seule source de données parente.
Composant de données révoqué	Identifie si le composant de données a été révoqué dans la MITRE-ATT&CK base de connaissances.
Outil de détection	Outil qui complète la source de données en détectant les techniques utilisées. L'outil de détection est mappé avec le capteur d'alerte dans SIR.
Commentaire	Description du mappage de la source de données et des composants de données.
Révoqué	Identifie si le mappage du composant de données à la technique est révoqué par MITRE-ATT&CK.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Passez en revue les sources de données et les composants de données répertoriés et modifiez les valeurs en fonction de votre environnement.
3. Pour ajouter un composant de données, procédez comme suit.
   a. Accédez à la **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Techniques**.
   b. Cliquez sur une technique dont vous souhaitez modifier la source de données : informations sur le composant de données.
   c. Déverrouiller la source de données : composant de données.
   d. Utilisez la liste de recherche pour sélectionner MITRE-ATT&CK des composants de données.
   e. Verrouiller la source de données : composant de données.
   f. Cliquez sur **Mettre à jour**.

Dans l'illustration suivante, vous voyez comment ajouter des composants de données.



Traduction automatique

Définir la couverture de détection de la technique

Définissez la couverture de détection des techniques que votre organisation doit mesurer et détectez les techniques spécifiques des adversaires.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : accès en écriture
- Rôle requis : sn_ti.read : accès en lecture

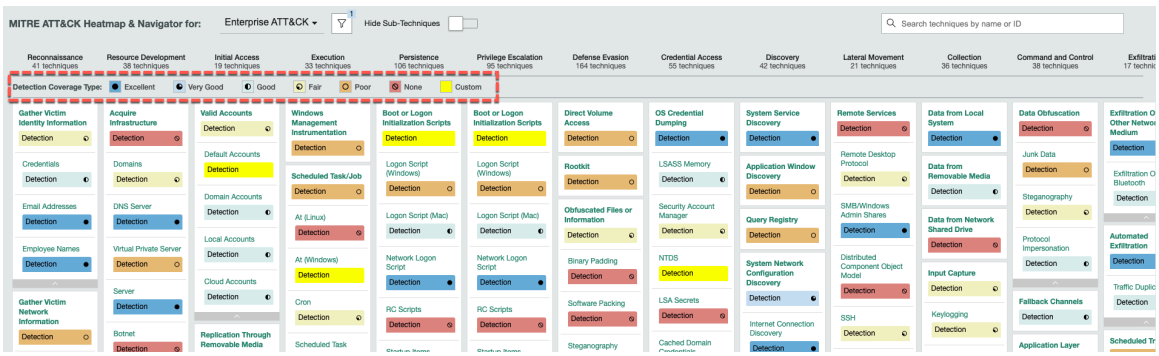
Pourquoi et quand exécuter cette tâche

Les définitions de couverture de technique sont utilisées dans le mappage global de détection de technique. Vous pouvez utiliser la couverture technique du système de base. La couverture technique du système de base comprend les types de couverture Aucune, Médiocre, Passable, Bon, Très bonne et Excellente. La couverture de la technique du système de base est également associée à des couleurs prédéfinies. Vous pouvez personnaliser les entrées et les couleurs du type de couverture, ou créer vos propres entrées. Par exemple, vous pouvez modifier les types de couverture du système de base en Non applicable, Couverture partielle et Couverture complète. Vous pouvez également créer des mesures numériques pour les types de couverture tels que 0 à 25 %, 25 à 50 % et 50 à 100 %. Le type de modifications apportées à la couverture du système de base ne se limite pas aux exemples partagés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les personnalisations que vous apportez au type et à la couleur de couverture sont utilisées dans le mappage de détection technique global , ainsi que dans la carte thermique.

Remarque : Si vous modifiez la définition de couverture du système de base, les icônes Type de couverture ne s'affichent pas avec les techniques de la carte thermique. La carte thermique fonctionne comme prévu lorsque vous modifiez les mêmes champs que la couverture de détection technique et les couleurs de couverture définies par le système de base. Toutefois, si vous supprimez des champs existants de la couverture globale de détection de la technique, la carte thermique n'affiche pas les icônes de type de couverture.



Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Définition de couverture de détection**.
2. Passez en revue les entrées globales de détection des techniques et personnalisez les entrées pour votre environnement.

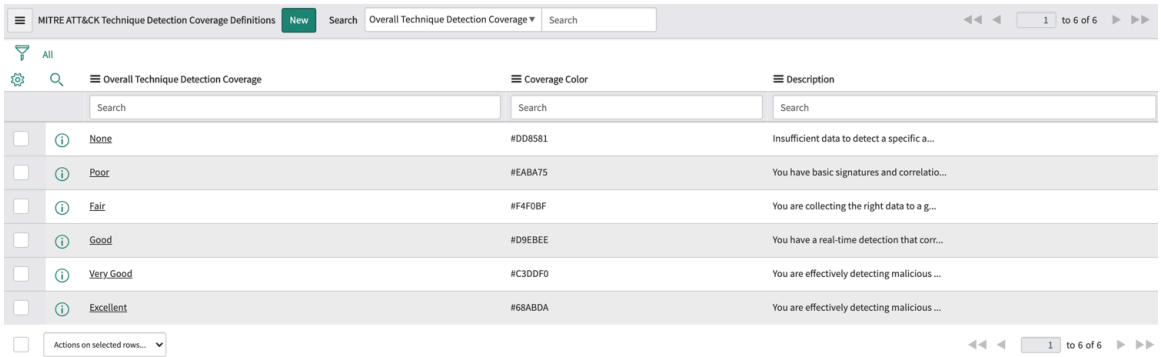
Définition de couverture de détection

Champ	Description
Couverture globale de détection de technique	Nom de la couverture globale de détection de la technique. La couverture technique du système de base se compose de Aucune, Médiocre, Acceptable, Bon, Très bonne ou Excellente.
Couleur de couverture	Couleur affectée au score de couverture de détection. La couleur que vous définissez est utilisée pour la couverture de détection de la technique dans la carte thermique. Vous pouvez personnaliser les couleurs à l'aide de codes HEX et de valeurs RVB(A).
Description	Couverture globale de détection de la technique. Reportez-vous à la définition du système de base dans la définition de notation.

L'illustration suivante montre la liste Définition de couverture de détection.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour ajouter une entrée, cliquez sur **Nouveau**, complétez les entrées, puis cliquez sur **Soumettre**.

MITRE-ATT&CK Définition de notation

Définissez le système de notation de MITRE-ATT&CK votre organisation afin de mesurer l'efficacité avec laquelle votre organisation peut détecter des techniques de validation spécifiques.

Définition de notation

Score	Mappage de score	Description
Aucun	0	Données insuffisantes pour détecter une technique spécifique de l'adversaire.
Médiocre	1	Des signatures de base et des règles de corrélation sont en place pour détecter les techniques spécifiques de l'adversaire. La détection des menaces ne se fait pas en temps réel et ne couvre qu'un nombre minimal d'aspects d'une technique. Par exemple, la chasse n'a lieu que sur un seul point de terminaison à la fois. Votre organisation peut encore avoir des milliers ou des centaines d'événements que les chasseurs doivent examiner et corréler avec d'autres événements pour trouver des valeurs aberrantes. Le nombre de faux positifs est élevé.
Acceptable	2	La collecte des bonnes données dans une large mesure et la qualité des données sont équitables. Par exemple, votre organisation commence peut-être à ajouter des journaux Sysmon, ETW, PowerShell, etc. Cependant, la détection des menaces n'est toujours pas en temps réel. Votre organisation ne dispose peut-être pas de tous les bons outils pour agréger et analyser efficacement les données. Les chasseurs doivent exécuter manuellement des requêtes et les corréler pour analyser les données avec précision. Le nombre de faux positifs est élevé.
Bien	3	Détection en temps réel qui met en corrélation et intègre plusieurs données sur vos terminaux. La détection des menaces couvre de nombreux aspects des procédures d'une technique. Vos adversaires pourraient éventuellement

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définition de notation (suite)

Score	Mappage de score	Description
		contourner la détection grâce à l'évasion et à l'obscurcissement. Votre organisation peut facilement identifier les faux positifs et les filtrer. Votre organisation utilise des techniques de science des données de base pour analyser les données du référentiel central.
Très bien	4	Détectez efficacement les techniques malveillantes en temps réel et couvrez la plupart des aspects des procédures d'une technique. La possibilité que vos adversaires contournent la détection avec des méthodes d'évasion et d'obscurcissement est plus difficile qu'au niveau Bon. Votre organisation peut facilement identifier les faux positifs et les filtrer. Votre organisation utilise des techniques avancées de science des données pour détecter les techniques des adversaires.
Excellent	5	Détectez efficacement les techniques malveillantes en temps réel et couvrez tous les aspects des procédures d'une technique. Votre organisation a une bonne compréhension de votre environnement avec la bonne automatisation et la bonne qualité des données. La possibilité que vos adversaires contournent la détection avec des méthodes d'évasion et d'obscurcissement n'est pas possible à ce niveau. Le nombre de faux négatifs est faible.

Mapper la couverture de détection de votre technique à une technique

Mappez votre couverture globale de détection des techniques avec celle qui permet à votre organisation de détecter des techniques spécifiques de vos adversaires.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : accès en écriture
- Rôle requis : sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la couverture de détection technique pour obtenir une vue d'ensemble de la couverture globale de détection de technique de votre organisation. Par exemple, si un adversaire attaque votre organisation, vous voyez le type de couverture dont vous disposez pour détecter les techniques de l'attaquant.

La technique et l'ID sont automatiquement renseignés pour toutes les collections et techniques que vous avez activées. Le type de couverture et la définition de notation que vous avez définis sont disponibles en tant qu'option que vous pouvez sélectionner dans la couverture globale de détection de technique.

Vous pouvez mapper la couverture globale de détection de la technique avec la technique pour terminer le mappage. Vous ne pouvez associer une technique qu'à une seule couverture globale de détection de technique.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

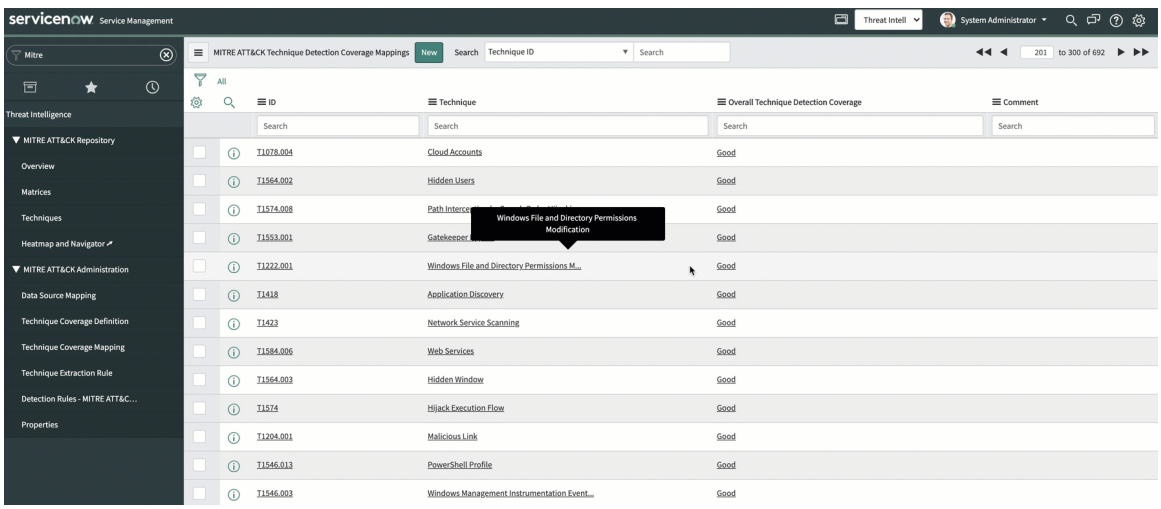
Le mappage de couverture de détection technique que vous définissez est utilisé dans la visualisation de couverture dans la carte thermique.

Remarque : Vous pouvez obtenir la couverture globale de détection de la technique à l'aide de calculs spécifiques à votre organisation. Vous pouvez utiliser n'importe quel produit de simulation de violation et d'attaque (BAS), le référentiel de cyberanalyse (CAR) ou toute autre méthode nécessaire pour définir la définition de notation, et l'utiliser dans cette procédure pour le mappage global de la couverture de détection technique.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Mappage de couverture de détection**.

   Dans cette illustration, vous voyez que la sous-technique Comptes dans le cloud (T1078.004) a une excellente couverture dans l'organisation et que la couverture globale de détection de la technique est mappée sur **Excellent**.



2. Examinez chaque technique et mappez votre couverture globale de détection des techniques en fonction de votre définition de couverture de détection et de la disponibilité de la couverture de votre organisation.

Définir la couverture d'atténuation

Définissez la couverture d'atténuation pour chaque atténuation associée à une technique afin d'obtenir une visibilité sur la façon dont votre organisation peut prévenir les attaques qui se produisent en raison d'une technique particulière.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- Rôle requis : sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Les définitions de couverture d'atténuation sont utilisées dans le mappage global de couverture de l'atténuation et de la technique. Vous pouvez utiliser la couverture d'atténuation du système de base. La couverture d'atténuation du système de base se compose des types de couverture Aucune, Médiocre, Passable, Bon, Très bonne et Excellente. La couverture d'atténuation du système de base est également associée à des couleurs prédéfinies et à des pourcentages de couverture. Vous pouvez personnaliser les types de couverture (ajouter ou supprimer des types de couverture), les pourcentages de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

couverture pour les limites inférieures et supérieures et les couleurs, ou créer votre couverture d'atténuation personnalisée.

Les personnalisations que vous apportez aux types de couverture, aux couleurs ou aux pourcentages sont utilisées dans le mappage de couverture d'atténuation, ainsi que dans la carte thermique.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Définition de couverture d'atténuation**.
2. Examinez les entrées de détection d'atténuation et personnalisez les entrées pour votre environnement.

Définition de couverture d'atténuation de technique

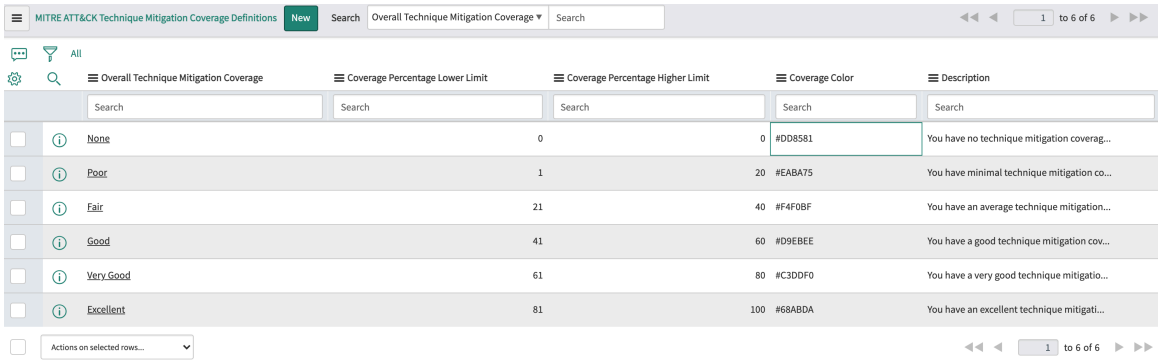
Champ	Description
Couverture globale de l'atténuation de la technique	Nom de la couverture d'atténuation de la technique. La couverture d'atténuation du système de base se compose de Aucune, Médiocre, Acceptable, Bon, Très bonne ou Excellente.
Limite inférieure du pourcentage de couverture	Limite inférieure en pourcentage de la couverture de l'atténuation. Définissez les valeurs numériques comprises entre 0 et 100.
Limite supérieure du pourcentage de couverture	Limite de pourcentage supérieure de la couverture de l'atténuation. Définissez les valeurs numériques comprises entre 0 et 100.
Couleur de couverture	Couleur affectée au score de couverture de détection. La couleur que vous définissez est utilisée pour la couverture de l'atténuation de la technique dans la carte thermique. Vous pouvez personnaliser les couleurs à l'aide de codes HEX et de valeurs RVB(A).
Description	Couverture globale de détection d'atténuation. Consultez la définition du système de base dans la définition de couverture d'atténuation de technique.

Remarque : Assurez-vous de ne pas chevaucher les plages de pourcentages de couverture si vous personnalisez les limites de pourcentage (inférieures ou supérieures). Par exemple, si un enregistrement de couverture comporte des plages comprises entre 0 et 20, l'enregistrement consécutif suivant doit avoir une plage de limite inférieure supérieure ou égale à 21 pour éviter de chevaucher la plage de pourcentages de couverture.

L'illustration suivante montre la liste des définitions de couverture d'atténuation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour ajouter une entrée, cliquez sur **Nouveau**, complétez les entrées, puis cliquez sur **Soumettre**.

Définitions de couverture d'atténuation de technique

Définissez la couverture d'atténuation de votre organisation afin de mesurer et détecter efficacement les techniques spécifiques des adversaires.

Définitions de couverture d'atténuation de technique MITRE ATT&CK

Couverture globale de l'atténuation de la technique	Limite inférieure du pourcentage de couverture	Limite supérieure du pourcentage de couverture	Couleur de couverture	Description
Aucun	0	0	#DD8581	Vous n'avez pas de couverture d'atténuation technique, et vos contrôles de défense n'ont pas la capacité d'empêcher une attaque dans n'importe quel scénario.
Médiocre	1	20	#EABA75	Vous disposez d'une couverture minimale de l'atténuation de la technique. Les chances d'une attaque sont très élevées, et vos contrôles de défense peuvent empêcher une attaque dans 0 à 20 % des scénarios.
Acceptable	21	40	#F4F0BF	Vous disposez d'une couverture

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définitions de couverture d'atténuation de technique MITRE ATT&CK (suite)

Couverture globale de l'atténuation de la technique	Limite inférieure du pourcentage de couverture	Limite supérieure du pourcentage de couverture	Couleur de couverture	Description
				moyenne d'atténuation de technique. Les chances d'une attaque sont élevées, et vos contrôles de défense peuvent empêcher une attaque dans 21 à 40 % des scénarios.
Bien	41	60	#D9EBEE	Vous disposez d'une bonne couverture technique d'atténuation. Cependant, les chances d'une attaque sont relativement élevées, et vos contrôles de défense peuvent empêcher une attaque dans 41 à 60 % des scénarios.
Très bien	61	80	#C3DDF0	Vous avez une très bonne couverture technique d'atténuation. Les chances d'une attaque sont faibles, et vos contrôles de défense peuvent empêcher une attaque dans 61 à 80 % des scénarios.
Excellent	81	100	#68ABDA	Vous disposez d'une excellente couverture technique d'atténuation et les chances

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définitions de couverture d'atténuation de technique MITRE ATT&CK (suite)

Couverture globale de l'atténuation de la technique	Limite inférieure du pourcentage de couverture	Limite supérieure du pourcentage de couverture	Couleur de couverture	Description
				d'une attaque utilisant cette technique sont très faibles et vos contrôles de défense peuvent empêcher une attaque dans 81 à 100 % des scénarios.

Mappez votre couverture d'atténuation à une technique

Mappez votre couverture d'atténuation avec la technique qui vous permet de détecter la stratégie d'atténuation globale de votre organisation.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : écrire, supprimer l'accès
- Rôle requis : sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Les atténuations vous permettent d'empêcher un adversaire d'exécuter avec succès des techniques ou des sous-techniques contre votre organisation. Chaque MITRE-ATT&CK technique contient des mesures d'atténuation que vous pouvez déployer dans votre organisation pour réduire le risque d'attaque. Vous pouvez utiliser la couverture d'atténuation pour obtenir une vue d'ensemble de la stratégie d'atténuation globale de votre organisation. Par exemple, si un adversaire attaque votre organisation, vous voyez le type de couverture dont vous disposez pour atténuer les techniques de l'attaquant.

La technique et les informations d'atténuation sont automatiquement renseignées pour toutes les collections et techniques que vous avez activées. Vous pouvez sélectionner la définition de couverture d'atténuation que vous avez définie dans la couverture d'atténuation de technique.

Vous pouvez identifier les atténuations qui sont pertinentes pour votre organisation. Si une atténuation est pertinente, vous pouvez définir si les stratégies d'atténuation ont été déployées. Vous pouvez spécifier si les stratégies sont appliquées dans le cadre de la politique SOC de votre organisation. Vous pouvez également identifier si votre organisation dispose d'outils préventifs pour atténuer les techniques d'un attaquant et mapper tous les contrôles de sécurité que votre organisation a déployés pour minimiser les risques de sécurité. Renseignez la couverture d'atténuation (pourcentage) pour chacun des enregistrements.

Après avoir mappé les informations pour chacune des techniques, le calculateur de couverture d'atténuation remplit automatiquement la couverture d'atténuation calculée. Pour calculer la couverture globale de l'atténuation pour n'importe quelle technique, les enregistrements de mappage d'atténuation de technique doivent être actifs et pertinents pour l'organisation. Les enregistrements qui sont inactifs et non pertinents ne sont pas pris en compte pour le calcul de la couverture globale des techniques d'atténuation. En fonction des valeurs de la couverture d'atténuation de technique calculée et de la définition de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

couverture d'atténuation, votre couverture d'atténuation de technique globale (calculée) est renseignée.

Les personnalisations que vous apportez aux types de couverture, aux couleurs ou aux pourcentages sont utilisées dans le mappage de couverture d'atténuation, ainsi que dans la carte thermique.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Mappage de couverture d'atténuation**.
2. Passez en revue chaque technique pour le mappage d'atténuation et mettez à jour la **couverture d'atténuation (pourcentage)** pour calculer la disponibilité de la couverture de votre organisation.

Mappages de couverture d'atténuation de technique

Champ	Description
ID	L'identité unique de la technique. Les ID sont automatiquement renseignés pour toutes les collections et techniques que vous avez activées.
Technique	Comment un adversaire atteint un objectif tactique en effectuant une action. Les informations sur les techniques sont automatiquement renseignées pour toutes les collections et techniques que vous avez activées.
Atténuation	Atténuations qui vous permettent d'empêcher un adversaire d'exécuter avec succès des techniques ou des sous-techniques contre votre organisation. Les informations sur l'atténuation sont automatiquement renseignées pour toutes les collections et techniques que vous avez activées.
Est pertinent	Option permettant de spécifier si l'atténuation est pertinente pour votre organisation.
Actif	Option permettant de spécifier si les stratégies d'atténuation sont déployées dans votre organisation. Il s'agit d'une option obligatoire pour calculer la couverture d'atténuation de la technique.
Outils préventifs	Option permettant de spécifier si votre organisation dispose d'outils préventifs pour atténuer les techniques d'un attaquant.
Politique SOC	Les politiques SOC qui définissent les stratégies d'atténuation au sein de votre organisation.
Contrôles de sécurité	Les contrôles de sécurité de votre organisation contiennent les stratégies

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d'atténuation visant à minimiser les risques de sécurité.
Couverture de l'atténuation (pourcentage)	Système de notation pour calculer la couverture d'atténuation de la technique. Définissez des valeurs numériques comprises entre 0 et 100. Il s'agit d'une option obligatoire pour calculer la couverture d'atténuation de la technique.
Couverture d'atténuation de technique calculée (pourcentage)	La couverture d'atténuation de technique calculée en pourcentage. Cette valeur est déterminée en fonction de la formule définie dans le calculateur de couverture d'atténuation.
Couverture globale d'atténuation de la technique (calculée)	La couverture globale de l'atténuation de la technique. Cette valeur est déterminée en fonction de la couverture d'atténuation définie pour votre organisation.
Commentaire	Description de la technique et mappage de couverture d'atténuation.
Révoqué	La technique de mappage de couverture d'atténuation est révoquée.

Dans cette illustration, vous voyez que la technique Comptes valides a cinq atténuations associées, chacune avec une couverture d'atténuation de 16 pour la formation des utilisateurs, 92 pour les conseils des développeurs d'applications, 16 pour les politiques de mot de passe, 91 pour la gestion des comptes privilégiés et 14 pour l'atténuation des comptes valides. La couverture d'atténuation calculée est de 45,8 %.



Calculateur global de couverture d'atténuation de technique

La couverture globale de l'atténuation de la technique est déterminée en fonction de la formule définie dans le calculateur de couverture d'atténuation.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- Rôle requis : sn_ti.read : accès en lecture

Traduction automatique

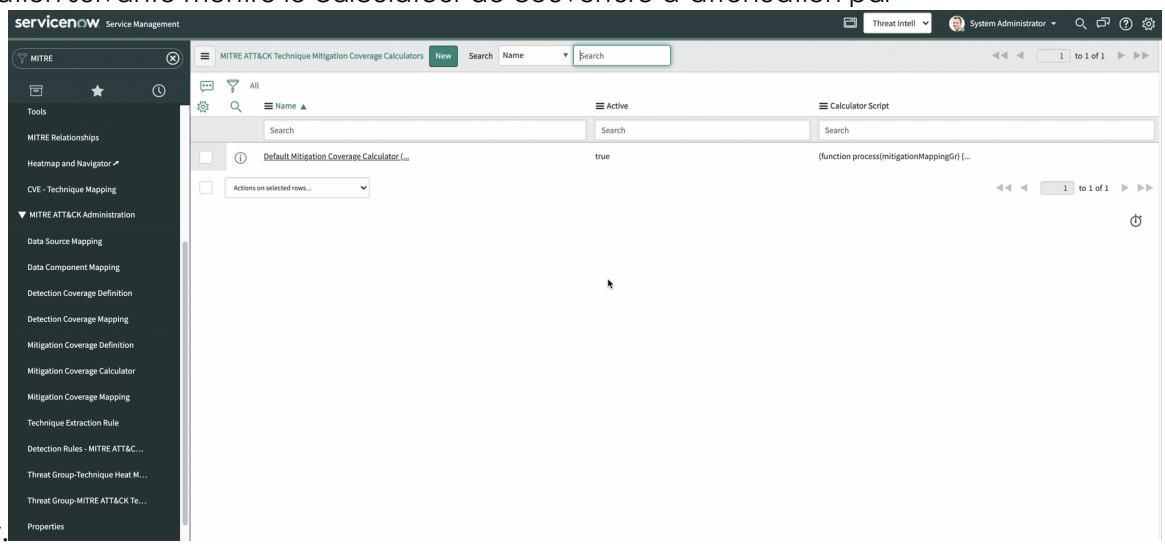
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

- Vous ne pouvez définir comme actif qu'un seul calculateur de couverture d'atténuation par domaine.
- Le calculateur de couverture d'atténuation du système de base est un calculateur de moyenne.
- Toute personnalisation du script du calculateur doit garantir que le résultat final est une valeur numérique comprise entre 0 et 100.
- La définition de couverture d'atténuation est appliquée en fonction de la plage de la sortie finale.

Procédure

Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Calculateur de couverture d'atténuation**.
L'illustration suivante montre le calculateur de couverture d'atténuation par défaut.



Créer et mapper des règles de détection

Créez des règles de détection et associez-les aux tactiques et techniques. Avec ce mappage, vous pouvez voir la couverture des règles de détection dans votre organisation.

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

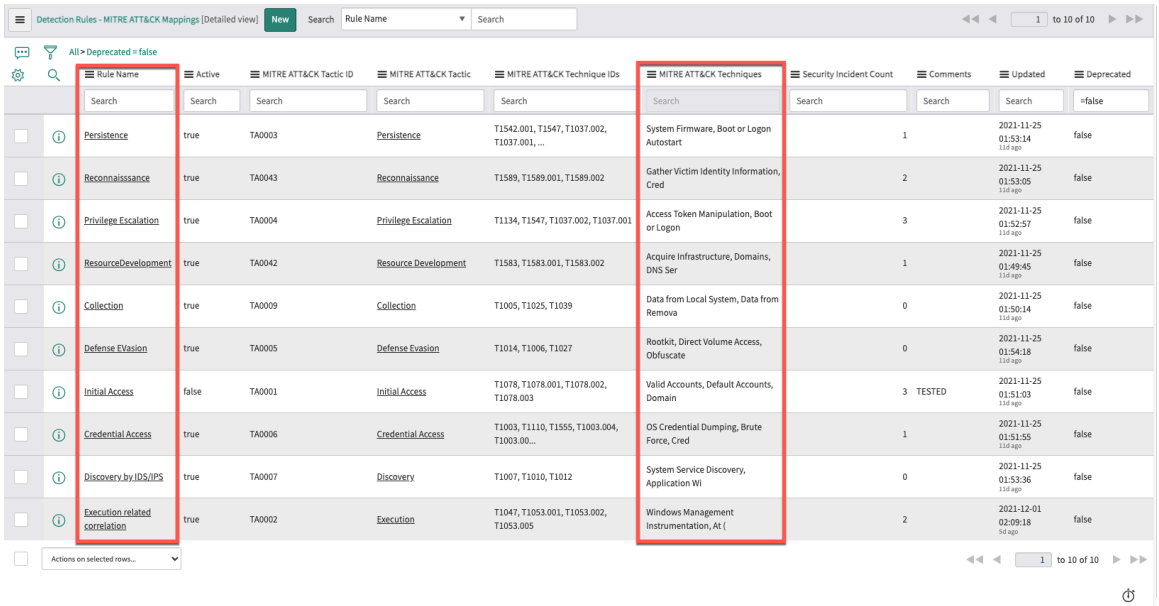
Le mappage des règles de détection permet à votre organisation de voir quelles règles de détection sont disponibles pour identifier des techniques spécifiques.

L'objectif principal du mappage est de fournir une visibilité si votre organisation dispose des règles de détection nécessaires pour identifier quand une alerte ou un événement est déclenché à la suite d'une attaque par un adversaire utilisant une technique spécifique.

Par exemple, consultez l'illustration suivante qui présente une liste des règles de détection mappées à diverses techniques. Vous pouvez également afficher ces informations dans le ou la MITRE-ATT&CK navigateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Si vous n'avez pas l'intention d'utiliser les règles d'extraction automatique du SIEM du système de base, activez le déploiement automatique des TTP en fonction du mappage de la règle de MITRE-ATT&CK détection. Vous pouvez renseigner l'alerte ou la règle d'événement qui déclenche l'incident de sécurité dans le champ Nom de la règle d'alerte . Vous pouvez également renseigner le champ Nom de la règle d'alerte à l'aide de l'intégration SIEM, de l'analyse des e-mails, de la création manuelle... Pour plus d'informations, consultez Informations de MITRE-ATT&CK déploiement à partir des règles de détection.

Remarque :

La fonctionnalité de règles de détection a été mise à jour pour inclure le mappage d'une seule tactique à plusieurs techniques. Auparavant, vous pouviez associer une seule tactique à une seule technique. Si vous mettez à niveau le module d'extension de la Renseignements sur les menaces version 12.0.4 vers une version supérieure, passez en revue les points suivants avant d'utiliser les règles de détection dans MITRE-ATT&CK le module.

- Vous trouvez plusieurs enregistrements fusionnés en un seul enregistrement si les champs (nom de la règle, capteur d'alerte, source, catégorie, sous-catégorie et MITRE-ATT&CK tactique) sont communs.
- Les anciens enregistrements sont marqués comme vrais dans la colonne déconseillée et faux dans la colonne active.
- Les nouveaux enregistrements fusionnés sont disponibles pour utilisation et sont marqués comme faux dans la colonne déconseillée et vrai dans la colonne active.
- Une fois que vous avez vérifié la mise à niveau et constaté que toutes vos règles de détection ont correctement été migrées, vous pouvez supprimer les anciens enregistrements marqués comme vrais dans la colonne Déconseillé.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Règles de détection : Mappages MITRE ATT&CK**.
2. Utilisez l'une des méthodes suivantes pour créer votre règle de détection :
   Méthode 1 : créer manuellement des règles de détection.

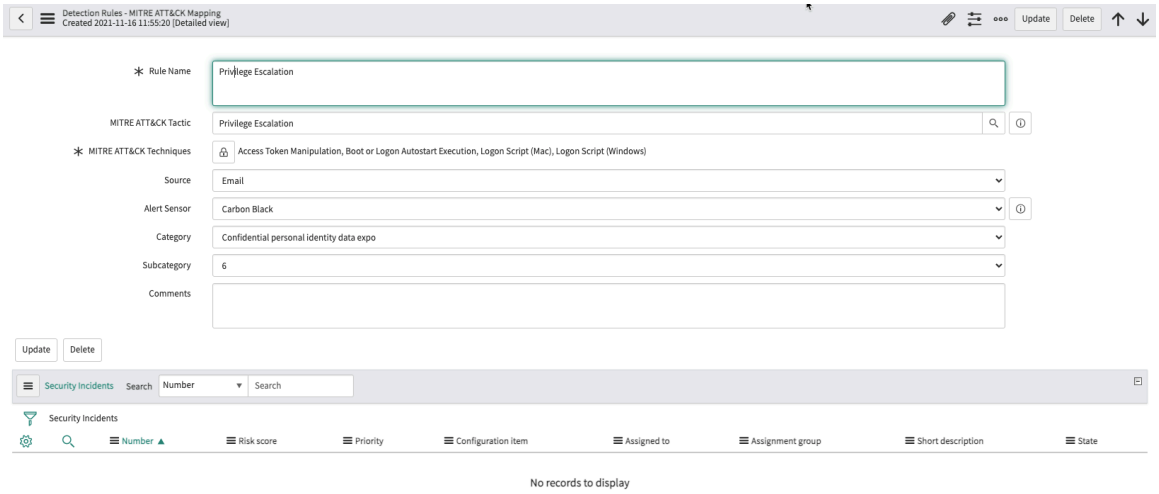
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Cliquez sur **Nouveau** et remplissez les champs sur le formulaire.

Règles de détection : MITRE-ATT&CK mappage

Champ	Description
Nom de la règle	Nom de la règle de détection.
MITRE-ATT&CK Tactique	Tactique pertinente MITRE-ATT&CK .
MITRE-ATT&CK Les techniques	Technique pertinente MITRE-ATT&CK . Vous pouvez sélectionner plusieurs techniques pour une seule tactique.
Source	Source de l'incident de sécurité, telle que la messagerie, le pare-feu, la surveillance du réseau, etc.
Capteur d'alerte	Intégration de sécurité via laquelle vous ingérez les données d'alerte ou d'événement telles que CarbonBlack, CrowdStrike, McAfee, etc.
Sous-catégorie	Sous-catégorie qui précise le problème.
Catégorie	Catégorie qui identifie le type de problème de sécurité.
MITRE-ATT&CK Technique	Technique pertinente MITRE-ATT&CK . Vous pouvez sélectionner plusieurs techniques pour une seule tactique.
Nombre d'incidents de sécurité	Nombre d'incidents de sécurité auxquels les techniques sont ajoutées. Ce nombre s'affiche lorsque vous avez activé le déploiement automatique des MITRE-ATT&CK informations des règles d'alerte aux incidents de sécurité.
Déconseillé	Le mappage de la règle de détection est déconseillé.
Actif	Option permettant de spécifier si la règle de détection est active et déployée dans votre environnement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



b. Cliquez sur **Envoyer**.

Méthode 2 : importer et créer des règles de détection.

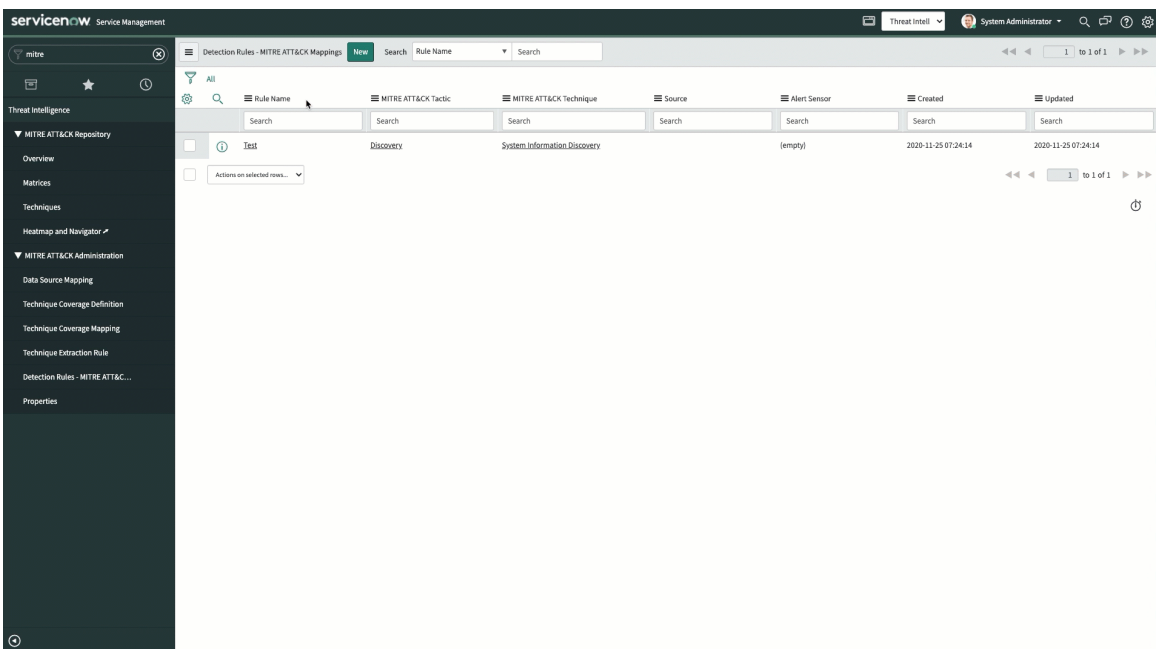
a. Cliquez avec le bouton droit sur l'en-tête de colonne Nom de la règle.

b. Dans la liste, cliquez sur **Importer**.

c. Cliquez sur **Créer un modèle Excel**.

d. Cliquez sur **Télécharger** une fois l'exportation terminée. Un modèle Excel portant le nom de fichier sn_ti_alert_rules_mitre_attack_technique_mapping est téléchargé sur votre ordinateur.

Dans l'illustration suivante, vous voyez comment exporter le modèle Excel, renseigner les détails dans la feuille de calcul, charger le fichier, prévisualiser les champs et le réimporter dans le Now Platformfichier .



e. Ouvrez la feuille de calcul, sélectionnez le deuxième onglet de feuille et vérifiez ce que vous avez saisi. Renseignez les champs du formulaire, puis enregistrez votre fichier.

Traduction automatique

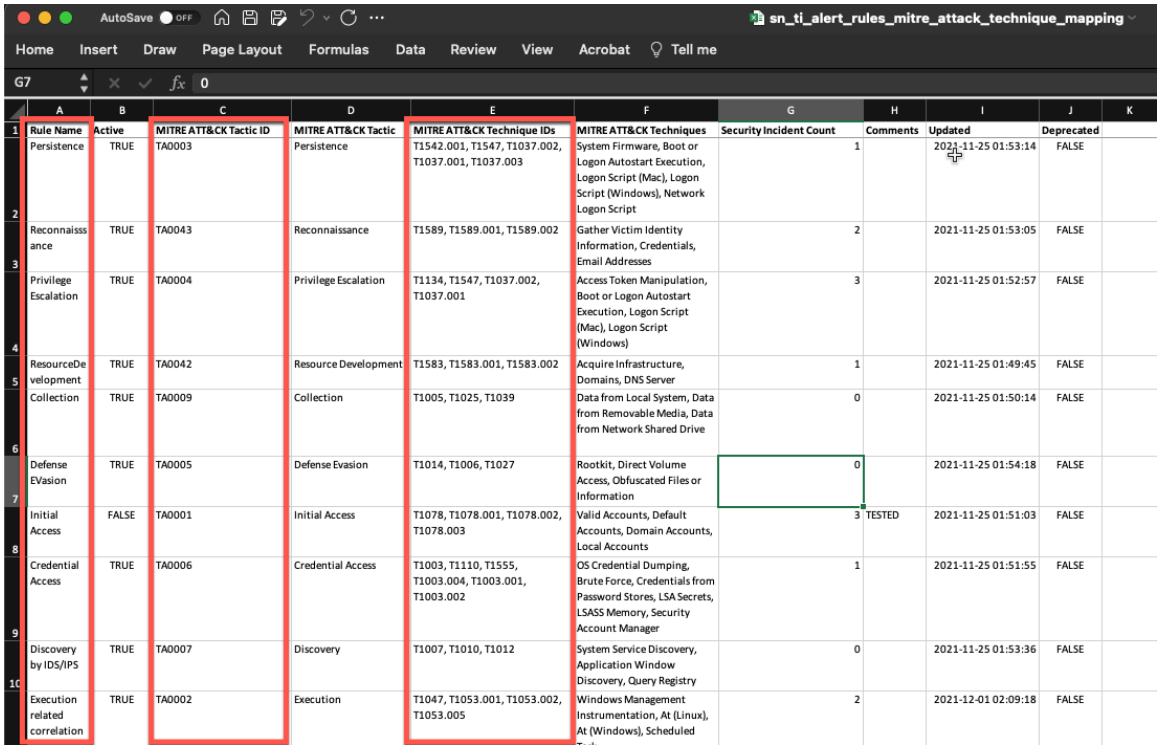
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer un modèle

Champ	Description
Nom de la règle	Nom de la règle de détection.
Actif	Option permettant de spécifier si la règle de détection est active et déployée dans votre environnement.
Capteur d'alerte	Intégration de sécurité via laquelle vous ingérez les données d'alerte ou d'événement telles que CarbonBlack, CrowdStrike, McAfee, etc.
Catégorie	Catégorie qui identifie le type de problème de sécurité.
Commentaires	Description de la règle de détection.
Déconseillé	Le mappage de la règle de détection est déconseillé.
MITRE-ATT&CK ID de la technique	MITRE-ATT&CK ID de technique, par exemple T1546.008, pour les fonctions d'accessibilité.
MITRE-ATT&CK ID tactique	MITRE-ATT&CK ID de tactique, par exemple TA0003, pour Persistance.
Nombre d'incidents de sécurité	Nombre d'incidents de sécurité auxquels les techniques sont ajoutées. Ce nombre s'affiche lorsque vous avez activé le déploiement automatique des MITRE-ATT&CK informations des règles d'alerte vers les incidents de sécurité et que la règle de détection est active.
Source	Source de l'incident de sécurité, telle que la messagerie, le pare-feu, la surveillance du réseau, etc.
Sous-catégorie	Sous-catégorie qui précise le problème.
MITRE-ATT&CK Tactique	Tactique pertinente MITRE-ATT&CK .
MITRE-ATT&CK Technique	Technique pertinente MITRE-ATT&CK .

L'illustration suivante montre le modèle de feuille de calcul. Les champs obligatoires sont mis en évidence en rouge : nom de la règle, MITRE-ATT&CK ID de tactique et MITRE-ATT&CK ID de technique.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



sn_ti_alert_rules_mitre_attack_technique_mapping

	A	B	C	D	E	F	G	H	I	J	K
1	Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated	
2	Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE	
3	Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE	
4	Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE	
5	ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE	
6	Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE	
7	Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE	
8	Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE	
9	Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE	
10	Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE	
	Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE	

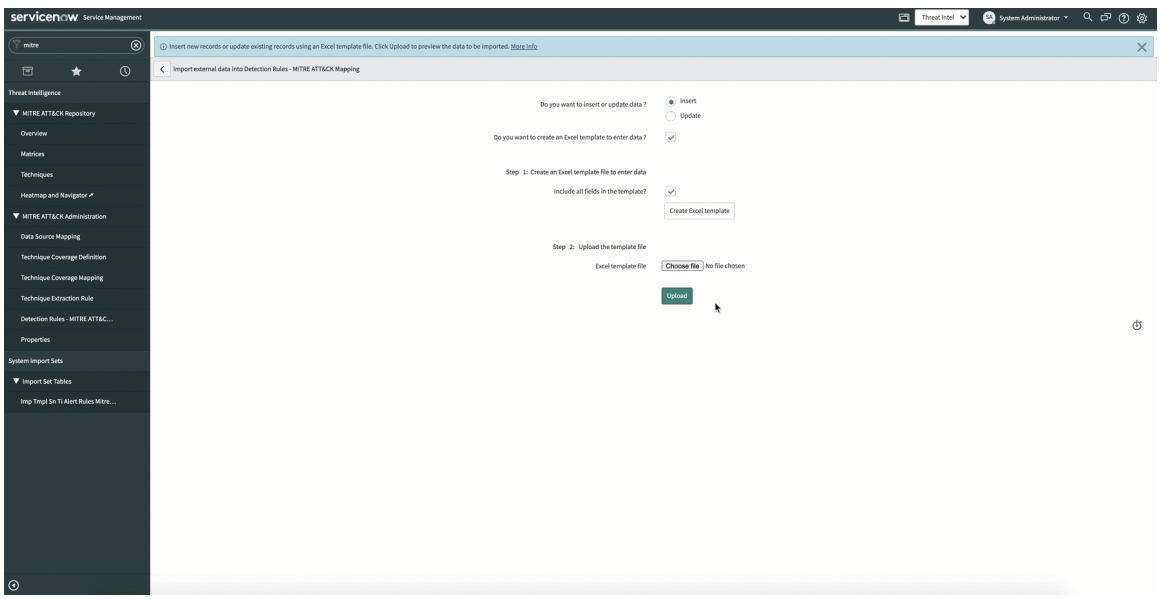
f. Cliquez sur **Choisir un fichier** et sélectionnez la feuille de calcul sur votre ordinateur.

g. Cliquez sur **Charger**.

h. Cliquez sur **Prévisualiser les données importées**.

i. Prévisualisez les mappages et cliquez sur **Terminer l'importation**.

L'illustration suivante montre comment charger la feuille de calcul, prévisualiser les données, examiner les erreurs éventuelles et terminer le processus d'importation du mappage des règles de détection.



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles de la technique d'extraction automatique pour l'importation d'informations MITRE-ATT&CK

Utilisez les règles d'extraction automatique du système de base pour importer les MITRE-ATT&CK informations à partir de toutes les intégrations tierces existantes.

Utiliser des règles d'extraction automatique de la recherche de menaces

Utilisez les règles d'extraction automatique de la recherche de menaces pour importer les MITRE-ATT&CK informations à partir de toutes les intégrations tierces existantes Renseignements sur les menaces .

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Lorsqu'une Renseignements sur les menaces intégration, telle que Sandbox ou TIP, prend en charge le MITRE-ATT&CK cadre de travail et si les MITRE-ATT&CK informations sont analysées à chaque niveau d'intégration, elles s'affichent dans chaque enregistrement de résultat de recherche de menace. Cependant, toutes les Renseignements sur les menaces intégrations n'analysent pas les MITRE-ATT&CK informations. La règle d'extraction automatique globale de la recherche des menaces peut extraire MITRE-ATT&CK des informations de toutes les Renseignements sur les menaces intégrations.

Vous pouvez choisir de déployer automatiquement les MITRE-ATT&CK informations à partir des résultats de la recherche de menace jusqu'à un incident de sécurité. Pour le déploiement automatique des résultats de la recherche de menaces sur les incidents de sécurité, activez la propriété système. Vous pouvez également déployer les informations manuellement pour chaque recherche de menace.

Le système Renseignements sur les menaces de base extrait automatiquement les informations de la MITRE-ATT&CK charge utile brute des intégrations tierces vers l'enregistrement des résultats de la recherche de menace, si l'intégration Renseignements sur les menaces vous fournit des informations telles que MITRE-ATT&CK la technique ou la tactique.

Si les informations ne sont pas disponibles dans le MITRE-ATT&CK champ de charge utile brute de l'enregistrement de recherche de menace, vous devez définir votre propre règle pour l'extraction automatique à partir de l'intégration tierce.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Règle d'extraction de la technique**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Règle d'extraction de technique

Champ	Description
Nom	Nom de la règle d'extraction automatique.
Type de règle	Type de règle d'extraction automatique. Sélectionnez **Recherche de menace**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ignorer l'extraction automatique	La définition par défaut est désactivée. Ce paramètre permet l'extraction automatique des MITRE-ATT&CK techniques.
Moteur source	Moteur source.
Global	Réglage du moteur source. Lorsque vous définissez le moteur source sur **Global**, l'extraction s'exécute sur tous les résultats d'intégration de recherche de menace.
Description	Description de la règle d'auto-extraction.
Méthode de traitement	Regex ou une méthode de script que vous spécifiez pour lier les informations de technique à partir de la charge utile brute.
Regex Extraction	Option que vous spécifiez pour le **champ cible** lors de l'utilisation de la méthode d'extraction regex. Regex est la valeur par défaut.
Extraction de script	Processus que vous sélectionnez lors de l'exécution d'un script. Le script passe en revue les éléments suivants : ◦ threatLookupResultSysId :sys_id de l'enregistrement de résultat de la recherche de menace ◦ sourceName : nom de la source de recherche de menaces.
Extraction tactique	Option que vous spécifiez pour extraire des informations relatives à la tactique à partir de la charge utile brute. Si une charge utile contient des informations spécifiques liées aux tactiques et techniques, vous pouvez extraire ces informations et les ajouter à l'incident de sécurité.

4. Cliquez sur **Envoyer**.

Utiliser les règles d'extraction automatique SIEM

Utilisez les règles d'extraction automatique du SIEM pour importer les informations à partir de n'importe MITRE-ATT&CK quelle intégration tierce du SIEM existante Opérations de sécurité .

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

La règle d'extraction de la technique est disponible pour toutes les intégrations SIEM du système Opérations de sécurité de base telles que les intégrations Splunk, IBM QRadar et ArcSight. Lorsque l'équipe ingère des données d'alerte ou d'événement provenant de

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ces intégrations SIEM et qu'elles Now Platform contiennent MITRE-ATT&CK des informations, il Now Platform traite la charge utile brute et extrait automatiquement les MITRE-ATT&CK informations.

Si votre Now Platform contient des intégrations SIEM du système de base, cela signifie que les règles d'extraction de technique sont déjà créées dans le MITRE-ATT&CK module. Vous devez examiner et modifier les règles si nécessaire.

Activez la règle d'extraction automatique SIEM ou la règle d'alerte à la fois.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Règle d'extraction de la technique**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

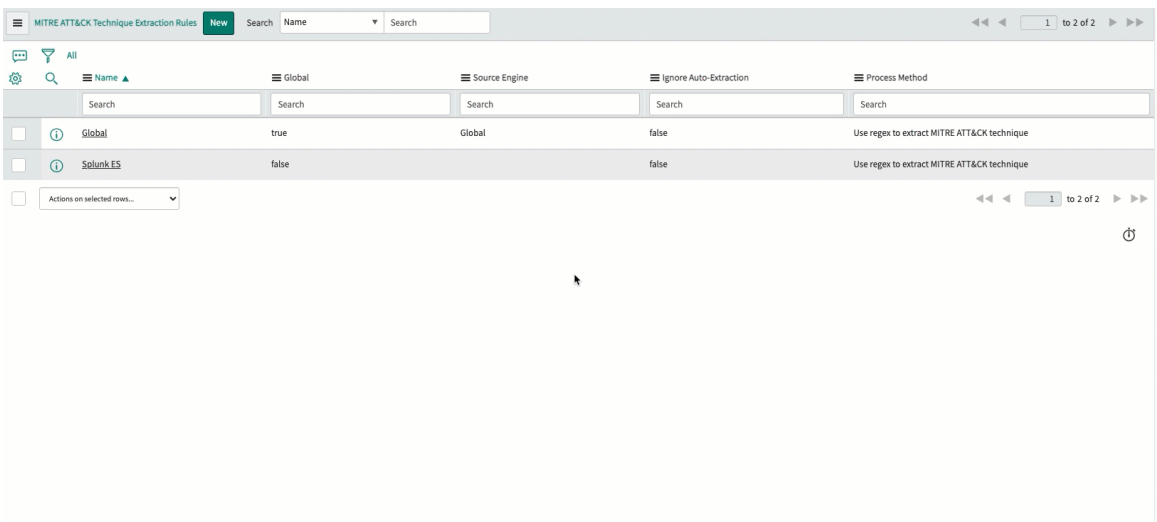
Formulaire Règle d'extraction de technique

Champ	Description
Nom	Nom de la règle d'extraction automatique.
Type de règle	Type de règle d'extraction automatique. Sélectionnez **SIEM.**
Ignorer l'extraction automatique	La définition par défaut est désactivée. Ce paramètre permet l'extraction automatique des MITRE-ATT&CK techniques.
Importer la table	Table d'importation automatiquement mappée pour les intégrations SIEM du système de base. Passez en revue ce champ pour d'autres intégrations SIEM afin d'obtenir des informations et effectuez une MITRE-ATT&CK mappage en conséquence.
Champ d'importation	Champ d'importation automatiquement mappé pour les intégrations SIEM du système de base. Passez en revue ce champ pour d'autres intégrations SIEM afin d'obtenir des informations et effectuez une MITRE-ATT&CK mappage en conséquence.
Description	Règle d'auto-extraction.
Méthode de traitement	Regex ou une méthode de script que vous spécifiez pour lier les informations de technique à partir de la charge utile brute.
Regex Extraction	Option que vous spécifiez pour le **champ cible** lors de l'utilisation de la méthode regex. L'extraction Regex est la méthode de traitement par défaut.
Extraction de script	Méthode de traitement de script que vous pouvez utiliser si vous souhaitez personnaliser la façon dont les MITRE-ATT&CK informations sont extraites.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Extraction tactique	Option que vous spécifiez pour extraire des informations relatives à la tactique à partir de la charge utile brute. Si une charge utile contient des informations spécifiques liées aux tactiques et techniques, vous pouvez extraire ces informations et les ajouter à l'incident de sécurité.

Dans l'illustration suivante, vous verrez un exemple de règle d'extraction de la Splunk Enterprise technique SIEM dans la vue de formulaire. Cette règle est similaire à toutes les autres règles d'extraction de technique SIEM.



4. Cliquez sur **Envoyer**.

Examiner le groupe de menaces et MITRE-ATT&CK le mappage des techniques

Passez en revue les informations de mappage de relations objet à objet des groupes de menaces et des techniques importées à partir MITRE TAXII des collections. Ce mappage vous permet d'afficher le groupe de techniques et le mappage de technique correspondant.

Avant de commencer

Rôle requis :

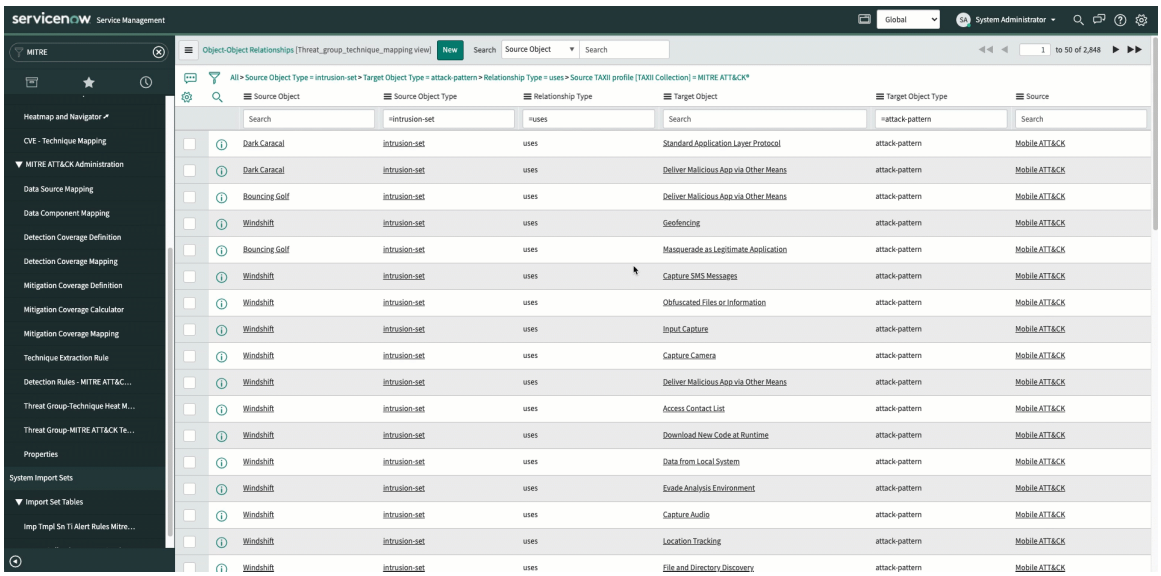
- sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Groupe de menaces : techniques MITRE ATT&ck**.
2. Cliquez avec le bouton droit sur **l'objet source** , puis sélectionnez **Grouper par objet source** pour afficher tous les schémas d'attaque associés à un groupe de menaces.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'illustration suivante montre le groupe de menaces admin@338 et les différents modèles d'attaque adoptés par ce groupe de menaces qui font partie de la source d'attaque de l'entreprise.



Définition de la carte thermique du groupe de menaces vers la technique

Définissez la définition de la carte thermique de groupe de menaces à technique afin de pouvoir mesurer et détecter les schémas d'attaque que les groupes de menaces utilisent pour attaquer votre organisation sur la carte thermique. La probabilité d'une attaque utilisant une technique particulière augmente lorsque vous avez un nombre élevé d'attaquants.

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : accès en écriture
- sn_ti.read : accès en lecture

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Groupe de menaces : définition de la carte thermique de la technique**.
2. Passez en revue la définition de la carte thermique groupe de menaces à technique et personnalisez les entrées pour votre environnement.

Groupe de menaces : définitions de la carte thermique de la technique

Champ	Description
Nombre de groupes de menaces (plage minimale)	Nombre minimal de groupes de menaces utilisant une technique particulière.
Nombre de groupes de menaces (plage maximale)	Nombre maximal de groupes de menaces utilisant une technique particulière. La probabilité d'une attaque utilisant une technique particulière augmente lorsque vous avez un nombre élevé d'attaquants.
Couleur de carte thermique	Couleur affectée à la catégorie de groupe de menaces. La couleur que vous définissez

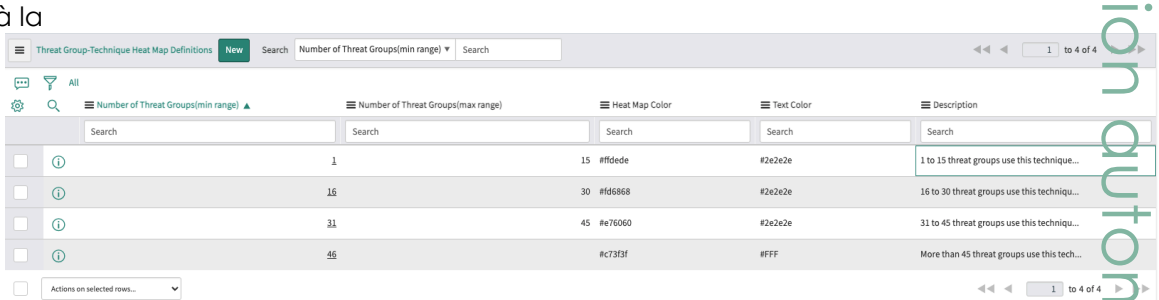
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	est utilisée pour mettre en surbrillance la catégorie du groupe de menaces dans la carte thermique. Vous pouvez personnaliser les couleurs à l'aide de codes HEX et de valeurs RVB(A).
Couleur du texte	Couleur affectée au texte du groupe de menaces. La couleur que vous définissez est utilisée pour mettre en surbrillance les groupes de menaces dans la carte thermique. Vous pouvez personnaliser les couleurs à l'aide de codes HEX et de valeurs RVB(A).
Description	Description de la plage et de la définition du groupe de menaces.

Remarque : Assurez-vous de ne pas chevaucher les plages de nombre de groupes de menaces si vous personnalisez la plage de groupes de menaces (min ou max).

L'illustration suivante montre la liste des définitions de la carte thermique des groupes de menaces à la technique.



3. Pour ajouter une entrée, cliquez sur **Nouveau**, complétez les entrées, puis cliquez sur **Soumettre**.

Examiner les MITRE-ATT&CK propriétés système

Examinez les valeurs des MITRE-ATT&CK propriétés système.

Avant de commencer

Rôle requis : sn_ti.admin, sn_si.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Propriétés**.
2. Renseignez les champs du formulaire.

MITRE-ATT&CK Formulaire Propriétés

Champ	Description
Déployer automatiquement les informations MITRE ATT&CK des observables vers l'incident de sécurité	Déploiement des MITRE-ATT&CK informations des observables vers l'incident de sécurité. Pour plus d'informations,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
[sn_ti.rollup_mitre_att&ck_technique_observable_si]	consultez Associer des informations MITRE ATT&CK à des observables. Valeur par défaut : oui
Déployer automatiquement les informations MITRE ATT&CK à partir des résultats de la recherche de menace vers l'incident de sécurité [sn_ti.rollup_mitre_att&ck_technique_threat_lookup_si]	Déploiement des MITRE-ATT&CK informations depuis les résultats de la recherche de menaces jusqu'à l'incident de sécurité. Pour plus d'informations, consultez Extraction automatique de la recherche de menaces. Valeur par défaut : oui
Déployer automatiquement les informations MITRE ATT&CK des règles d'alerte aux incidents de sécurité [sn_ti.rollup_mitre_att&ck_technique_alert_rule_si]	Déploiement automatique des MITRE-ATT&CK informations TTP à partir des règles d'alerte vers les incidents de sécurité. Pour plus d'informations, reportez-vous à la section Règles de détection des cartes. Valeur par défaut : non
Déployer automatiquement les informations MITRE ATT&CK des incidents de sécurité enfants vers l'incident de sécurité parent [sn_ti.rollup_mitre_att&ck_technique_child_si_v]	Déployer MITRE-ATT&CK automatiquement les informations des incidents de sécurité enfants vers l'incident de sécurité parent. Valeur par défaut : oui
L'activation de cette propriété permet le mappage des champs d'incident de sécurité tels que la catégorie et la sous-catégorie avec les règles de détection dans la table « Règles de détection : mappage MITRE ATT&ck » [sn_ti.enable_category_mapping_with_alert_rule]	Catégorie et sous-catégorie dans la page de mappage Règles de détection - MITRE ATT&CK . Valeur par défaut : non
Délai (en heures) pour calculer « CVE - Nombre de VUL » [sn_ti.time_to_calculate_cve_vits_count]	Durée planifiée en heures pour calculer les informations CVE et VUL. Valeur par défaut : 24

3. Cliquez sur **Enregistrer**.

Utilisation MITRE-ATT&CK pour détecter et analyser les menaces

Utilisez le MITRE-ATT&CK cadre de travail dans le Renseignements sur les menaces et le module pour détecter et analyser les SIR menaces qui pèsent sur votre organisation.

Associer des MITRE-ATT&CK™ informations à des incidents de sécurité

Associez les MITRE-ATT&CK tactiques et les techniques à l'incident de sécurité pour une meilleure analyse des incidents de sécurité et des menaces.

Avant de commencer

Rôle requis : sn_si.analyst

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Ajoutez les informations sur les tactiques et les techniques à l'incident de sécurité afin de pouvoir corréler vos informations sur les MITRE-ATT&CK incidents de sécurité et les menaces pour une meilleure analyse. Par exemple, votre organisation peut recevoir des informations relatives aux tactiques, techniques et procédures (TTP) de vos sources tierces, telles que Renseignements sur les menaces des rapports ou d'autres sources extérieures au Réponse aux incidents de sécurité. Vous rajoutez ensuite ces informations pour SIR une meilleure corrélation et une meilleure analyse des menaces.

Vous pouvez choisir de déployer les MITRE-ATT&CK informations automatiquement à partir des résultats de l'extraction automatique des menaces, des observables ou d'un incident de sécurité enfant vers un incident de sécurité. Pour une reprise automatique jusqu'aux incidents de sécurité, activez la propriété système. Vous pouvez également déployer les informations manuellement pour chaque recherche de menace ou observable.

Procédure

1. Accédez à la **Tout** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez enrichir avec les MITRE-ATT&CK informations.
3. Cliquez sur le lien connexe **Associer la technique MITRE ATT&CK** .
   La fenêtre Associate MITRE ATT&CK Technique (Associer une technique MITRE ATT&CK) s'affiche.

   Cette illustration montre comment naviguer vers la liste connexe et rechercher une technique associée MITRE-ATT&CK , examiner l'ATT&CK d'entreprise source, ajouter un impact tactique et ajouter une technique d'arrêt/redémarrage du système.

   Associer des informations MITRE à un incident de sécurité
4. Sélectionnez **Source**.

   Remarque : Seules les collections et lesmatrices qui ont été activées apparaissent dans la liste source.

   Les tactiques et techniques associées à la source peuvent être sélectionnées. Vous pouvez également associer plusieurs sources.
5. Sélectionnez la **tactique** et les **techniques**.
6. Facultatif : Examinez les informations en fonction de leur pertinence par rapport à l'incident de sécurité et procédez comme suit :
   - Pour supprimer complètement l'association, cliquez sur l'icône de la corbeille. Cliquer sur cette icône supprime la source et ses tactiques et techniques associées.
   - Pour supprimer une tactique, cliquez sur l'icône moins en regard de la tactique.
   - Pour supprimer une technique, cliquez sur l'icône x en regard de la technique.
7. Cliquez sur **Enregistrer**.

Résultats

Les MITRE-ATT&CK informations sont associées à l'incident de sécurité. Vous pouvez maintenant afficher les informations associées dans la **carte MITRE ATT&CK**.

Associer des MITRE-ATT&CK informations à des incidents de sécurité fermés

Vous pouvez désormais associer MITRE-ATT&CK des tactiques et des techniques aux incidents de sécurité fermés pour une meilleure analyse des incidents de sécurité et des menaces.

Associer des informations MITRE à un incident de sécurité

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation de la MITRE-ATT&CK carte pour afficher les informations connexes dans un incident de sécurité

Vous pouvez utiliser la MITRE-ATT&CK carte pour afficher les MITRE-ATT&CK informations connexes dans un incident de sécurité.

Une fois que les informations sont déployées à partir d'une recherche de menace, d'un observable ou d'une intégration SIEM, elles sont ajoutées à l'incident de sécurité. Ensuite, les informations agrégées sont présentées dans la MITRE-ATT&CK carte. La **carte MITRE ATT&CK** offre deux vues :

- Vue Navigateur : cette vue, qui est similaire au MITRE-ATT&CK navigateur, affiche toutes les techniques qui ont été ajoutées ou déployées manuellement à partir des tables de recherche d'observables ou de menaces. **Afficher l'origine des techniques** affiche la source de la technique si elle a été déployée manuellement ou via une source. **Afficher l'ID** affiche l'ID de la technique.

  L'illustration suivante montre comment naviguer vers la vue **Navigateur de carte MITRE ATT&CK** . En cliquant sur l'un des liens disponibles, les informations s'ouvrent dans le Renseignements sur les menaces module.

  Carte MITRE ATT&CK : vue de navigateur et vue de liste

- Vue de liste : cette vue affiche les données sous forme de liste ou de tableau. Vous pouvez voir toutes les données réparties dans différentes tables et groupes dans cette vue.

  L'illustration suivante montre comment accéder à la vue de liste Carte MITRE ATT&CK. En cliquant sur l'un des liens disponibles, les informations s'ouvrent dans le Renseignements sur les menaces module.

Associer des MITRE-ATT&CK informations à des observables

Associez MITRE-ATT&CK des tactiques et des techniques à un observable pour une meilleure analyse des incidents de sécurité et des menaces à un niveau granulaire.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Certains SIEM peuvent fournir des MITRE-ATT&CK informations avec des événements, des alertes ou des observables. Pour associer les MITRE-ATT&CK informations à un niveau granulaire, vous pouvez ajouter les informations à un observable.

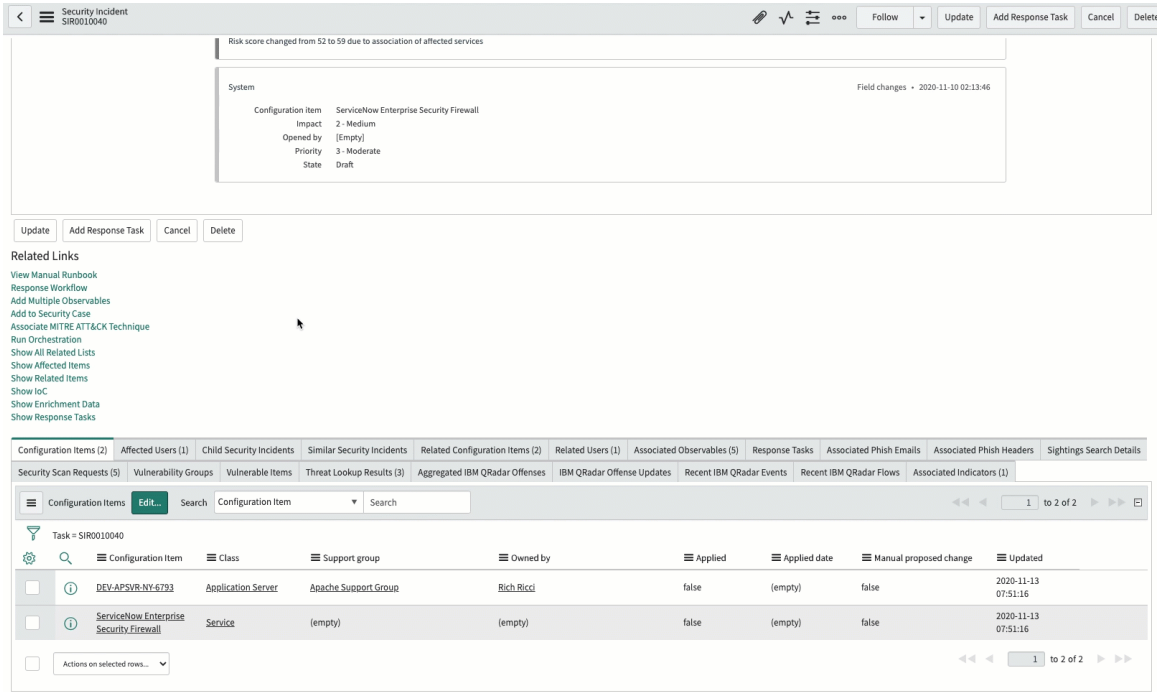
Vous pouvez choisir de déployer automatiquement les MITRE-ATT&CK informations des observables vers un incident de sécurité. Pour le déploiement automatique des observables sur les incidents de sécurité, activez la propriété système. Vous pouvez également déployer les informations manuellement pour chaque observable.

Procédure

1. Accédez à la **Tout** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez enrichir avec les MITRE-ATT&CK informations.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Pointez sur l'observable que vous souhaitez associer, cliquez avec le bouton droit de la souris et sélectionnez **Associer la technique MITRE ATT&CK**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'illustration suivante, vous pouvez voir comment naviguer à partir de la liste connexe pour **associer la technique MITRE ATT&CK**, examiner la source et ajouter une tactique et une technique.



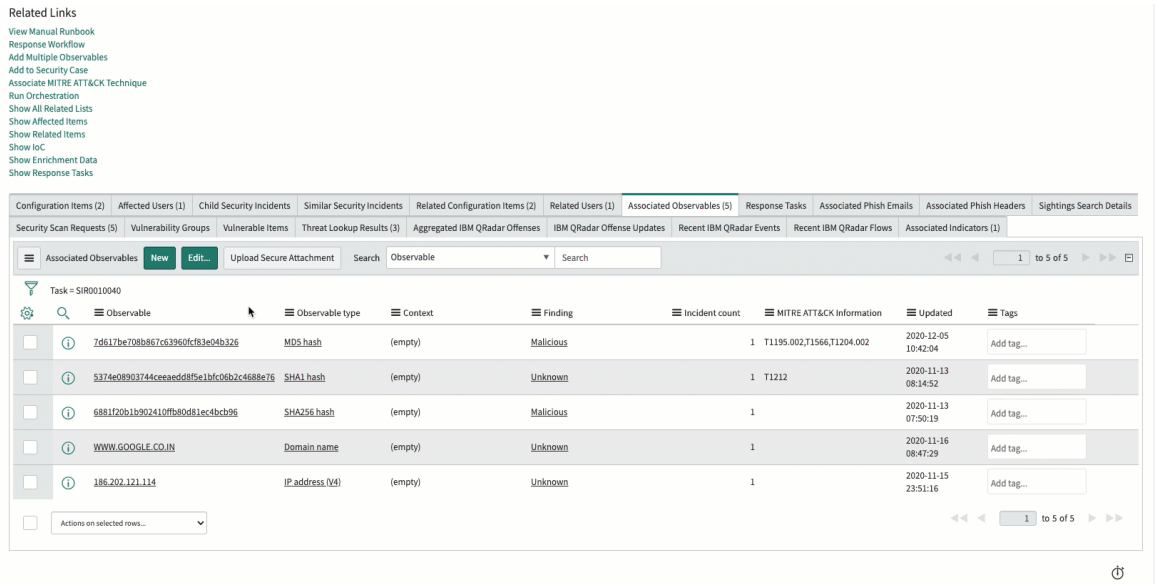
5. Dans les listes sources, examinez la **source**.

   Remarque : Seules les collections et lesmatrices qui ont été activées apparaissent dans la liste source.

6. Passez en revue la **tactique** et les **techniques**, et ajoutez-les ou supprimez-les en fonction de leur pertinence par rapport à l'observable.
7. Cliquez sur **Enregistrer**.
   Les tactiques et techniques que vous avez ajoutées s'affichent dans la MITRE-ATT&CK colonne Informations de la liste connexe Observables.
8. Sélectionnez l'observable, puis dans le menu Actions, cliquez sur **Déployer les informations MITRE ATT&CK sur SI**.
   Si vous avez activé Déploiement automatique de MITRE-ATT&CK Informations des observables à l'incident de sécurité, les informations sont automatiquement remontées. Si vous n'avez pas activé la reprise automatique, vous devez le faire manuellement.

   L'illustration suivante montre comment sélectionner un observable et déployer les informations dans un MITRE-ATT&CK incident de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Pour afficher une vue agrégée des techniques associées aux observables, sélectionnez deux observables ou plus dans la liste, puis dans le menu **Actions** de la liste des lignes sélectionnées, cliquez sur **Afficher les informations MITRE ATT&ck**.

Résultats

Une vue agrégée des informations MITRE ATT&CK pour les observables sélectionnés s'affiche.

Associer des MITRE-ATT&CK informations au ticket de sécurité

Associez MITRE-ATT&CK des tactiques et des techniques à un ticket de sécurité pour améliorer la gestion des tickets de sécurité et l'analyse des menaces à un niveau granulaire.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

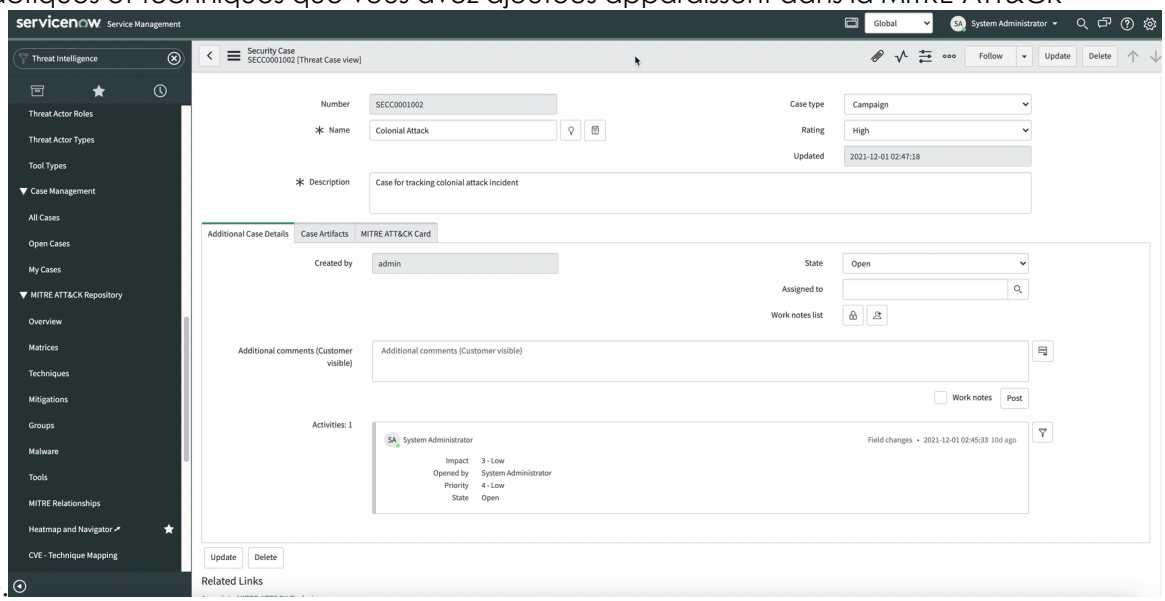
1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
2. Sélectionnez le ticket de sécurité que vous souhaitez enrichir avec les informations MITRE-ATT&CK.
3. Dans la liste connexe, cliquez sur **Associer la technique MITRE ATT&CK**.

   Dans l'illustration suivante, vous pouvez voir comment naviguer à partir de la liste connexe pour **associer la technique MITRE ATT&CK**, examiner la source et ajouter une tactique et une technique.

4. Dans les listes sources, examinez la **source**.
5. Passez en revue la **tactique** et les **techniques**, et ajoutez-les ou supprimez-les en fonction de leur pertinence par rapport au cas.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Enregistrer**.
   Les tactiques et techniques que vous avez ajoutées apparaissent dans la MITRE-ATT&CK carte.



Informations de déploiement à l'aide des MITRE-ATT&CK résultats de la recherche de menace

Si vous n'avez pas activé le cumul automatique des MITRE-ATT&CK informations, vous pouvez le faire manuellement.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

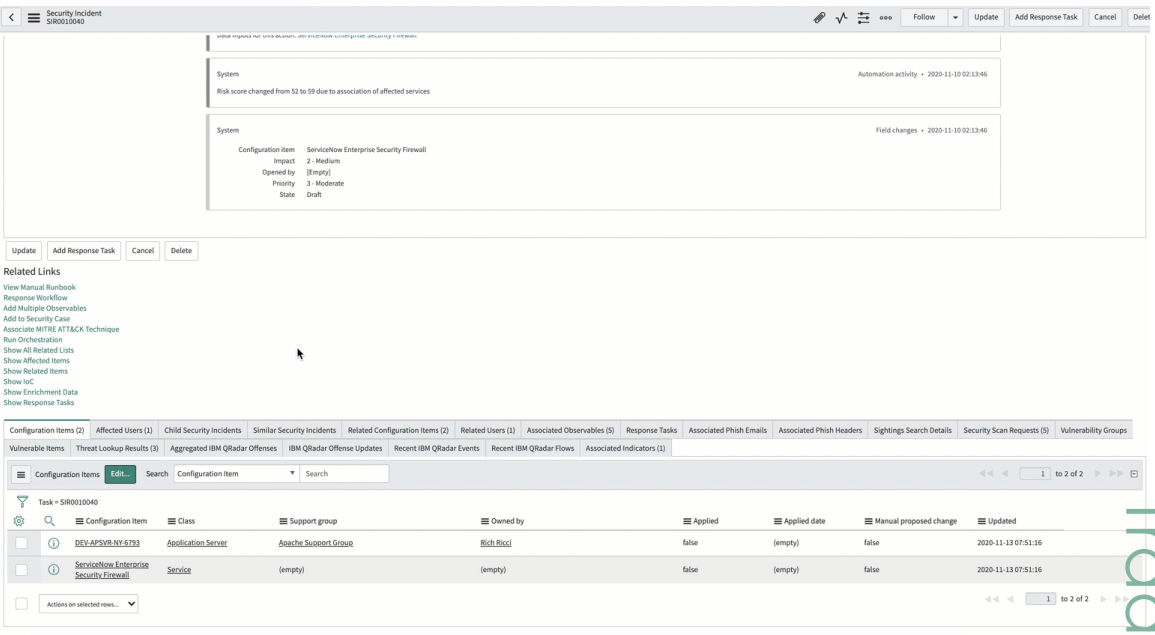
Si vous avez activé Déploiement automatique de MITRE-ATT&CK informations provenant des résultats de la recherche de menace à l'incident de sécurité, les informations sont automatiquement déployées. Si vous n'avez pas activé la reprise automatique, vous pouvez le faire manuellement.

Procédure

1. Accédez à la **Tout** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez enrichir avec les MITRE-ATT&CK informations.
3. Cliquez sur **Afficher toutes les listes connexes** et dans l'onglet **Résultats de la recherche de menace** .
4. Sélectionnez l'observable, puis dans le menu Actions, cliquez sur **Déployer les informations MITRE ATT&CK sur SI.**
   Vous pouvez sélectionner plusieurs observables et déployer les informations.
5. Cliquez sur **Recharger** pour confirmer les modifications.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'illustration suivante montre comment sélectionner un observable et déployer les résultats de la recherche de menace sur l'incident de sécurité.



Vous pouvez afficher la MITRE-ATT&CK carte pour confirmer que les résultats de la recherche de menace ont été déployés jusqu'à l'incident de sécurité.

Informations de MITRE-ATT&CK déploiement à partir des règles de détection

Activez le déploiement des MITRE-ATT&CK informations à partir des règles de détection vers les incidents de sécurité pour une meilleure analyse des incidents de sécurité et des menaces.

Avant de commencer

Rôle requis : aucun.

Assurez-vous d'avoir :

- Activez le déploiement automatique des informations MITRE ATT&ACK à partir des règles d'alerte vers la propriété d'incidents de sécurité dans le module Propriétés . Par défaut, cette option est désactivée. Pour plus d'informations, reportez-vous à la section Examiner les propriétés système MITRE-ATT&CK.
- Effectuez le mappage des règles de détection aux MITRE-ATT&CK TTP dans le module Règles de détection : module de mappage TTP MITRE ATT&CK . Le nom de la règle de détection doit correspondre au nom de la règle d'alerte qui déclenche l'incident de sécurité. Pour plus d'informations, consultez Créer et mapper des règles de détection.

Pourquoi et quand exécuter cette tâche

Si vous n'avez pas l'intention d'utiliser les règles d'extraction automatique du SIEM du système de base, activez le déploiement automatique des TTP en fonction du mappage de la règle de MITRE-ATT&CK détection. Vous pouvez renseigner l'alerte ou la règle d'événement qui déclenche l'incident de sécurité dans le champ Nom de la règle d'alerte . Vous pouvez également renseigner le champ Nom de la règle d'alerte à l'aide de l'intégration SIEM, de l'analyse des e-mails, de la création manuelle, etc.

Procédure

1. Accédez à la **Administration MITRE ATT&CK** > **Propriétés**.
2. Activez le déploiement automatique des informations MITRE ATT&ACK à partir des règles d'alerte vers la propriété incidents de sécurité, puis cliquez sur **Enregistrer**.

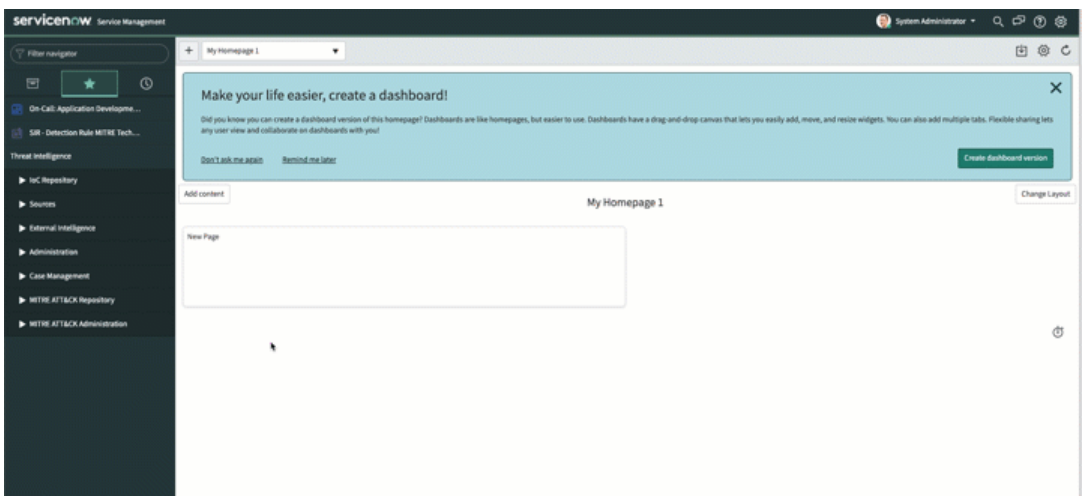
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, cette option est désactivée.

3. Vous devez renseigner le champ Nom de la **règle d'alerte** de l'incident de sécurité avec les règles d'alerte requises.

   Remarque : Veillez à ajouter le nom exact de la règle d'alerte . Pour ajouter plusieurs règles, vous devez les ajouter à l'aide d'un séparateur de virgules.

4. Cliquez avec le bouton droit sur le formulaire, puis cliquez sur **Enregistrer**.
   Si la valeur Nom de la règle d'alerte dans l'incident de sécurité correspond à un enregistrement dans le module Règle de détection - MITRE ATT&CK TTP Mapping, les techniques et tactiques correspondantes associées à la règle d'alerte sont automatiquement liées à l'incident de sécurité.



5. Ouvrez l'incident de sécurité, sélectionnez la **carte MITRE ATT&CK** et validez si les techniques sont déployées.
6. Activez **l'option Afficher l'origine des techniques** pour afficher l'origine des techniques. L'origine des techniques doit être la règle de détection.

Déployer des MITRE-ATT&CK informations à partir d'incidents de sécurité enfants

Si vous n'avez pas activé le cumul automatique des MITRE-ATT&CK informations, vous pouvez le faire manuellement.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Si vous avez activé Déploiement automatique de MITRE-ATT&CK Informations provenant d'incidents de sécurité enfants, les informations sont automatiquement remontées. Si vous n'avez pas activé la reprise automatique, vous pouvez le faire manuellement.

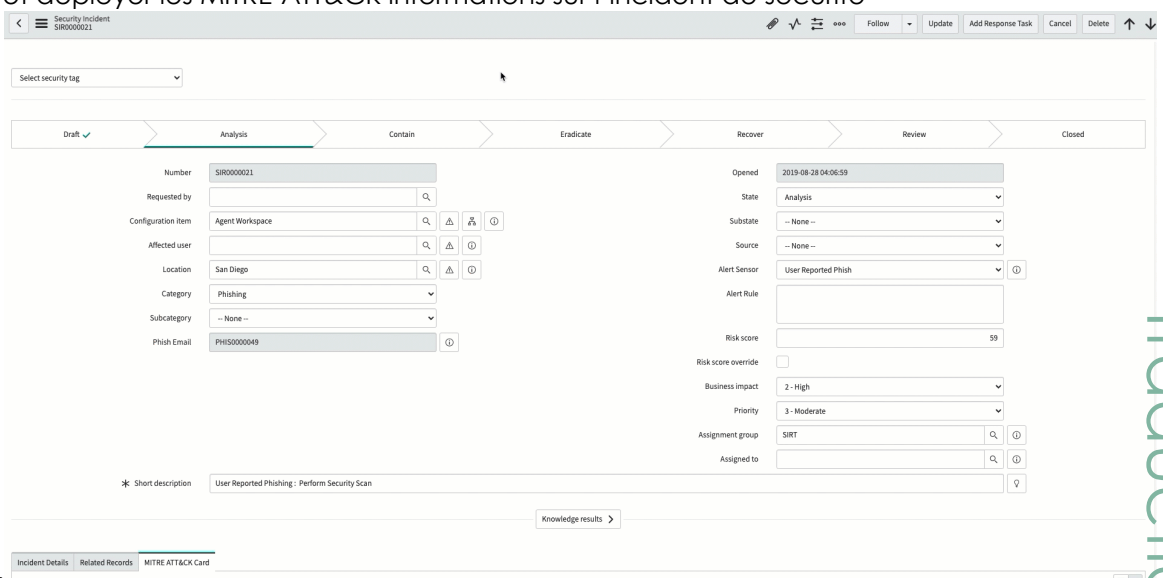
Procédure

1. Accédez à la **Tout** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité parent que vous souhaitez enrichir avec les informations enfant MITRE-ATT&CK .
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Incidents de sécurité enfants** .
4. Sélectionnez l'incident de sécurité enfant, puis, dans le menu Actions, cliquez sur **Déployer les informations MITRE ATT&CK sur le SI.**

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez cliquer sur **Afficher les informations MITRE ATT&CK** pour afficher les informations MITRE de l'incident de sécurité enfant avant de déployer les informations MITRE ATT&CK.

5. Cliquez sur **Recharger** pour confirmer les modifications.
6. Cliquez sur la **carte MITRE ATT&CK** pour afficher l'origine des techniques. L'illustration suivante montre comment sélectionner un incident de sécurité enfant et déployer les MITRE-ATT&CK informations sur l'incident de sécurité parent.



Vous pouvez afficher la carte MITRE-ATT&CK pour confirmer que les informations d'incident MITRE-ATT&CK de sécurité enfant ont été déployées vers l'incident de sécurité parent.

Effectuer une analyse des liens et une chasse aux menaces à l'aide MITRE-ATT&CK de filtres spécifiques

Corrélez et effectuez une analyse des liens des observables, des incidents de sécurité et MITRE-ATT&CK des informations connexes afin que votre organisation puisse commencer à rechercher les menaces.

Avant de commencer

Rôle requis : sn_ti.mitre_analyst, sn_si.read

Pourquoi et quand exécuter cette tâche

Une fois que vous avez associé les incidents de sécurité à MITRE-ATT&CK des informations, vous pouvez utiliser les filtres spécifiques pour la chasse aux MITRE-ATT&CK menaces. Utilisez les MITRE-ATT&CK filtres avec les filtres existants Réponse aux incidents de sécurité pour corréler et effectuer une analyse de liens.

Procédure

1. Accédez à la **Tout** > **Incidents de sécurité** > **Afficher les incidents**.
2. Cliquez sur **Mettre à jour la liste personnalisée** pour ajouter les MITRE colonnes.
3. Sélectionnez une condition de filtre afin de visualiser MITRE les informations connexes et les associations avec des incidents de sécurité ou des observables :
   - MITRE-ATT&CK Groupe d'adversaires
   - MITRE-ATT&CK Source de données
   - MITRE-ATT&CK Procédure (programme malveillant)
   - MITRE-ATT&CK Procédure (outils)

Traduction automatique

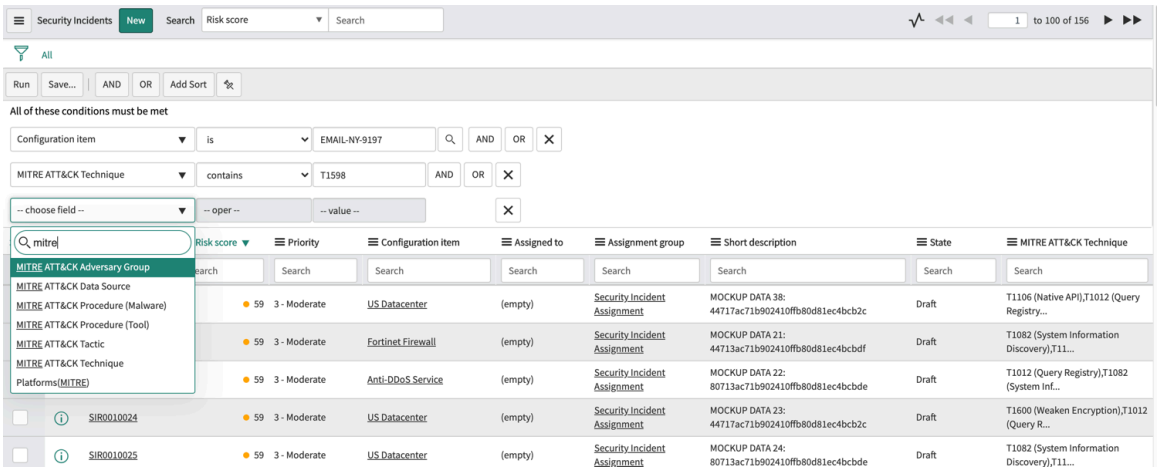
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- MITRE-ATT&CK Tactique
- MITRE-ATT&CK Technique

4. Créez une condition de filtre basée sur les critères ci-dessus et cliquez sur **Exécuter** pour effectuer une analyse de lien ou une corrélation entre les incidents de sécurité, les observables et MITRE-ATT&CK les informations connexes.

   Remarque : Les MITRE-ATT&CK données sont stockées sous forme de chaîne et vous ne pouvez utiliser **contains** que comme opérateur pour les conditions de filtre.

   Par exemple, si vous souhaitez vérifier qu'un élément de configuration (CI) est compromis, sélectionnez un CI. Vous pouvez ensuite corréler le CI avec les techniques présentes en ajoutant un MITRE-ATT&CK ID de technique. Vous pouvez ensuite continuer à développer vos critères de filtre pour corréler les informations et pour la chasse aux menaces.



MITRE-ATT&CK Carte thermique et navigateur

Vous pouvez utiliser la carte thermique et le MITRE-ATT&CK navigateur pour la navigation de base et pour visualiser la couverture globale de détection de votre technique.

Vue d'ensemble de la MITRE-ATT&CK carte thermique et du navigateur

Vous pouvez utiliser le navigateur avec les filtres primaires pour la navigation de base et l'observation des matrices ATT&CK. La carte thermique met en évidence le spectre de la couverture de détection, y compris les angles morts où votre organisation n'a aucune couverture. Cette option est disponible une fois que vous avez mappé la couverture de détection de la technique.

À l'aide de la carte thermique et du navigateur, vous pouvez :

- Identifiez rapidement et efficacement les options de détection de votre organisation et mettez en évidence les lacunes dans la couverture de détection des techniques.
- Traquez les menaces et effectuez une corrélation des menaces à l'aide des fonctionnalités associées.

Accéder à la carte thermique et au MITRE-ATT&CK navigateur

Accédez à la carte thermique et au MITRE-ATT&CK navigateur afin de visualiser la matrice qui vous permet d'utiliser ATT&CK.

Avant de commencer
Rôle requis : sn_ti.read, sn_ti.mitre_analyst

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous pouvez examiner la carte thermique, utiliser les filtres pour la corréler et effectuer une analyse des liens des informations, des observables et des incidents de MITRE-ATT&CK sécurité dans votre organisation.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Carte thermique et navigateur**.
   La carte thermique et le navigateur s'ouvrent dans un nouvel onglet.
2. Sélectionnez la source pour remplir la carte thermique.

   Remarque : Seules les collections et lesmatrices qui ont été activées apparaissent dans la liste source.

   Dans l'illustration suivante, vous voyez comment naviguer vers la carte thermique et le navigateur, et comment sélectionner la source, qui est Enterprise ATT&CK dans cet exemple.

   Accéder à la source et la sélectionner pour remplir la carte thermique
3. Utilisez le champ de recherche pour trouver rapidement une tactique ou une technique particulière à l'aide de son nom ou de son ID.

   L'illustration suivante montre comment rechercher une tactique, une technique ou toute information qu'elles contiennent. Utilisez la recherche pour explorer rapidement une tactique ou une technique spécifique.
4. Cliquez sur **Filtres** et sélectionnez un filtre parmi les filtres primaires ou avancés .
5. Cliquez sur **Appliquer** et contrôlez les filtres comme suit :
   - Pour enregistrer vos filtres, créez une vue personnalisée. Vous pouvez créer et enregistrer trois vues personnalisées.
   - Pour supprimer les filtres sélectionnés, cliquez sur **Restaurer les filtres par défaut** pour charger votre vue enregistrée par défaut.
   - Pour effacer tous les filtres et votre vue existante, cliquez sur **Effacer tous les filtres**.

   Remarque : Les vues que vous enregistrez sont spécifiques à un utilisateur.
6. Cliquez sur **Masquer les sous-techniques** pour supprimer toutes les sous-techniques de la vue de la carte thermique.
   Si une technique comporte des sous-techniques, vous pouvez cliquer sur l'icône de développement pour afficher les sous-techniques.

À l'aide des vues personnalisées

Les vues personnalisées de la carte thermique et du MITRE-ATT&CK navigateur vous permettent d'enregistrer et d'afficher vos filtres préférés la prochaine fois que vous atterrirez sur la carte thermique.

Remarque : Vous pouvez créer et enregistrer trois vues personnalisées pour chaque MITRE-ATT&CK collection par utilisateur.

Créer une vue

Une fois que vous avez sélectionné les filtres requis dans les filtres primaires ou avancés , cliquez sur le bouton représentant des points de suspension (...) dans l'en-tête Filtres et

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sélectionnez **Créer une nouvelle vue**. Entrez le nom de la vue personnalisée et **enregistrez la vue**.

Vues par défaut

Cliquez sur **Enregistrer cette vue par défaut** pour charger directement la vue la prochaine fois que vous atterrirez sur la carte thermique. Vous pouvez définir une vue par défaut pour chacune des collections.

Remarque : Si vous mettez à niveau le module d'extension Renseignements sur les menaces à partir d'une version antérieure, votre vue par défaut existante de l'ancienne version apparaît comme une vue personnalisée.

L'illustration montre comment créer une vue personnalisée dans la carte thermique

Mettre à jour une vue

Vous pouvez apporter des mises à jour à une vue personnalisée existante en modifiant les filtres primaires ou avancés requis. Sélectionnez une vue personnalisée, mettez à jour les filtres selon vos besoins, puis cliquez sur le bouton représentant des points de suspension (...) dans l'en-tête Filtres et sélectionnez **Mettre à jour la vue** pour enregistrer les filtres.

Cette illustration montre comment mettre à jour une vue personnalisée.

Gérer les vues personnalisées

Utilisez les cases à cocher en regard de chaque vue personnalisée pour appliquer le filtre d'affichage personnalisé sélectionné.

Cliquez sur le bouton représentant des points de suspension (...) en regard du nom de chaque vue personnalisée pour contrôler les vues personnalisées comme suit :

- Définissez une vue par défaut.
- Supprimez une vue personnalisée comme vue par défaut. Cela ne supprime pas la vue personnalisée.
- Renommez la vue personnalisée.
- Supprimez la vue personnalisée.

Cette illustration montre comment gérer les vues personnalisées.

Exporter une vue enregistrée

Pour exporter les vues personnalisées enregistrées vers des fichiers JSON, cliquez sur les points de suspension (...) dans l'en-tête Filtres et sélectionnez **Exporter les vues enregistrées**. Cliquez sur l'icône de téléchargement de la vue personnalisée que vous souhaitez télécharger sur votre ordinateur local.

Cette illustration montre comment exporter des vues personnalisées.

Importer une vue

Vous ne pouvez importer que des fichiers JSON. Pour importer les vues personnalisées, cliquez sur le bouton représentant des points de suspension (...) dans l'en-tête Filters (Filtres) et sélectionnez **Importer la vue (json).**

Vérifiez les conditions suivantes lors de l'importation des vues :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous ne pouvez importer que le format de fichier JSON.
- Vous ne pouvez importer qu'une seule vue ou un seul fichier à la fois.
- Vous ne pouvez pas importer si vous avez déjà trois vues personnalisées dans vos filtres. Supprimez une vue personnalisée et importez-la.
- Vous ne pouvez pas importer une vue avec un nom de vue personnalisé existant. Renommez une vue avant de l'importer.

Cette illustration montre comment importer une vue.

Navigateur avec filtres primaires

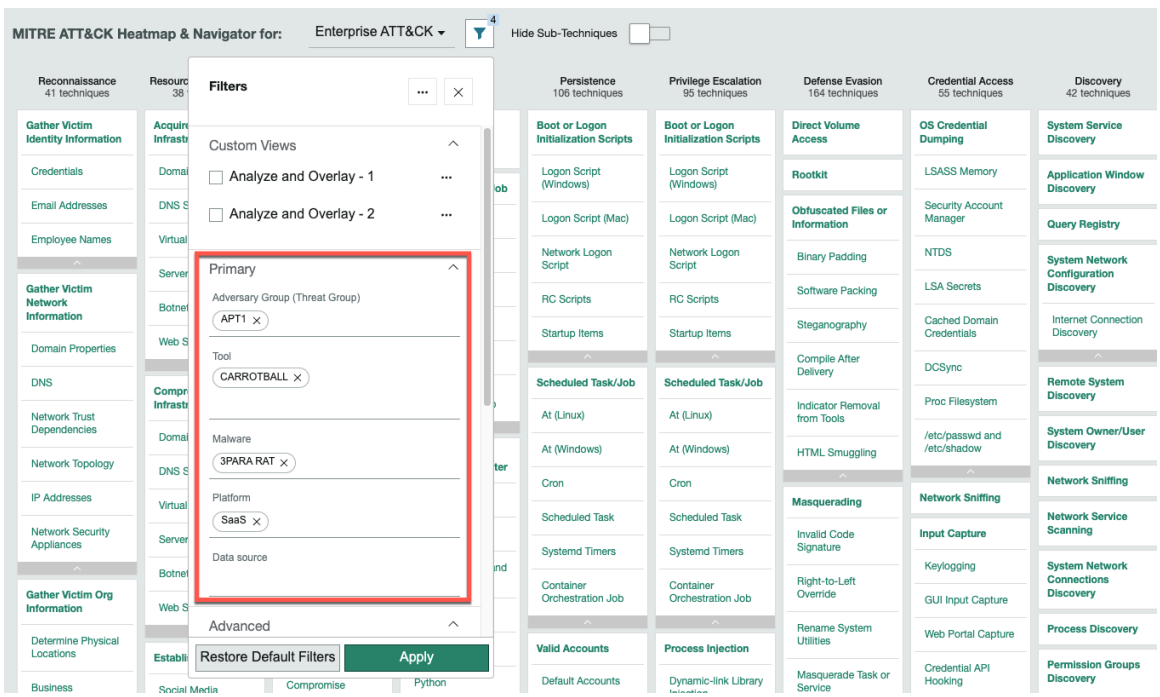
Utilisez les filtres primaires pour filtrer les techniques dans le MITRE-ATT&CK navigateur. Les informations contenues dans le MITRE-ATT&CK référentiel peuvent être sélectionnées.

Filtre	Description
Groupe d'adversaires (groupe de menaces)	Ensembles d'activités d'intrusion connexes qui sont suivis par un nom commun dans la communauté de sécurité. Les groupes peuvent désigner divers groupes de menaces, groupes d'activités, acteurs de menace, ensembles d'intrusion et campagnes. Vous pouvez ajouter plusieurs groupes au filtre **Groupe d'adversaires (groupe de menaces**). Par exemple, vous ajoutez APT1 et AT12, car il s'agit de deux groupes de menaces attribués à la Chine. Bien que les deux groupes puissent cibler des sources différentes, ils pourraient utiliser des techniques similaires.
Outil	Logiciel légitime utilisé par les auteurs de menace pour effectuer des attaques. Vous pouvez comprendre comment les auteurs de menace exécutent les campagnes si vous savez comment et quels outils sont utilisés par les auteurs de menace. La catégorie Outils comprend les logiciels introuvables sur un système d'entreprise et les logiciels disponibles dans un système d'exploitation déjà présent dans un environnement tel que les utilitaires Microsoft Windows. Par exemple, gsecdump est un dumper d'informations d'identification accessible au public que le groupe d'adversaires APTI1 utilise pour obtenir des hachages de mots de passe et des secrets LSA (Local Security Authority) à partir des systèmes d'exploitation Microsoft Windows.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Filtre	Description
Programme malveillant	Logiciel commercial, fermé personnalisé ou open source destiné à être utilisé à des fins malveillantes par des adversaires. Par exemple, PlugX, CHOPSTICK, etc
Plateforme	Tactiques et techniques représentées MITRE-ATT&CK dans une plateforme particulière. Par exemple, MITRE-ATT&CK prend en charge ces plateformes dans la matrice ATT&CK d'entreprise : Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Réseau.
Source de données	Sources de données que vous collectez dans votre environnement et utilisez pour détecter MITRE-ATT&CK des techniques. Il peut s'agir, par exemple, de la surveillance des DLL et des extensions de navigateur.

L'illustration suivante montre tous les filtres principaux disponibles dans le MITRE-ATT&CK navigateur.



Utilisation d'une carte thermique avec des fonctionnalités primaires et avancées

Vous pouvez utiliser une carte thermique avec des filtres avancés pour effectuer une analyse en corrélant les incidents de sécurité avec MITRE-ATT&CK des informations.

Afficher les ID de technique

Vous pouvez afficher les MITRE-ATT&CK ID de techniques avec les noms de techniques lorsque vous sélectionnez le filtre **Afficher les ID de techniques** .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les ID de techniques sur une carte thermique

Afficher les techniques pertinentes par priorité

Pour filtrer les techniques en fonction de leur priorité pertinente dans le navigateur, sélectionnez **Filtrer par filtre de priorité pertinente de la technique** , puis sélectionnez la **priorité pertinente** dans le menu. Vous pouvez affecter plusieurs priorités pour le filtrage. Vous pouvez également pointer du doigt les techniques de la carte thermique pour connaître la priorité de la technique.

Les informations de priorité pertinentes sont basées sur l'ordre de priorité que vous avez défini dans le champ de priorité pertinente des techniques .

Cette illustration montre le filtrage par priorité pertinente.

Afficher la couverture de détection technique

Pour afficher la couverture globale de la détection de la technique dans la carte thermique, sélectionnez le filtre **Afficher la couverture de détection** de la technique. La carte thermique met en évidence le spectre visuel de la couverture de détection, y compris les angles morts où vous n'avez aucune couverture. La définition de notation du système de base et les couleurs ont été définies dans la couverture de détection de technique. Les informations ont été extraites automatiquement de la couverture globale de détection de la technique.

Par exemple, les zones de la carte thermique marquées en rouge indiquent un manque de détection. Les zones marquées en bleu indiquent la présence de capacités de détection complètes. Les zones marquées en orange, jaune et bleu clair reflètent des capacités de détection partielles.

- La visualisation des couleurs est basée sur la définition de la technique et le codage couleur que vous définissez.
- La visualisation de la couverture est basée sur le mappage de couverture de détection technique que vous définissez.
- Si vous modifiez la définition de couverture du système de base, les icônes Type de couverture ne s'affichent pas avec les techniques de la carte thermique.

> **Remarque :** La carte thermique fonctionne comme prévu lorsque vous modifiez les mêmes champs que la couverture de détection technique et les couleurs de couverture définies par le système de base.

Dans cette illustration, vous voyez la couverture de détection de technique pour toutes les techniques et sous-techniques et le type de couverture avec leurs couleurs et icônes.

Couverture de détection technique de carte thermique

Afficher la couverture d'atténuation de technique

Pour afficher la couverture globale de l'atténuation de la technique dans la carte thermique, sélectionnez le filtre Afficher la couverture de l'atténuation de la technique. La carte thermique met en évidence le spectre visuel de la couverture d'atténuation, y compris les zones que vous ne couvrez pas. La couverture d'atténuation, les couleurs et les plages de pourcentage ont été définies dans la définition de couverture d'atténuation. L'information est extraite de la couverture globale de l'atténuation des techniques.

Par exemple, les techniques surlignées en rouge indiquent qu'il n'y a pas de couverture d'atténuation, l'orange indique une mauvaise couverture d'atténuation et le bleu indique une excellente couverture d'atténuation.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

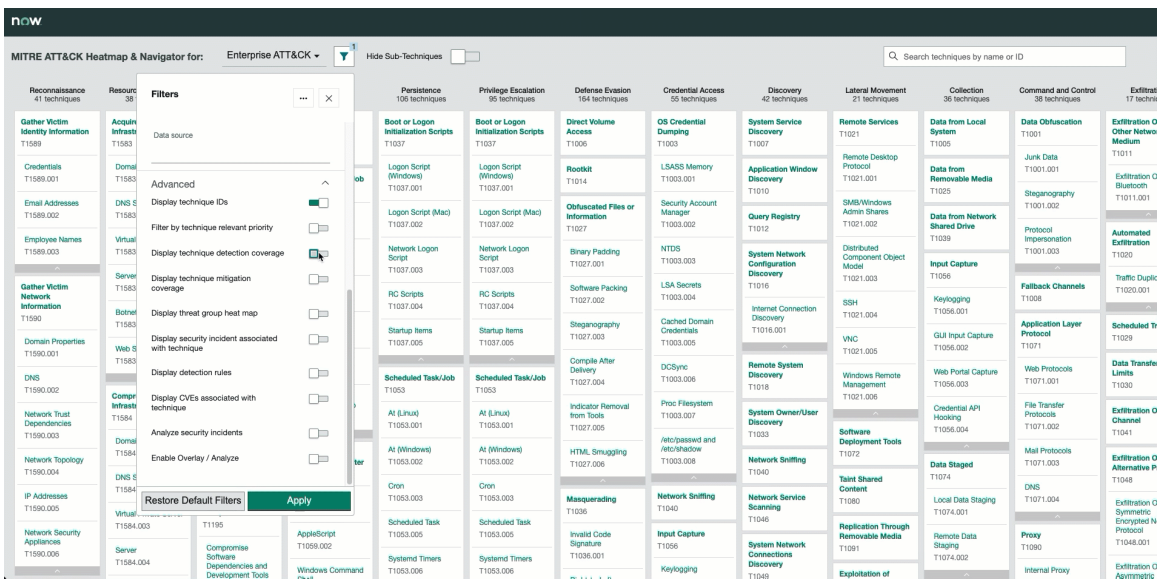
- La visualisation des couleurs est basée sur la définition d'atténuation de technique et le codage couleur que vous définissez.
- La visualisation de la couverture est basée sur le mappage de couverture d'atténuation de technique que vous définissez.
- Si vous modifiez la définition de couverture d'atténuation du système de base, les icônes Type de couverture d'atténuation ne s'affichent pas avec les techniques de la carte thermique.

> **Remarque :** La carte thermique fonctionne comme prévu lorsque vous modifiez les mêmes champs que la couverture d'atténuation de technique et les couleurs de couverture définies par le système de base.

Cette illustration montre la carte thermique de couverture d'atténuation de technique

Afficher la couverture de détection et d'atténuation

Vous pouvez utiliser les filtres de couverture de détection de technique et d'atténuation de technique ensemble pour obtenir un aperçu de la pertinence de la détection de technique et atténuer la couverture pour votre organisation.



Cette illustration montre comment utiliser simultanément le filtre de détection et d'atténuation.

Afficher le groupe de menaces

Pour afficher les informations du groupe de menaces à la technique sur la carte thermique, sélectionnez **Afficher la carte thermique du groupe de menaces**. Vous pouvez mesurer le nombre de groupes de menaces qui utilisent une technique particulière. La probabilité d'une attaque utilisant une technique particulière augmente lorsque vous avez un nombre élevé d'attaquants. Les plages de groupes de menaces et les couleurs de la carte thermique ont été définies dans la définition de la carte thermique Groupe de menaces – Technique.

- La visualisation des couleurs pour la carte thermique et le texte est basée sur la définition de la carte thermique du groupe de menaces à la technique.
- La visualisation de la plage de groupes de menaces est basée sur le mappage de groupes de menaces à techniques.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous ne pouvez pas utiliser le filtre **Afficher la carte thermique du groupe de menaces** lorsque la couverture de détection de technique ou la couverture d'atténuation de technique sont activées. Cette illustration montre les informations sur le groupe de menaces sur la carte thermique.

Afficher les incidents de sécurité associés à la technique

Pour afficher les techniques qui sont fréquemment exploitées dans votre organisation et qui ont donné lieu à des incidents de sécurité, cliquez sur **Afficher l'incident de sécurité associé à la technique**. Vous pouvez afficher plus d'informations sur chacun des incidents de sécurité associés en cliquant sur le lien qui s'ouvre dans une nouvelle fenêtre pour analyse. Incidents de sécurité associés à une technique.

- Priorité : sélectionnez **Priorité de l'incident de sécurité** pour filtrer en fonction de la priorité de l'incident de sécurité.
- Plage de dates : sélectionnez la **plage de dates des incidents de sécurité** pour filtrer les problèmes de sécurité par plage de dates.
- Faux positifs : sélectionnez **Filtrer les incidents de sécurité signalés comme faux positifs** pour supprimer les problèmes de faux positifs. La sélection de ce filtre réduit le nombre d'incidents de sécurité que vous voyez sur la carte thermique.

Lorsque vous utilisez ce filtre avec le filtre **Afficher la couverture de détection de technique** , il vous donne un aperçu de la pertinence de la couverture de détection de technique pour votre organisation jusqu'à la date sélectionnée.

Par exemple, lorsque vous activez les deux filtres, vous pouvez voir que dans le cadre de la tactique d'évasion défensive, la technique de mascarade n'est pas couverte. Si l'on regarde plus loin, la technique de masquage est liée à la tâche ou au service de mascarade, qui est également associé à un incident de sécurité. Cela montre qu'il existe une lacune dans la couverture de détection de technique pour la technique de masquage et que vous voudrez peut-être réviser la couverture globale de détection de technique.

Afficher les règles de détection

Pour voir si vous avez défini les règles de détection pour une technique particulière, cliquez sur **Afficher les règles de détection**. Vous pouvez également voir chaque règle de détection associée avec sa définition.

Ces informations sont basées sur le mappage de règles de détection que vous avez défini. Affichez les règles de détection associées.

Afficher les CVE associés à la technique

Pour afficher les informations sur les vulnérabilités et les expositions communes (CVE) associées à chacune des techniques, cliquez sur **Afficher les CVE associés à la technique**. Les informations CVE à technique sont basées sur les informations disponibles dans le module CVE - Technique Mapping. Cela vous donne un aperçu des vulnérabilités connues et vous permet de savoir si des adversaires peuvent potentiellement exploiter votre organisation.

Important : La carte thermique est améliorée pour afficher uniquement les CVE pertinents associés aux VIT

Pour afficher les VIT associés aux CVE et aux techniques, sélectionnez **Afficher les VIT associés aux CVE et aux techniques**. En outre, pour filtrer davantage les techniques sans VIT, sélectionnez **Masquer les techniques sans VIT**. Les informations CVE et VIT que vous affichez sont extraites du Réponse aux vulnérabilités produit dans votre environnement. Vous pouvez

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

afficher la liste filtrée des CVE et des VIT dans la carte thermique et accéder à chaque CVE ou VIT pour chaque technique de la carte thermique.

Remarque :

- **L'affichage des CVE associés à la technique** n'est disponible que lorsque le Réponse aux vulnérabilités produit est installé dans votre environnement.
- Les informations VIT et CVE sont calculées en fonction de la tâche planifiée que vous définissez dans le MITRE-ATT&CK Propriétés de. La tâche planifiée du système de base est définie sur 24 heures.

Lorsque vous utilisez ce filtre avec le filtre **Afficher l'incident de sécurité associé à la technique** , vous pouvez savoir si les vulnérabilités connues ont causé des incidents de sécurité dans votre organisation.

Vous pouvez afficher plus d'informations sur chaque CVE afin d'analyser si les CVE sont pertinents pour votre organisation. Pour ce faire, affichez les éléments de vulnérabilité. Si des éléments de vulnérabilité sont créés, vous pouvez afficher plus d'informations sur les informations CI associées dans le Réponse aux vulnérabilités module. Vous pouvez également passer en revue la gravité et la priorité pour prendre des décisions éclairées. Examinez les CVE pour prendre des décisions éclairées.

Analyser les incidents de sécurité

Pour analyser les incidents de sécurité et examiner les techniques utilisées par un adversaire pour une attaque, cliquez sur **Analyser les incidents de sécurité**. Vous pouvez ajouter plusieurs incidents de sécurité à des fins d'analyse à l'aide de chaînes séparées par des virgules.

Ce filtre vous aide à analyser un incident de sécurité. Vous pouvez savoir pourquoi l'incident s'est produit, quelles techniques ont été exploitées, si des acteurs malveillants connus ont été impliqués, si les acteurs malveillants ont utilisé une séquence particulière pour une attaque, etc. Étant donné que vous pouvez analyser plusieurs incidents de sécurité en même temps, vous pouvez corréler les informations pour voir s'ils sont liés ou s'il s'agit d'un incident isolé. Si les incidents de sécurité sont liés et que vous observez une tendance, vous pouvez examiner leur progression sur la chaîne de destruction pour arrêter l'attaque ou élaborer une stratégie de défense pour votre organisation.

Lorsque vous utilisez le filtre **Analyser les incidents de sécurité** avec des filtres primaires, tels qu'un **groupe d'adversaires**, vous pouvez établir une corrélation si des adversaires connus sont impliqués. Par exemple, lorsque plusieurs incidents de sécurité sont en cours d'analyse, les techniques associées aux incidents de sécurité sont présentes sous la forme d'une chaîne de frappe. Lorsque vous chevauchez les informations avec celles de l'adversaire, vous remarquez un chevauchement entre les techniques associées à l'incident de sécurité et les techniques associées à l'adversaire. Seules les informations sur la technique superposée s'affichent si les deux filtres sont activés.

Analyser les incidents de sécurité

Utilisation de la superposition pour analyser les incidents de sécurité et les groupes d'adversaires

Utilisez le filtre **Activer la superposition/Analyser** pour afficher le comportement de l'adversaire et analyser un ou plusieurs des incidents de sécurité et corréler les informations pour voir si une attaque est un incident isolé ou une attaque coordonnée par un adversaire connu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, vous pouvez désormais afficher les incidents de sécurité et le comportement de la chaîne de destruction de l'adversaire dans la même vue. Cette vue fournit des informations de chevauchement qui vous informent de l'attaque et du comportement connu de l'adversaire. Cela vous permet d'analyser s'il s'agit d'une attaque isolée ou d'une attaque coordonnée par un adversaire connu.

L'activation du filtre d'analyse de superposition ignore tous les filtres primaires, à l'exception du filtre de **groupe Adversaire** , et ignore le filtre avancé **Filtrer par priorité pertinente de technique** lors de la génération d'une vue.

Une fois que vous avez activé le filtre d'analyse de superposition, utilisez la palette de couleurs pour affecter des couleurs aux éléments suivants :

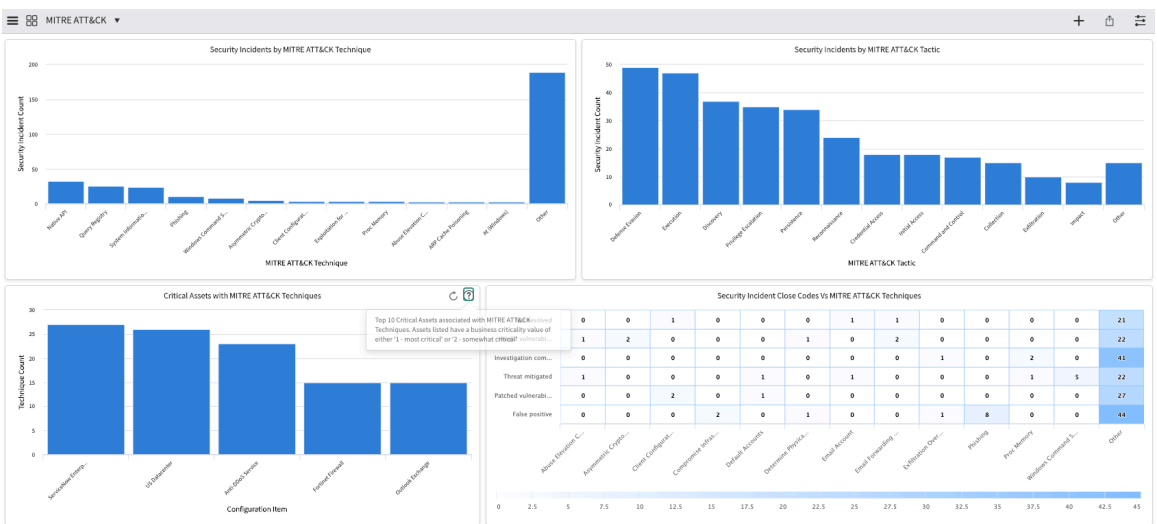
- Analyser l'incident de sécurité
- Groupe d'adversaires
- Superposition

L'illustration suivante montre que le groupe d'adversaires APT18 est réparti sur plusieurs techniques et tactiques dans la chaîne de destruction. L'analyse montre également qu'il existe trois techniques qui se superposent au groupe d'adversaires et aux incidents de sécurité que vous suivez. Cette illustration montre les informations de superposition de l'adversaire et de l'incident de sécurité.

Utilisation du MITRE-ATT&CK tableau de bord

Le MITRE-ATT&CK tableau de bord fournit une vue de direction de la couverture des sources de données, des tactiques et des techniques utilisées dans votre organisation.

Le MITRE-ATT&CK module de vue d'ensemble affiche MITRE-ATT&CK des informations sur les incidents de sécurité, y compris les tendances et les rapports. Vous pouvez cliquer sur n'importe quelle partie d'un widget (barre, point de données, table, etc.) pour afficher les données spécifiques à cette partie.



Utilisez le tableau de bord pour afficher vos données liées à la MITRE-ATT&CK sécurité

Utilisez le MITRE-ATT&CK tableau de bord pour obtenir une vue d'ensemble de la couverture des sources de données, des tactiques et des techniques utilisées dans votre organisation.

Avant de commencer

Rôle requis : sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

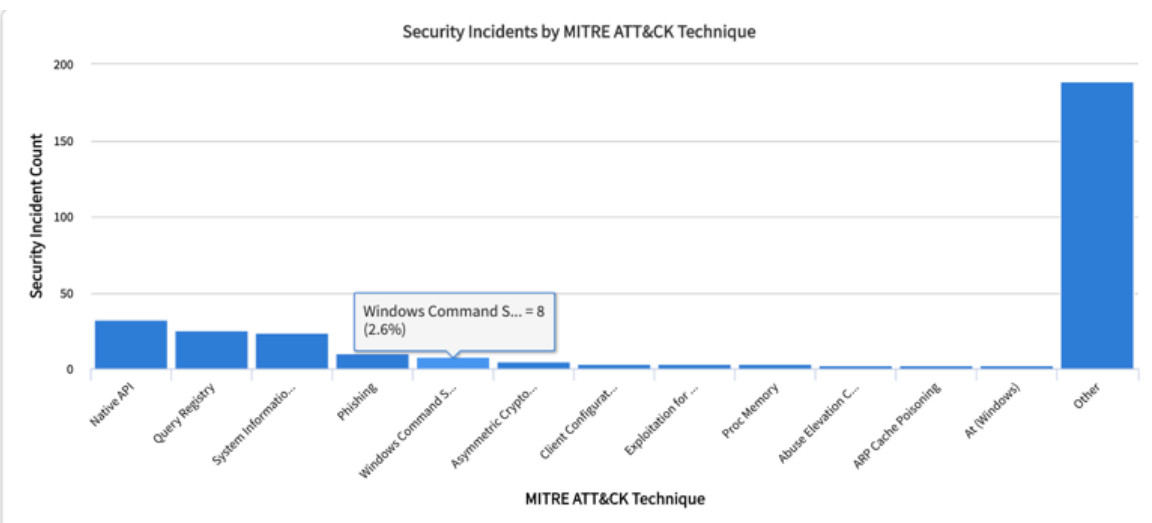
1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Vue d'ensemble**.
2. Cliquez sur l'un des widgets suivants pour afficher des détails supplémentaires :
   - Incidents de sécurité par MITRE-ATT&CK technique
   - Incidents de sécurité par MITRE-ATT&CK tactique
   - Actifs critiques avec MITRE-ATT&CK techniques
   - Codes de fermeture des incidents de sécurité par rapport aux MITRE-ATT&CK techniques
   - Techniques MITRE-ATT&CK par couverture de détection
   - Techniques MITRE-ATT&CK par couverture d'atténuation
   - Groupes de menaces par technique MITRE-ATT&CK
   - CVE par la technique MITRE-ATT&CK

Widgets MITRE-ATT&CK

Le MITRE-ATT&CK module de vue d'ensemble se compose de widgets qui vous permettent de corréler les informations avec les informations sur les MITRE-ATT&CK incidents de sécurité dans votre environnement.

Exemple d'incidents de sécurité par MITRE-ATT&CK technique

Dans cet exemple, le widget **Incidents de sécurité par technique MITRE ATT&ck** affiche les techniques par incident de sécurité dans l'environnement d'une organisation au cours des 90 derniers jours.

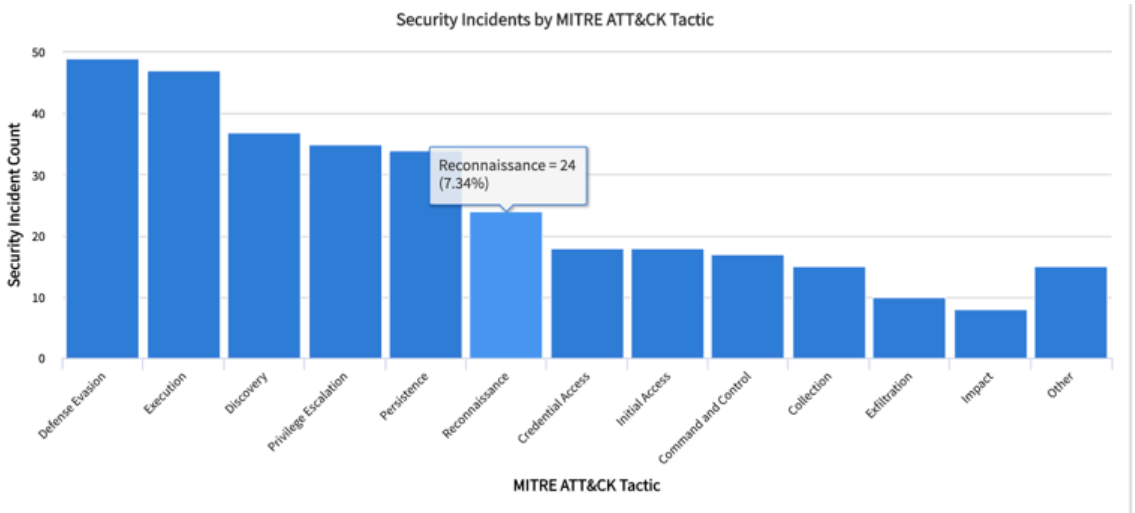


Exemple d'incidents de sécurité par MITRE-ATT&CK tactique

Dans cet exemple, le widget **Security Incidents by MITRE ATT&CK Tactic (Incidents de sécurité par MITRE ATT&CK Tactic**) affiche les principales tactiques par incident de sécurité dans l'environnement d'une organisation au cours des 90 derniers jours.

Traduction automatique

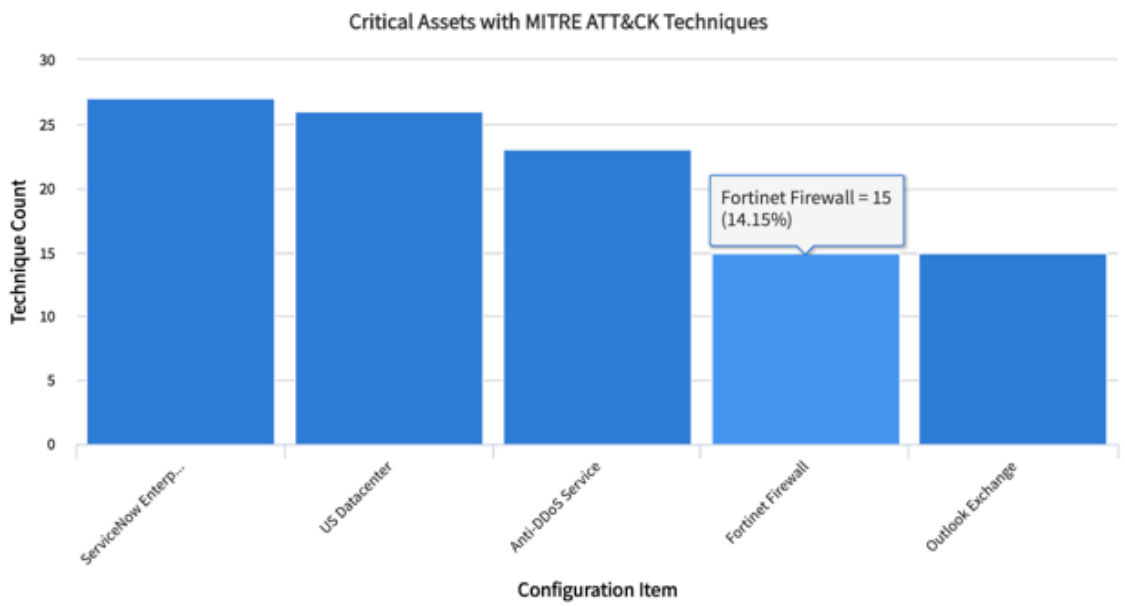
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Exemple d'actifs critiques avec MITRE-ATT&CK techniques

Dans cet exemple, le widget **Actifs critiques avec les techniques MITRE ATT&CK** affiche les 10 principaux actifs critiques associés aux MITRE-ATT&CK techniques. Les actifs ont une criticité opérationnelle de 1 (très critique) ou de 2 (assez critique).

Ce rapport permet à une organisation de voir les types et le nombre de techniques utilisées pour mener des attaques contre les actifs critiques.



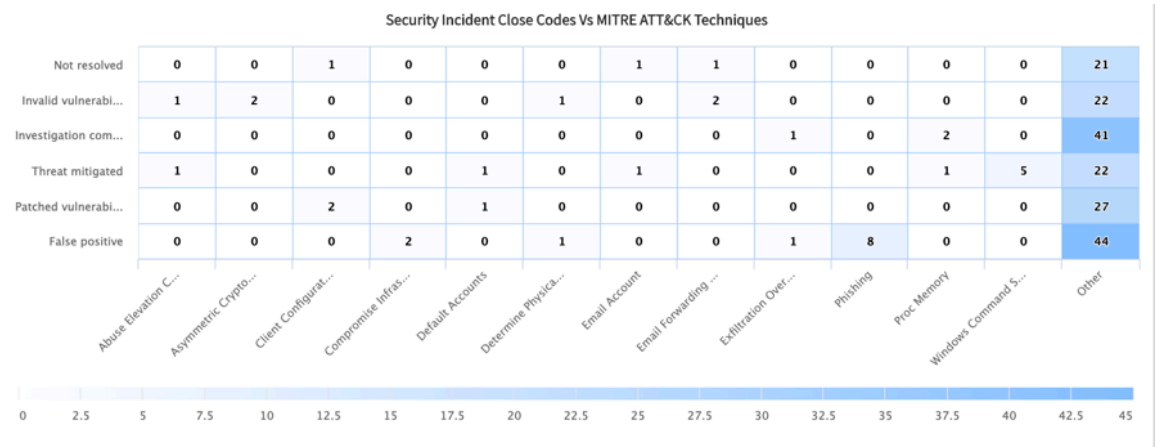
Exemple de codes de fermeture d'incidents de sécurité par rapport aux MITRE-ATT&CK techniques

Dans cet exemple, le widget **Codes de fermeture d'incident de sécurité par rapport à** *MITRE-ATT&CK* **Techniques** affiche les codes de fermeture d'incident de sécurité qui ont été mappés par rapport aux principales techniques identifiées dans l'environnement d'une organisation.

L'axe X affiche les principales techniques utilisées pour mener des attaques contre l'entreprise, et l'axe Y affiche les codes fermés.

Traduction automatique

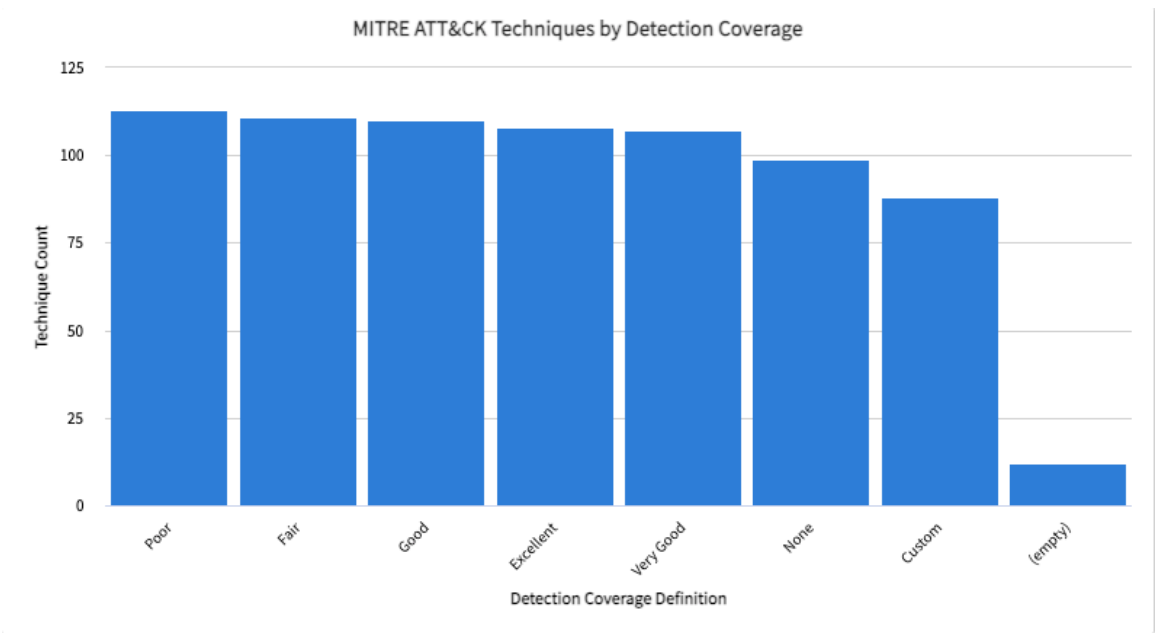
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Exemple de couverture de détection par MITRE-ATT&CK techniques

Dans cet exemple, le widget **MITRE-ATT&CK Techniques par couverture de détection** affiche le nombre de techniques par couverture de détection dans votre environnement.

L'axe X affiche le nombre de techniques et l'axe Y affiche les types de couverture de détection.

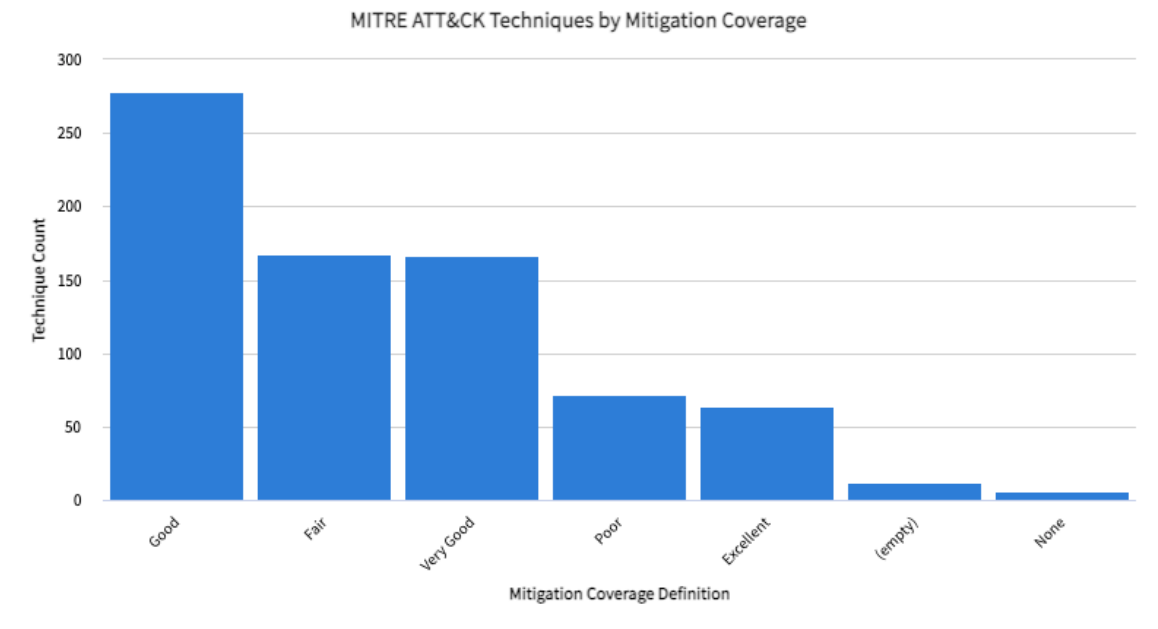


Exemple de couverture d'atténuation par MITRE-ATT&CK techniques

Dans cet exemple, le widget **Techniques MITRE-ATT&CK par couverture d'atténuation** affiche le nombre de techniques par couverture d'atténuation dans votre environnement.

L'axe X affiche le nombre de techniques et l'axe Y affiche les types de couverture d'atténuation.

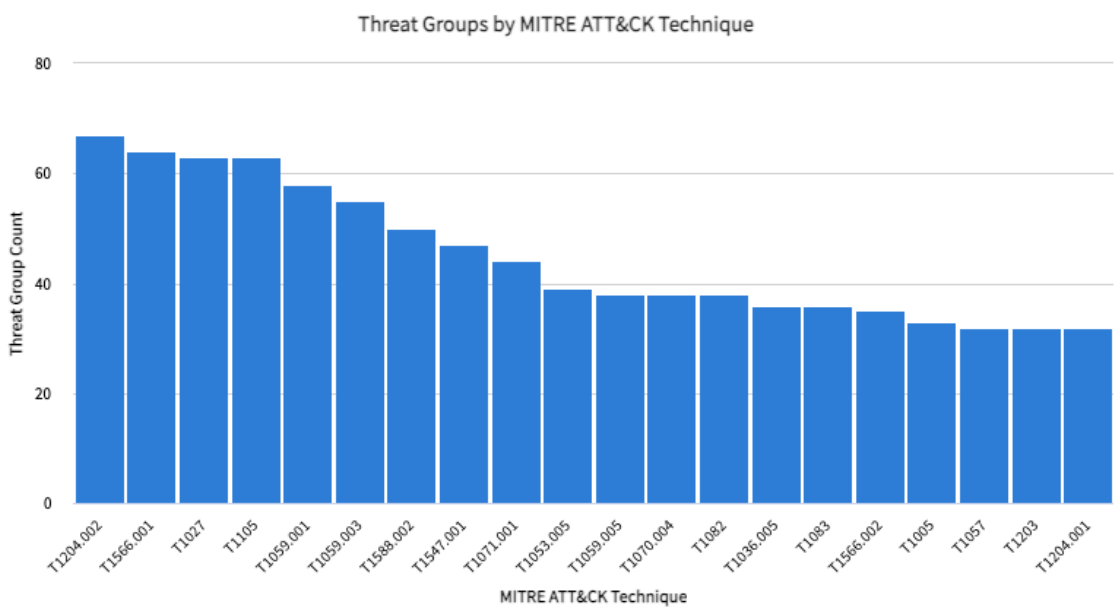
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Exemple de groupes de menaces par MITRE-ATT&CK techniques

Dans cet exemple, le widget **Groupes de menaces par technique MITRE-ATT&CK** affiche les techniques par nombre de groupes de menaces. Ce widget affiche 20 techniques avec le nombre de groupes de menaces le plus élevé.

L'axe X affiche le nombre de groupes de menaces et l'axe Y affiche les MITRE-ATT&CK techniques.



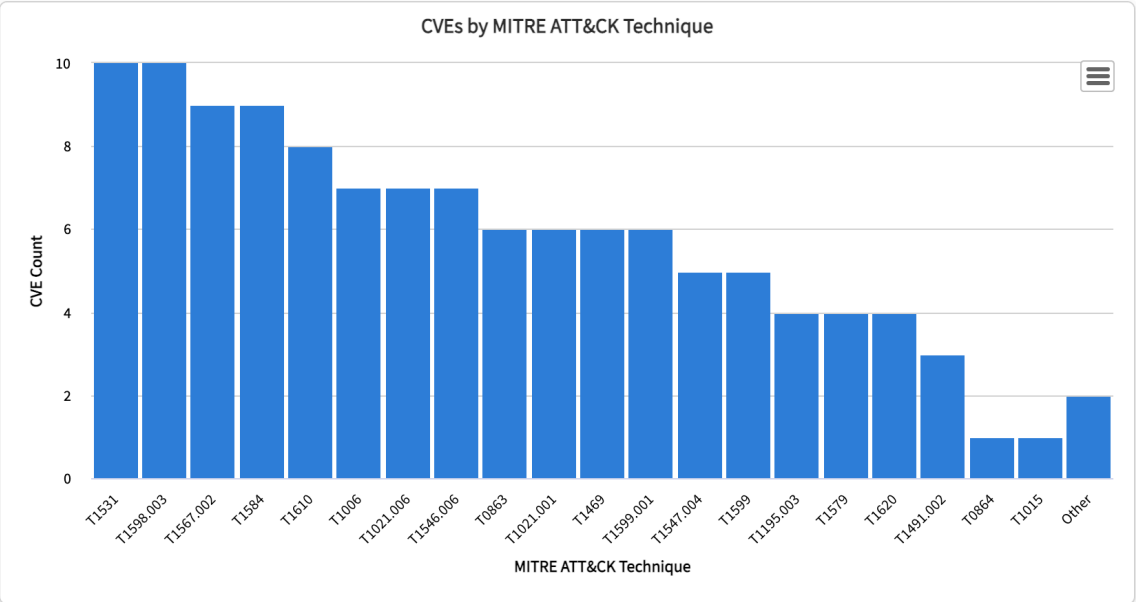
Exemple de CVE par MITRE-ATT&CK techniques

Dans cet exemple, le widget **CVEs by MITRE-ATT&CK Technique affiche les** techniques avec le nombre de CVE pertinent dans votre environnement.

L'axe des x affiche le nombre de CVE pertinent et l'axe des y affiche les MITRE-ATT&CK techniques.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Administration Renseignements sur les menaces

Le Renseignements sur les menaces système de base est prêt à l'emploi lors de l'activation. Vous pouvez ajouter des enregistrements à certains modules dans le menu de l'application Administration, mais la plupart sont déjà renseignés avec des informations standard du secteur.

Les applications suivantes sont disponibles dans le module **Administration** de la Renseignements sur les menaces barre de navigation :

Applications d'administration de Threat Intelligence

Application	Description
Propriétés	Renseignements sur les menaces Les propriétés vous permettent de contrôler le fonctionnement de différents aspects du système, y compris la définition des clés API.
Mécanismes d'attaque	Ce module organise les schémas d'attaque de manière hiérarchique, en fonction des mécanismes fréquemment utilisés lors de l'exploitation d'une vulnérabilité.
Motivations de l'attaque	Ce module répertorie les motivations d'attaque possibles qui déterminent l'intensité d'une attaque par un acteur de menace ou un ensemble d'intrusions.
Méthodes de Découverte	Ce module décrit comment les incidents de sécurité sont détectés.
Actualise	Cette fonctionnalité a été déconseillée.
Types des indicateurs	Ce module est utilisé pour caractériser les indicateurs de cybermenace composés de modèles qui identifient certaines conditions observables, ainsi que d'informations contextuelles sur la signification des modèles et sur la façon dont ils sont traités et sur le moment où ils sont traités.
Types d'infrastructure	Ce module répertorie les classifications possibles de l'infrastructure.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications d'administration de Threat Intelligence (suite)

Application	Description
Effets souhaités	Cette application est utilisée pour exprimer l'effet escompté d'un acteur de menace.
Options de logiciel malveillant	Ce module répertorie les capacités possibles des logiciels malveillants.
Types de programmes malveillants	Ce module répertorie les classifications possibles des logiciels malveillants.
Notifications	Ce module permet de créer des notifications par e-mail. Il s'agit de préciser quand ils sont envoyés, qui les reçoit et ce qu'ils contiennent.
Types des observables	Ce module répertorie les classifications possibles d'un observable, telles qu'une adresse IP ou un hachage de fichier.
Types de rapports	Ce module répertorie les classifications possibles des rapports de menace.
Rôles d'acteur de menace	Ce module énumère les rôles que jouent les auteurs de menace.
Types d'acteurs de menace	Ce module caractérise les acteurs malveillants (ou adversaires) représentant une menace de cyberattaque, y compris l'intention présumée et le comportement historiquement observé.
Calculateurs de résultats de la recherche de menace	Ce module calcule les résultats en fonction des réponses reçues. Pour les intégrations tierces qui fournissent les résultats calculés, le calculateur de résultat de la recherche de menace mappe les résultats aux résultats pris en charge dans le système. Pour plus d'informations, consultez Calculateurs de résultats de la recherche de menace.
Types d'outil	Ce module répertorie les classifications possibles des outils.

Calculateurs de résultats de la recherche de menace

Le calculateur de résultat de la recherche de menace vous aide à calculer les résultats observables en fonction des réponses reçues.

Vous pouvez créer un calculateur de résultat de recherche de menace pour votre intégration et utiliser un script pour déterminer comment vous souhaitez identifier les différents résultats observables. Le calculateur de résultat de la recherche de menaces inclut un exemple de script fourni avec le système de base, que vous pouvez utiliser pour identifier les résultats observables ou modifier ce script en fonction de vos besoins.

Pour les intégrations tierces qui fournissent les résultats calculés, le calculateur de résultat de la recherche de menaces mappe les résultats aux résultats pris en charge dans le système de base.

Résultats de la recherche de menace de déploiement

Lorsque vous avez plusieurs résultats de recherche de menaces pour un observable des différents fournisseurs d'intégration, les résultats récents de la recherche de menaces de tous les fournisseurs sont pris en compte, et les résultats observables globaux sont marqués comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déployer les résultats de la recherche de menace

Dernier résultat observable	Résultat observable global
Malveillant	Si l'un des fournisseurs d'intégration signale l'observable comme malveillant, le résultat observable global est alors marqué comme malveillant.
Suspect	Si aucun des fournisseurs d'intégration ne signale l'observable comme malveillant, l'un d'entre eux le signale comme suspect, puis le résultat global de l'observable est marqué comme suspect.
Nettoyer	Si tous les fournisseurs d'intégration signalent l'observable comme Propre, le résultat global de l'observable est marqué comme Propre.
Inconnu	Si aucun des fournisseurs d'intégration ne signale l'observable comme malveillant ou suspect et que l'un d'entre eux le signale comme inconnu, le résultat global de l'observable est marqué comme inconnu.

Utilisation des calculateurs de résultats de la recherche de menace

Utilisez le calculateur de résultats de la recherche de menaces pour calculer les résultats observables pour votre intégration.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Administration** > **Calculateurs de résultats de la recherche de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Champ	Description
Fournisseur de la recherche de menace	Nom du fournisseur de recherche de menace.
Type d'observable	Spécifiez la classification du type d'observable auquel le script s'applique. Par exemple, adresse IP ou hachage de fichier, etc. Le script s'applique à tous les observables si vous ne sélectionnez aucun type d'observable.
Script de résultat	Éditeur de script permettant de déterminer comment identifier les différents résultats observables. Le calculateur de résultats de la recherche de menaces contient un exemple de script avec le système de base. Vous pouvez utiliser ce script pour déterminer les résultats observables ou modifier ce script en fonction de vos besoins.

4. Cliquez sur **Mettre à jour**.

Traduction automatique

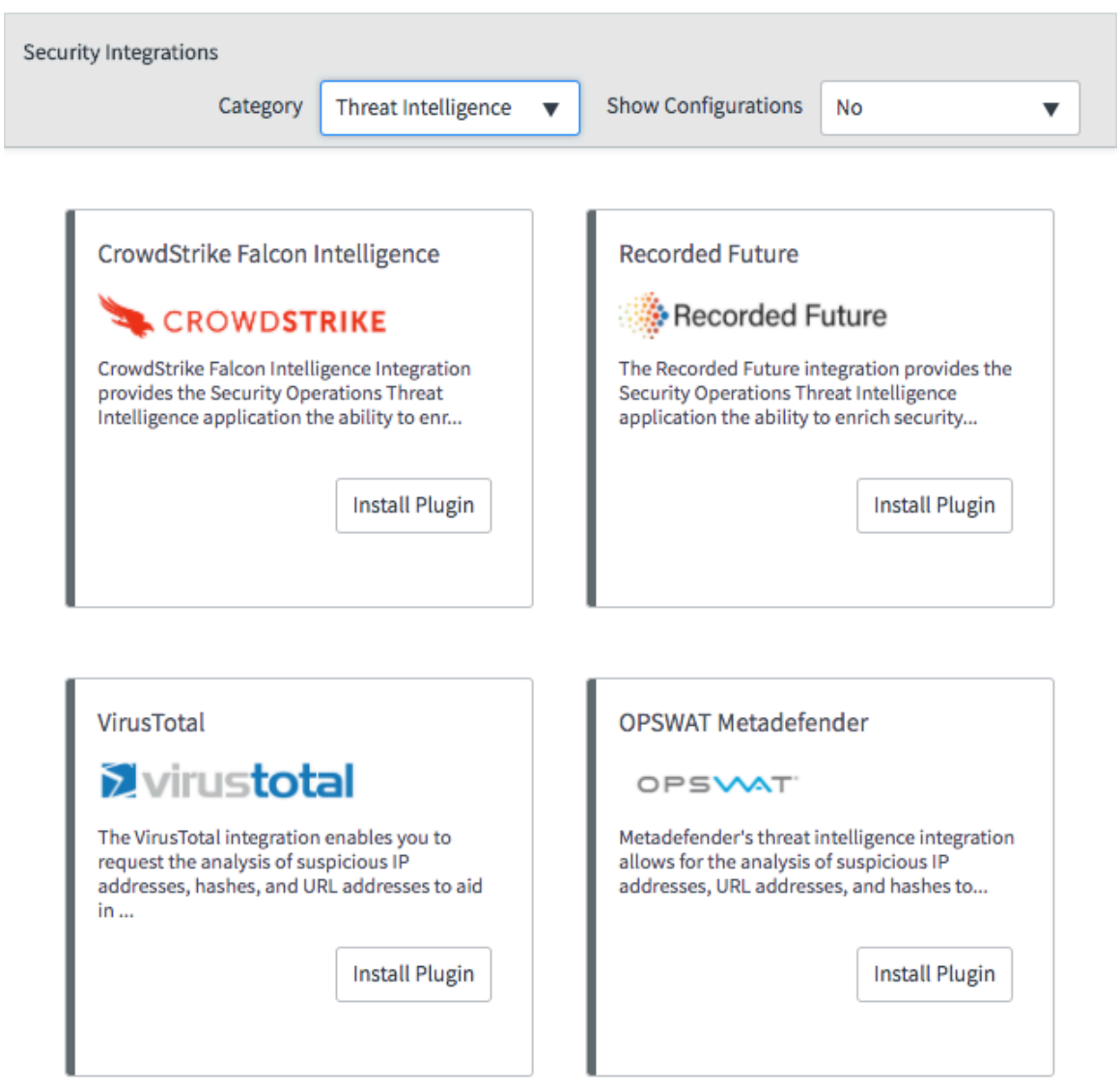
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Renseignements sur les menaces

Le Renseignements sur les menaces système de base comprend des intégrations à des progiciels tiers de détection de programmes malveillants. Cette section fournit des instructions pour l'activation des modules d'extension et la configuration des intégrations ServiceNow tierces. Vous y trouverez également des directives de base pour le développement de vos propres intégrations, ainsi que des détails sur les intégrations spécifiques incluses dans le système de base.

Configurations d'intégration

Le système de base comprend une série de « cartes » pour chacune des implémentations d'intégration que vous pouvez activer et utiliser. En outre, des cartes s'affichent pour toutes les intégrations publiées sur le ServiceNow Store qui ont des dépendances sur Opérations de sécurité des modules d'extension. Vous pouvez afficher les cartes d'intégration en sélectionnant **Security Operations** > **Configurations d'intégration**.



Vous pouvez filtrer les intégrations visibles à l'aide du menu déroulant **Catégorie** . Le menu déroulant **Afficher les configurations** vous permet de voir plusieurs instances d'implémentations qui autorisent leur création.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Boutons sur les cartes d'intégration

Les cartes d'intégration affichent différents boutons en fonction de l'état actuel de l'intégration et de la source de la carte.

Bouton	Description
Installer le module d'extension	Cliquez sur ce bouton pour installer le module d'extension applicable afin d'activer l'intégration. Une fois le module d'extension installé, le bouton bascule sur **Configurer**.
Configurer	Cliquez sur ce bouton pour entrer les informations de configuration de l'intégration. Pour certaines intégrations, vous devrez peut-être saisir des clés API ou des URL acquises à partir du site Web de l'intégration tierce.
Nouveau	Certaines intégrations, telles que Carbon Black et IBM QRadar, vous permettent de définir plusieurs implémentations d'une même intégration. Pour ces intégrations, cliquez sur **Nouveau** une fois le module d'extension activé. Les cartes vous permettent d'installer des modules d'extension (le cas échéant) et de configurer les implémentations à utiliser.
Ouvrir la page	Dans le système de base, votre instance envoie une requête au ServiceNow Store pour toutes les applications qui ont des dépendances à Opérations de sécurité des modules d'extension. Lorsque ces applications sont trouvées et que les modules d'extension d'application associés sont activés, leurs cartes d'intégration s'affichent avec les autres cartes d'intégration de sécurité. Cliquez sur **Ouvrir la page** pour accéder au site web de l'application tierce pour configurer l'intégration. Une fois la configuration terminée, le bouton **Ouvrir la page** bascule sur **Configurer**.

Intégration de CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence enrichit Renseignements sur les menaces avec les données des incidents de sécurité et des observables associés.

Explorer

- Vue d'ensemble de l'intégration CrowdStrike Falcon Intelligence
- Intégrations de Réponse aux incidents de sécurité

Configurer

Activer et configurer l'intégration CrowdStrike Falcon Intelligence

Utiliser

- Effectuer des recherches sur les observables
- Recherche de menace : CrowdStrike Falcon Intelligence flux

Développer

- ServiceNow Opérations de sécurité Directives de développement de l'intégration
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté des opérations de sécurité
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Vue d'ensemble de l'intégration CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence fournit des renseignements sur la cybersécurité qui s'intègrent facilement à Opérations de sécurité.

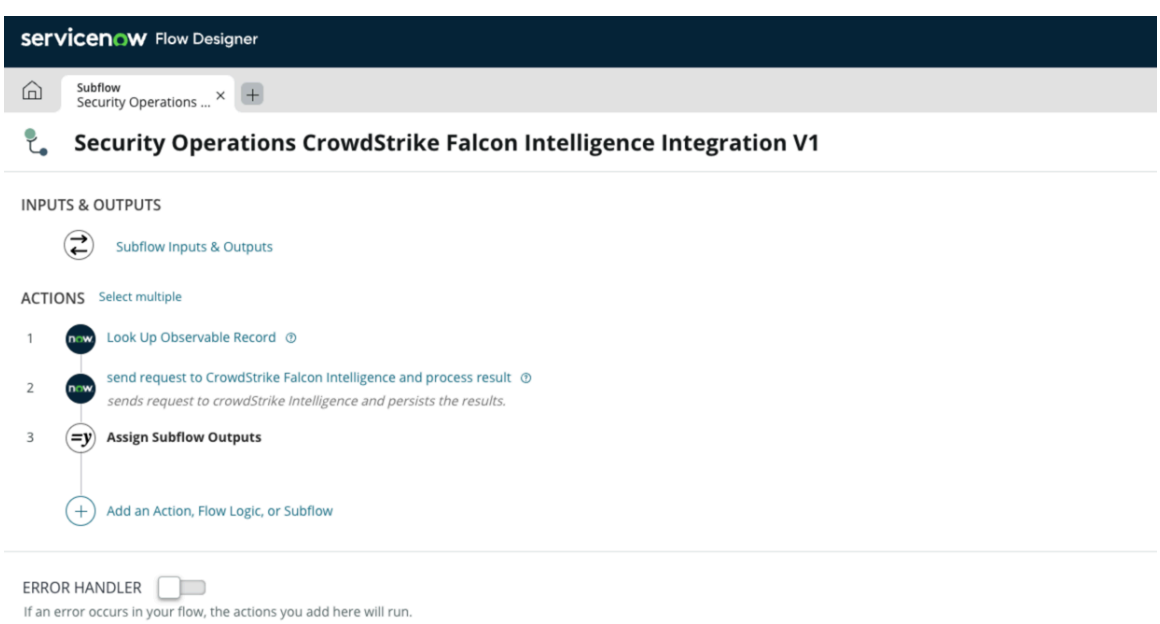
Remarque : Le Renseignements sur les menaces module d'extension est requis pour implémenter l'intégration CrowdStrike Falcon Intelligence .

Recherche de menace : CrowdStrike Falcon Intelligence flux

La fonction Recherche de menaces : CrowdStrike Falcon Intelligence Flow Designer effectue une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par , les observables sont analysés à CrowdStrike Falcon Intelligencela recherche de programmes malveillants et les résultats sont renvoyés.

Ce flux est déclenché lorsque Security Operations Integration - Aptitude Recherche de menace vous publiez un ou plusieurs observables dans une liste de surveillance et que l'implémentation de CrowdStrike Falcon Intelligence est sélectionnée. Une fois publiées, les listes de suivi peuvent être consultées dans le logiciel CrowdStrike Falcon Host.

Rôle requis : administrateur



Pour en savoir plus sur les activités utilisées par ce concepteur de flux, reportez-vous à la section Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer et configurer l'intégration CrowdStrike Falcon Intelligence

La fonctionnalité de configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration CrowdStrike Falcon Intelligence . Avant de pouvoir utiliser le CrowdStrike Falcon Intelligence, vous devez le télécharger à ServiceNow Store partir du et ajouter la clé API et l'ID appropriés.

Avant de commencer

Rôle requis : administrateur

- Le Renseignements sur les menaces module d'extension doit être installé et activé avant de pouvoir utiliser l'intégration CrowdStrike Falcon Intelligence .
- Obtenez l'ID du client API et le secret du client API sous votre CrowdStrike Falcon Intelligence profil.
- Si vous mettez à niveau CrowdStrike Falcon Intelligence l'intégration à partir d'une version précédente, vous devez supprimer la configuration existante et en configurer une nouvelle. L'intégration prend en charge l'authentification OAuth2. Cette mise à jour nécessite que vous saisissiez **l'ID du client API** et le **secret du client API** pour vous authentifier et terminer la configuration.
- Dans les **périmètres de l'API** du CrowdStrike Falcon Intelligence portail, activez le paramètre de **lecture** pour les **indicateurs (Falcon X)** ou **les IOC (indicateurs de compromission).**

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Dans la CrowdStrike Falcon Intelligence carte, cliquez sur **Configurer**.
4. Renseignez les champs du formulaire pour finaliser la configuration :

Configuration CrowdStrike Falcon Intelligence

Champ	Description
Nom	Nom de l'intégration, par exemple `demo-1`.
ID client API	L'ID client que vous obtenez à partir de la section des paramètres de votre profil de compte dans CrowdStrike Falcon Intelligence le portail.
Secret client API	Clé secrète du client que vous obtenez à partir de la section des paramètres de votre profil de compte dans CrowdStrike Falcon Intelligence le portail.

5. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Une fois configuré, il est possible de CrowdStrike Falcon Intelligence le sélectionner pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Have I been pwned? intégration

L'intégration Opérations de sécurité Have I been pwned? vous permet de soumettre des recherches sur les noms de domaine et les adresses e-mail pour déterminer si les données personnelles des utilisateurs ont été compromises par des violations de données.

Explorer Intégrations de Réponse aux incidents de sécurité	**Configurer** • Configuration de l'intégration de Security Operations Have I been pwned? • Activer l'intégration Security Operations Have I been pwned?
Utiliser Effectuer des recherches sur les observables Recherche de menace : Have I been pwned? flux	**Développer** • ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide • Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service et assistance client	

Configuration de l'intégration de Security Operations Have I been pwned?

Have I been pwned? est une ressource gratuite utilisée pour évaluer si une personne a pu être mise en danger en raison de la compromission ou de la violation de données de son compte en ligne. Il s'intègre facilement à Opérations de sécurité.

Avant de pouvoir utiliser l'intégration Have I been pwned? , vous devez activer le module d'extension. Si nécessaire, vous pouvez également mettre à jour votre certification X509 SSL.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les Réponse aux incidents de sécuritémodules d'extension , Renseignements sur les menaces, et Opérations de sécurité Have I been pwned? sont requis pour implémenter l'intégration Opérations de sécurité Have I been pwned? .

Recherche de menace : Have I been pwned? flux

Le flux Recherche Have I been pwned? de menace - effectue une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par , les observables sont analysés à Have I been pwned?la recherche de programmes malveillants et les résultats sont renvoyés.

Rôle requis : sn_si_admin

Ce flux est déclenché lorsque Security Operations Integration - Aptitude Recherche de menace vous effectuez une recherche de menace sur un ou plusieurs observables et que l'implémentation Have I been pwned? est sélectionnée. Pour plus d'informations, consultez Effectuer des recherches sur les observables.

Ai-je été pwned flow



Pour en savoir plus sur les activités utilisées par ce flux, reportez-vous à Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Activer l'intégration Security Operations Have I been pwned?

La fonctionnalité de configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration Opérations de sécurité Have I been pwned? . Avant de pouvoir utiliser l'intégration Have I been pwned? , vous devez la télécharger à ServiceNow Storepartir du fichier .

Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être installé et activé avant de pouvoir utiliser l'intégration Opérations de sécurité Have I been pwned? .

Rôle requis : sn_si_admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Téléchargez l'intégration à partir de ServiceNow Store.
Cette intégration prend en charge une API ouverte et ne nécessite pas de configuration supplémentaire. Have I been pwned? peut maintenant être sélectionné pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Mettre à jour votre certificat X.509

Si vous avez besoin d'une connexion SSL pour l'intégration, il peut arriver que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou qu'il ait expiré. Cette tâche est facultative.

Avant de commencer
Rôle requis : admin

Procédure

1. Procurez-vous le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.

   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
   Par exemple : `https://<3rdparty>/`.

   b. Cliquez sur l'icône de cadenas dans la ligne d'adresse.

   c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .

   d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .

   e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.

   f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
   Il doit commencer par `-----BEGIN CERTIFICATE` ----- et se terminer par `-----END CERTIFICATE`-----.

2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Ajoutez le certificat à l'enregistrement du fournisseur d'identité.
   a. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
   b. Sélectionnez le fournisseur d'identité par défaut actif pour lequel vous avez créé le nouveau certificat.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Faites défiler vers le bas jusqu'à la liste connexe **des certificats X.509** , puis cliquez sur **Modifier**.

d. Déplacez le certificat nouvellement créé vers la colonne **Sélectionné** .

6. Cliquez sur **Enregistrer**.
   Les autres champs de l'enregistrement sont générés automatiquement.

> **Remarque :** Si vous avez un certificat qui a expiré, vous devez le supprimer. Pour plus d'informations sur la suppression du certificat expiré, reportez-vous à KB0691439 Remplacement d'un certificat SAML arrivant à expiration .

Intégration de MISP pour Opérations de sécurité

Avec Intégration de MISP pour Opérations de sécurité, vous pouvez enquêter sur les incidents de sécurité à l'aide de recherches de perception, de l'enrichissement des observables et de la création ou de la mise à jour d'événements dans MISP. En utilisant MISP, vous pouvez enquêter plus rapidement sur les attaques ciblées, améliorer le taux de détection et réduire le nombre de faux positifs dans votre environnement.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

MISP Vue d'ensemble

MISP, qui signifie Malware Information Sharing Platform, vous permet d'échanger et de partager des renseignements sur les menaces et des indicateurs de compromission (IoC) sur les logiciels malveillants et les attaques ciblés au sein de votre communauté de membres de confiance. Vous pouvez également partager MISP des informations avec des communautés privées ou ouvertes. En échangeant MISP des informations, vous pouvez enquêter plus rapidement sur les attaques ciblées, améliorer le taux de détection et réduire le nombre de faux positifs dans votre environnement.

MISP et Security Operations

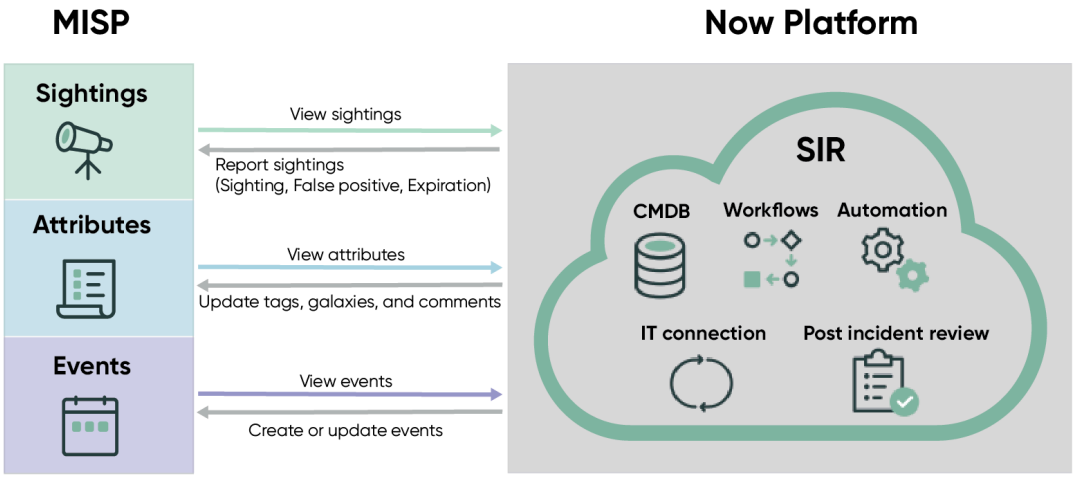
Consultez l'exemple suivant pour découvrir comment les informations circulent avec les MISP applications Security Operations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble de MISP et Security Operations

Now Platform - MISP integration overview



Fonctionnalités principales

Cette intégration comprend les choses que vous pouvez faire avec les MISP fonctionnalités clés :

- Connectez-vous au privé et au public MISP instances.
- Prise en charge de la recherche de perception manuelle et automatique des observables.
- Exécution de la recherche de perception à partir de la gestion des tickets.
- Signaler ou mettre à jour des observations pour un attribut :
  - Signaler un observable comme observation (global)
  - Signaler un observable comme faux positif (global)
  - Signaler un observable comme expiré
- Prise en charge de l'enrichissement manuel et automatique des observables. Les résultats incluent les informations d'attribut MISP et d'événement associées aux observables.
- Enrichissement des attributs, y compris MISP l'ajout ou la mise à jour de balises, de galaxies ou decommentaires. Ajouter ou supprimer des galaxies à un événement ou à un MISP attribut
- Création d'événements dans MISP de SIR: prend en charge la création manuelle et automatique d'événements dans MISP à partir de SIR.
- Mettre à jour un événement à partir duquel il inclut l'ajout MISPSIR ou la mise à jour de balises, degalaxies ou d'attributs.
- Ajouter des observables associés à un incident de sécurité en tant qu'attributs MISP event.
- Extraction automatique MITRE-ATT&CK™ Informations provenant de MISP attributs et associer les informations à SIR des incidents de sécurité.
- Ajouter automatiquement SIR MITRE-ATT&CK™ l'information sous forme de galaxies à un MISP event.

Concepts clés

Cette intégration comprend les concepts clés suivants que vous devez connaître :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- MISP est une plateforme de renseignements sur les menaces (TIP). Les TIP vous permettent de collecter, de corréler, de catégoriser, de partager et d'intégrer des données sur les menaces de sécurité en temps réel afin de faciliter la hiérarchisation des actions et de faciliter la prévention, la détection et la réponse aux attaques.
- MISP est un TIM (Threat Intelligence Management). Les TIM vous permettent de transformer les données sur les menaces en renseignements sur les menaces par le biais du contexte et de hiérarchiser automatiquement les menaces en fonction de la notation et de la pertinence définies par l'utilisateur.
- MISP Couche de données
  - Les événements sont des encapsulations d'informations contextuellement liées.
  - Les attributs sont des points de données individuels, qui peuvent être des indicateurs ou des données associées.
  - Les objets sont des compositions d'attributs de modèle personnalisées.
  - Les références d'objet sont les relations entre les autres blocs de construction.
  - Les perceptions sont des occurrences temporelles spécifiques d'un point de données détecté.
- MISP Couche de contexte
  - Les balises sont des étiquettes attachées à des événements ou à des attributs et peuvent provenir de taxonomies.
  - Les amas de galaxies sont des éléments de base de connaissances que vous pouvez utiliser pour étiqueter des événements ou des attributs provenant de galaxies.
  - Les relations de grappes désignent des relations prédéfinies entre les grappes.
- Les indicateurs contiennent un modèle que vous pouvez utiliser pour détecter les cyber-activités suspectes ou malveillantes.
- Il MISP peut s'agir d'indicateurs de réseau (adresse IP), d'indicateurs système (une chaîne en mémoire) ou même de détails de compte bancaire. Les attributs dans MISP sont connus sous le nom d'observables dans d'autres SIEM ou formats tels que STIX.
  - Un type décrit l'attribut. Par exemple, MD5 ou une URL.
  - La catégorie de l'attribut décrit un attribut. Par exemple, une livraison de charge utile.
  - Une balise IDS détermine si un attribut peut être automatiquement utilisé pour la détection.

Remarque : Pour plus d'informations sur MISP les concepts, consultez le site Web de la documentation MISP

Comment votre organisation peut-elle bénéficier des avantages suivants ? Intégration de MISP pour Opérations de sécurité

Les analystes de sécurité doivent acquérir et maintenir une connaissance situationnelle du paysage des menaces, ce qui signifie qu'ils doivent consolider et intégrer manuellement une quantité écrasante de données sur les menaces. La collecte, la consolidation et l'intégration de ces données prennent un temps précieux, ce qui ralentit la détection et l'analyse des menaces. Intégration de MISP pour Opérations de sécurité Permet aux analystes de détecter davantage de menaces et de réagir plus rapidement en intégrant les MISP renseignements de sécurité dans une instance existante Now Platform .

À l'aide de , Intégration de MISP pour Opérations de sécuritévotre organisation peut effectuer les actions suivantes :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Permettez à vos analystes de sécurité de réagir rapidement et dans le bon contexte.
- Améliorez l'efficacité de votre équipe de sécurité en automatisant les flux d'incidents pour détecter et contenir les menaces.
- Réduisez le temps de recherche manuelle et permettez aux analystes de sécurité de rendre opérationnels et d'organiser les indicateurs à partir du Now Platformfichier .

En savoir plus sur cette intégration

Identificateur de document	Titre de document
MISP site web de documentation	Site web de la documentation MISP
ServiceNow site web de la documentation produit	Site web de la documentation produit ServiceNow

Administration MISP

Vous pouvez configurer l'intégration MISP dans le Now Platform pour effectuer une recherche de perception, un enrichissement des observables, et pour créer et mettre à jour des événements dans MISP.

Premiers pas avec Intégration de MISP pour Opérations de sécurité

Passez en revue les informations suivantes avant de configurer votre Intégration de MISP pour Opérations de sécuritéfichier .

Liste de vérification

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles , Renseignements sur les menaceset Réponse aux incidents de sécurité et requisNow Platform.	Les rôles suivants sont utilisés dans les MISP fonctionnalités de :Now Platform • L'administrateur (admin) installe les applications à partir des rôles d'administrateur ServiceNow Store d'incident de sécurité (sn_si.admin) et d'administrateur de Threat Intelligence (sn_ti.admin) et les affecte. • sn_si.admin et sn_ti.admin peuvent configurer l'intégration et configurer les profils de création automatique MISP d'événements. • sn_sec_misp.write : le rôle d'analyste MISP dispose d'autorisations de lecture et d'écriture sur MISP les données qui incluent les données d'événement et d'attribut. Pour plus d'informations, consultez Configurer Threat Intelligence.
Affectez les rôles d'utilisateur requis MISP .	Examiner le MISP rôles d'utilisateur et les autorisations requises pour utiliser le Intégration de MISP pour Opérations de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	Remarque : Pour en savoir plus sur les rôles d'utilisateur dans MISP, consultez la section Rôles du site web de documentation MISP .
Vérifiez que vous utilisez la MISP version 2.4.137 ou une version ultérieure.	Le Intégration de MISP pour Opérations de sécurité est testé avec un minimum de MISP version 2.4.137 .
Vérifiez que les ServiceNow applications de base requises pour prendre en charge le MISP module sont installées et activées.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. • Réponse aux incidents de sécurité • ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) • ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) Pour plus d'informations sur la configuration de votre Now Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une application Security Operations et activer une application ServiceNow Store.
Séparation de domaine	Vérifiez la section Séparation de domaine si vous avez l'intention de séparer les données, les processus et les tâches administratives.

MISP Rôles et autorisations d'utilisateur

Passez en revue les rôles d'utilisateur requis dans l'intégration Intégration de MISP pour Opérations de sécurité .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enrichissement des observables et autorisations de recherche de perception

Remarque :

- Toutes les **ServiceNow** options d'intégration MISP nécessitent les autorisations de base pour **gérer les événements de l'organisation** et **l'accès aux clés d'authentification**. Assurez-vous de disposer de ces autorisations de base avant de poursuivre.
- Pour ajouter des galaxies locales, l'utilisateur qui configure l'intégration doit appartenir à l'organisation hôte du serveur MISP correspondant.

Capacité MISP	Tagueur	Éditeur de balises
Enrichissement des observables (lecture seule)	#	#
Recherche de perception (lecture seule)	#	#

Signaler les autorisations de perception

Capacité MISP	Créateur de perception
Rapporter une observation	#

Autorisations d'attribut et d'événement

Capacité MISP	Tagueur	Éditeur de balises
Modifier les balises d'événement/d'attribut	#	#
Modifier les galaxies d'événements/d'attributs	#	#
Modifier les commentaires sur l'attribut	#	#
Ajouter un nouvel attribut à l'événement	#	#
Créer un événement dans MISP	#	#

Installez et configurez le Intégration de MISP pour Opérations de sécurité

Installez et configurez le Intégration de MISP pour Opérations de sécurité à partir de ServiceNow Store sur votre Now Platform instance afin de pouvoir commencer à enquêter sur les incidents de sécurité à l'aide des MISP données.

Avant de commencer

Assurez-vous d'avoir installé les certificats SSL valides sur le serveur MISP.

Rôle requis : sn_si.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Téléchargez le Intégration de MISP pour Opérations de sécurité à partir de et ServiceNow Store installez-le.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la MISP vignette Intégration SIR/TI et cliquez sur **Configurer**.
4. Renseignez les champs du formulaire.

MISP - Formulaire Configuration de l'intégration SIR/TI

Champ	Description
Nom	Nom de la configuration d'instance MISP .
MISP URL serveur	URL du MISP serveur qui sert de point de terminaison REST au MISP serveur.
Clé API	Clé API configurée pour votre compte d'utilisateur sur le MISP serveur. La clé API correspond à la **clé d'authentification** dans le MISP serveur.
Déploiement sur site	Option que vous pouvez sélectionner si votre MISP serveur est déployé dans une instance sur site. Lorsque vous sélectionnez l'option **Déploiement sur site** , vous devez utiliser la Serveur MID pour vous connecter au MISP serveur.
Application MID	Champ de chaîne qui identifie le nom de l'application MID utilisée pour communiquer avec MISP. Ce champ est obligatoire lorsque vous sélectionnez l'option **Déploiement sur site** . Pour plus d'informations sur la configuration du serveur MID pour votre application, consultez Configurer un serveur MID pour chaque application

5. Cliquez sur **Envoyer**.

Résultats

Une fois la configuration validée et envoyée avec succès, l'intégration MISP SIR/TI est enregistrée sous forme de vignette sur la page Intégrations de sécurité.

Passer en revue les paramètres d'intégration MISP

Examinez les Intégration de MISP pour Opérations de sécurité paramètres et modifiez les propriétés système par défaut en fonction de votre environnement.

Avant de commencer

Rôle requis : sn_si.admin, sn_ti.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Intégration de MISP** > **Paramètres d'intégration**.
2. Modifiez les paramètres suivants selon vos besoins.

Paramètres d'intégration MISP

Nom de la propriété		Description
Enrichissement des éléments observables	Temps (en heures) avant l'extraction de nouvelles données	Délai en heures avant de pouvoir extraire de nouvelles données. Type : nombre entier Valeur par défaut : 24
Recherche de perception	Exécuter automatiquement la recherche de perception lorsque de nouveaux observables sont associés à l'incident de sécurité	Recherche de perception qui s'exécute chaque fois qu'un nouvel observable est associé à un incident de sécurité. Valeur par défaut : oui
	Intervalle de recherche (en jours) pour la recherche sur la perception dans MISP	Nombre de jours pendant lesquels les données de recherche d'observation font l'objet d'une MISPrecherche. Utilisez cette option uniquement pour la fonction de recherche automatique de perception. Valeur par défaut : 90
Synchronisation des données	Période d'intervalle (en minutes) pour que les balises soient récupérées et synchronisées avec MISP	MISP Balises récupérées au moment de la configuration de l'intégration. Une fois que les données sont dans le Now Platform, cette propriété définit la fréquence à laquelle les données avec le MISP serveur sont synchronisées. La valeur est définie en minutes. Valeur par défaut : 1 440 (minutes ou 24 heures)
	Période d'intervalle (en minutes) pour actualiser les galaxies MISP à partir de sources configurées	MISP Galaxies extraites au moment de la configuration de l'intégration. Une fois que les données sont dans le Now Platform, cette propriété définit la fréquence à laquelle les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété		Description
		données avec le MISP serveur sont synchronisées. La valeur est définie en minutes. Valeur par défaut : 1 440 (minutes ou 24 heures)
	Période d'intervalle (en minutes) pour les organisations à extraire et à synchroniser avec MISP	MISP Organisations récupérées au moment de la configuration de l'intégration. Une fois que les données sont dans le Now Platform, cette propriété définit la fréquence à laquelle les données avec le MISP serveur sont synchronisées. La valeur est définie en minutes. Valeur par défaut : 1 440 (minutes ou 24 heures)
MITRE™ Technique Extraction	Déployer MITRE-ATT&CK automatiquement les techniques des résultats de l'enrichissement de l'observable MISP (balises) vers l'incident de sécurité	Déploiement des MITRE-ATT&CK informations à partir des résultats de l'enrichissement des MISP observables (balises) vers l'incident de sécurité. Valeur par défaut : oui
	Déployer MITRE-ATT&CK automatiquement les techniques des résultats de l'enrichissement de l'observable MISP (Galaxies) vers l'incident de sécurité	Déploiement des MITRE-ATT&CK informations à partir des résultats de l'enrichissement de l'observable MISP (galaxies) vers l'incident de sécurité. Valeur par défaut : oui

Remarque :

- Pour utiliser les fonctions d'extraction technique MITRE™ dans MISP, vous devez activez l'option MITRE-ATT&CK de la fonctionnalité Renseignements sur les menaces module.
- L'introduction Intégration de MISP pour Opérations de sécurité de deux règles d'extraction technique du système MITRE-ATT&CK de base pour MISP les MISP galaxies et MISP les balises. Pour plus d'informations sur les règles d'extraction automatique dans MITRE-ATT&CK, consultez Règles de la technique d'extraction automatique pour l'importation d'informations MITRE-ATT&CK.

3. Cliquez sur **Enregistrer**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Vos paramètres d'intégration modifiés sont enregistrés et appliqués.

Configurer MISP les recherches de perception

Configurez les Now Platform recherches de perception des observables dans l'instance MISP . Grâce à ces informations, vous pouvez déterminer la fréquence à laquelle les menaces se produisent.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations qui sont nécessaires pour utiliser les MISP fonctionnalités bidirectionnelles.
- Rôle requis : sn_si.admin, sn_ti.admin

Pourquoi et quand exécuter cette tâche
Le workflow Security Operations Integration - Recherche de perceptions exécute les recherches de perception. Ce workflow accepte une liste d'observables, trouve toutes les options d'implémentation, crée les requêtes basées sur les configurations de recherche de perception et exécute les recherches basées sur le workflow configuré.

Le Intégration de MISP pour Opérations de sécurité fournit un profil de recherche de perception du système de base qui vous permet de configurer des recherches de perception automatiques. Avec ce profil, vous pouvez accéder aux informations de perception observables connexes d'une organisation et également voir les perceptions externes d'autres organisations.

Procédure

1. Accédez à la **Tout** > **Intégration de MISP** > **Configuration de la recherche de détections**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire de configuration de la recherche de perceptions

Champ	Description
Nom	Nom du profil d'aptitude.
Est une recherche enregistrée	Configuration de recherche enregistrée lorsque vous sélectionnez cette option. Les requêtes de configuration de recherche enregistrées sont des exemples de requêtes. Vous pouvez les remplacer par les paramètres de votre environnement et créer des configurations de recherche enregistrées supplémentaires si nécessaire.
Source de recherche de perceptions	Source pour la recherche de perceptions. Sélectionnez le magasin de MISP journaux comme source.
Actif	Option qui permet d'enregistrer la configuration de la recherche. Seules les configurations de recherche actives peuvent effectuer une recherche d'observations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type d'observable	Type d'observable tel que l'adresse IP, la valeur de hachage, l'URL et le nom de domaine.
Nombre maximum d'observables par recherche	Nombre maximal d'observables que vous pouvez afficher à partir d'une requête de recherche.
Rechercher	Chaîne de recherche par défaut qui est `$(observable)`. Toutefois, vous pouvez définir votre propre requête de recherche en spécifiant les paramètres pris en charge par la banque de MISP journaux.

4. Cliquez sur **Envoyer**.

Résultats
Vous avez créé un profil de MISP configuration de recherche de perceptions.

Configurer le mode de création d'un événement automatique

Configurez l'pour créer automatiquement des Now Platform événements dans MISP.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations qui sont nécessaires pour utiliser les MISP fonctionnalités bidirectionnelles.
- Rôle requis : sn_si.admin, sn_ti.admin

Procédure

1. Accédez à la **Tout** > **Intégration de MISP** > **Profils de création automatique d'événements**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire de nom

Champ	Description
Nom	Nom du profil de création automatique d'événements.
Description	Brève description du profil. Une description plus détaillée est partagée via les attributs à l'étape suivante de la création de l'événement.
Ordre	Ordre du profil lorsque les conditions de déclenchement sont remplies. La valeur par défaut est 100. Laissez ce paramètre sur la valeur par défaut. Si vous créez plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le profil

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	avec le numéro le plus bas a la priorité la plus élevée.
Source	MISP Source pour la création de l'événement.
Actif	Option qui indique si le profil est actif ou inactif. L'option est désactivée par défaut pour indiquer que le profil est désactivé. Ce profil n'est pas actif tant que vous n'avez pas terminé toutes les étapes de configuration du profil et que vous n'avez pas cliqué sur **Terminer**.

4. Cliquez sur **Continuer**.

Configurer les conditions de déclenchement d'un événement

Configurez les conditions de déclenchement d'événement dans le Now Platform afin de pouvoir déclencher automatiquement un événement lorsque MISP les conditions sont remplies.

Avant de commencer

Rôle requis : sn_sec_misp.write

Procédure

1. Dans le formulaire Conditions de déclenchement, renseignez les détails qui peuvent déclencher un événement.
   Vous pouvez créer une logique de composé en fournissant les conditions de déclenchement basées sur des champs d'incident de sécurité ou des champs d'observables. Vous pouvez également créer des événements dans MISP si les observables n'ont pas d'événement correspondant dans MISP. Vous pouvez choisir de créer une logique de composé à l'aide d'une combinaison des trois conditions de déclenchement : Déclencher en fonction des champs d'incident de sécurité, Déclencher en fonction des champs observables et Créer un événement MISP, si un observable n'a pas d'événements correspondants dans MISP. Si vous sélectionnez plusieurs déclencheurs, vous pouvez les joindre à l'aide de la condition ET. Envisagez de créer un profil avec de nouvelles conditions si vous devez utiliser la condition OU.

Formulaire de conditions de déclenchement d'événement

Champ	Description
Déclencher en fonction des champs d'incident de sécurité	MISP Événement que vous pouvez créer si toutes les conditions de déclenchement d'un incident de sécurité sont remplies.
Conditions de déclenchement des incidents de sécurité	Filtres de la première ligne que vous pouvez définir à l'aide des listes et des champs du générateur de conditions. Pour ajouter d'autres conditions, cliquez sur ET ou OU. Si ET est sélectionné, toutes les conditions doivent être mises en correspondance. Si OU est sélectionné,

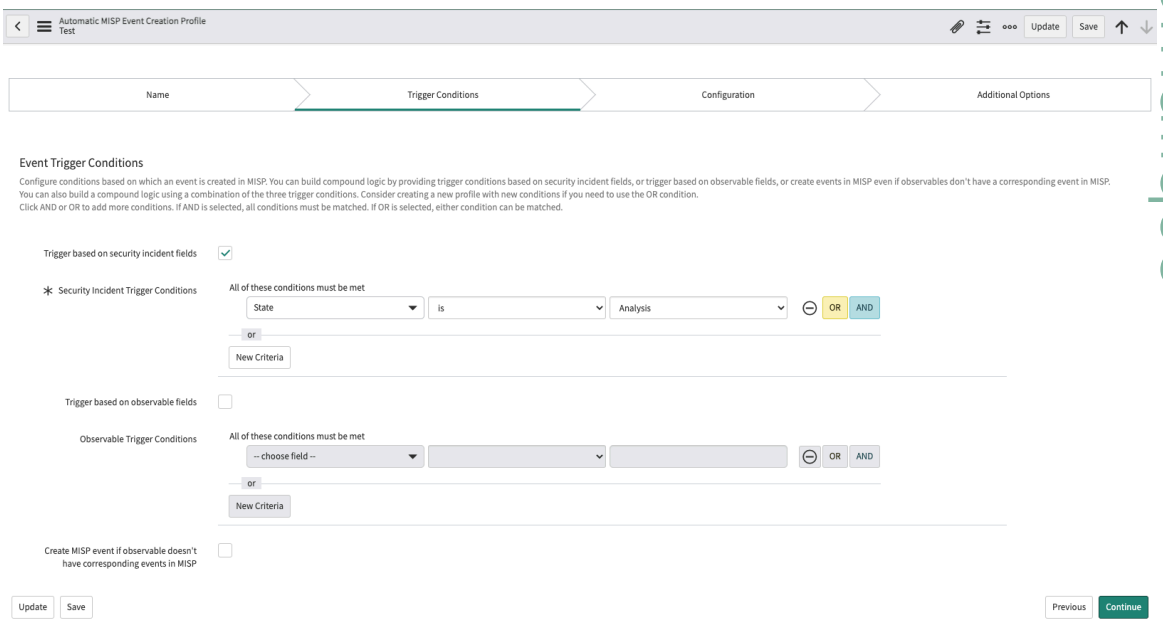
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.
Déclencher en fonction des champs observables	MISP Événement que vous pouvez créer si toutes les conditions de déclenchement observables sont remplies.
Conditions de déclenchement des observables	Filtres de la première ligne que vous pouvez définir à l'aide des listes et des champs du générateur de conditions. Pour ajouter d'autres conditions, cliquez sur ET ou OU. Si ET est sélectionné, toutes les conditions doivent être mises en correspondance. Si OU est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.
Créer un événement MISP en l'absence d'événements correspondants pour l'observable dans MISP	MISP Événement que vous pouvez créer si un observable ne dispose pas d'événements correspondants dans MISP.

Conditions de déclenchement d'événement

L'exemple suivant montre les conditions de déclenchement d'événement lors de la configuration du profil de création d'événement MISP .



2. Cliquez sur **Continuer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mapper les champs de l'événement MISP

Mappez les champs d'événements MISP dans le afin que les informations sur les incidents de sécurité soient disponibles lors MISP de la Now Platform création des événements.

Avant de commencer

Rôle requis : sn_sec_misp.write

Procédure

1. Renseignez les champs du formulaire.

Formulaire de mappage de champs d'événements MISP par défaut

Champ	Description
Informations sur l'événement	Informations sur l'événement Now Platform Réponse aux incidents de sécuritéqui sont automatiquement créées à partir du . Le champ **Informations sur l'événement** prend en charge les variables de substitution à l'aide de ${SIR FIELD LABEL}$. Lors de la création d'un événement, ces variables sont remplacées par les valeurs de champ réelles d'incident de sécurité. La variable de substitution ${URL}$ est remplacée par l'URL de l'incident de sécurité.
Distribution	Option qui contrôle qui peut voir cet événement après sa publication. Cette option contrôle également si l'événement est synchronisé avec d'autres serveurs. La distribution est héritée par les attributs, et le paramètre le plus restrictif l'emporte. Les options de distribution sont les suivantes : ◦ Votre organisation uniquement : permet uniquement aux membres de votre organisation de voir cet événement. L'événement peut être transféré vers une autre instance par l'un des membres de votre organisation, où seule votre organisation peut avoir accès à son affichage. Les événements avec ce paramètre ne sont pas synchronisés. ◦ Cette communauté uniquement : permet aux utilisateurs qui font partie de votre MISP communauté d'afficher l'événement, y compris votre propre organisation, les organisations présentes sur ce MISP serveur et les organisations qui exécutent des serveurs qui se MISP synchronisent avec ce serveur. Toute autre organisation qui se connecte à vos serveurs liés n'est pas autorisée à afficher l'événement.

Traduction automatique

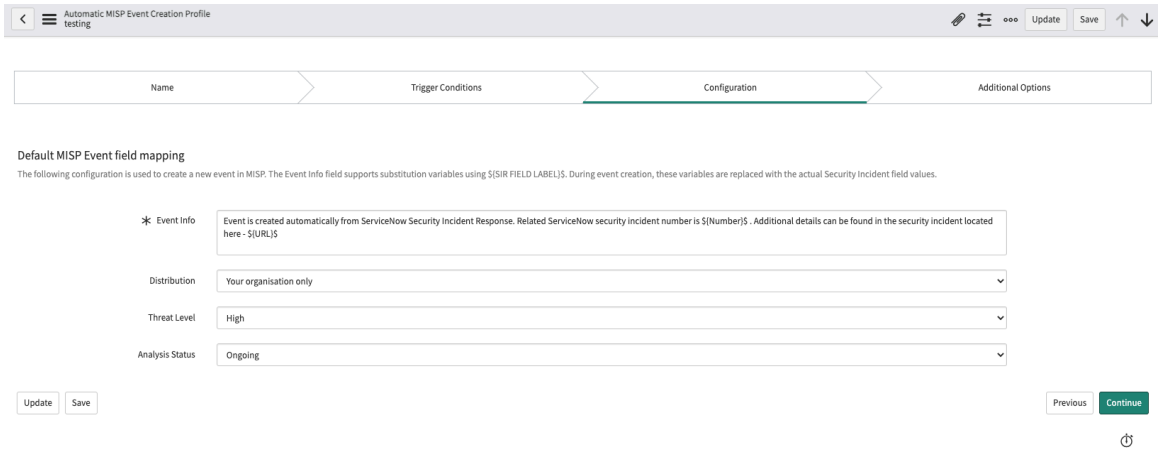
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Communautés connectées : permet aux utilisateurs qui font partie de votre MISP communauté de voir l'événement, y compris toutes les organisations sur ce MISP serveur, toutes les organisations sur les MISP serveurs qui se synchronisent avec ce serveur et les organisations d'hébergement des serveurs qui se connectent à n'importe quel serveur situé à deux sauts. Toute autre organisation connectée aux serveurs liés situés à deux sauts de distance n'est pas autorisée à afficher l'événement. ◦ Toutes les communautés : partage l'événement avec toutes les MISP communautés.
Niveau de menace	Champ qui indique le niveau de risque de l'événement. Vous pouvez classer les incidents en trois catégories de menace différentes (faible, moyenne, élevée). Ce champ peut également rester non défini. Les options sont les suivantes : ◦ Faible : programme malveillant de masse général ◦ Moyen : menaces persistantes avancées (APT) ◦ Élevé : APT sophistiquées et attaques 0-day
État de l'analyse	Étape actuelle de l'analyse de l'événement, avec les options possibles suivantes : ◦ Initial : L'analyse ne fait que commencer ◦ En cours : l'analyse est en cours ◦ Terminé : l'analyse est terminée

L'exemple suivant montre le formulaire que vous pouvez utiliser pour créer un événement dans MISP.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de champ d'événement MISP par défaut



2. Cliquez sur **Continuer**.

Mapper ou associer des SIR observables en tant qu'attributs à MISP des événements

Mappez les Réponse aux incidents de sécurité types des observables aux types d'attributs MISP , car les types d'attributs et les MISPSIR observables peuvent être différents.

Avant de commencer

Rôle requis : sn_sec_misp.write

Pourquoi et quand exécuter cette tâche

Le Intégration de MISP pour Opérations de sécurité fournit un mappage de système de base que vous utilisez lorsque vous ajoutez SIR des observables en tant qu'attributs à un MISP événement.

Vous pouvez choisir de modifier le mappage du système de base pour l'adapter à votre environnement. Par exemple, vous pouvez mapper plusieurs SIR observables à un seul type d'attribut MISP . Si des types d'observables ne sont pas mappés, **l'autre** MISP type d'attribut est sélectionné par défaut.

Procédure

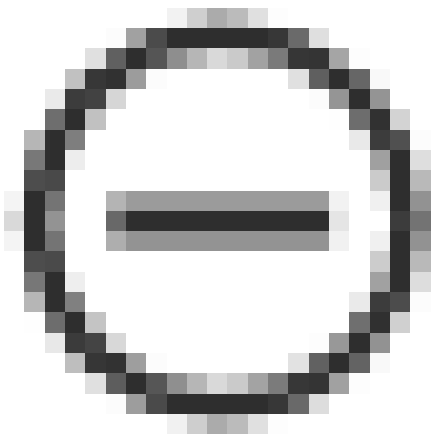
1. Sur le formulaire Options supplémentaires, mappez les types observable SIR et MISP attribut.

2. Mappez les Réponse aux incidents de sécurité types des observables aux types d'attributs MISP , comme décrit dans la table suivante.

Correspondance entre les observables du SIR et les types d'attributs du MISP

Champ	Description
Ajouter tous les observables associés en tant qu'attributs	Option que vous activez pour ajouter les observables disponibles dans un incident de sécurité à un MISP événement en tant qu'attributs. Cette option active le mappage dans la section Mappage du type d'observable au type d'attribut.
Mappage entre type observable et type d'attribut	Option permettant de mapper les SIR types observables aux types d'attributs

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	MISP . Par exemple, vous pouvez mapper le numéro CVE à l'attribut de vulnérabilité dans SIRMISP. Vous ne pouvez ajouter un SIR type d'observable qu'à un seul type d'attribut MISP . Le système de base fournit un mappage des types observables aux types d'attributs SIRMISP . Si des types d'observables SIR ne sont pas mappés à un type d'attribut MISP , l'observable est alors mappé à **l'autre** type d'attribut dans MISP. Pour ajouter un nouveau mappage, cliquez sur **Ajouter un type d'observable**, recherchez le type d'observable, puis effectuez un SIR mappage au type d'attribut correspondant MISP . Cliquez sur l'icône Supprimer le  pour supprimer l'association de mappage d'attribut SIR et MISP . **Remarque :** Pour en savoir plus sur MISP les types d'attributs, consultez la documentation MISP .
Filtrer les observables en fonction des balises de sécurité	Option permettant de filtrer les observables en fonction des balises de sécurité sélectionnées. **Balises de sécurité** : ajoutez des balises pour filtrer les observables. Par exemple, si vous ajoutez une balise appelée « Bloquer à partir du partage » ou « TLP : blanc », si l'une de ces balises est associée à l'un des observables, ces observables ne sont pas

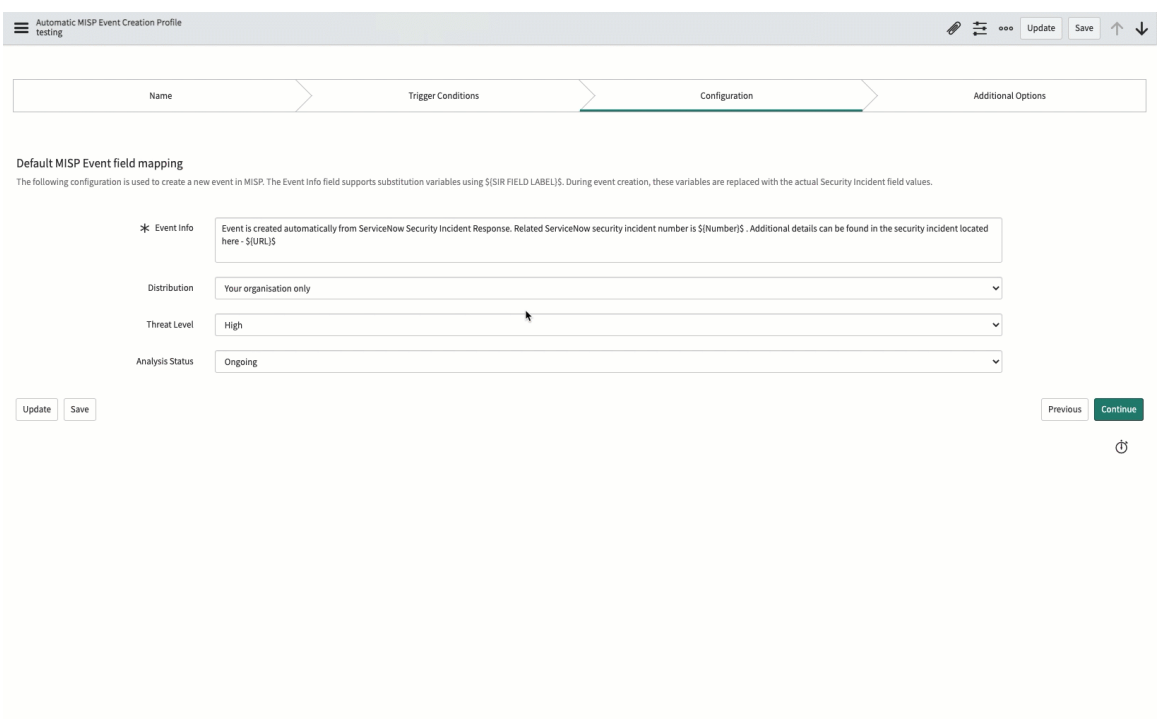
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	ajoutés en tant qu'attributs à l'événement MISP lors de la création de l'événement MISP.
Définir le marqueur IDS d'attribut lorsque le résultat observable est malveillant	Option qui vous permet de savoir que si un observable est marqué comme malveillant dans SIR, le marqueur IDS est activé pour l'attribut correspondant dans MISP Si le marqueur IDS n'est pas défini, l'attribut est considéré comme une information contextuelle et n'est pas utilisé pour la détection automatique des intrusions.

L'exemple suivant montre comment accéder à la page des options supplémentaires. Sur cette page, vous pouvez activer le mappage des observables SIR et des types d'attributs MISP, ajouter de nouveaux SIR types d'observables, tels que le réseau IPV6 et le réseau IPV4, et les mapper à l'adresse IP du domaine de type d'attribut MISP .

Mappage des SIR observables et MISP des types d'attributs



Synchroniser MITRE-ATT&CK les informations en MISP événements

Synchronisez les informations avec MISP des MITRE-ATT&CK attributs pour une meilleure analyse des incidents de sécurité et des menaces.

Avant de commencer

Rôle requis : sn_sec_misp.write

Procédure

Dans le formulaire Options supplémentaires, examinez les options pour synchroniser les informations avec les MITRE-ATT&CKMISP attributs.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Options avancées

Champ	Description
Synchroniser les techniques d'incident MITRE-ATT&CK™ de sécurité en tant que galaxies locales à l'événement MISP	Option permettant de synchroniser les techniques d'incident Now Platform SIRMITRE-ATT&CK™ de sécurité en tant que galaxies locales dans l'événement MISP . **Remarque :** Pour ajouter des galaxies locales, l'utilisateur qui a configuré l'intégration doit appartenir à l'organisation hôte du serveur correspondant MISP .
Synchroniser les techniques d'incident MITRE-ATT&CK™ de sécurité en tant que galaxies globales à l'événement MISP	Option permettant de synchroniser les techniques d'incident Now Platform SIRMITRE-ATT&CK™ de sécurité en tant que galaxies globales dans l'événement MISP .

Résultats
Vous avez créé un profil qui vous permet de créer automatiquement des événements dans MISP à Now Platformpartir du . Vous pouvez maintenant afficher les événements dans la liste connexe des événements MISP associés.

Ajouter des balises MISP aux événements

Ajoutez des balises MISP aux événements MISP créés.

Avant de commencer
Rôle requis : sn_sec_misp.write

Procédure
1. Dans le formulaire Options supplémentaires, accédez à **Sélectionner les balises MISP à ajouter à la section d'événement** de la vue de formulaire.
2. Passez en revue les options permettant d'ajouter des balises aux événements créés.

Formulaire Options avancées

Champ	Description
Ajouter des balises à l'événement MISP créé	Option qui vous permet d'ajouter automatiquement des balises MISP aux événements créés à partir de ServiceNow.
Balises (locales)	Les balises sélectionnées seront ajoutées en tant que balises locales à l'événement MISP.
Balises (globales)	Les balises sélectionnées seront ajoutées en tant que balises globales à l'événement MISP.

3. Cliquez sur **Enregistrer**.

Résultats
L'ajout de balises MISP facilite la classification de l'événement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MISP Données d'événement

Vous pouvez examiner les données des MISP événements afin d'afficher des informations détaillées sur les MISP événements.

MISP Données d'événement dans la vue de liste

Accéder à la vue de liste à partir de **MISP** > **Données d'événements MISP**.

Utilisez la vue de liste pour obtenir une vue d'ensemble rapide des données de l'événement MISP .

Vue de liste d'événements MISP

Champ	Description
ID d'événement	ID d'événement affecté par MISP la date à laquelle l'événement a été créé ou importé pour la première fois dans le MISP serveur.
Info	Brève description de l'événement.
Analyse	Étape actuelle de l'analyse de l'événement avec les options possibles suivantes : • Initial : L'analyse ne fait que commencer • En cours : l'analyse est en cours • Terminé : l'analyse est terminée
Niveau de menace	Niveau de risque de l'événement. Les incidents peuvent être classés en trois catégories de menace différentes (faible, moyenne, élevée). Ce champ peut rester non défini. Les options sont les suivantes : • Faible : programme malveillant de masse général • Moyen : menaces persistantes avancées (APT) • Élevé : APT sophistiquées et attaques 0-day
Balises MISP	Balises associées à l'événement MISP .
Galaxies MISP	Galaxies associées à l'événement MISP .
Org. du propriétaire	Organisation propriétaire de l'événement sur l'instance MISP . Ce champ n'est visible que par les administrateurs.
Org. du créateur	Organisation qui a créé l'événement sur l'instance MISP .
Distribution	Distribution de l'attribut individuel. Un attribut peut avoir un niveau de distribution différent de celui de l'événement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue de liste d'événements MISP (suite)

Champ	Description
Lien hypertexte d'événement MISP	Lien vers l'événement MISP stocké sur le MISP serveur.
Source MISP	MISP Source où l'événement est créé.

MISP Données d'événement dans la vue de formulaire

Utilisez la vue de formulaire pour obtenir des informations détaillées sur les MISP événements.

Vue de formulaire d'événement MISP

Champ	Description
ID d'événement	ID d'événement affecté par MISP la date à laquelle l'événement a été créé ou importé pour la première fois dans le MISP serveur.
UUID	ID qui identifie de manière unique les événements et les attributs.
Org. du créateur	Organisation qui a créé l'événement sur l'instance MISP .
Org. du propriétaire	Organisation propriétaire de l'événement sur l'instance MISP . Ce champ n'est visible que par les administrateurs.
Créateur	Utilisateur qui a créé l'événement en MISP.
Dernier changement	Date de la dernière modification de l'événement.
Source MISP	MISP Source où l'événement est créé.
Date de création (dans MISP)	Date à laquelle l'événement a été créé ou importé pour la première fois sur le MISP serveur.
Niveau de menace	Niveau de risque de l'événement. Les incidents peuvent être classés en trois catégories de menace différentes (faible, moyenne, élevée). Ce champ peut rester non défini. Les options sont les suivantes : • Faible : programme malveillant de masse général • Moyen : menaces persistantes avancées (APT) • Élevé : APT sophistiquées et attaques 0-day
Analyse	Étape actuelle de l'analyse de l'événement avec les options possibles suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue de formulaire d'événement MISP (suite)

Champ	Description
	• Initial : L'analyse ne fait que commencer • En cours : l'analyse est en cours • Terminé : l'analyse est terminée
Distribution	Distribution de l'attribut individuel. Un attribut peut avoir un niveau de distribution différent de celui de l'événement.
Publié	État indiquant si l'événement a été publié ou non. La publication permet d'utiliser les attributs de l'événement pour toutes les exportations éligibles et informe les utilisateurs qui se sont abonnés aux alertes d'événements.
Lien hypertexte d'événement MISP	Lien vers l'événement MISP stocké sur le MISP serveur.
Info	Brève description de l'événement.
Balises (locales)	Balises disponibles sur l'instance de l'organisation hôte pour activer le balisage pour la synchronisation et le filtrage des exportations. MISP Les événements ne sont pas modifiés MISP lorsque vous utilisez des balises locales. Les balises locales sont toujours supprimées avant d'être synchronisées avec d'autres instances et communautés de MISP partage.
Balises (globales)	Balises disponibles globalement pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des balises globales aux MISP instances, vous pouvez modifier les événements.
Galaxies (locales)	Galaxies disponibles sur l'instance de l'organisation hôte pour la synchronisation et le filtrage des exportations. MISP Les événements ne sont pas modifiés lorsque vous utilisez des galaxies MISP locales. Ces galaxies locales sont toujours dépouillées avant d'être synchronisées avec d'autres MISP instances et communautés de partage.
Galaxies (globales)	Galaxies disponibles dans le monde entier pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des galaxies globales, MISP vous pouvez modifier les événements.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Événements associés MISP

Vous pouvez utiliser la vue de liste des événements associés MISP pour afficher les événements qui ont été créés manuellement ou automatiquement dans le contexte d'un incident de sécurité.

Événements MISP associés

Champ	Description
Incident de sécurité	SIR incident de sécurité. Cliquez sur l'incident de sécurité pour afficher l'incident de sécurité.
Événement MISP	MISP ID d'événement. Cliquez sur l'événement MISP pour afficher l'événement MISP dans le Now Platform.
Source MISP	MISP Source où l'événement est créé. Cliquez sur la MISP source pour l'afficher.
Mode de création d'événements	État indiquant si l'événement a été créé manuellement ou automatiquement avec le profil de création d'événement. Cliquez sur l'événement MISP pour afficher l'événement associé MISP .
Profil de création automatique d'événements	Profil de création d'événement utilisé pour créer l'événement automatique. Cliquez sur le profil pour afficher le profil de création automatique d'événements MISP.

MISP Informations utilisateur

Vous pouvez utiliser la MISP page Informations utilisateur pour afficher tous les utilisateurs associés pour le Now Platform Intégration de MISP pour Opérations de sécurité.

Informations sur l'utilisateur MISP

Champ	Description
Source	Source du MISP compte utilisateur.
ID d'utilisateur	ID d'utilisateur attribué par le serveur lors de la création d'un MISP compte utilisateur.
E-mail de l'utilisateur	Adresse e-mail d'un utilisateur. Seuls les administrateurs d'organisation peuvent voir les adresses e-mail des utilisateurs de leur propre organisation.
Organisation	Organisation à laquelle un utilisateur appartient.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations sur l'utilisateur MISP (suite)

Champ	Description
Nom de rôle	Nom du rôle qui définit les privilèges d'utilisateur attribués à un utilisateur. Pour en savoir plus sur les rôles dans MISP, consultez la documentation MISP .
ID de rôle	ID de rôle d'utilisateur dans MISP. Par exemple, Administrateur permanent, Audit permanent ou Tagueur permanent, etc.
Autorisation	Les autorisations dont dispose un utilisateur. Les autorisations disponibles dans MISP sont les suivantes : • mode lecture seule • Gérer ses propres événements • Gérer les événements de l'organisation • Gérer la publication des événements de l'organisation
Autorisation de perception	Autorisation qui permet à un utilisateur d'effectuer des recherches de perception.
Autorisation du tagueur	Autorisation qui permet à un utilisateur d'effectuer un balisage.

Séparation de domaine et MISP

L'application Séparation de domaine est prise en charge dans MISP. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Support : basique.

Comment fonctionne Séparation de domaine avec MISP

Procédez comme suit pour réaliser Séparation de domaine :

- Créez un utilisateur avec les rôles requis dans votre domaine.
- Effectuez les Intégration de MISP pour Opérations de sécurité procédures dans votre domaine.

Dépannage de l'intégration MISP

Cette section couvre des conseils de dépannage importants qui peuvent vous aider à résoudre les problèmes courants que vous pouvez rencontrer lors de la configuration ou de l'exécution de l'intégration MISP.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Problèmes SSL

Lors de la connexion via l'intégration MISP, assurez-vous d'avoir installé un certificat CA valide sur le serveur MISP, qui n'a pas expiré. Vous pouvez importer RSA ou vos propres certificats dans la plateforme et vous assurer que le nom commun du certificat correspond au nom d'hôte. Pour plus d'informations, consultez Installez et configurez le Intégration de MISP pour Opérations de sécurité et MISP Rôles et autorisations d'utilisateur.

Utilisation MISP pour enquêter et analyser les menaces

Vous pouvez utiliser les MISP données du Now Platform Renseignements sur les menaces module et du module pour examiner et analyser les Now Platform SIR menaces qui pèsent sur votre organisation.

Recherches de perception dans MISP

Vous pouvez effectuer des recherches de perception sur les observables de l'instance MISP pour déterminer la fréquence à laquelle certains types d'attaques, telles que les attaques de hameçonnage ou les communications avec une adresse IP ou une URL malveillante, se produisent dans votre réseau. Chaque occurrence est considérée comme une observation.

Perceptions dans MISP

Les observations indiquent qu'un indicateur, un objet ou un attribut a été vu et que sa validité est confirmée. Sightings in MISP est un système qui vous permet de répondre aux attributs d'un événement. Il est conçu pour fournir à vos utilisateurs une méthode simple pour confirmer qu'ils ont vu un attribut donné, ce qui lui donne plus de crédibilité. Vous pouvez voir un attribut plusieurs fois.

Remarque : Les observables sont connus sous le nom d'attributs dans MISP.

Certains attributs sont considérés comme des faux positifs, ce qui signifie qu'il ne s'agit pas d'observations valides. D'autres attributs ne sont valides que pour une certaine durée, comme une campagne d'hameçonnage qui ne dure qu'une semaine. Vous pouvez affecter une date d'expiration aux attributs valides pour une certaine durée, mais chaque organisation ne peut affecter qu'une seule date d'expiration valide à un attribut.

Les perceptions qui sont créées MISP par les utilisateurs d'organisations marquées comme locales dans le serveur MISP correspondant sont appelées perceptions internes. Les perceptions qui sont créées MISP par les utilisateurs d'organisations qui sont marquées comme distantes dans le serveur correspondant MISP sont appelées perceptions externes.

Recherches de perception dans SIR

Le workflow Security Operations Integration - Recherche de perceptions exécute la recherche de perceptions. Ce workflow accepte une liste d'observables, trouve toutes les options d'implémentation, crée les requêtes basées sur les configurations de recherche de perception et exécute les recherches basées sur le workflow configuré.

Les recherches de perception aident les analystes à déterminer la prévalence d'une menace dans le temps. Vous pouvez sélectionner un ou plusieurs observables et la plage de dates pour votre recherche à partir d'un incident de sécurité. Les résultats sont inclus dans les listes connexes Perceptions d'incident de sécurité, Résultats de recherche de perceptions et Détails de recherche de perceptions .

Lorsque vous commencez à analyser un incident, vous pouvez configurer votre Now Platform organisation pour effectuer automatiquement une recherche de perceptions ou effectuer manuellement une recherche de perceptions observables afin d'identifier les autres utilisateurs de votre organisation qui sont touchés par la même attaque de hameçonnage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer les recherches automatiques de perception dans MISP

Activez l'exécution automatique de la recherche de perception dans MISP afin que le workflow Intégration de Security Operations - Recherche de perceptions soit déclenché chaque fois que de nouveaux observables sont associés à un incident de sécurité.

Avant de commencer

Vérifiez que le Profil de configuration de la recherche de perceptions pour MISP est actif.

Rôle requis : sn_si.analyst

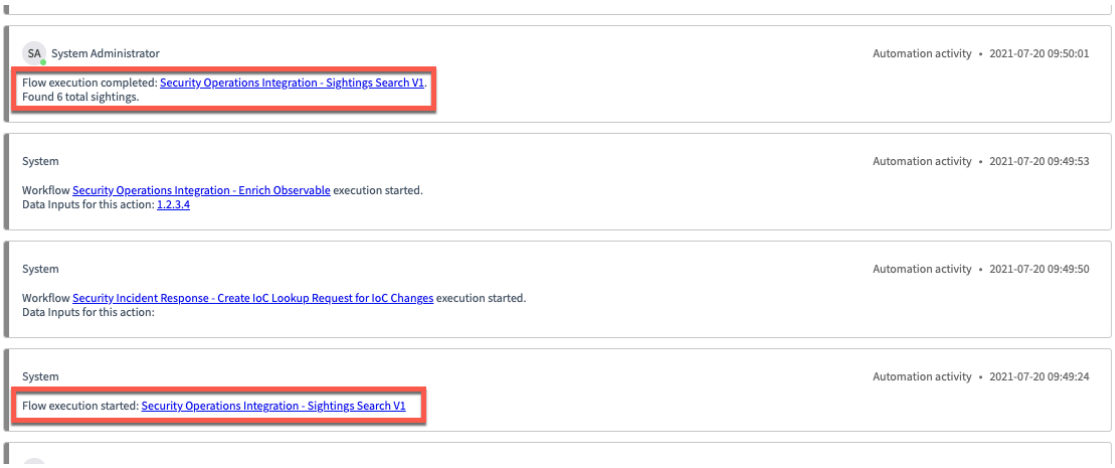
Pourquoi et quand exécuter cette tâche

Si vous activez l'aptitude de recherche de perception pour qu'elle s'exécute automatiquement dans le MISP Configuration de l'intégration, la recherche de perception dans MISP se déclenche lorsque de nouveaux observables sont associés à un incident de sécurité. Par défaut, l'option **Exécuter automatiquement la recherche de perception lorsque de nouveaux observables sont associés à l'incident de sécurité** est activée.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables que vous souhaitez afficher dans les données de recherche de MISP perceptions.
3. Examinez les notes de travail après que de nouveaux observables ont été associés à l'incident de sécurité.
   Une note de travail est publiée lorsque le workflow Security Operations Integration - Recherche de perceptions est déclenché.

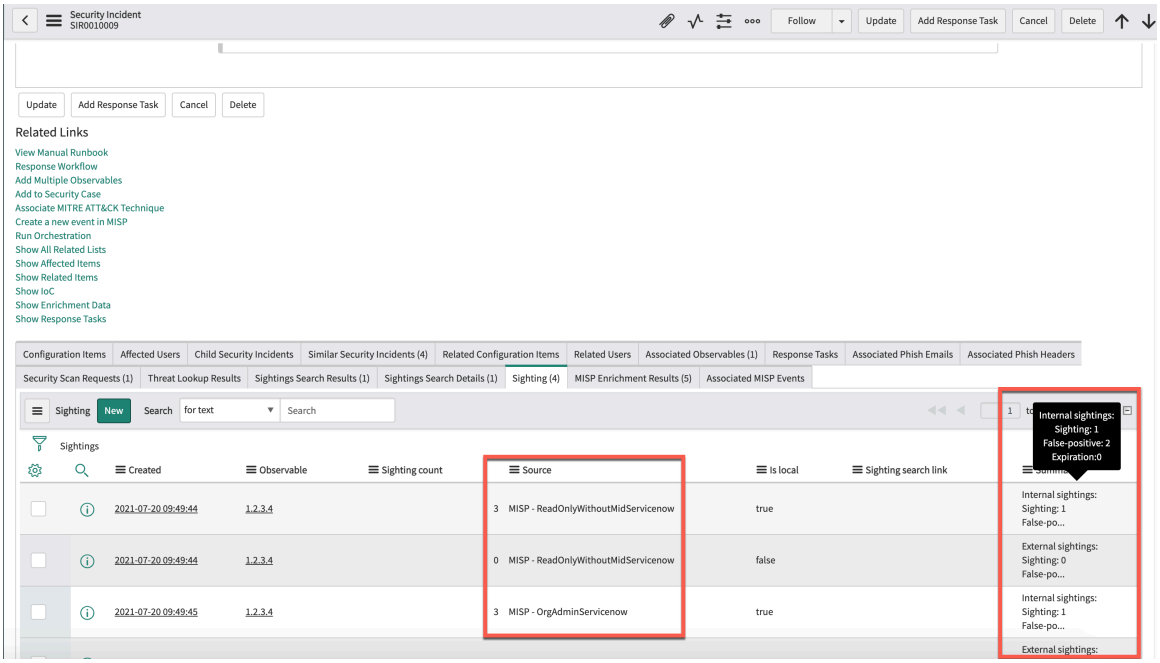
   L'exemple suivant montre la section des notes de travail.



4. Affichez les informations agrégées des observables qui sont observés dans tous les événements (globaux) et classés par leurs perceptions internes ou externes une fois l'exécution du workflow terminée.
   Consultez les informations contenues dans les listes connexes Perceptions, Résultats de recherche de perceptions et Détails de recherche de perceptions . L'exemple suivant montre l'enregistrement de recherche de perceptions qui a été créé dans la liste connexe Perceptions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Enregistrement de recherche de perceptions

Champ	Description
Créé	Date et heure de création de l'enregistrement de recherche de perceptions.
Observable	Observable recherché par la requête.
Nombre de perception	Nombre de perceptions internes et externes.
Source	Source de l'observable. Si l'observable provient d'une MISP organisation, l'enregistrement est précédé des mots `MISP`.
Est local	État indiquant si l'observation a été signalée par un utilisateur interne.
Lien de recherche sur la perception	Lien de recherche de perception dans l'instance MISP .
Résumé	Type d'observations associées à l'enregistrement. Les trois types d'observations sont la perception, le faux positif et l'expiration. La colonne Résumé s'affiche uniquement lorsque le Intégration de MISP pour Opérations de sécurité est installé. Si d'autres sources que MISP s'affichent, l'entrée de colonne Résumé est vide pour cet enregistrement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Effectuer une recherche manuelle de perception dans MISP

Sélectionnez un ou plusieurs observables et effectuez une recherche de perception manuelle dans l'application pour déterminer la prévalence d'une menace dans le Now Platform Intégration de MISP pour Opérations de sécurité temps.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations pour l'utilisation des MISP fonctionnalités bidirectionnelles.
- Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour lesquels vous souhaitez exécuter la MISP recherche de perceptions.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Sélectionnez l'observable, puis dans le menu Actions, cliquez sur **Exécuter la recherche de perceptions**.
   Vous pouvez sélectionner plusieurs observables pour une recherche d'observations.
   La boîte de dialogue Exécuter la recherche de perceptions s'ouvre.
5. Spécifiez la plage de dates pour rechercher les données de recherche d'observations.

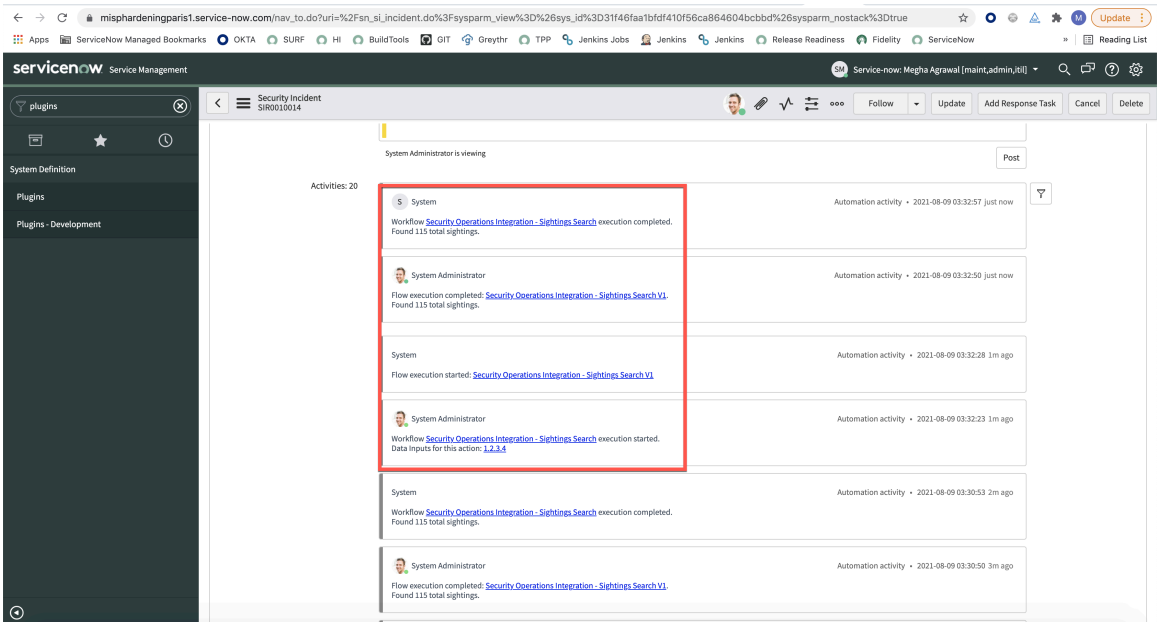
Boîte de dialogue Exécuter la recherche d'observations

Champ	Description
Dernier	Nombre d'heures ou de jours avant la création de l'incident à rechercher. La valeur par défaut est de 7 jours. La limite est de 99 heures ou jours.
entre	Plage de dates à rechercher. Les dates par défaut sont les suivantes : ◦ Date et heure de création de l'incident. ◦ Date et heure précédant sept jours l'ouverture de l'incident.

6. Cliquez sur **Rechercher**.
   L'exemple suivant montre les résultats de la recherche manuelle de perception dans les notes de travail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Résultats

Un enregistrement de recherche de perceptions est créé. Une fois l'exécution du workflow terminée, vous pouvez afficher les informations agrégées des observables observables sur tous les événements (globaux) et classés par leurs perceptions internes ou externes. Les données de perception agrégées et associées sont affichées dans l'incident de sécurité sous les listes connexes Perceptions, Résultats de recherche de perceptions et Détails de recherche de perceptions .

Signaler des observations à MISP

Signalez les perceptions de données sur les menaces afin de pouvoir réagir aux faux positifs dans vos données et d'accroître votre sensibilisation lorsqu'une menace réellement positive se produit. Vous pouvez également ajouter une date d'expiration pour un observable ou un attribut particulier.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations pour l'utilisation des MISP fonctionnalités bidirectionnelles.
- Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Le Intégration de MISP pour Opérations de sécurité vous permet de rapporter des observations à l'échelle MISP globale pour tous les événements. Pour signaler une observation à un événement spécifique, vous devez utiliser l'instance MISP et signaler l'observation localement.

Pour signaler une observation à MISP, l'observable ou l'attribut doit être disponible dans l'instance MISP .

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour lesquels vous souhaitez signaler les observations MISP .
3. Cliquez sur **Afficher toutes les listes connexes** et la liste connexe Observations.

Traduction automatique

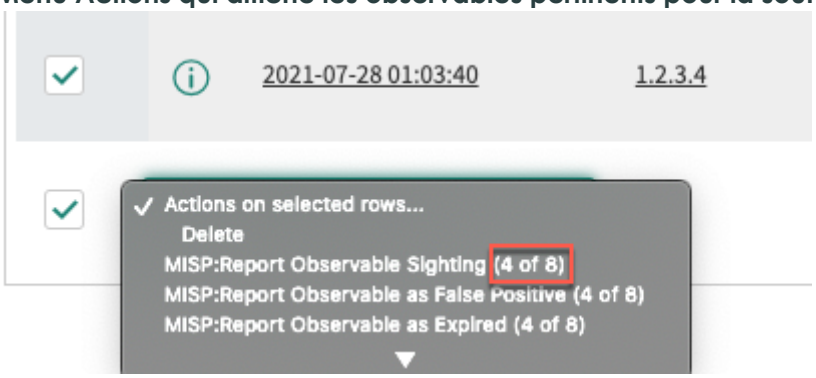
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez l'observable et, dans le menu Actions, sélectionnez l'une des options suivantes.

Option	Description
MISP : signaler une observation observable	Signaler l'observable comme vu à MISP. Si l'observable est associé à plusieurs événements, il est mis à jour dans tous les événements.
MISP : signaler un observable comme faux positif	Signaler l'observable comme faux positif à .MISP
MISP : signaler un observable comme expiré	Signaler l'observable comme expiré à MISP.

Si vous sélectionnez des observables qui ne sont pas spécifiques à une MISP source, le menu Actions affiche le nombre de sources pertinentes MISP . L'exemple suivant montre que quatre observables sur huit sont pertinents pour MISP. L'exemple suivant montre le menu Actions et les observables pertinents pour la soumission.

Menu Actions qui affiche les observables pertinents pour la soumission



5. Facultatif : Si vous avez sélectionné l'option **MISP : signaler une observation observable** , vous devez remplir les champs de la boîte de dialogue Signaler une observation observable vers MISP.

Boîte de dialogue Signaler une observation observable à MISP

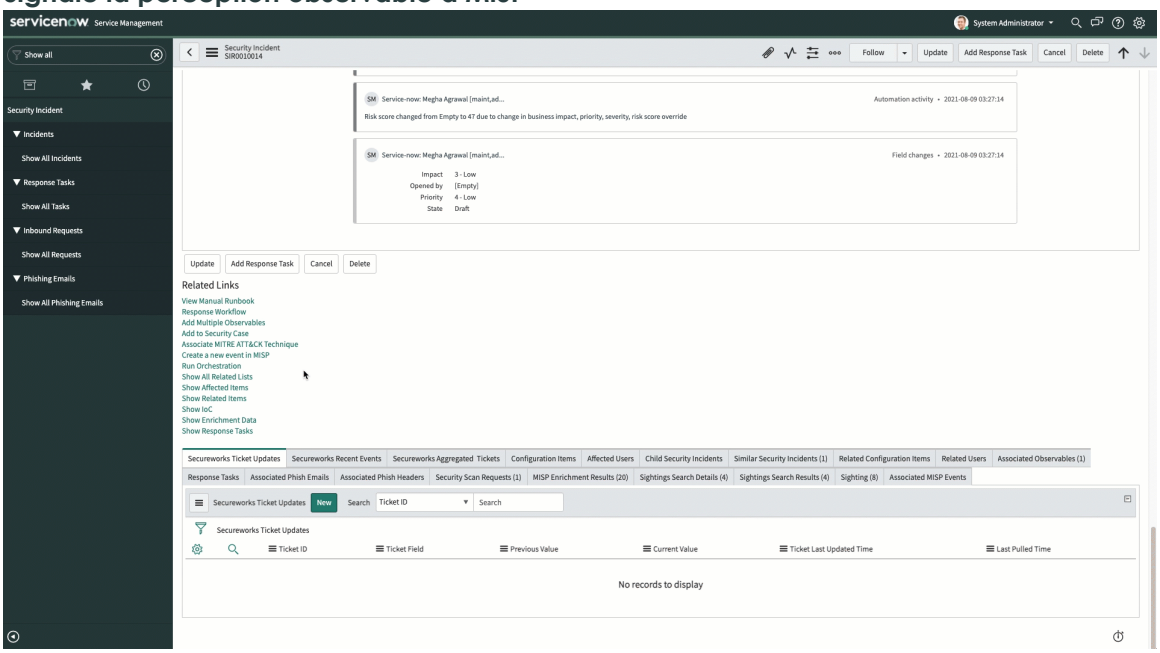
Champ	Description
Source	Champ source qui correspond à la MISP source de l'observation.
Date	Champ de date qui correspond à la date à laquelle l'observable est observé. Si la date est vide, la date et l'heure actuelles sont renseignées au format MISP.

L'exemple suivant montre comment accéder à la liste connexe Observations dans l'incident de sécurité. Dans cette liste, vous pouvez sélectionner un observable et signaler l'observation observable à MISP. Le message de réussite indique que l'observation a été soumise avec succès à MISP.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signale la perception observable à MISP



a. Cliquez sur **Signaler une observation.**

6. Facultatif : Si vous avez sélectionné l'option **MISP : signaler un observable comme faux positif** , vous devez renseigner les champs de la boîte de dialogue Signaler un observable comme faux positif vers MISP .

Signaler l'observable comme faux positif dans la boîte de MISP dialogue

Champ	Description
Source (facultatif)	Champ source correspondant à la MISP source. Utilisez ce champ pour déclarer l'observable comme faux positif.
Date	Champ de date correspondant à la date à laquelle l'observable s'est avéré être un faux positif. Si la date est vide, la date et l'heure actuelles sont renseignées au format MISP.

a. Cliquez sur **Signaler un faux positif**.

7. Facultatif : Si vous avez sélectionné l'option **MISP : signaler un observable comme expiré** , vous devez renseigner les champs de la boîte de dialogue Signaler l'expiration de l'observable à MISP .

Boîte de dialogue Signaler l'expiration de l'observable à MISP

Champ	Description
Source	Champ source correspondant à la MISP source. Utilisez ce champ pour définir un observable comme expiré.
Date	Champ de date qui correspond à la date à laquelle l'observable a expiré. Si la date

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	est vide, la date et l'heure actuelles sont renseignées au format MISP.

a. Cliquez sur **Expiration du rapport**.

Résultats
Les perceptions sont mises à jour avec succès sur le MISP serveur.

Enrichissement des observables dans MISP

En enrichissant les observables avec des informations supplémentaires provenant de diverses MISP sources au cours des enquêtes de réponse aux incidents, vous pouvez contenir les menaces identifiées.

Activer l'enrichissement automatique des observables dans MISP

Activez l'enrichissement Now Platform MISP automatique des observables lorsque de nouveaux observables sont associés à l'incident de sécurité.

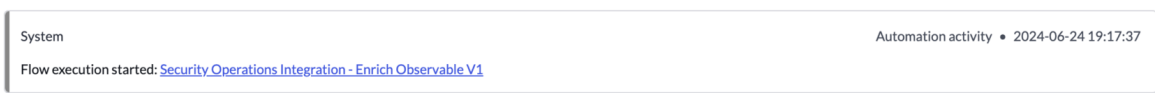
Avant de commencer

- Activer la Réponse aux incidents de sécurité propriété système pour l'option **Active ou désactive la tâche planifiée, Rechercher des observables d'incident de sécurité** pour déclencher l'aptitude d'enrichissement des observables dans SIR.
- Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour MISP lesquels vous souhaitez enrichir les données observables.
3. Examinez les notes de travail après que de nouveaux observables ont été associés à l'incident de sécurité.

   L'exemple suivant montre qu'une note de travail est publiée lorsque le flux Intégration de Security Operations - Enrichissement des observables se déclenche.

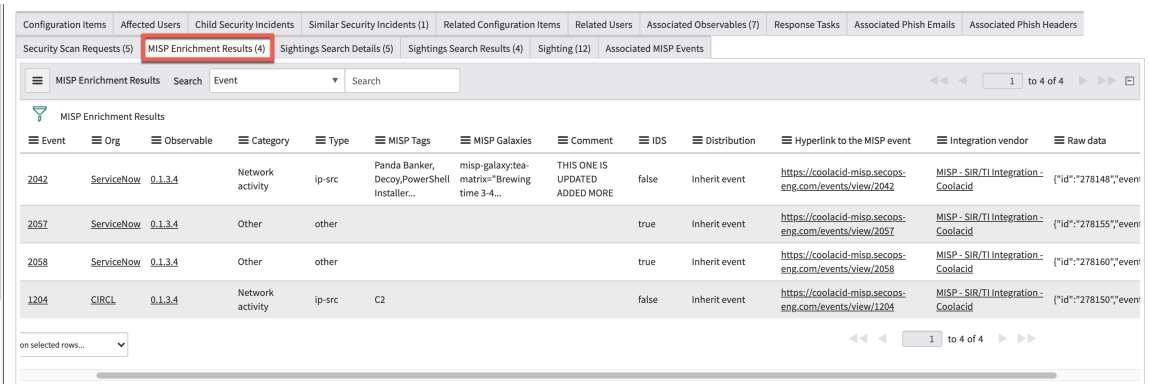
4. Dans la MISP liste connexe Résultats de l'enrichissement de l'incident de sécurité, affichez les résultats de l'enrichissement une fois l'exécution du flux terminée.

   Remarque : Vous devez configurer pour que la liste connexe des résultats de l'enrichissement MISP apparaisse dans les listes connexes des incidents de sécurité. Pour plus d'informations, consultez Configuration des listes connexes.

   L'exemple suivant montre les résultats d'enrichissement dans le MISPfichier .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le tableau suivant présente les résultats de l'enrichissement MISP.

Résultats de l'enrichissement MISP

Champ	Description
Événement	ID de l'événement. Cliquez sur Ouvrir pour afficher l'enregistrement dans l'instance Now Platform .
Org	Organisation qui a initialement créé l'événement.
Observable	Observable associé à l'événement.
Catégorie	Catégorie de l'attribut. Consultez la liste des catégories dans la documentation MISP .
Type	Type de l'attribut. Consultez la liste des types dans la documentation MISP .
Balises MISP	Liste des balises associées à l'attribut MISP .
Galaxies MISP	Liste des galaxies associées à l'attribut MISP .
Commentaire	Commentaire contextuel permettant de décrire plus précisément l'attribut. Ces commentaires ne sont pas utilisés à des fins de corrélation et sont purement informatifs.
IDS	Indicateur de compromis, qui lui permet d'être inclus dans toutes les exportations éligibles.
Distribution	Distribution de l'attribut après sa publication. Un attribut peut avoir un niveau de distribution différent de celui de l'événement. Dans les deux cas, le niveau de distribution le plus bas est utilisé.
Lien hypertexte vers l'événement MISP	Lien vers l'événement MISP , qui est stocké sur le MISP serveur.
Fournisseur de l'intégration	Fournisseur d'intégration qui fournit les données pour l'enrichissement.
Données brutes	Données brutes associées à l'attribut MISP .

Traduction automatique

Effectuer un enrichissement manuel de l'observable dans MISP

Sélectionnez un ou plusieurs observables et effectuez un enrichissement manuel des observables afin de pouvoir enrichir les observables avec des informations supplémentaires provenant de diverses MISP sources.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations pour l'utilisation des MISP fonctionnalités bidirectionnelles.
- Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour lesquels vous souhaitez effectuer l'enrichissement.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Sélectionnez l'observable et, dans le menu Actions, cliquez sur **Exécuter l'enrichissement de l'observable**.
   Vous pouvez sélectionner plusieurs observables pour une recherche d'observations.
   La boîte de dialogue Exécuter l'enrichissement de l'observable s'affiche.
5. Sélectionnez une MISP source et, dans la colonne Sélectionné, sélectionnez une implémentation pour enrichir les observables sélectionnés.
6. Cliquez sur **Envoyer**.
   Une note de travail indique que le workflow Intégration de Security Operations - Enrichissement des observables s'est déclenché. Les workflows d'implémentation associés s'exécutent pour effectuer l'enrichissement. Vous pouvez afficher les notes de travail dans l'incident de sécurité pour afficher l'état.

   L'exemple suivant montre comment afficher les notes de travail pour un enrichissement manuel de l'observable.

Notes de travail pour l'enrichissement manuel des observables



Le message d'enrichissement répertorie l'événement créé. Vous pouvez afficher l'événement dans le Now Platform ou dans l'instance MISP et afficher les détails de l'enregistrement dans l'onglet Résultats de l'enrichissement MISP.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter ou supprimer des balises aux MISP attributs

Ajoutez ou supprimez des balises pour MISP classer des événements ou des attributs. Vous pouvez utiliser le balisage globalement pour activer votre classification ou utiliser des balises localement lorsque vous ne souhaitez pas que MISP les événements soient modifiés pendant votre classification.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations pour l'utilisation des MISP fonctionnalités bidirectionnelles.
- Vérifiez que l'attribut que vous modifiez appartient à la même organisation que l'utilisateur MISP .
- Notez que les balises et les galaxies qui sont à votre disposition sont basées sur la source et ses MISP autorisations de distribution.
- Rôle requis : sn_sec_misp.write

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables, les attributs ou les événements pour lesquels vous souhaitez ajouter les balises.
3. Cliquez sur **Afficher toutes les listes connexes** et la liste connexe Résultats de l'enrichissement MISP.
4. Cliquez sur l'icône ⓘ en regard d'un enregistrement, puis cliquez sur **Ouvrir l'enregistrement**.
   L'exemple suivant montre comment examiner les **résultats d'enrichissement MISP** et comment ouvrir un MISP enregistrement d'enrichissement.

   Enregistrement du résultat d'enrichissement MISP
   Ouverture de l'enregistrement des résultats d'enrichissement MISP

5. Passez en revue l'enregistrement des résultats de l'enrichissement MISP.

Résultat de l'enrichissement MISP

Champ	Description
Observable	
Événement	ID d'événement affecté par le serveur lors de la MISP première création ou importation de l'événement dans MISP. Prévisualisez l'événement ou cliquez sur l'enregistrement pour afficher les données de l'événement dans la page Données de l'événement MISP .
Org	Organisation qui a créé l'attribut MISP .
Catégorie	Catégorie de l'attribut que vous ajoutez à l'événement spécifique dans MISP. Vous pouvez sélectionner une option telle qu'une référence interne, l'activité réseau, la fraude financière, etc.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type	Type d'attribut MISP .
Fournisseur de l'intégration	Fournisseur d'intégration qui fournit les données pour l'enrichissement des observables.
Date de création (dans MISP)	Date de création ou d'importation initiale de l'événement dans MISP.
IDS	État indiquant si un observable est marqué comme malveillant dans SIR. L'attribut correspondant dans MISP est également marqué comme vrai.
Distribution	Contrôles des options de distribution, tels que les personnes qui peuvent voir cet événement après sa publication. Cette option contrôle également si l'événement est synchronisé avec d'autres serveurs. La distribution est héritée par les attributs, et le paramètre le plus restrictif l'emporte. Les options de distribution sont les suivantes : ◦ Votre organisation uniquement : permet uniquement aux membres de votre organisation de voir cet événement. L'événement peut être transféré vers une autre instance par l'un des membres de votre organisation, où seule votre organisation a l'accès pour le visualiser. Les événements avec ce paramètre ne sont pas synchronisés. ◦ Cette communauté uniquement : permet aux utilisateurs qui font partie de votre MISP communauté d'afficher l'événement, y compris votre propre organisation, les organisations présentes sur ce MISP serveur et les organisations qui exécutent des serveurs qui se MISP synchronisent avec ce serveur. Toute autre organisation connectée à ces serveurs liés n'est pas autorisée à visionner l'événement. ◦ Communautés connectées : permet aux utilisateurs qui font partie de votre MISP communauté de voir l'événement (y compris toutes les organisations sur ce serveur, toutes les organisations sur MISP les MISP serveurs qui se synchronisent avec ce serveur et les organisations d'hébergement des serveurs qui se connectent à n'importe quel serveur situé à deux sauts). Toute autre organisation connectée aux serveurs liés situés à deux sauts de distance n'est pas autorisée à afficher l'événement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Toutes les communautés : partage l'événement avec toutes les MISP communautés, ce qui permet à l'événement d'être disponible gratuitement.
Lien hypertexte vers l'événement MISP	Lien vers l'événement MISP stocké sur le MISP serveur.
Données brutes	Détails bruts pour l'enregistrement de données d'enrichissement observable.
Commentaire	Commentaires que vous ajoutez pour les attributs. Ces commentaires sont fournis à titre informatif uniquement et ne sont pas utilisés à des fins de corrélation.
Balises (locales)	Balises disponibles sur l'instance de l'organisation hôte pour activer le balisage pour la synchronisation et le filtrage des exportations. MISP Les événements ne sont pas modifiés MISP lorsque vous utilisez des balises locales. Ces balises sont toujours supprimées avant d'être synchronisées avec d'autres instances et communautés de MISP partage.
Balises (globales)	Balises disponibles globalement pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des balises globales aux MISP instances, vous modifiez les événements.
Galaxies (locales)	Galaxies disponibles sur l'instance de l'organisation hôte pour la synchronisation et le filtrage des exportations. MISP Les événements ne sont pas modifiés lorsque vous utilisez des galaxies MISP locales. Ces galaxies sont toujours dépouillées avant d'être synchronisées avec d'autres MISP instances et communautés de partage.
Galaxies (globales)	Galaxies disponibles dans le monde entier pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des galaxies globales, MISP les événements sont modifiés.

Traduction automatique

6. Pour modifier une balise locale ou globale, cliquez sur l'icône dans l'une des options suivantes :

- **Balises (locales)**
- **Balises (globales)**

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Dans la boîte de dialogue Balises d'attributs MISP, entrez le nom de la balise à rechercher et ajoutez-la.
8. Cliquez sur **Mettre à jour les balises vers l'attribut MISP**.

   L'exemple suivant montre qu'en cliquant sur l'icône d'édition des balises locales, vous pouvez rechercher et ajouter les balises C3, Adware, C2 et Botnet 3101, et mettre à jour le serveur MISP avec les balises. Le message de confirmation indique que toutes les balises ont été mises à jour dans MISP.

   Ajout de balises locales dans l'attribut MISP.
   Les balises sont mises à jour avec succès dans le MISP serveur.
9. Pour afficher les changements dans l'enregistrement, cliquez sur **Recharger le formulaire** dans le message de réussite.

Ajouter ou supprimer des galaxies à un événement ou à un MISP attribut

Ajoutez ou supprimez des galaxies afin MISP de classer ces objets en tant qu'amas et MISP de les associer à des événements ou à MISP des attributs.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations pour l'utilisation des MISP fonctionnalités bidirectionnelles.
- Pour ajouter des galaxies locales, l'utilisateur qui a configuré l'intégration doit appartenir à l'organisation hôte du serveur correspondant MISP .
- Notez que les balises et les galaxies qui sont à votre disposition sont basées sur la source et ses MISP autorisations de distribution.
- Rôle requis : sn_sec_misp.write

Procédure

1. Cliquez sur l'icône dans l'une des options suivantes.

- **Galaxies (locales)**
- **Galaxies (globales)**

2. Dans la boîte de dialogue Galaxies d'événements MISP, renseignez les détails.

Boîte de dialogue Galaxies d'événements MISP

Champ	Description
ID d'événement	ID d'événement affecté par le serveur lors de la MISP première création ou importation de l'événement dans MISP.
Espace de noms	Espace de noms dans lequel la galaxie est stockée. Vous pouvez utiliser des espaces de noms pour regrouper des galaxies similaires.
Galaxies	Galaxie dans laquelle vous stockez les informations du cluster.
Grappes	Informations sur les amas de la galaxie.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Mettre à jour les galaxies vers l'attribut MISP**.
   L'exemple suivant montre qu'en cliquant sur l'icône d'édition des galaxies locales, vous pouvez sélectionner l'espace de noms déconseillé, sélectionner la galaxie Attaque Enterprise - Modèle d'attaque et ajouter les informations du cluster. Une fois les informations de la galaxie mises à jour, vous pouvez afficher le message de réussite.

   Ajout d'informations sur les galaxies dans MISP via la Now Platform

4. Pour afficher les changements dans l'enregistrement, cliquez sur **Recharger le formulaire** dans le message de réussite.

Résultats
Les informations de la galaxie sont mises à jour avec succès dans le MISP serveur.

Ajouter des commentaires à l'attribut MISP

Ajoutez des commentaires pour les MISP attributs. Les commentaires que vous ajoutez le sont uniquement à des fins d'information et ne sont pas utilisés à des fins de corrélation des MISP données.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations pour l'utilisation des MISP fonctionnalités bidirectionnelles.
- Vérifiez que l'attribut que vous modifiez appartient à la même organisation que l'utilisateur MISP .
- Rôle requis : sn_sec_misp.write

Procédure

1. Cliquez sur l'icône Modifier dans le champ .
2. Saisissez votre commentaire dans le champ Commentaire d'attribut.
3. Cliquez sur **Mettre à jour le commentaire sur l'attribut MISP**.
   L'exemple suivant montre qu'en cliquant sur l'icône de modification en regard du champ de commentaire, vous pouvez ajouter un commentaire, puis mettre à jour l'attribut MISP . Une fois le commentaire mis à jour, vous pouvez afficher le message de réussite.

   Ajout d'informations sur les galaxies dans MISP via Now Platform.

4. Pour afficher les changements dans l'enregistrement, cliquez sur **Recharger le formulaire** dans le message de réussite.

Résultats
Le commentaire est mis à jour avec succès dans le MISP serveur.

Gestion d'événements dans MISP

Vous pouvez créer des événements automatiquement ou manuellement à MISP partir du Now Platformfichier . Vous pouvez également modifier les données d'événement dans MISP à partir du Now Platformfichier .

Vérification des événements créés automatiquement dans MISP

Vous pouvez vérifier les événements créés automatiquement après avoir configuré le profil de création d'événements dans votre Now Platform instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Profil de création automatique d'événements

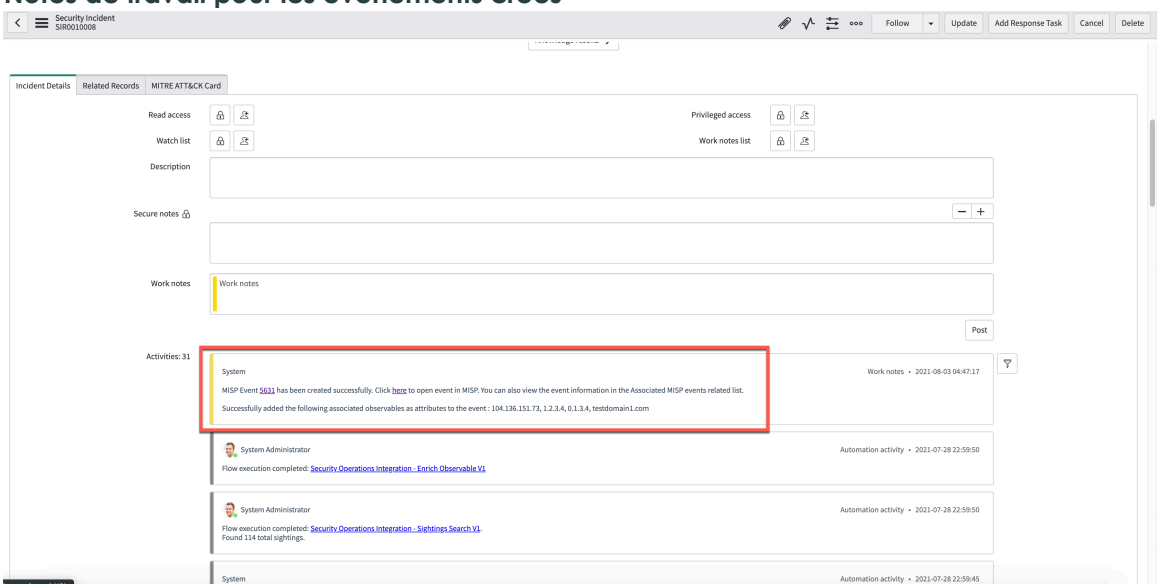
La configuration du profil de création automatique d'événements est effectuée par les rôles d'utilisateur sn_si.admin ou sn_ti.admin dans le **Intégration de MISP** > **Profils de création automatique d'événements** module.

Affichage des données de l'événement MISP

Vous pouvez afficher les événements créés des manières suivantes :

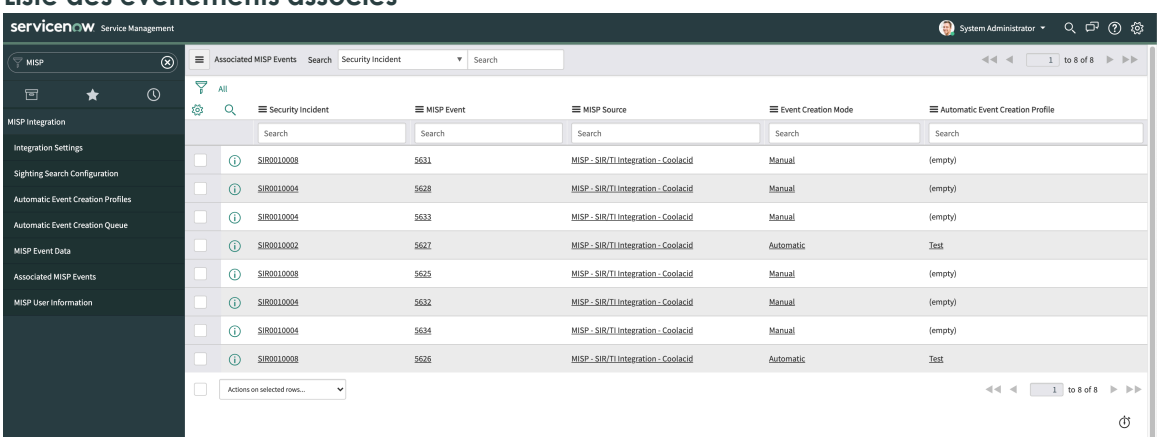
- Affichez les notes de travail pour les événements créés. Vous pouvez afficher les détails de l'événement dans l'instance Now Platform ainsi que tel qu'il apparaît sur le MISP serveur, comme illustré dans l'exemple suivant.

Notes de travail pour les événements créés



- Cliquez sur la liste connexe Événements MISP associés . Ici, vous pouvez afficher l'événement par rapport à l'incident de sécurité et aux MISP ressources, comme illustré dans l'exemple suivant.

Liste des événements associés

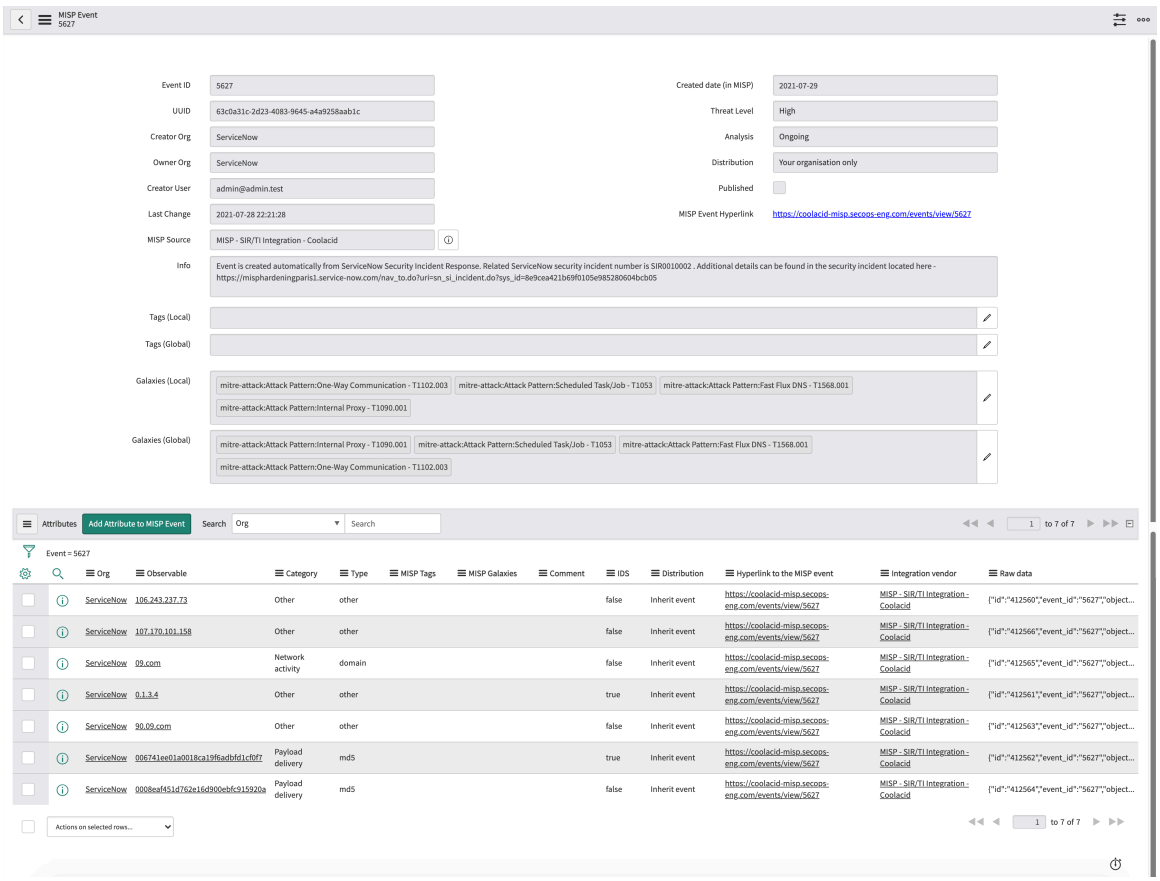


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Affichez les données d'événement MISP dans la vue de formulaire pour examiner les informations détaillées sur les MISP événements, comme illustré dans l'exemple suivant.

Données d'événement dans la vue de formulaire



Créer manuellement un événement dans MISP

Créez manuellement des événements à MISP partir de pour Now Platform capturer des informations contextuelles représentées sous forme d'attributs et d'objets.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations pour l'utilisation des MISP fonctionnalités bidirectionnelles.
- Rôle requis : sn_sec_misp.write

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour lesquels vous souhaitez créer un événement.
3. Cliquez sur **Créer un nouvel événement dans MISP**.
4. Renseignez les champs de la boîte de dialogue Créer un nouvel événement dans MISP.

Créer un événement dans la boîte de dialogue MISP

Champ	Description
Date	Date de création de l'événement en MISP.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Informations sur l'événement	Informations sur l'événement Now Platform Réponse aux incidents de sécuritéqui sont automatiquement créées à partir du .
Niveau de menace	Niveau de risque de l'événement. Vous pouvez classer les incidents en trois catégories de menace différentes (faible, moyenne, élevée). Ce champ peut également rester non défini. Les options sont les suivantes : ◦ Faible : programme malveillant de masse général ◦ Moyen : menaces persistantes avancées (APT) ◦ Élevé : APT sophistiquées et attaques 0-day
Source	MISP Source pour la création de l'événement.
Distribution	Option qui contrôle qui peut voir cet événement après sa publication. Cette option contrôle également si l'événement est synchronisé avec d'autres serveurs. La distribution est héritée par les attributs. Le réglage le plus restrictif l'emporte. Les options de distribution sont les suivantes : ◦ Votre organisation uniquement : permet uniquement aux membres de votre organisation de voir cet événement. L'événement peut être transféré vers une autre instance par l'un des membres de votre organisation, où seule votre organisation a l'accès pour le visualiser. Les événements avec ce paramètre ne sont pas synchronisés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Cette communauté uniquement : permet aux utilisateurs qui font partie de votre MISP communauté d'afficher l'événement, y compris votre propre organisation, les organisations présentes sur ce MISP serveur et les organisations qui exécutent des serveurs qui se MISP synchronisent avec ce serveur. Toute autre organisation connectée à des serveurs liés n'est pas autorisée à afficher l'événement. ◦ Communautés connectées : permet aux utilisateurs qui font partie de votre MISP communauté d'afficher l'événement, y compris toutes les organisations sur ce serveur, toutes les organisations sur MISP les MISP serveurs qui se synchronisent avec ce serveur et les organisations d'hébergement des serveurs qui se connectent à n'importe quel serveur situé à deux sauts. Toutes les autres organisations connectées aux serveurs liés situés à deux sauts de ce serveur ne peuvent pas afficher l'événement. ◦ Toutes les communautés : partage l'événement avec toutes les MISP communautés.
Analyse	Étape actuelle de l'analyse de l'événement avec les options possibles suivantes : ◦ Initial : L'analyse ne fait que commencer ◦ En cours : l'analyse est en cours ◦ Terminé : l'analyse est terminée

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ		Description
Options avancées	Ajouter les observables associés SIR en tant qu'attributs à l'événement MISP	Option permettant d'ajouter des observables disponibles dans un incident de sécurité à un MISP événement en tant qu'attributs. Cette option active l'option **Définir le marqueur IDS d'attribut lorsque le résultat observable est malveillant** .
	Définir le marqueur IDS d'attribut lorsque le résultat observable est malveillant	Observable marqué comme malveillant dans SIR. L'attribut correspondant dans MISP est également marqué comme vrai.
	Filtrer les observables en fonction des balises de sécurité	Option permettant de filtrer les observables en fonction des balises de sécurité sélectionnées. Cette option permet de distinguer et de gérer les événements MISP dans Threat Intelligence. **Balises de sécurité** : ajoutez des balises pour filtrer les observables. Par exemple, si vous ajoutez une balise appelée « Bloquer à partir du partage » ou « TLP : blanc », si l'une de ces balises est associée à l'un des observables, ces observables ne sont pas ajoutés en tant qu'attributs à l'événement MISP lors de la création de l'événement MISP.
	Synchroniser les techniques d'incident de sécurité MITRE ATT&CK en tant que galaxies locales à l'événement MISP	Option permettant de synchroniser les techniques d'incident Now Platform SIRMITRE-ATT&CK™ de sécurité en tant que galaxies locales dans l'événement MISP .
	Synchroniser les techniques d'incident de sécurité ATT&CK MITRE en tant que galaxies globales à l'événement MISP	Option permettant de synchroniser les techniques d'incident Now Platform SIRMITRE-ATT&CK™ de sécurité en tant que galaxies globales dans l'événement MISP .

Traduction automatique

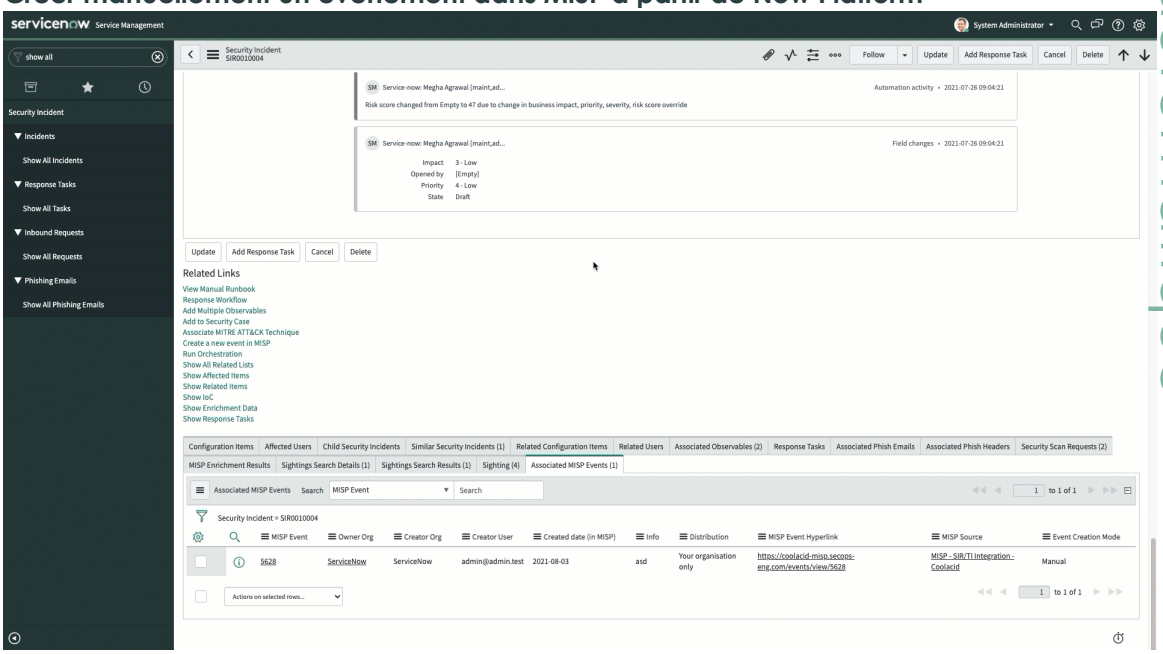
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ		Description
	Ajouter des balises à l'événement MISP	Option qui vous permet d'ajouter des balises MISP aux événements créés à partir de ServiceNow. Cette option affiche les options suivantes : ◦ **Local (balises) :**Les balises sélectionnées seront ajoutées en tant que balises locales à l'événement MISP. ◦ **Global (balises) :**Les balises sélectionnées seront ajoutées en tant que balises globales à l'événement MISP.

5. Cliquez sur **Créer un nouvel événement MISP**.

L'exemple suivant montre qu'en créant un événement dans MISP, vous pouvez afficher les résultats dans l'incident de sécurité. Vous pouvez également afficher les notes de travail, l'événement dans l'instance Now Platform et l'événement dans le MISP serveur, comme illustré dans l'exemple suivant.

Créer manuellement un événement dans MISP à partir de Now Platform



Vous pouvez afficher les résultats des manières suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Un message de réussite s'affiche en haut de la page de l'incident de sécurité. Vous pouvez afficher les détails de l'événement dans l'instance Now Platform , ainsi que tel qu'il apparaît sur le MISP serveur.
- Dans les notes de travail, vous pouvez voir le message de réussite avec plus de détails. Vous pouvez également afficher les détails de l'événement dans l'instance Now Platform et tel qu'il apparaît sur le MISP serveur.
- Dans la liste connexe Événements MISP associés , vous pouvez afficher l'événement par rapport à l'incident de sécurité et aux MISP ressources.

Ajouter des attributs à un MISP événement

Ajoutez des attributs à un événement, tels que le type, la catégorie et d'autres informations contextuelles sur l'événement.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations pour l'utilisation des MISP fonctionnalités bidirectionnelles.
- Vérifiez que l'événement que vous ajoutez ou mettez à jour l'attribut appartient à la même organisation que l'utilisateur MISP .
- Rôle requis : sn_sec_misp.write

Procédure

1. Accédez à la **Tout** > **MISP** > **Événements MISP associés**.
   Vous pouvez également accéder à la liste connexe Événement MISP associé dans n'importe quel incident de sécurité.
2. Cliquez sur l'événement MISP pour lequel vous souhaitez ajouter un attribut.
3. Cliquez sur **Ajouter un attribut à l'événement MISP**.
4. Renseignez les champs de la boîte de dialogue Ajouter un attribut à l'événement.

Boîte de dialogue Ajouter un attribut à l'événement

Champ	Description
Valeur	Valeur réelle de l'attribut. Entrez des données sur la valeur en fonction de ce qui est valide pour le type d'attribut choisi. Par exemple, pour un attribut de type ip-src (adresse IP source), 11.11.11.11 est une valeur valide. **Remarque :** Vous ne pouvez sélectionner que des attributs ou des observables qui partagent le contexte avec l'événement. Les observables ne peuvent pas déjà avoir un attribut dans MISP.
Catégorie	Catégorie de l'attribut. La catégorie décrit l'aspect du programme malveillant pour cet attribut. Un exemple serait les mécanismes de persistance du logiciel malveillant ou de l'activité du réseau.

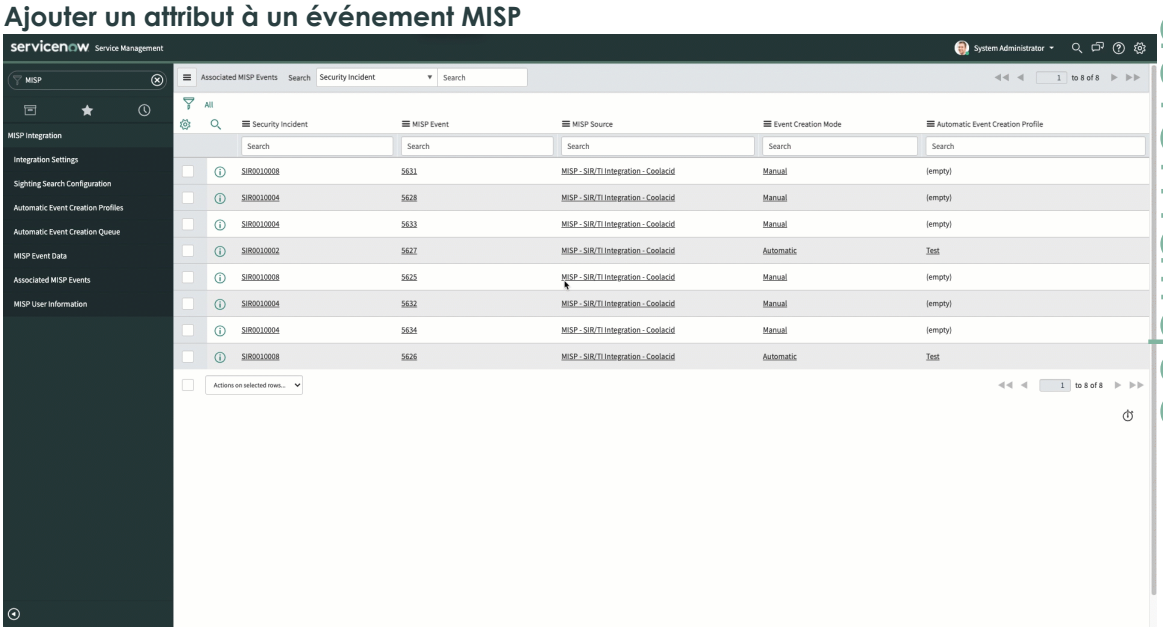
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type	Type qui explique la catégorie. Par exemple, si un attaquant utilise une adresse IP pour une attaque, une adresse e-mail source ou un fichier envoyé via une pièce jointe peuvent tous décrire la livraison de la charge utile d'un logiciel malveillant. Ces types d'attributs ont la catégorie de livraison de la charge utile.
Distribution	Utilisateurs pouvant afficher cet attribut. La distribution est héritée par attributs. Le réglage le plus restrictif l'emporte.
Utiliser l'attribut comme signature IDS	Observable marqué comme malveillant dans SIR. L'attribut correspondant dans MISP est également marqué comme vrai.
Commentaires	Commentaires que vous ajoutez pour les attributs.

L'exemple suivant montre qu'en naviguant à partir de la liste Événements MISP associés, vous pouvez afficher l'enregistrement d'événement 5627 et ajouter des attributs à l'événement. Les attributs incluent la valeur (testdomain.com), la catégorie en tant qu'analyse externe et le type en tant que domaine. Vous pouvez également activer IDS. Le message de réussite sur l'enregistrement d'événement indique que l'attribut est ajouté à l'événement, comme illustré dans l'exemple suivant.

Ajouter un attribut à un événement MISP



5. Cliquez sur **Ajouter un attribut à l'événement MISP**.

Résultats

Vous pouvez afficher l'attribut ajouté dans la section Attributs.

Ajouter des balises à un MISP événement

Ajoutez des balises Now Platform MISP pour classer des événements ou des attributs. Vous pouvez utiliser le balisage globalement pour activer votre classification ou utiliser des balises

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

localement lorsque vous ne souhaitez pas que MISP les événements soient modifiés pendant votre classification.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations pour l'utilisation des MISP fonctionnalités bidirectionnelles.
- Vérifiez que l'événement que vous modifiez appartient à la même organisation que l'utilisateur MISP .
- Notez que les balises et les galaxies qui sont à votre disposition sont basées sur la source et ses MISP autorisations de distribution.
- Rôle requis : sn_sec_misp.write

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient l'événement pour lequel vous souhaitez ajouter des balises.
3. Cliquez sur **Afficher toutes les listes connexes** et la liste connexe Résultats de l'enrichissement MISP.
4. Cliquez sur l'ID d'événement dans la liste des résultats d'enrichissement.
   Vous pouvez également naviguer à partir du **MISP** > **Événements MISP associés** module.
5. Passez en revue l'enregistrement de l'événement MISP.

Vue de formulaire d'événement MISP

Champ	Description
ID d'événement	ID d'événement affecté par MISP la date à laquelle l'événement a été créé ou importé pour la première fois dans le MISP serveur.
UUID	ID qui identifie de manière unique les événements et les attributs.
Org. du créateur	Organisation qui a créé l'événement sur l'instance MISP .
Org. du propriétaire	Organisation propriétaire de l'événement sur l'instance MISP . Ce champ n'est visible que par les administrateurs.
Créateur	Utilisateur qui a créé l'événement en MISP.
Dernier changement	Date de la dernière modification de l'événement.
Source MISP	MISP Source où l'événement est créé.
Date de création (dans MISP)	Date à laquelle l'événement a été créé ou importé pour la première fois sur le MISP serveur.
Niveau de menace	Niveau de risque de l'événement. Les incidents peuvent être classés en trois catégories de menace différentes (faible,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	moyenne, élevée). Ce champ peut rester non défini. Les options sont les suivantes : ◦ Faible : programme malveillant de masse général ◦ Moyen : menaces persistantes avancées (APT) ◦ Élevé : APT sophistiquées et attaques 0-day
Analyse	Étape actuelle de l'analyse de l'événement avec les options possibles suivantes : ◦ Initial : L'analyse ne fait que commencer ◦ En cours : l'analyse est en cours ◦ Terminé : l'analyse est terminée
Distribution	Distribution de l'attribut individuel. Un attribut peut avoir un niveau de distribution différent de celui de l'événement.
Publié	État indiquant si l'événement a été publié ou non. La publication permet d'utiliser les attributs de l'événement pour toutes les exportations éligibles et informe les utilisateurs qui se sont abonnés aux alertes d'événements.
Lien hypertexte d'événement MISP	Lien vers l'événement MISP stocké sur le MISP serveur.
Info	Brève description de l'événement.
Balises (locales)	Balises disponibles sur l'instance de l'organisation hôte pour activer le balisage pour la synchronisation et le filtrage des exportations. MISP Les événements ne sont pas modifiés MISP lorsque vous utilisez des balises locales. Les balises locales sont toujours supprimées avant d'être synchronisées avec d'autres instances et communautés de MISP partage.
Balises (globales)	Balises disponibles globalement pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des balises globales aux MISP instances, vous pouvez modifier les événements.
Galaxies (locales)	Galaxies disponibles sur l'instance de l'organisation hôte pour la synchronisation et le filtrage des exportations. MISP Les événements ne sont pas modifiés lorsque vous utilisez des galaxies MISP locales. Ces galaxies locales sont toujours dépouillées avant d'être synchronisées avec d'autres

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	MISP instances et communautés de partage.
Galaxies (globales)	Galaxies disponibles dans le monde entier pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des galaxies globales, MISP vous pouvez modifier les événements.

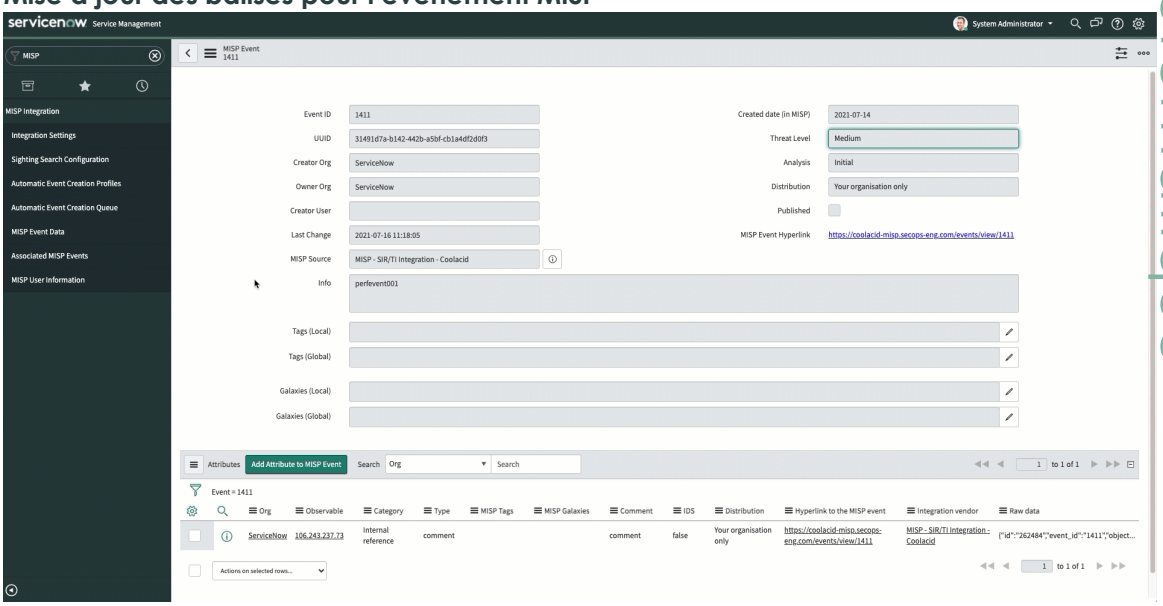
6. Pour modifier une balise locale ou globale, cliquez sur l'icône dans l'une des options suivantes :

- **Balises (locales)**
- **Balises (globales)**

7. Dans la boîte de dialogue Balises d'événements MISP, entrez le nom de la balise à rechercher et ajoutez les balises.
8. Cliquez sur **Mettre à jour les balises pour l'événement MISP**.

   L'exemple suivant montre qu'en cliquant sur l'icône d'édition des balises locales, vous pouvez rechercher et ajouter les balises C3, Adware, C2 et Botnet 3101, et mettre à jour le serveur MISP avec les balises. Le message de confirmation indique que toutes les balises sont mises à jour dans MISP.

Mise à jour des balises pour l'événement MISP



9. Cliquez sur **Recharger le formulaire** dans le message de réussite pour afficher les changements dans l'enregistrement.

Résultats

Les balises sont mises à jour avec succès dans le MISP serveur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mettre à jour les galaxies vers un événement ou un MISP attribut

Ajoutez ou supprimez des galaxies afin Now Platform MISP de classer ces objets comme un amas dans l'instance MISP et de les associer à des événements ou à MISP des attributs.

Avant de commencer

- Examiner le MISP Rôles d'utilisateur et autorisations requis pour utiliser les MISP fonctionnalités bidirectionnelles.
- Pour ajouter des galaxies locales, l'utilisateur qui a configuré l'intégration doit appartenir à l'organisation hôte du serveur correspondant MISP .
- Les balises et les galaxies disponibles sont basées sur la source et ses MISP autorisations de distribution.
- Rôle requis : sn_sec_misp.write

Procédure

1. Cliquez sur l'icône dans l'une des options suivantes.

   - **Galaxies (locales)**
   - **Galaxies (globales)**

2. Dans la boîte de dialogue Galaxies d'événements MISP, tapez et recherchez pour ajouter les balises.
3. Cliquez sur **Mettre à jour les galaxies vers l'événement MISP**.

   L'exemple suivant montre comment cliquer sur l'icône d'édition pour les galaxies locales, sélectionner l'espace de noms déconseillé, sélectionner la galaxie Enterprise Attack - Attack Pattern et ajouter des informations sur l'amas. Une fois les informations de la galaxie mises à jour, vous pouvez afficher le message de réussite.

   Mettre à jour les informations de la galaxie sur l'événement MISP



   Les galaxies sont mises à jour avec succès dans le MISP serveur.

4. Cliquez sur **Recharger le formulaire** dans le message de réussite pour afficher les changements dans l'enregistrement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déployer des informations à MITRE-ATT&CK l'aide MISP des résultats d'enrichissement

Cumulez manuellement les résultats de l'enrichissement MISP si vous n'avez pas activé le déploiement automatique des MISP informations.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

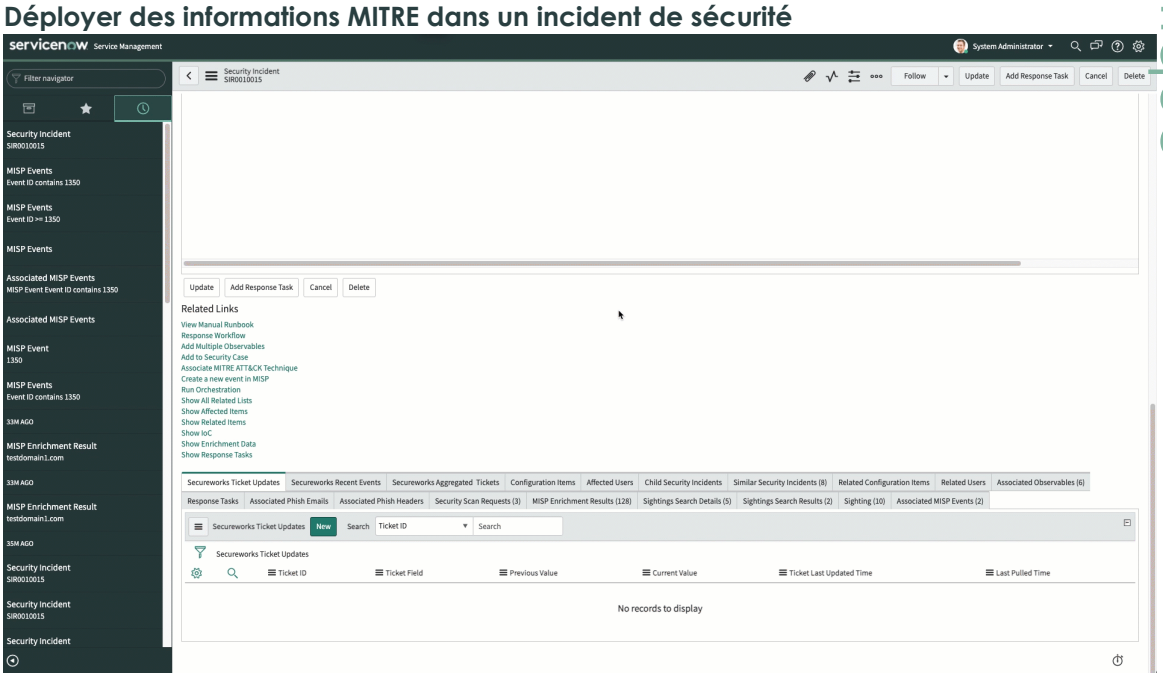
Utilisez les règles d'extraction automatique du système de base pour importer les MITRE-ATT&CK informations à partir de l'intégration MISP . L'introduction Intégration de MISP pour Opérations de sécurité de deux règles d'extraction technique du système MITRE-ATT&CK de base pour MISP les MISP galaxies et MISP les balises. Pour plus d'informations sur les règles d'extraction automatique dans MITRE-ATT&CK, consultez Règles de la technique d'extraction automatique pour l'importation d'informations MITRE-ATT&CK.

Si vous avez activé Déploiement automatique de MITRE-ATT&CK l'information à l'aide de MISP Résultats de l'enrichissement à un incident de sécurité, les informations sont automatiquement déployées. Si vous n'avez pas activé la reprise automatique, vous pouvez effectuer cette tâche manuellement.

Procédure

1. Accédez à la **Tout** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez enrichir avec les MITRE-ATT&CK informations.
3. Cliquez sur **Afficher toutes les listes connexes** et sur **l'onglet Résultats de l'enrichissement MISP** .
4. Sélectionnez l'observable et, dans le menu Actions, cliquez sur **Déployer les informations MITRE ATT&CK sur SI.**
   Vous pouvez sélectionner plusieurs observables, puis déployer les informations.
5. Pour confirmer les modifications, cliquez sur **Recharger**.
   L'exemple suivant montre comment sélectionner un observable et déployer les résultats de l'enrichissement MISP dans l'incident de sécurité.

Déployer des informations MITRE dans un incident de sécurité



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Vous pouvez afficher la MITRE-ATT&CK carte pour confirmer que les résultats de l'enrichissement MISP ont été déployés jusqu'à l'incident de sécurité.

Intégration d'OPSWAT Metadefender

OPSWAT Metadefender permet de télécharger les données sur les menaces, détectées par le scanner tiers Metadefender, dans l'application pour le suivi, la hiérarchisation et la Renseignements sur les menaces résolution.

Explorer • Vue d'ensemble de l'intégration OPSWAT Metadefender • Intégrations de Renseignements sur les menaces	Configuration Activer et configurer l'intégration OPSWAT Metadefender
Utiliser Effectuer des recherches sur les observables	Développer • ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide • Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service et assistance client	

Vue d'ensemble de l'intégration OPSWAT Metadefender

OPSWAT Metadefender est une solution de sécurité qui permet d'accéder à plusieurs machines anti-malware et s'intègre facilement à Opérations de sécurité.

Avant de pouvoir utiliser l'intégration OPSWAT Metadefender , vous devez activer le module d'extension et configurer l'intégration. Si nécessaire, vous pouvez également mettre à jour votre certification X509 SSL.

Recherche de menace : flux Metadefender OPSWAT

Le flux Recherche de menace - OPSWAT Metadefender effectue une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par OPSWAT Metadefender, les observables sont analysés à la recherche de logiciels malveillants et les résultats sont renvoyés.

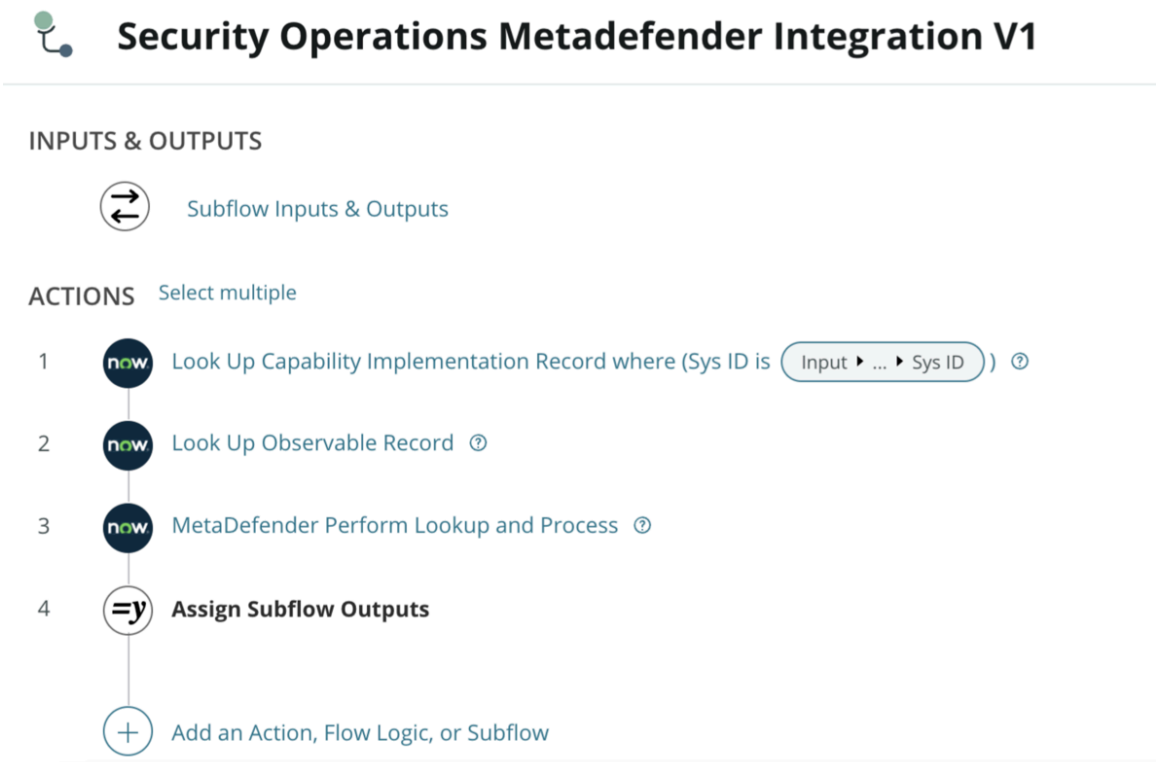
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce flux est déclenché lorsque Security Operations Integration - Aptitude Recherche de menace vous effectuez une recherche de menace sur un ou plusieurs observables et que l'implémentation OPSWAT Metadefender est sélectionnée. Pour plus d'informations, consultez Effectuer des recherches sur les observables.

Rôle requis : sn_si.admin

Recherche de menace : flux Metadefender OPSWAT



Pour en savoir plus sur les activités utilisées par ce flux, reportez-vous à Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Activer et configurer l'intégration OPSWAT Metadefender

Avant de pouvoir utiliser l'intégration OPSWAT Metadefender , vous devez la télécharger à ServiceNow Storepartir du fichier .

Avant de commencer

Rôle requis : administrateur

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Lorsque l'intégration est terminée, accédez au portail OPSWAT et obtenez la clé API Metadefender Cloud
3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la carte OPSWAT Metadefender, cliquez sur **Configurer**.
5. Entrez (ou collez) la **clé API** que vous avez acquise à partir du portail OPSWAT.
6. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Une fois configuré, OPSWAT Metadefender peut être sélectionné pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Mettre à jour votre certificat X.509

Si vous avez besoin d'une connexion SSL pour l'intégration, il peut arriver que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou qu'il ait expiré. Cette tâche est facultative.

Avant de commencer
Rôle requis : admin

Procédure

1. Procurez-vous le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.

   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
   Par exemple : `https://<3rdparty>/`.

   b. Cliquez sur l'icône de cadenas dans la ligne d'adresse.

   c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .

   d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .

   e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.

   f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
   Il doit commencer par `-----BEGIN CERTIFICATE` ----- et se terminer par `-----END CERTIFICATE`-----.

2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Ajoutez le certificat à l'enregistrement du fournisseur d'identité.
   a. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
   b. Sélectionnez le fournisseur d'identité par défaut actif pour lequel vous avez créé le nouveau certificat.
   c. Faites défiler vers le bas jusqu'à la liste connexe **des certificats X.509** , puis cliquez sur **Modifier**.
   d. Déplacez le certificat nouvellement créé vers la colonne **Sélectionné** .
6. Cliquez sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les autres champs de l'enregistrement sont générés automatiquement.

Remarque : Si vous avez un certificat qui a expiré, vous devez le supprimer. Pour plus d'informations sur la suppression du certificat expiré, reportez-vous à KB0691439 Remplacement d'un certificat SAML arrivant à expiration .

Intégration de VirusTotal

L'intégration VirusTotal vous permet de demander l'analyse des adresses IP, des fichiers, des hachages de fichiers et des adresses URL suspects afin d'aider à déterminer s'ils sont malveillants.

Explorer Intégrations de Renseignements sur les menaces	Configurer • Configuration de l'intégration VirusTotal • Activer et configurer l'intégration de VirusTotal
Utiliser • Effectuer des recherches sur les observables • Workflow Recherche de menace - VirusTotal	Développer • ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide • Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service et assistance client	

Configuration de l'intégration VirusTotal

VirusTotal est un service gratuit qui analyse les fichiers et les URL suspects et facilite la détection rapide des virus, des vers, des chevaux de Troie et de toutes sortes de logiciels malveillants. Il s'intègre facilement à Opérations de sécurité.

Avant de pouvoir utiliser l'intégration VirusTotal , vous devez activer le module d'extension et ajouter la clé API appropriée. Si nécessaire, vous pouvez également mettre à jour votre certification X509 SSL.

Si la source de VirusTotal recherche est utilisée et qu'un programme malveillant est rencontré, un observable est créé. Pour les recherches d'adresses IP, une liste

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

supplémentaire des URL qui partagent l'adresse IP est créée, et des observables sont créés pour chacune des URL.

Remarque :

- Le Renseignements sur les menaces module d'extension est requis pour implémenter VirusTotal l'intégration.
- L'intégration VirusTotal a été mise à niveau vers la version 3 des API.

Activer et configurer l'intégration de VirusTotal

Avant de pouvoir utiliser l'intégration de VirusTotal, vous devez la télécharger à partir du ServiceNow Storefichier .

Avant de commencer

Rôle requis : administrateur
Renseignements sur les menaces doit être installé et activé avant de pouvoir utiliser VirusTotal. L'intégration VirusTotal a été mise à niveau vers la version 3 des API.

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à VirusTotal et obtenez la clé API sous votre profil VirusTotal.
3. Dans votre instance, accédez à **Security Operations** > **Configuration de l'intégration**. Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la carte VirusTotal, cliquez sur **Configurer**.

VirusTotal Configuration

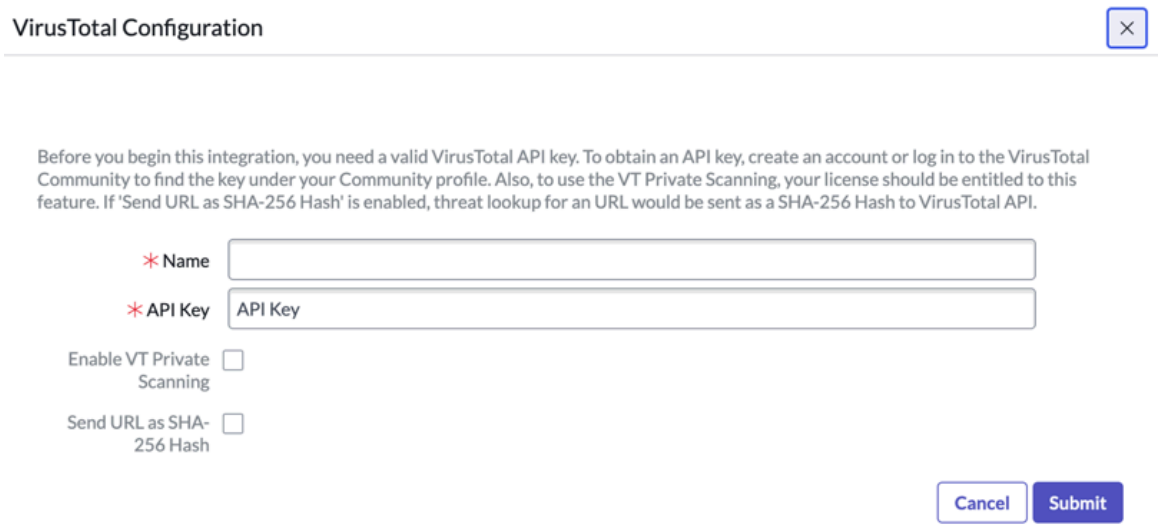
Champ	Description
Nom	Nom de l'intégration. Par exemple, VirusTotal.
Clé API	Entrez (ou collez) la **clé API** que vous avez acquise sur le site VirusTotal.
Activer l'analyse privée VT	Cochez cette case pour analyser les fichiers avec VirusTotal de manière à préserver la confidentialité. Les fichiers chargés via cette offre ne seront partagés avec personne en dehors de votre organisation et ne resteront dans VirusTotal que pendant une brève période. Les analyses qui en résulteront seront également éphémères et ne seront visibles que par votre groupe VirusTotal. **Important :** Pour utiliser VT Private Scanning, votre licence VirusTotal doit être autorisée à bénéficier de cette fonctionnalité.
Envoyer l'URL comme hachage SHA-256	Cochez cette case pour envoyer les URL comme hachages pour la recherche de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	menaces et protéger la confidentialité des utilisateurs sur l'intégration. **Remarque :** Si cette option est désactivée, l'URL est envoyée sous forme de codage Base64 à l'API VirusTotal.

5. Cliquez sur **Envoyer**.



Résultats
Une fois configuré, VirusTotal peut être sélectionné pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Workflow Recherche de menace - VirusTotal

Le workflow Recherche VirusTotal de menace effectue une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par , les observables sont analysés à VirusTotalla recherche de programmes malveillants et les résultats sont renvoyés.

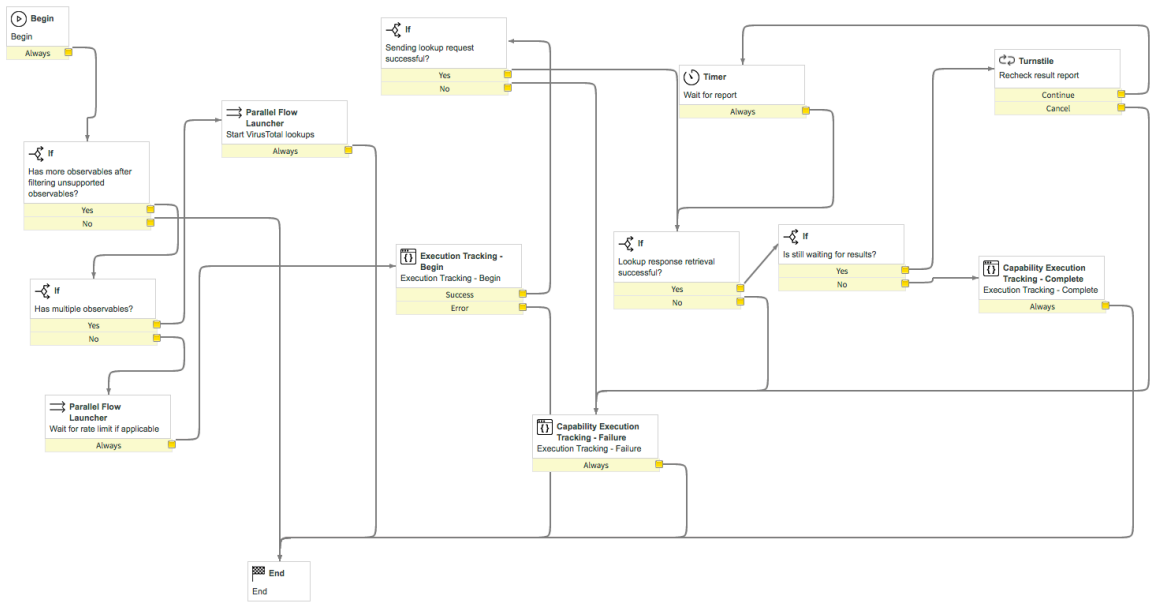
Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Ce workflow est déclenché lorsque Security Operations Integration - Aptitude Recherche de menace vous effectuez une recherche de menace sur un ou plusieurs observables et que l'implémentation VirusTotal est sélectionnée. Pour plus d'informations, consultez Effectuer des recherches sur les observables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow Recherche de menace - VirusTotal



Pour en savoir plus sur les activités utilisées par ce workflow, reportez-vous à la section Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Intégration de l'API WhoisXML

L'intégration de l'API WhoisXML vous permet de soumettre des recherches Whois sur les noms de domaine et les URL afin d'obtenir un contexte sur les observables d'URL et de mieux déterminer les menaces.

Explorer Intégrations de Renseignements sur les menaces	Configurer • Configuration de l'intégration de l'API WhoisXML • Activer et configurer l'intégration Whois de Security Operations
Utiliser Renseignements sur les menaces - Exécuter le workflow de recherche IoC	Développer • ServiceNow Opérations de sécurité Directives de développement de l'intégration • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide • Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté des opérations de sécurité	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

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

Configuration de l'intégration de l'API WhoisXML

Avant de pouvoir utiliser l'intégration Whois, vous devez activer le module d'extension et ajouter les informations d'identification. Si nécessaire, vous pouvez également mettre à jour votre certification X509 SSL.

Les modules d'extension d'intégration de l'API Renseignements sur les menaces WhoisXML sont requis pour implémenter l'intégration de l'API WhoisXML.

Activer et configurer l'intégration Whois de Security Operations

La fonctionnalité de configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration Security Operations Whois. Avant de pouvoir utiliser l'intégration Security Operations Whois, vous devez la télécharger à partir du , et vous devez disposer d'un compte valide à partir de l'API ServiceNow StoreWhoisXML.

Avant de commencer

Renseignements sur les menaces doit être installé et activé avant de pouvoir utiliser l'intégration Whois de Security Operations.

Rôle requis : administrateur

Procédure

1. Téléchargez l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Dans la fiche de l'API Whois, cliquez sur **Configurer**.
4. Entrez le nom d'utilisateur et le mot de passe de votre compte WhoisXML API.
5. Cliquez sur **Envoyer**.

Mettre à jour votre certificat X.509

Si vous avez besoin d'une connexion SSL pour l'intégration, il peut arriver que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou qu'il ait expiré. Cette tâche est facultative.

Avant de commencer

Rôle requis : admin

Procédure

1. Procurez-vous le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.

   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
   Par exemple : `https://<3rdparty>/`.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

b. Cliquez sur l'icône de cadenas dans la ligne d'adresse.

c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .

d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .

e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.

f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
Il doit commencer par `-----BEGIN CERTIFICATE` ----- et se terminer par `-----END CERTIFICATE`-----.

2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Ajoutez le certificat à l'enregistrement du fournisseur d'identité.
   a. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
   b. Sélectionnez le fournisseur d'identité par défaut actif pour lequel vous avez créé le nouveau certificat.
   c. Faites défiler vers le bas jusqu'à la liste connexe **des certificats X.509** , puis cliquez sur **Modifier**.
   d. Déplacez le certificat nouvellement créé vers la colonne **Sélectionné** .
6. Cliquez sur **Enregistrer**.
   Les autres champs de l'enregistrement sont générés automatiquement.

> **Remarque :** Si vous avez un certificat qui a expiré, vous devez le supprimer. Pour plus d'informations sur la suppression du certificat expiré, reportez-vous à KB0691439 Remplacement d'un certificat SAML arrivant à expiration .

Enrichir le workflow WhoIs des observables

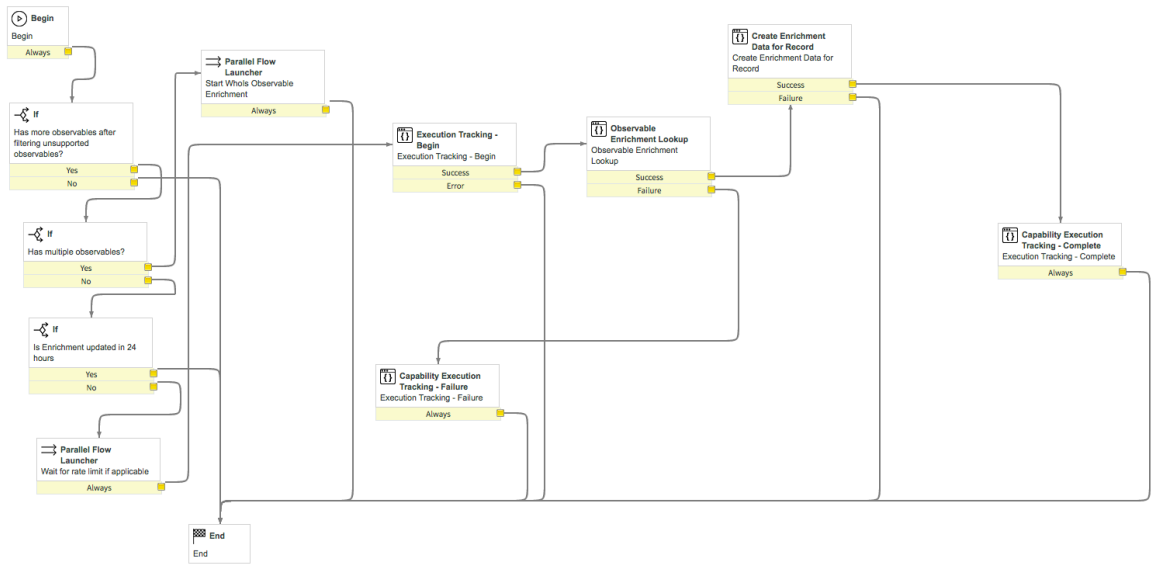
Le workflow **Enrichir les observables WhoIs** effectue un enrichissement sur les observables sélectionnés. Si les observables sont d'un type reconnu par le WhoisXML API Integration, les observables sont enrichis.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Ce workflow est déclenché lorsque Intégration de Security Operations : aptitude d'enrichissement des observables vous procédez à l'enrichissement d'un ou de plusieurs observables et que l'implémentation WhoIs est sélectionnée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enrichir le workflow WhoIs des observables



Les activités spécifiques à cette intégration sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Activité de recherche d'enrichissement d'observable

L'activité de workflow **Recherche d'enrichissement des observables** lance le processus d'enrichissement des observables.

L'activité de recherche d'enrichissement des observables peut être utilisée avec n'importe quel workflow d'observables pour commencer l'enrichissement.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	La recherche est réussie.
Échec	Une erreur s'est produite lors de la tentative de recherche. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
implementation_id	Identificateur système de l'implémentation utilisée pour effectuer la recherche.
domain_id	L'identificateur du domaine dans lequel la recherche est effectuée.
observable_ids	Un ou plusieurs observables sur lesquels effectuer l'action souhaitée. Les ID sont utilisés comme entrée de workflow.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
ID capacité d'exécution	Identificateur système de l'aptitude qui a lancé le workflow d'implémentation. Requis uniquement pour les workflows d'implémentation d'aptitude d'intégration tels que Splunk, Elasticsearch.
task_sys_id	Identificateur système pour toute tâche associée au workflow.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
response_data	Données brutes renvoyées par le point de terminaison d'API de l'implémentation pour le domaine donné.
mapping_id	L'identificateur pour le mappage d'enrichissement. Par exemple, l'intégration WhoIs renvoie des données dans deux formats différents, IP et URL, avec un ID de mappage pour chacun.

Threat Intelligence Orchestration

Orchestration des renseignements sur les menaces Les activités permettent aux utilisateurs de déterminer si une menace a déjà été vue dans d'autres incidents de sécurité ou sur d'autres systèmes à l'aide d'Orchestration de workflow.

Pour plus d'informations sur la modification Orchestration de la réponse aux incidents de sécurité des workflows ou la création de workflows personnalisés, voir Prise en main des workflows et Éditeur de workflow de workflow Éditeur de workflow .

Configurer Orchestration Threat Intelligence

Avant d'utiliser Orchestration des renseignements sur les menaces, effectuez des étapes de configuration de différentes parties du système, notamment le remplissage de la CMDB, la configuration du serveur MID et la configuration des informations d'identification.

Avant de commencer

Rôle requis : administrateur
Pour l'utiliser, Orchestration des renseignements sur les menaces vous avez besoin d'une CMDB entièrement remplie avec des noms de domaine. Pour plus d'informations, consultez Découverte .

Pourquoi et quand exécuter cette tâche

Procédure

1. Activez le module d'extension Renseignements sur les menaces .
2. Configurer Serveur MID
3. Configurer les informations d'identification du service Serveur MID
   Vous êtes maintenant prêt à utiliser les Orchestration des renseignements sur les menaces activités d'un workflow.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflows et activités Orchestration de Threat Intelligence

Le système de base inclut des workflows et des activités de workflow que vous pouvez utiliser pour automatiser les actions sur votre instance.

Renseignements sur les menaces - Exécuter le workflow de recherche IoC

Le workflow **Threat Intelligence : Exécuter une recherche IoC** vérifie s'il existe un observable non expiré et, dans ce cas, la recherche est définie sur **Terminée** et mise à jour avec les données de l'observable.

Avant de commencer

Rôle requis : sn_si.basic

Remarque : Ce workflow remplace Orchestration des renseignements sur les menaces les règles métier (**Remplir avec les tables IoC existantes**, **Mettre en file d'attente la recherche** et **Mettre à jour l'observable**) par des activités.

Si une recherche est insérée ou mise à jour et qu'elle répond aux conditions, la règle métier Rechercher déclenche ce workflow.

Pourquoi et quand exécuter cette tâche

Le workflow **Threat Intelligence : Exécuter une recherche IoC** vérifie s'il existe un observable non expiré et, dans ce cas, la recherche est définie sur **Terminée** et mise à jour avec les données de l'observable. Tous les indicateurs associés à l'observable sont réactivés.

Si l'observable a expiré, le workflow exécute les recherches et incrémente le **nombre de perceptions** dans l'observable existant et expiré.

S'il n'existe aucun observable corrélant, un nouvel observable avec indicateur est créé.

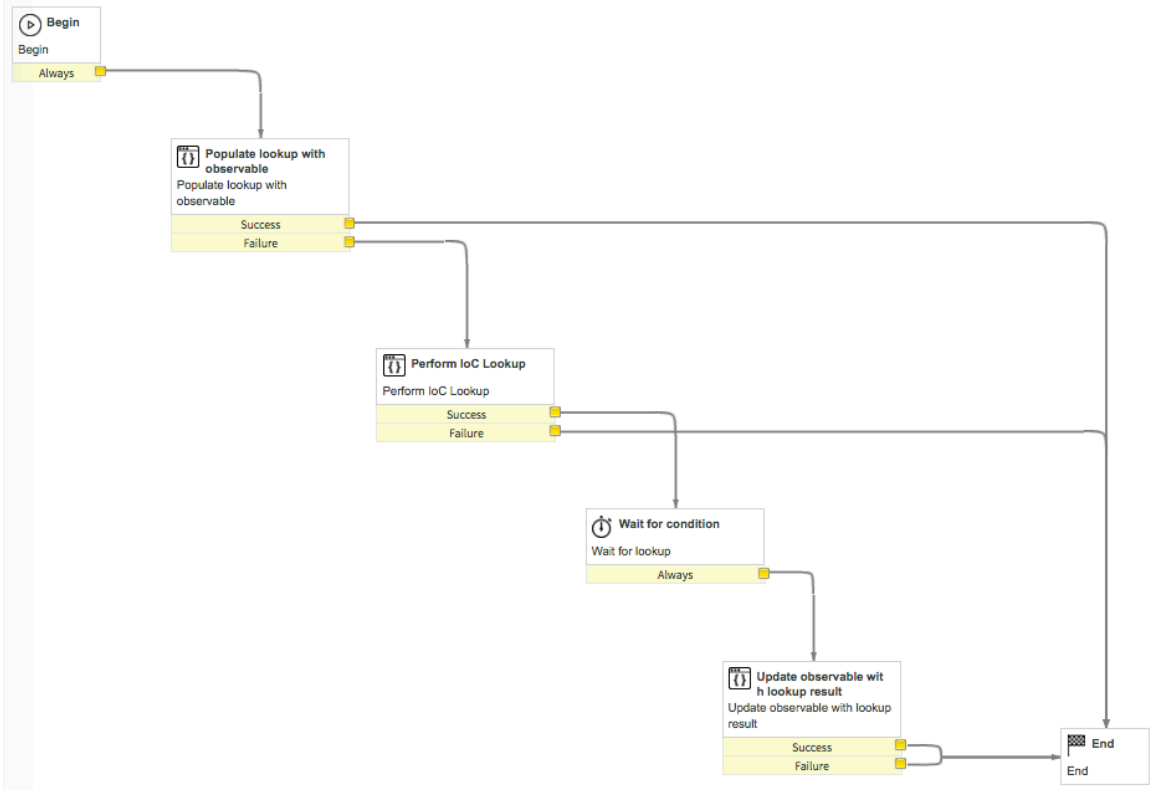
Les activités de processus du workflow comprennent :

- Remplir la recherche avec une activité observable
- Effectuer une activité de recherche d'IoC
- Attendre la recherche (activité principale)
- Mettre à jour l'observable avec l'activité de résultat de la recherche

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Threat Intelligence : exécuter le workflow de recherche IoC



Remplir la recherche avec une activité observable

Si un observable non expiré est trouvé, **l'activité de workflow Orchestration Threat Intelligence : remplir la recherche avec un observable fournit les données d'un** observable existant à une recherche. Cette activité peut accélérer le processus d'investigation et de correction.

Lorsqu'elles sont déclenchées par un workflow **Remplir la recherche avec des observables,** tente de trouver un observable existant pour une recherche qui correspond à la **valeur** et au **type** de la recherche fournie à l'activité en tant qu'entrée.

Si l'observable existe et n'est pas expiré, cette activité :

- Met à jour la recherche avec les informations trouvées dans l'observable
- Réactive un indicateur s'il est inactif, incrémente le **nombre de cas rencontrés** et met à jour la date du **dernier observé**
- Définit **l'état** sur Terminé.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable d'entrée	Description
scanID[chaîne]	Rechercher un identificateur

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie	Description
Vrai	Recherche trouvée valide et mise à jour.
Faux	Observable valide introuvable. L'observable est soit manquant, soit expiré.

Effectuer une activité de recherche d'IoC

L'activité de workflow **Orchestration - Effectuer une recherche IoC Orchestration Threat Intelligence** effectue une recherche donnée. Cette activité peut accélérer le processus d'investigation et de correction.

Lorsqu'elle est déclenchée par un workflow, **l'option Effectuer une recherche IoC** prend un scanID, recherche l'enregistrement de recherche et ajoute la recherche à la file d'attente en créant une entrée de file d'attente de recherche.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
scanID[chaîne]	Rechercher un identificateur

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
Vrai	A déclenché la recherche.
Faux	N'a pas déclenché la recherche.

Mettre à jour l'observable avec l'activité de résultat de la recherche

L'activité de workflow **Orchestration de Threat Intelligence : mettre à jour un observable avec le résultat de la recherche** met à jour l'enregistrement de l'observable. S'il n'en existe pas, il crée un nouvel observable. Cette activité est utile pour journaliser les informations.

Lorsqu'il est déclenché par un workflow **Mettre à jour un observable avec résultat de recherche** met à jour un observable existant pour inclure le nouveau **nombre de perceptions**, ajoute une note et, s'il est inactif, réactive tous les indicateurs. Le **nombre de rencontres** et la date du **dernier observé** dans l'indicateur sont également mis à jour.

S'il n'existe aucun observable corrélatif, le workflow crée un nouvel observable avec l'indicateur comme suit :

- Exécute les recherches IoC
- Crée un nouvel observable

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Crée un indicateur pour l'observable
- Ajoute un **nombre de perceptions** à l'observable
- Ajoute un **nombre de rencontres** et la date du **dernier observé** à l'indicateur
- Ajoute un message indiquant à partir de quelle recherche il a été créé

.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
scanID[chaîne]	Rechercher un identificateur.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
Vrai	La mise à jour ou la création de l'observable est réussie.
Faux	Échec de la mise à jour ou de la création de l'observable.

Exécuter l'activité Sources de recherche IoC par défaut

Lorsqu'elles sont déclenchées par un workflow, Renseignements sur les menaces**Exécuter les sources de recherche IoC par défaut** enregistrent un ID de demande de recherche et créent plusieurs recherches en fonction des valeurs de données saisies.

Pour chaque type de données, la colonne **d'analyse include_in_bulk** de la table des types de recherche pris en charge de chaque source de recherche est évaluée. Si vrai, une recherche est ajoutée à la demande de recherche.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
scan_request_id	Rechercher l'identificateur système de la demande

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
Nombre d'analyses créées	Entier

Security Case Management

Gestion des tickets de sécurité permet aux analystes de sécurité qui se livrent à la chasse aux menaces de recueillir des informations sur les activités suspectes dans leur environnement. Les enregistrements relatifs aux tickets, tels que les incidents de sécurité, les observables, les CI et les utilisateurs affectés peuvent être ajoutés aux tickets pour permettre une analyse large et spécifique.

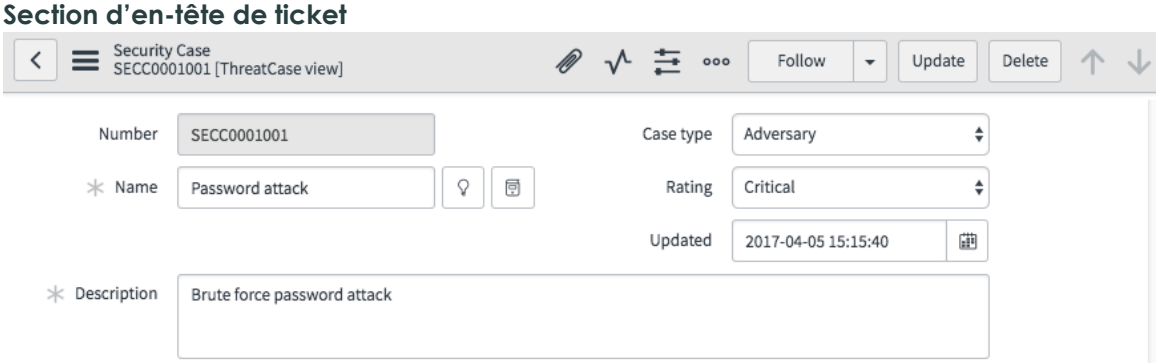
Grâce à la possibilité de parcourir facilement les enregistrements et les informations connexes, les analystes peuvent évaluer s'ils sont confrontés à une campagne ciblée, à une menace persistante avancée, etc.

Les tickets de sécurité peuvent être créés à partir de différentes sources sur votre instance, notamment Gestion des tickets de sécurité, Réponse aux incidents de sécurité, et Renseignements sur les menaces. Vous pouvez également créer des tickets à partir d'éléments de configuration et d'utilisateurs affectés dans les tables Éléments de configuration [cmdb.ci] et Utilisateurs [sys.user], respectivement. Une fois les tickets créés, chacune de ces sources peut également être utilisée pour ajouter de précieuses ressources d'analyse aux tickets existants.

Chaque ticket de sécurité se compose de trois sections principales, d'une section d'en-tête, d'une section avec des détails supplémentaires sur le ticket et d'une section d'artefacts de ticket contenant une collection d'enregistrements qui aident à construire un argument pour identifier et traiter des menaces particulières.

En-tête du ticket

Section d'en-tête de ticket



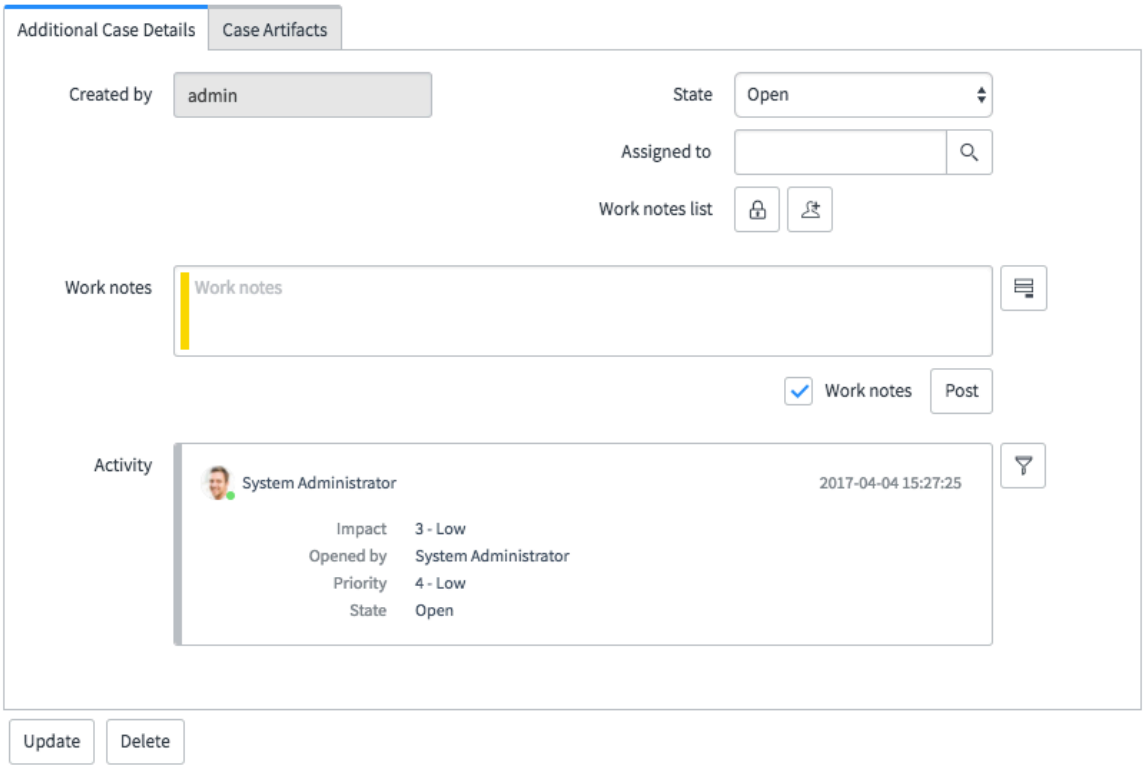
L'en-tête du ticket fournit des informations de base permettant d'identifier et de classer le ticket de sécurité. Le numéro de ticket utilise le préfixe SECC.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations supplémentaires sur le ticket

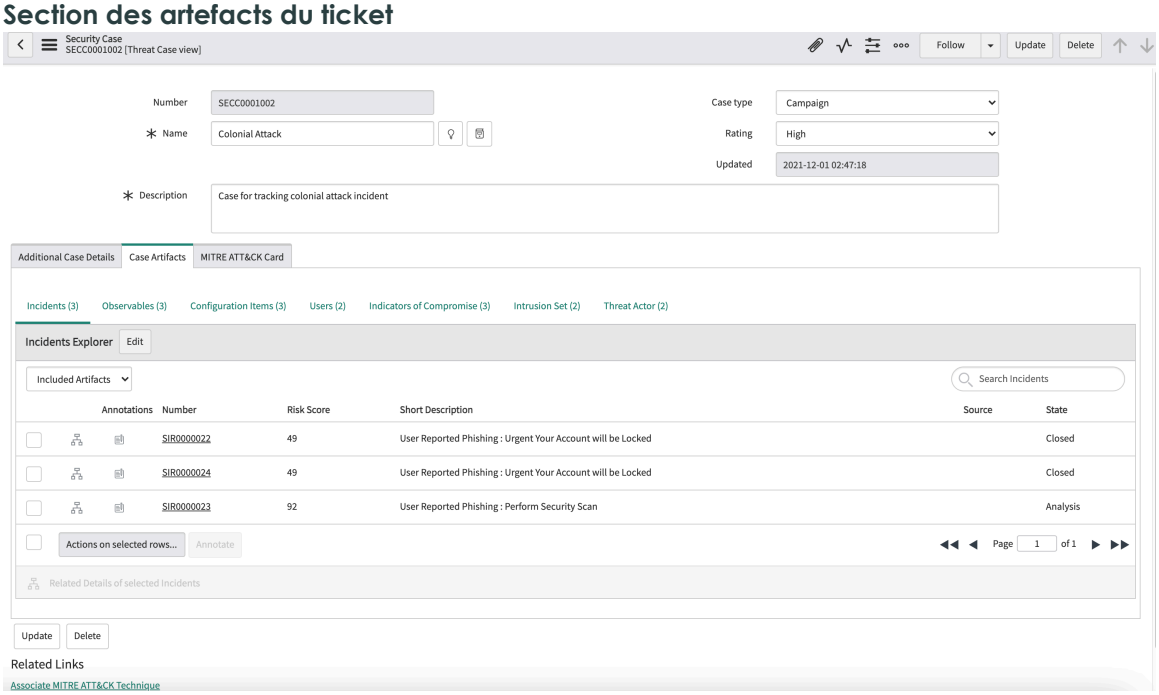
Section Détails supplémentaires du ticket



La section **Détails supplémentaires du ticket** fournit des informations spécifiques à l'analyse qui a déjà été effectuée sur le ticket, y compris son état actuel, ainsi que les notes de travail et les activités enregistrées pour le ticket.

Artefacts du ticket

Section des artefacts du ticket



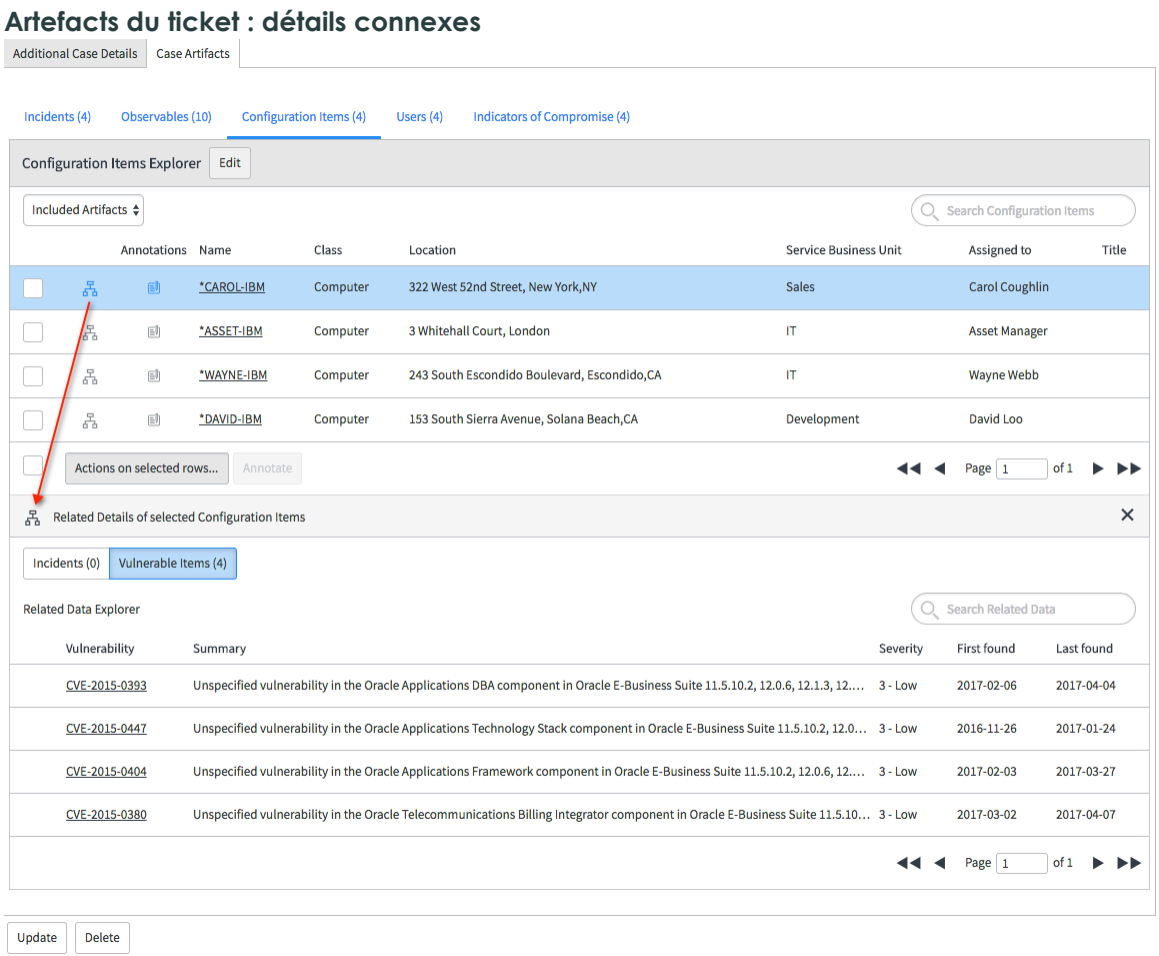
La section **Artefacts du ticket** fournit une série d'onglets d'informations contenues dans le ticket de sécurité.

Traduction automatique

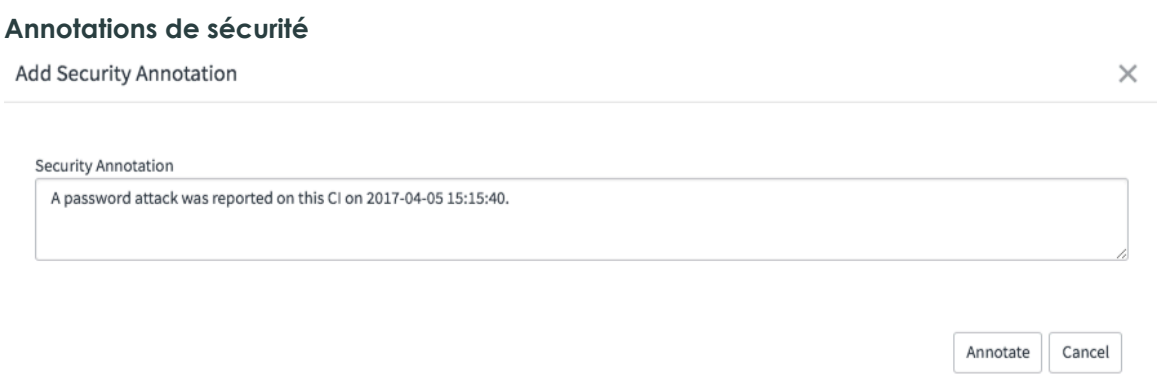
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez effectuer des recherches dans le contenu de chaque onglet. Vous pouvez également exclure des enregistrements spécifiques que vous avez déjà évalués comme étant sûrs ou qui n'ont aucune valeur dans votre enquête. Les enregistrements exclus ne sont pas supprimés, mais sont masqués. Si nécessaire, vous pouvez afficher les enregistrements exclus et les rajouter.

Dans chaque onglet, vous pouvez cliquer sur l'icône Détails supplémentaires pour afficher les informations connexes de l'enregistrement sélectionné. Par exemple, si vous cliquez sur l'onglet **Éléments de configuration** pour afficher l'Explorateur d'éléments de configuration, puis cliquez sur Détails supplémentaires pour un CI spécifique, vous pouvez afficher les incidents, les éléments vulnérables et les annotations associés à ce CI.



Vous pouvez également sélectionner un enregistrement et cliquer sur le bouton **Annoter** d'un artefact lié au ticket afin d'ajouter des annotations à l'enregistrement. Les annotations sont simplement des notes que chaque analyste peut faire sur un artefact particulier.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

D'autres outils que l'analyste peut utiliser pour examiner les cas sont les suivants :

- Exécuter une recherche de perceptions sur les observables d'un ticket
- Rechercher des artefacts de sécurité

Créer des tickets dans Gestion des tickets de sécurité

Les tickets sont utilisés pour suivre les informations relatives à une campagne ou à un acteur étatique qui menace votre organisation. Une fois le ticket créé, vous pouvez ajouter des artefacts qui vous permettent d'examiner et d'analyser toutes les informations connexes dans un seul enregistrement de ticket.

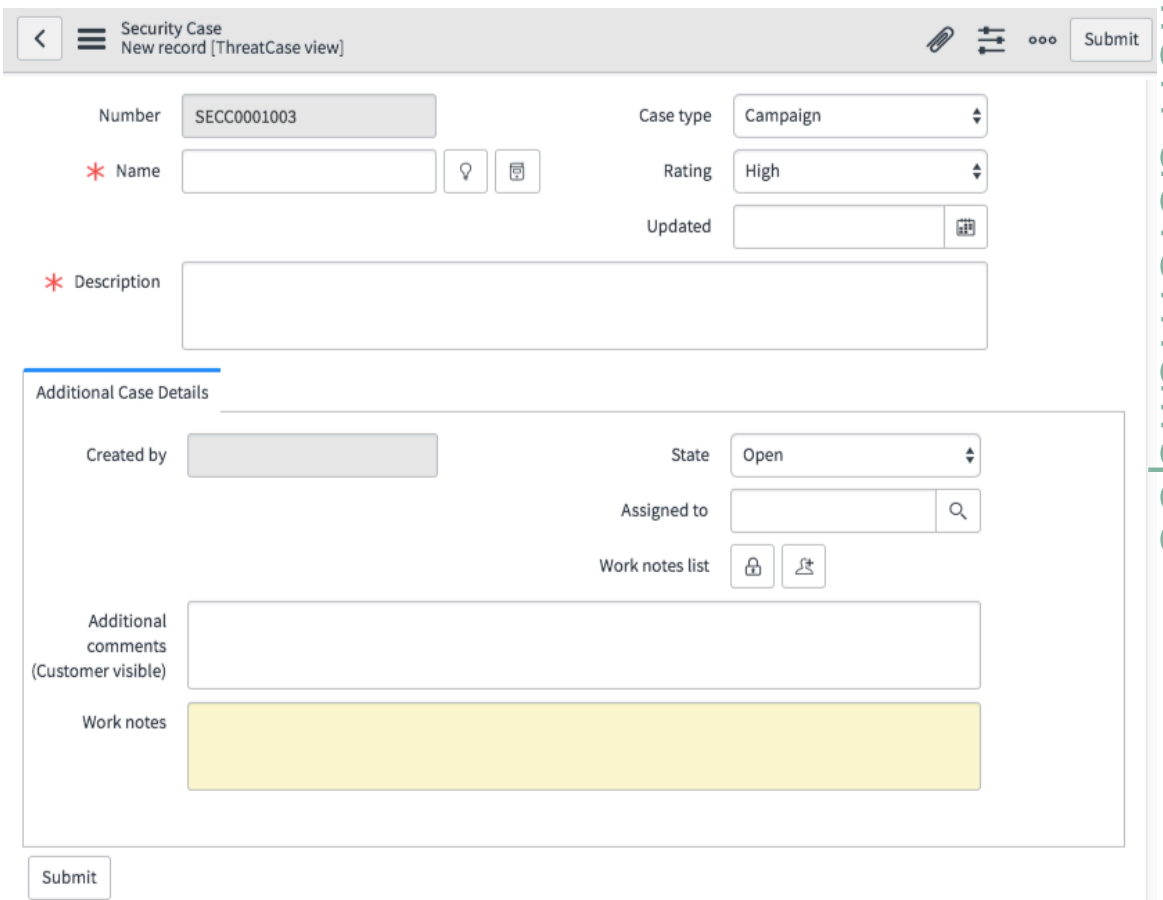
Avant de commencer

Rôle requis : sn_ti.case_use

r

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
   La liste des tickets de sécurité s'ouvre.
2. Cliquez sur **Nouveau**.
   L'écran Tickets de sécurité s'ouvre.



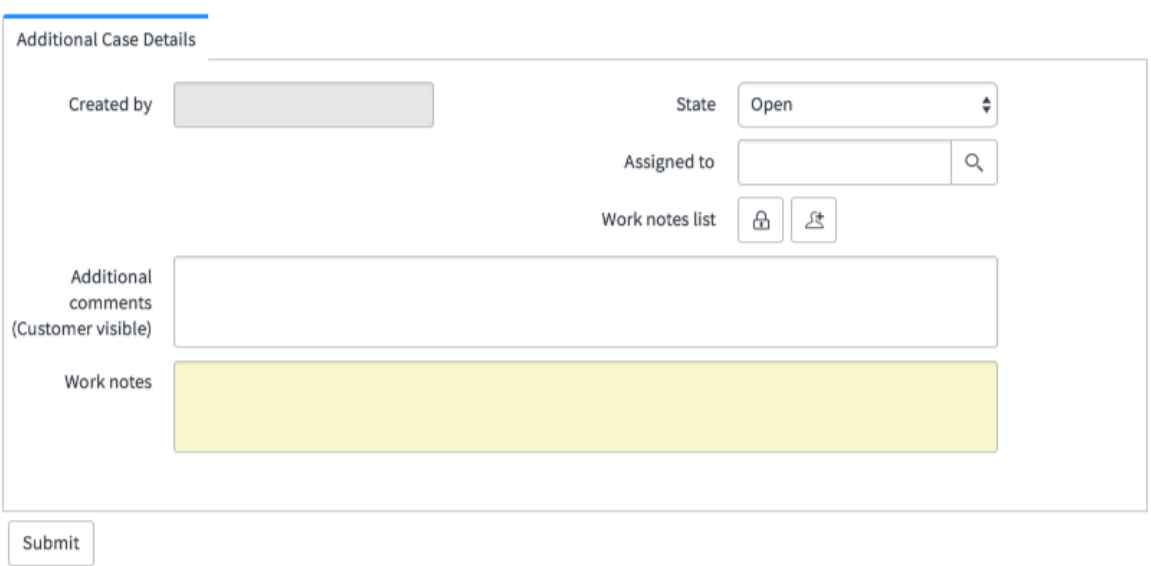
3. Renseignez les champs comme il convient.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Numéro du ticket	[Lecture seule] Le numéro de ticket.
Nom du ticket	Entrez un nom décrivant le ticket.
Type de ticket	Sélectionnez le type de ticket faisant l'objet de l'enquête.
Évaluation	Sélectionnez l'importance de ce ticket (de critique à faible).
Dernière mise à jour	[Lecture seule] Date et heure de la dernière mise à jour du ticket.
Description brève	Une brève description du ticket.

4. Cliquez sur l'onglet **Détails supplémentaires du ticket** .



5. Renseignez les champs comme il convient.

Champ	Description
Créé par	[Lecture seule] Nom de l'utilisateur qui a créé ce ticket.
État	État actuel du ticket. Lors de la création du ticket, la valeur par défaut de l'état est Brouillon.
Affecté à	Cliquez sur l'icône de recherche et affectez le ticket à un analyste.
Liste de notes de travail	Cliquez sur l'icône de verrouillage et ajoutez des utilisateurs internes qui peuvent afficher les notes de travail.
Commentaires supplémentaires	Si nécessaire, saisissez des notes sur le ticket qui seront visibles par le client.
Notes de travail	Si nécessaire, saisissez une note de travail pour le ticket.

6. Cliquez sur **Envoyer**.
Une fois l'enregistrement enregistré, vous pouvez cliquer sur l'onglet **Artefacts du ticket** et ajouter des artefacts au ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter des artefacts à un ticket

Après avoir créé un ticket, vous pouvez y ajouter des artefacts, tels que des incidents de sécurité, des CI et des indicateurs de compromission. Ces artefacts servent d'indices dans la résolution de l'affaire.

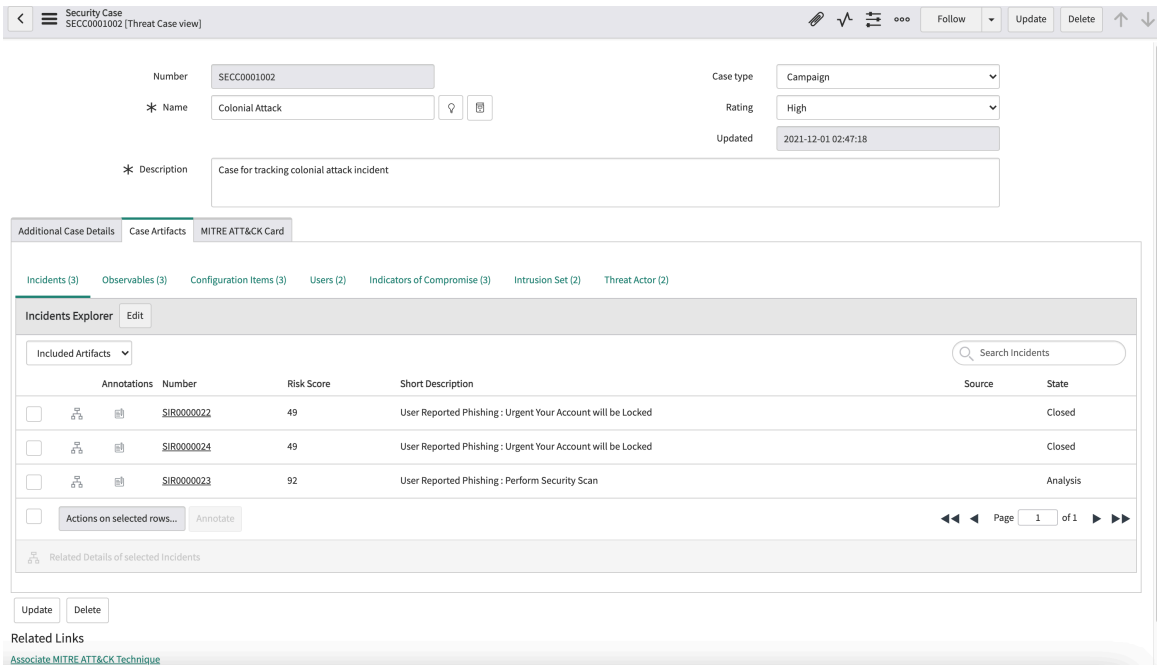
Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

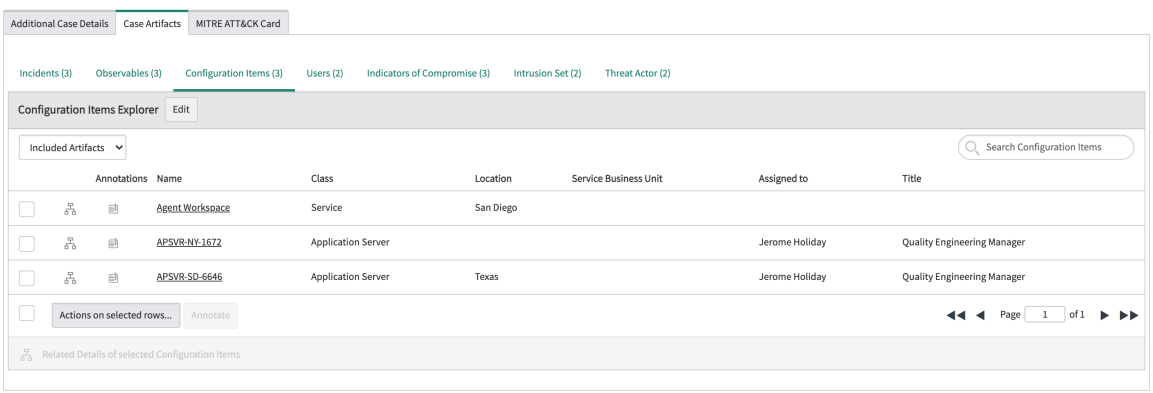
Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket auquel vous souhaitez ajouter des artefacts.
2. Cliquez sur la liste connexe **Artefacts du ticket** .



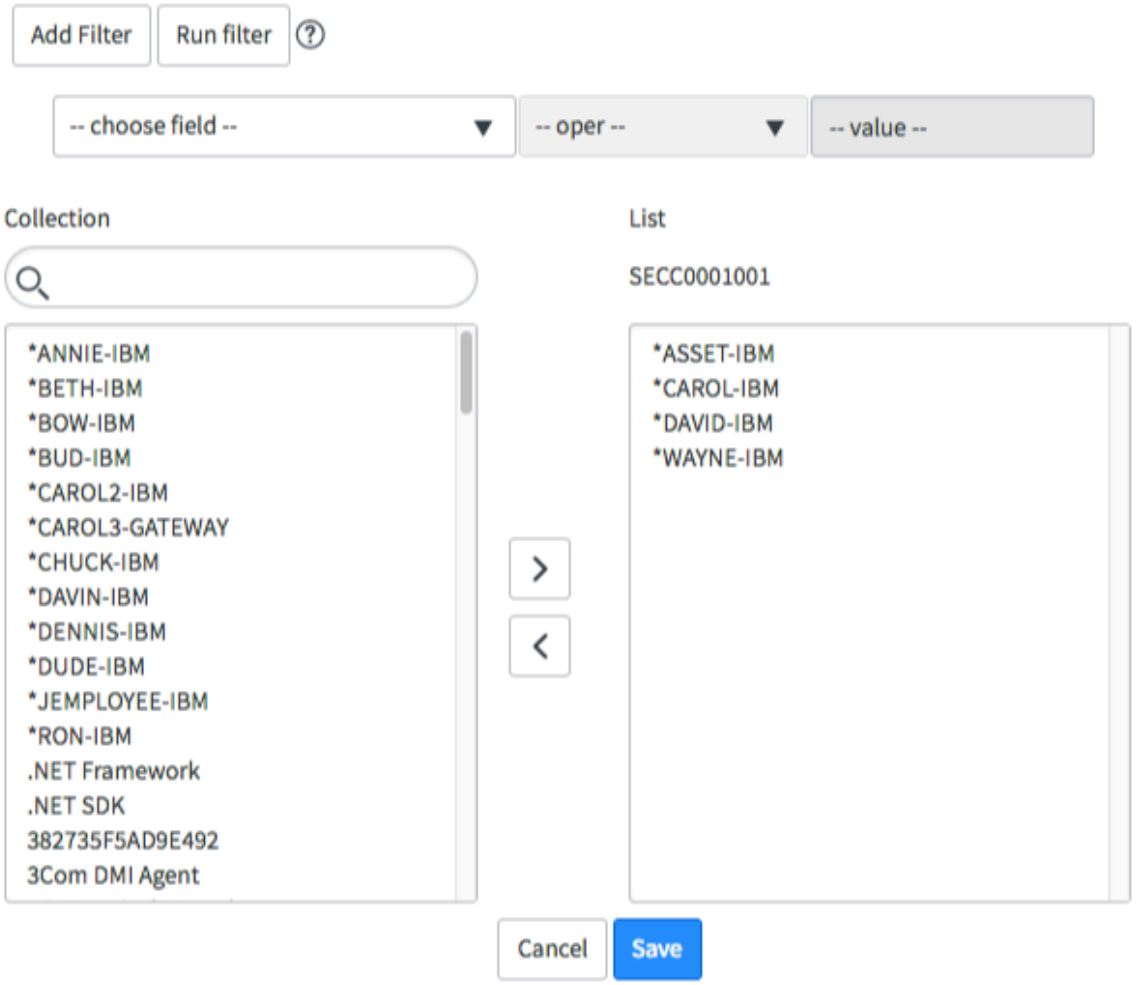
3. Cliquez sur l'onglet associé au type d'artefact que vous souhaitez ajouter au ticket. Par exemple, cliquez sur **Éléments de configuration** pour ajouter un ou plusieurs CI au ticket.



4. Cliquez sur **Modifier**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. À l'aide de la zone de sélection et des filtres, localisez les enregistrements d'artefacts que vous souhaitez ajouter au ticket et déplacez-les de la catégorie Collection vers la catégorie Liste, puis cliquez sur **Enregistrer**.
   La liste s'affiche dans l'onglet sélectionné et les artefacts sélectionnés sont ajoutés à la liste.

Information associée

- Ajouter des IoC et des observables à un ticket existant
- Ajouter des incidents de sécurité à un ticket existant
- Ajouter des CI aux tickets existants
- Ajouter des utilisateurs affectés à des tickets existants

Associer des MITRE-ATT&CK informations au ticket de sécurité

Associez MITRE-ATT&CK des tactiques et des techniques à un ticket de sécurité pour améliorer la gestion des tickets de sécurité et l'analyse des menaces à un niveau granulaire.

Avant de commencer

Rôle requis : sn_si.analyst

Traduction automatique

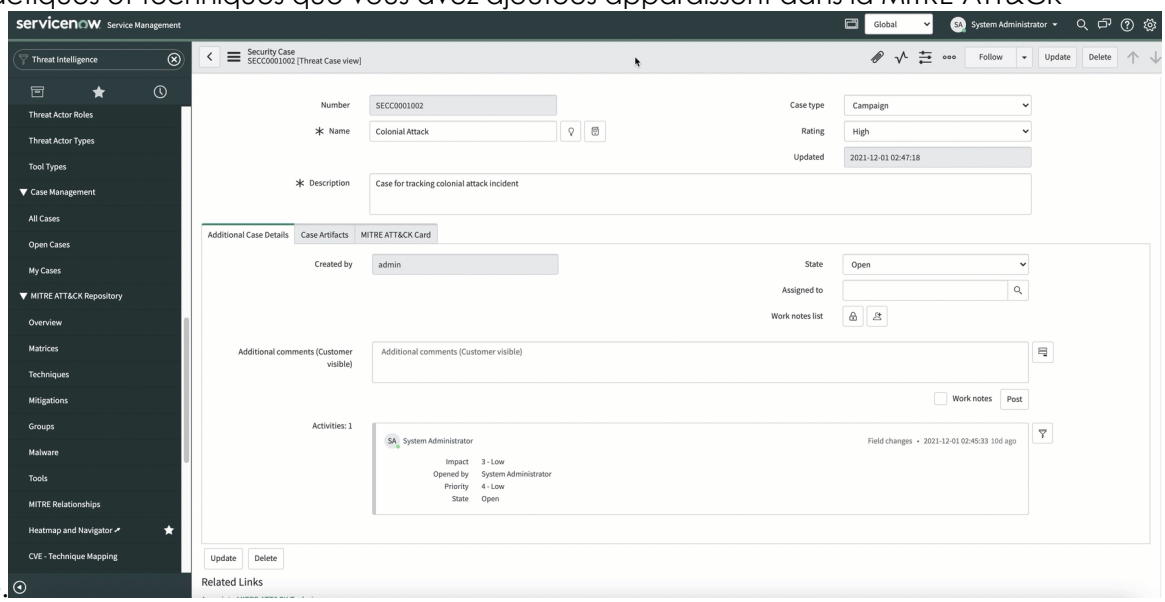
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
2. Sélectionnez le ticket de sécurité que vous souhaitez enrichir avec les informations MITRE-ATT&CK.
3. Dans la liste connexe, cliquez sur **Associer la technique MITRE ATT&CK**.

   Dans l'illustration suivante, vous pouvez voir comment naviguer à partir de la liste connexe pour **associer la technique MITRE ATT&CK**, examiner la source et ajouter une tactique et une technique.

4. Dans les listes sources, examinez la **source**.
5. Passez en revue la **tactique** et les **techniques**, et ajoutez-les ou supprimez-les en fonction de leur pertinence par rapport au cas.
6. Cliquez sur **Enregistrer**.
   Les tactiques et techniques que vous avez ajoutées apparaissent dans la MITRE-ATT&CK carte.



Création de tickets à partir d'artefacts de sécurité

En plus de créer des tickets manuellement à partir de Gestion des tickets de sécurité, vous pouvez également créer des tickets à partir d'artefacts de sécurité, tels que des incidents de sécurité, des indicateurs de compromission, des utilisateurs affectés et des éléments de configuration.

IoC et observables dans les tickets

Dans Renseignements sur les menaces, vous pouvez créer des tickets à partir d'IoC et d'observables, ainsi qu'ajouter des IoC et des observables aux tickets existants. Vous pouvez également créer des observables directement à partir d'un ticket.

Créer un ticket à partir d'IoC ou d'observables

Dans Renseignements sur les menaces, vous pouvez créer un ticket à partir d'artefacts (IoC ou observables). Une fois que les IoC ou les observables ont été utilisés pour créer un ticket, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

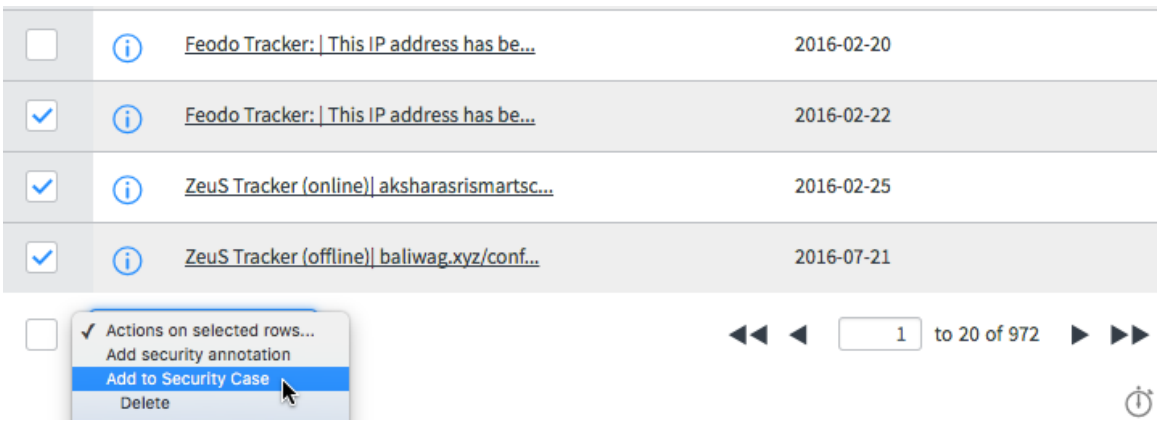
Rôle requis : sn_ti.case_user_write

Procédure

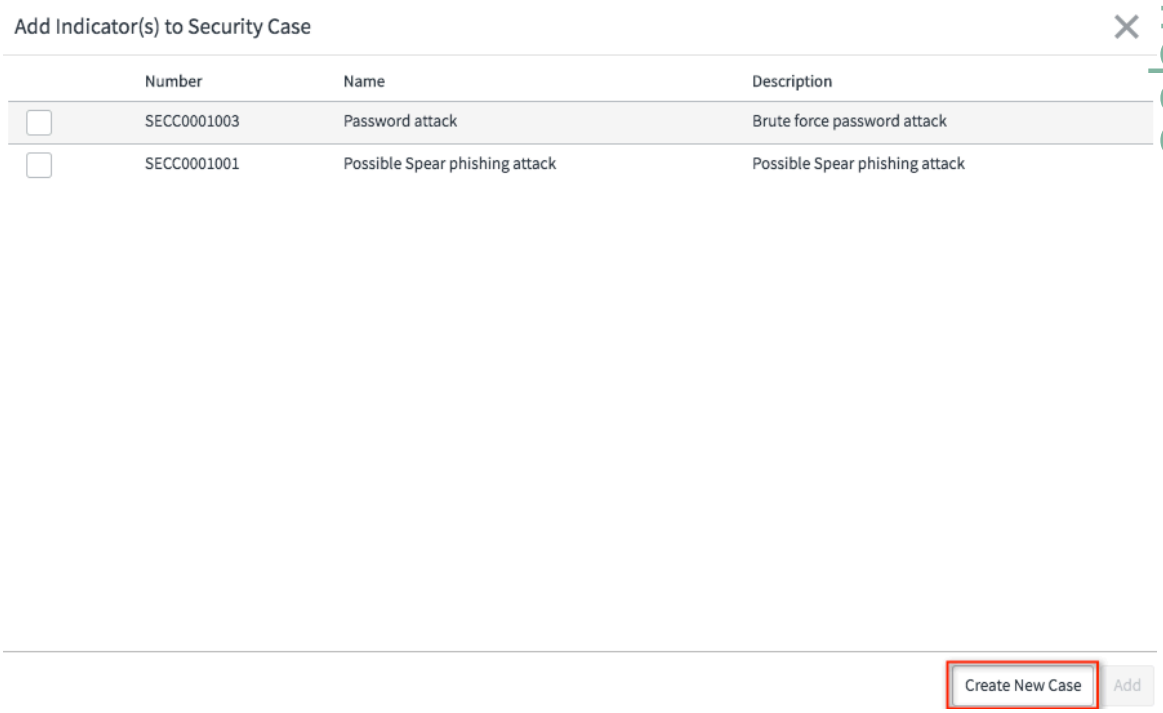
1. Accédez aux artefacts (IoC ou observables) que vous souhaitez utiliser pour créer un ticket.
   - Pour créer un ticket à partir d'IoCs, accédez à **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
   - Pour créer un ticket à partir d'observables, accédez à **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Dans la liste, sélectionnez les artefacts que vous souhaitez ajouter à un nouveau ticket.

   Remarque : Si vous sélectionnez plusieurs IoC ou observables, ils sont tous ajoutés au ticket.

3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.



La boîte **de dialogue Ajouter au ticket de sécurité s'ouvre** . Si des tickets vous sont déjà affectés, ils s'affichent dans la liste.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Créer un ticket**.
5. Renseignez les champs.

Champ	Description
Nom du ticket	Entrez un nom pour ce ticket.
Description	Entrez une description utile pour l'analyste de ticket.

6. Cliquez sur **Envoyer**.
   Un message en haut de la liste indique qu'un nouveau ticket a été créé, ainsi qu'un lien vers le ticket dans Gestion des tickets de sécurité.
7. Cliquez sur le lien pour afficher le nouveau ticket.

Ajouter des IoC et des observables à un ticket existant

Vous pouvez ajouter des IoC et des observables aux tickets existants. Une fois les incidents de sécurité ajoutés aux tickets, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Procédure

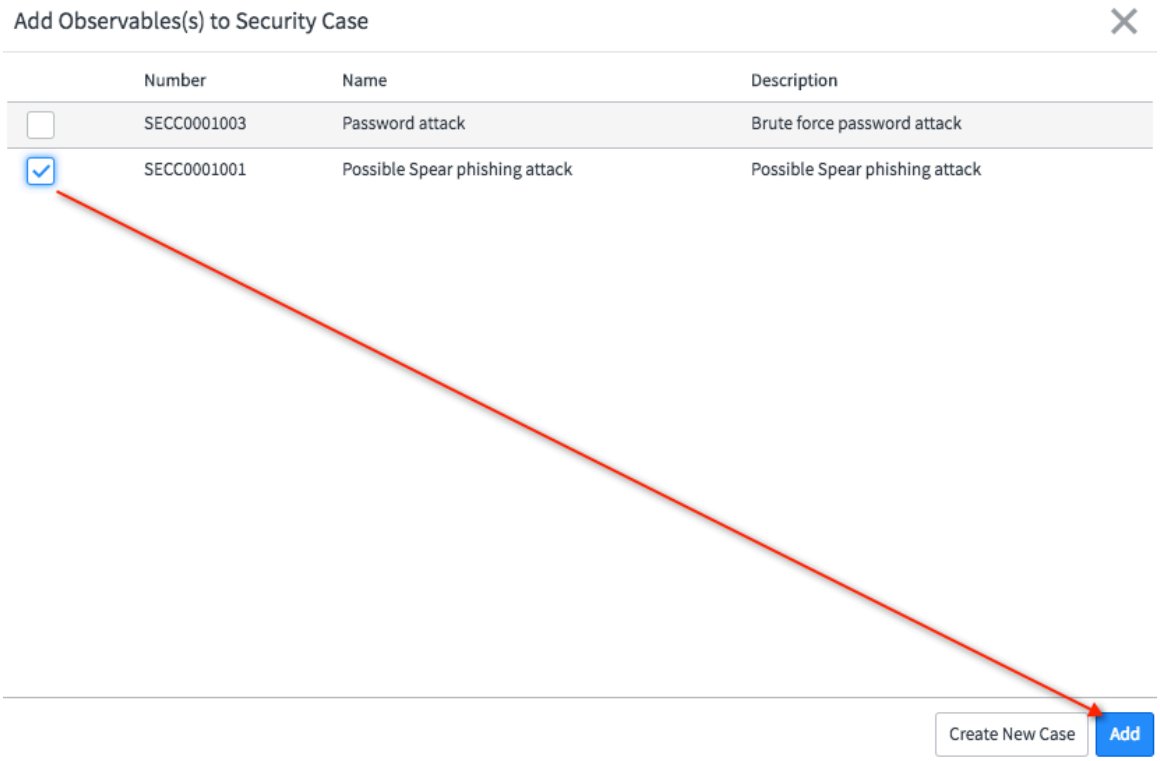
1. Accédez aux artefacts (IoC ou observables) que vous souhaitez ajouter aux tickets existants.
   - Pour ajouter des IoC à un ou plusieurs tickets, accédez à **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
   - Pour ajouter des observables à un ou plusieurs tickets, accédez à **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Dans la liste, sélectionnez les enregistrements d'artefact que vous souhaitez ajouter aux tickets existants.

   Remarque : Si vous sélectionnez plusieurs tickets, les IoC ou observables sélectionnés sont ajoutés à chacun des tickets sélectionnés.

3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.
   La boîte **de dialogue Ajouter au ticket de sécurité s'ouvre** . Si des tickets vous sont déjà affectés, ils s'affichent dans la liste.
4. Sélectionnez les tickets dans lesquels vous souhaitez ajouter les IoC ou observables sélectionnés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Ajouter**.
   Un message indique que les enregistrements sélectionnés ont été ajoutés aux tickets, ainsi qu'un lien vers les tickets dans Gestion des tickets de sécurité.

Créer un observable à partir d'un ticket

De nouveaux observables peuvent être créés à partir de tickets dans Gestion des tickets de sécurité.

Avant de commencer

Rôle requis : sn_ti.case_user

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
   La liste des tickets de sécurité s'ouvre.
2. Ouvrez un ticket existant ou cliquez sur **Nouveau** pour créer un nouveau ticket.
3. Cliquez sur le lien connexe **des artefacts du ticket** , puis cliquez sur l'onglet **Observables** .
4. Cliquez sur **Nouveau** et entrez les informations requises.

Champ	Description
Valeur	[Lecture seule] Le numéro de ticket.
Type d'observable	Entrez un nom décrivant le ticket.
Catégorie de type de l'observable	Sélectionnez le type de ticket faisant l'objet de l'enquête.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nombre d'incidents	Sélectionnez l'importance de ce ticket (de critique à faible).
Résultat	[Lecture seule] Date et heure de la dernière mise à jour du ticket.
Notes	Une brève description du ticket.

5. Cliquez sur l'onglet **Détails supplémentaires du ticket** .
6. Renseignez les champs comme il convient.

Champ	Description
Créé par	[Lecture seule] Nom de l'utilisateur qui a créé ce ticket.
État	État actuel du ticket. Lors de la création du ticket, la valeur par défaut de l'état est Brouillon.
Liste de notes de travail	Cochez la case pour afficher les notes de travail dans la section Détails supplémentaires du ticket de l'enregistrement de ticket.
Notes de travail	Si nécessaire, saisissez une note de travail pour le ticket. Si la **liste Notes de travail** est sélectionnée, la note de travail apparaît dans la section Détails supplémentaires du ticket de l'enregistrement de ticket.

7. Cliquez sur **Envoyer**.
   Si nécessaire, vous pouvez cliquer sur l'onglet **Artefacts du ticket** et ajouter des artefacts au ticket.

Exécuter une recherche de perceptions sur les observables d'un ticket

Vous pouvez rechercher des observables à l'aide de la fonctionnalité Recherche de perception pour déterminer leur fréquence. Chaque occurrence est considérée comme une observation. Vous pouvez limiter la recherche au nombre d'observations dans un nombre de jours sélectionné ou dans une plage de dates.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

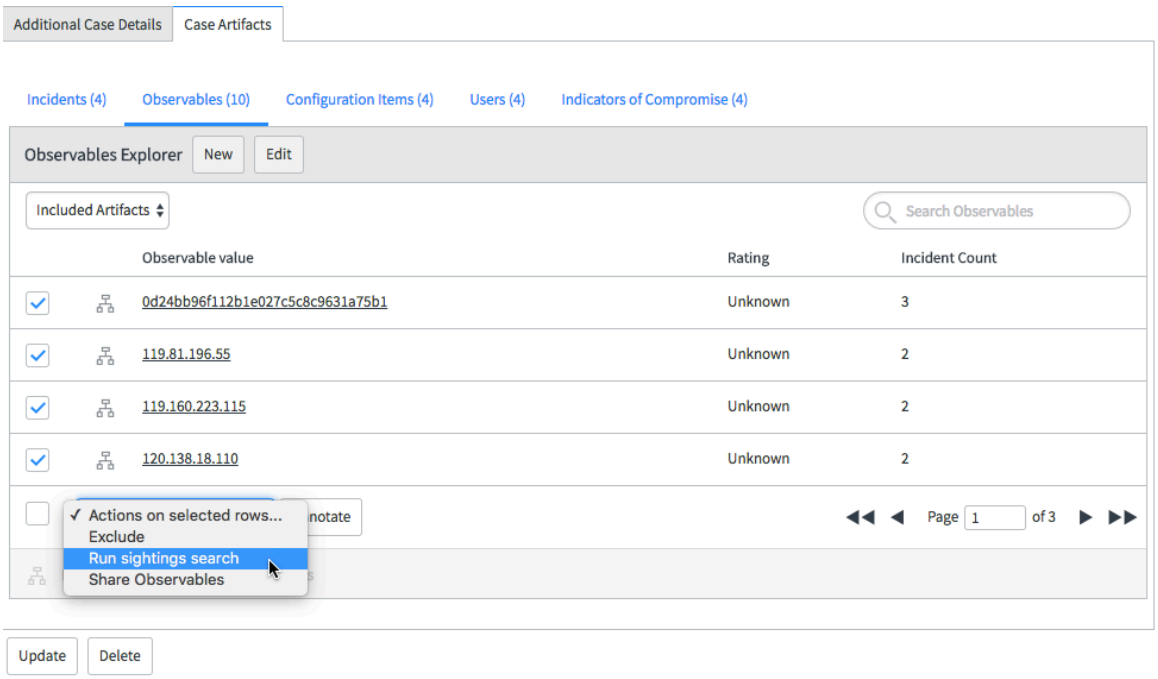
Rôle requis : sn_ti.case_user_write

Procédure

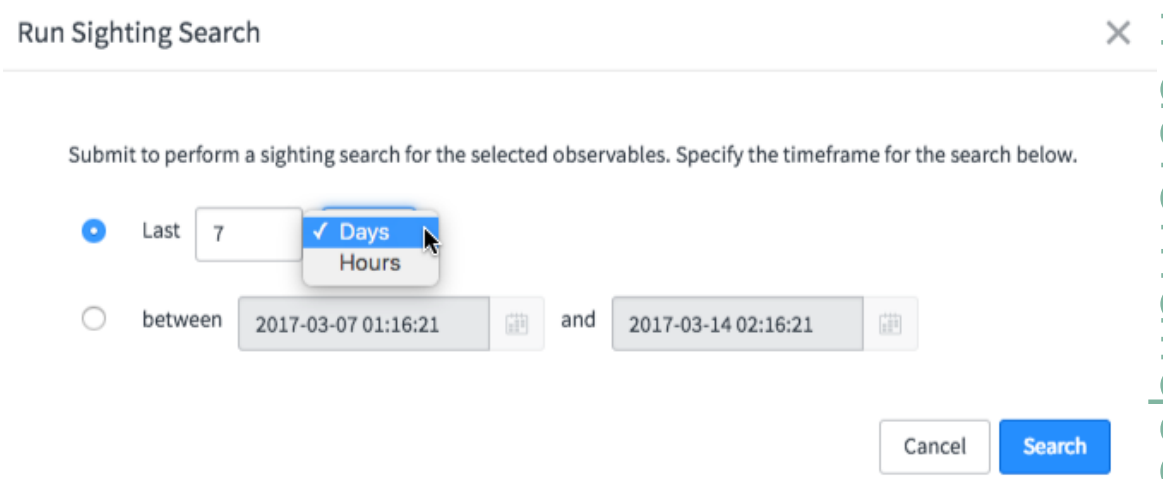
1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
2. Ouvrez le ticket qui contient des observables pour lesquels vous souhaitez exécuter une recherche de perceptions.
3. Cliquez sur le lien connexe **Artefacts du ticket** .
4. Cliquez sur l'onglet **Observables** .
5. Sélectionnez un ou plusieurs observables pour lesquels vous souhaitez rechercher des observations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Exécuter la recherche de perceptions**.
   La boîte **de dialogue Exécuter la recherche de perception** s'affiche.



7. Entrez le nombre de jours ou d'heures pendant lesquels vous souhaitez rechercher des observations des observables sélectionnés ou sélectionnez une plage de dates.
8. Cliquez sur **Rechercher**.

Incidents de sécurité dans les tickets

Dans Réponse aux incidents de sécurité, vous pouvez créer des tickets à partir d'incidents de sécurité, de CI et d'utilisateurs affectés, et ajouter ces artefacts à des tickets existants.

Créer un ticket à partir d'incidents de sécurité

Dans Réponse aux incidents de sécurité, vous pouvez créer des tickets à partir d'incidents de sécurité. Une fois que les incidents de sécurité ont été utilisés pour créer un nouveau ticket, vous pouvez l'utiliser Gestion des tickets de sécurité pour analyser les données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

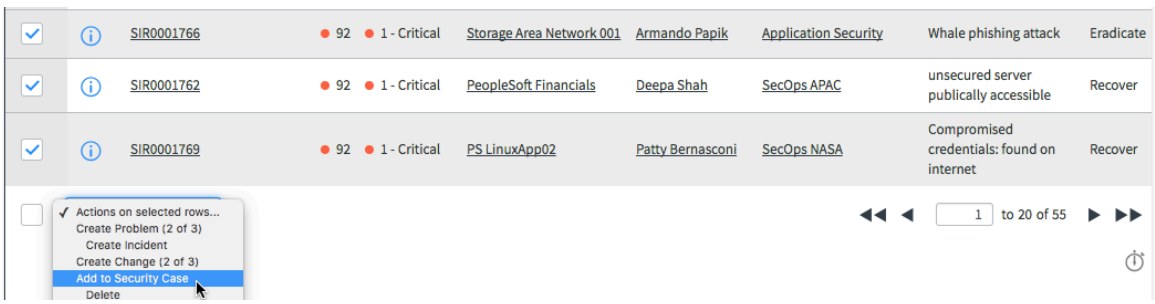
Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

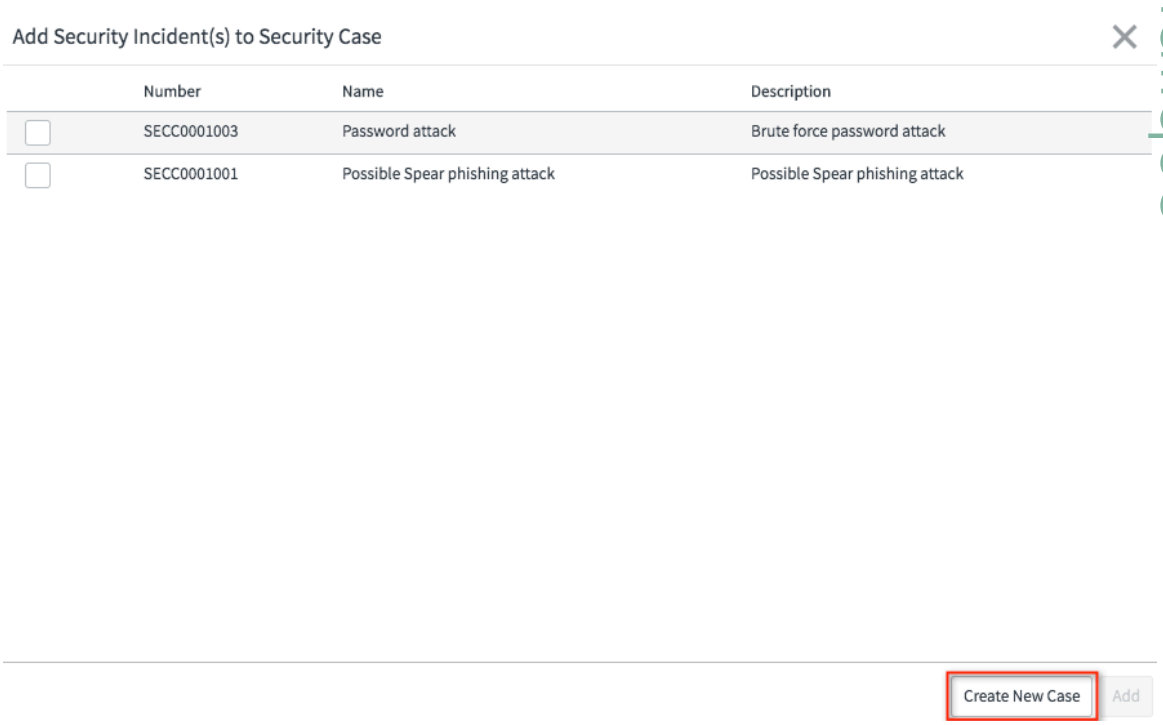
Vous devez accéder aux incidents de sécurité que vous souhaitez utiliser pour créer des tickets.

Procédure

1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents ouverts**.
   La liste des incidents de sécurité s'ouvre. Dans la liste, vous pouvez créer un nouveau ticket à partir d'un ou plusieurs incidents de sécurité, ou vous pouvez sélectionner un incident de sécurité spécifique et créer un nouveau ticket à partir du formulaire.
2. Pour créer un ticket à partir de la liste, sélectionnez les artefacts que vous souhaitez ajouter à un nouveau ticket.
3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.



La boîte **de dialogue Ajouter au ticket de sécurité s'ouvre** . Si des tickets vous sont déjà affectés, ils s'affichent dans la liste.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Créer un ticket**.
5. Renseignez les champs.

Champ	Description
Nom du ticket	Entrez un nom pour ce ticket.
Description	Entrez une description utile pour l'analyste de ticket.

6. Cliquez sur **Envoyer**.
   Un message en haut de la liste indique qu'un nouveau ticket a été créé, ainsi qu'un lien vers le ticket dans Gestion des tickets de sécurité.
7. Cliquez sur le lien pour afficher le nouveau ticket.

Ajouter des incidents de sécurité à un ticket existant

Vous pouvez ajouter des incidents de sécurité à un ou plusieurs tickets existants. Une fois les incidents de sécurité ajoutés aux tickets, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

Vous devez accéder aux incidents de sécurité que vous souhaitez ajouter aux tickets existants.

Procédure

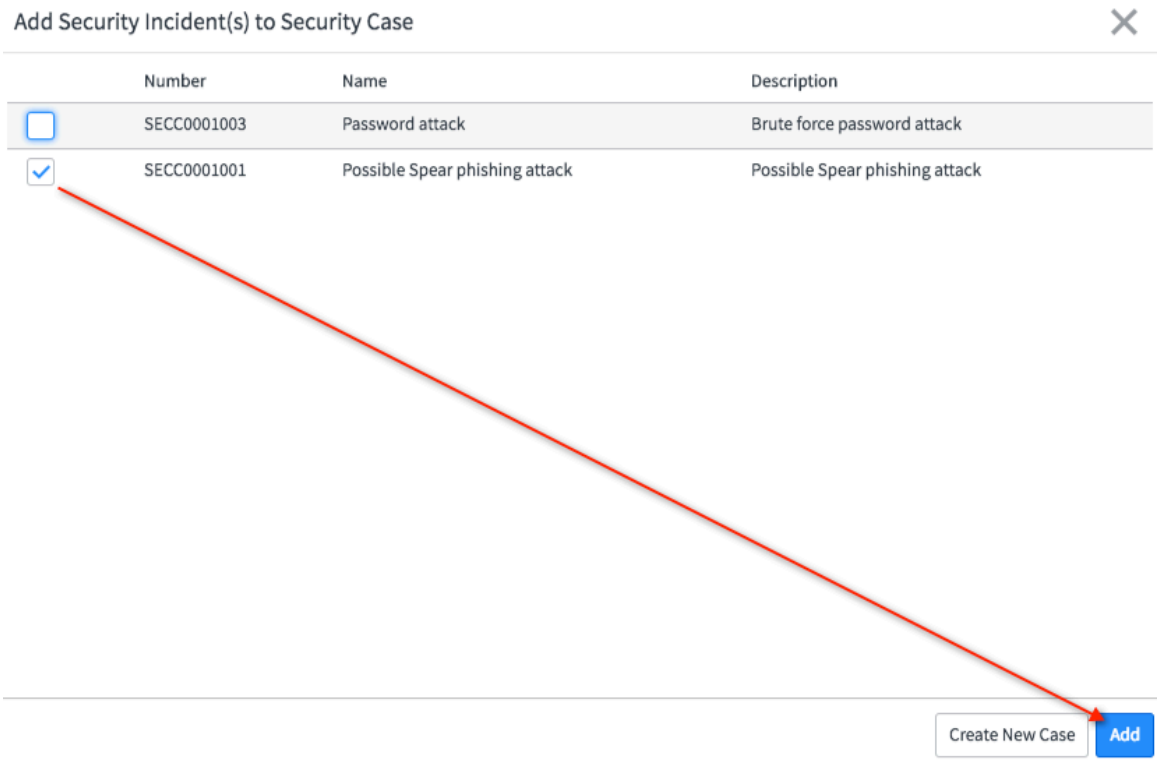
1. Accédez à la **Tout** > **Incident de sécurité** > **Incidents** > **Afficher les incidents ouverts**.
   La liste des incidents de sécurité s'ouvre.
2. Dans la liste, sélectionnez un ou plusieurs incidents de sécurité à ajouter aux tickets existants.

   Remarque : Si vous sélectionnez plusieurs incidents de sécurité, les incidents de sécurité sélectionnés sont ajoutés à chacun des tickets sélectionnés.

3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.
   La boîte **de dialogue Ajouter au ticket de sécurité s'ouvre** et affiche les tickets qui vous sont affectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez les tickets dans lesquels vous souhaitez ajouter les incidents de sécurité sélectionnés.
5. Cliquez sur **Ajouter**.
   Un message indique que les enregistrements sélectionnés ont été ajoutés aux tickets, ainsi qu'un lien vers les tickets dans Gestion des tickets de sécurité.

Éléments de configuration dans les tickets

Vous pouvez créer un ticket à partir d'un ou de plusieurs éléments de configuration (CI) dans la table Élément de configuration [cmdb_ci]. Vous pouvez également ajouter des CI à des tickets existants.

Créer un ticket à partir de CI

Vous pouvez créer un ticket de sécurité à partir d'éléments de configuration dans la table Élément de configuration [cmdb_ci]. Une fois que les CI ont été utilisés pour créer un ticket, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

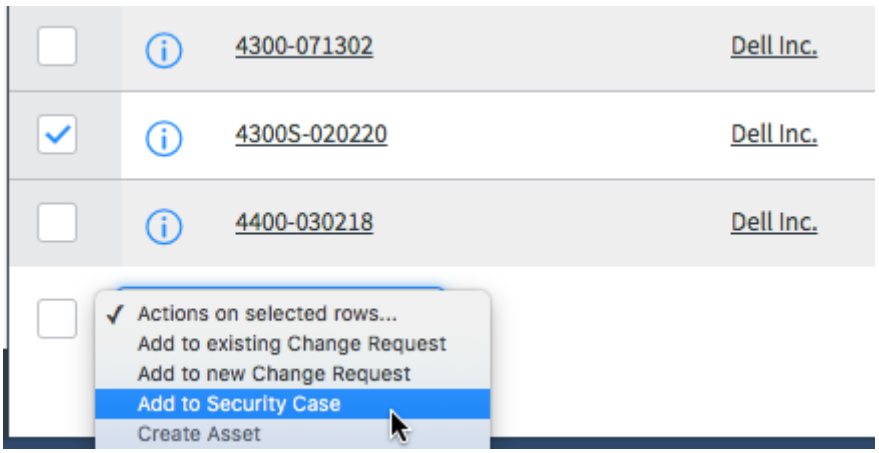
Vous devez accéder aux éléments de configuration que vous souhaitez utiliser pour créer un ticket.

Traduction automatique

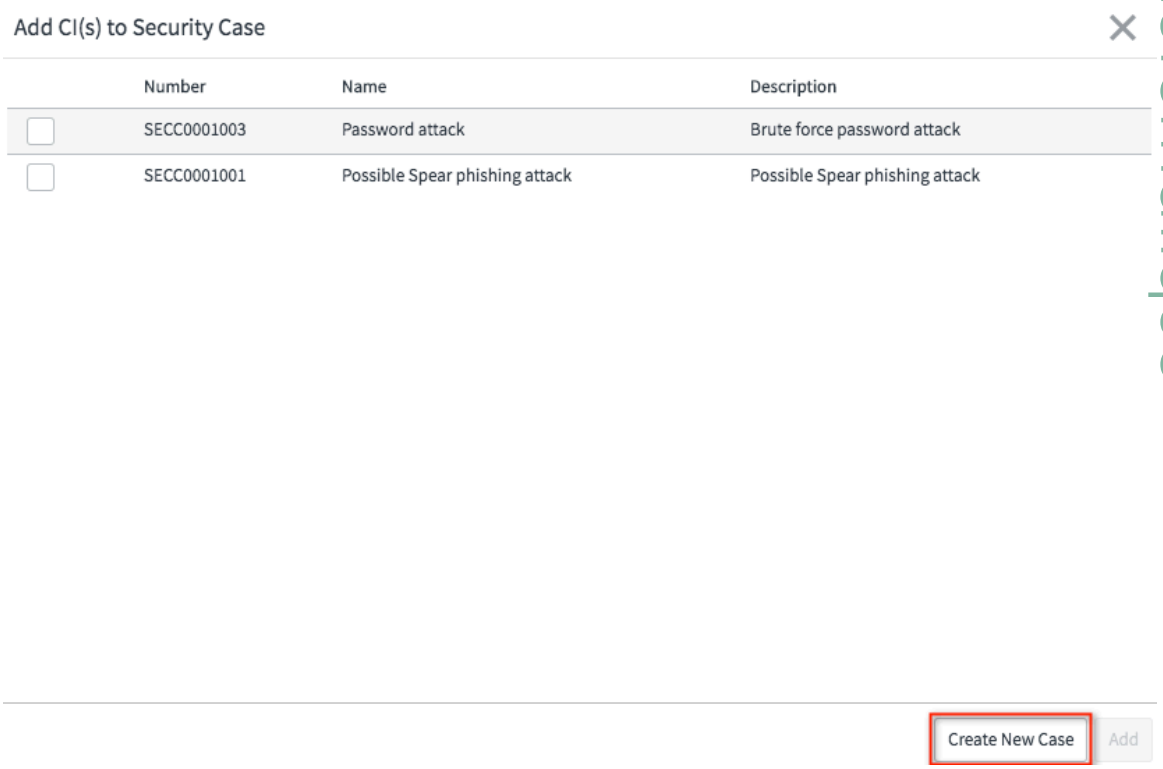
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Configuration** > **Éléments de base** > **Ordinateurs** pour afficher les CI des ordinateurs.
   La liste correspondant au type de CI sélectionné s'ouvre. Dans la liste, vous pouvez créer un ticket à partir d'un ou de plusieurs CI, ou sélectionner un CI spécifique et créer un nouveau ticket à partir du formulaire.
2. Dans la liste, sélectionnez les CI que vous souhaitez ajouter à un nouveau ticket.
3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.



La boîte **de dialogue Ajouter au ticket de sécurité s'ouvre** . Si des tickets vous sont déjà affectés, ils s'affichent dans la liste.



4. Cliquez sur **Créer un ticket**.
5. Renseignez les champs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom du ticket	Entrez un nom pour ce ticket.
Description	Entrez une description utile pour l'analyste de ticket.

6. Cliquez sur **Envoyer**.
   Un message en haut de la liste indique qu'un nouveau ticket a été créé, ainsi qu'un lien vers le ticket dans Gestion des tickets de sécurité.
7. Cliquez sur le lien pour afficher le nouveau ticket.

Ajouter des CI aux tickets existants

Vous pouvez ajouter des éléments de configuration à un ou plusieurs tickets existants. Une fois les CI ajoutés aux tickets, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

Vous devez accéder aux CI que vous souhaitez ajouter aux tickets existants.

Procédure

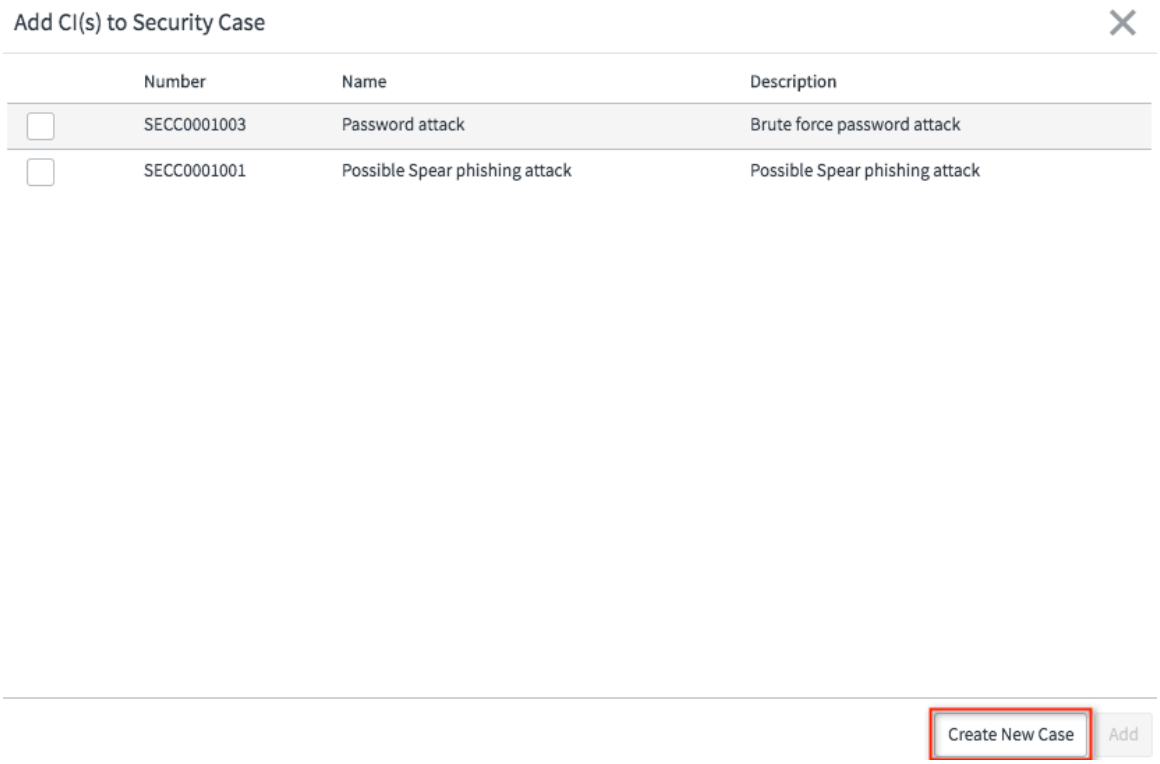
1. Accédez à la **Tout** > **Configuration** > **Éléments de base** > **Ordinateurs** pour afficher les CI des ordinateurs.
   La liste des CI sélectionnés s'affiche.
2. Dans la liste, sélectionnez un ou plusieurs CI à ajouter aux tickets existants.

   Remarque : Si vous sélectionnez plusieurs CI, les CI sélectionnés sont ajoutés à chacun des tickets sélectionnés.

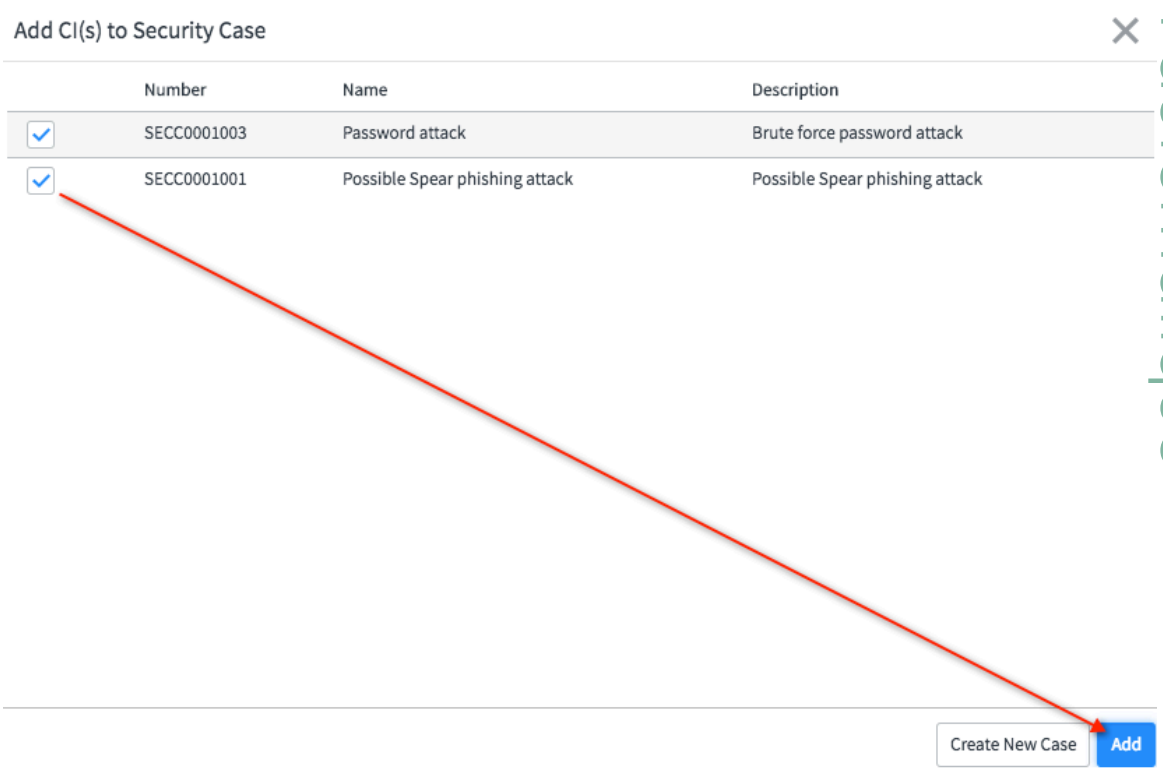
3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.
   La boîte **de dialogue Ajouter au ticket de sécurité s'ouvre** et affiche les tickets qui vous sont affectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez les tickets dans lesquels vous souhaitez ajouter les CI sélectionnés.



5. Cliquez sur **Ajouter**.
Un message indique que les enregistrements sélectionnés ont été ajoutés aux tickets, ainsi qu'un lien vers les tickets dans Gestion des tickets de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs affectés dans les tickets

Vous pouvez créer un ticket pour un ou plusieurs utilisateurs affectés dans la table Utilisateur [sys_user]. Vous pouvez également ajouter des utilisateurs aux tickets existants.

Créer un ticket à partir des utilisateurs affectés

Vous pouvez créer un ticket de sécurité à partir des utilisateurs affectés dans la table Utilisateur [sys_user]. Une fois que les utilisateurs affectés ont été utilisés pour créer un ticket, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

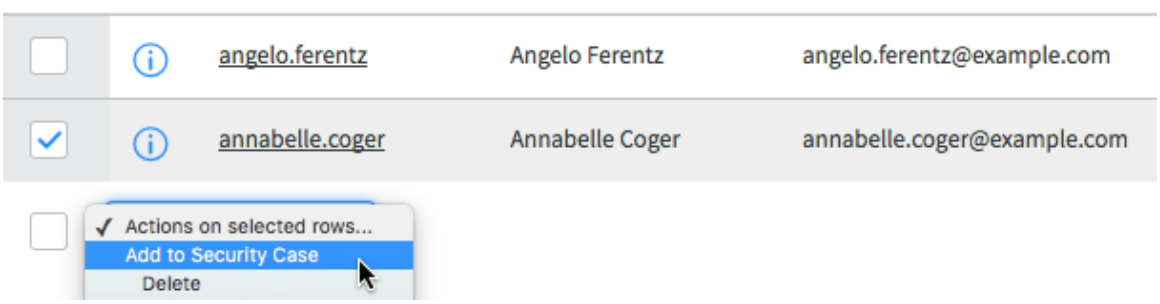
Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

Vous devez accéder aux utilisateurs que vous souhaitez utiliser pour créer un ticket.

Procédure

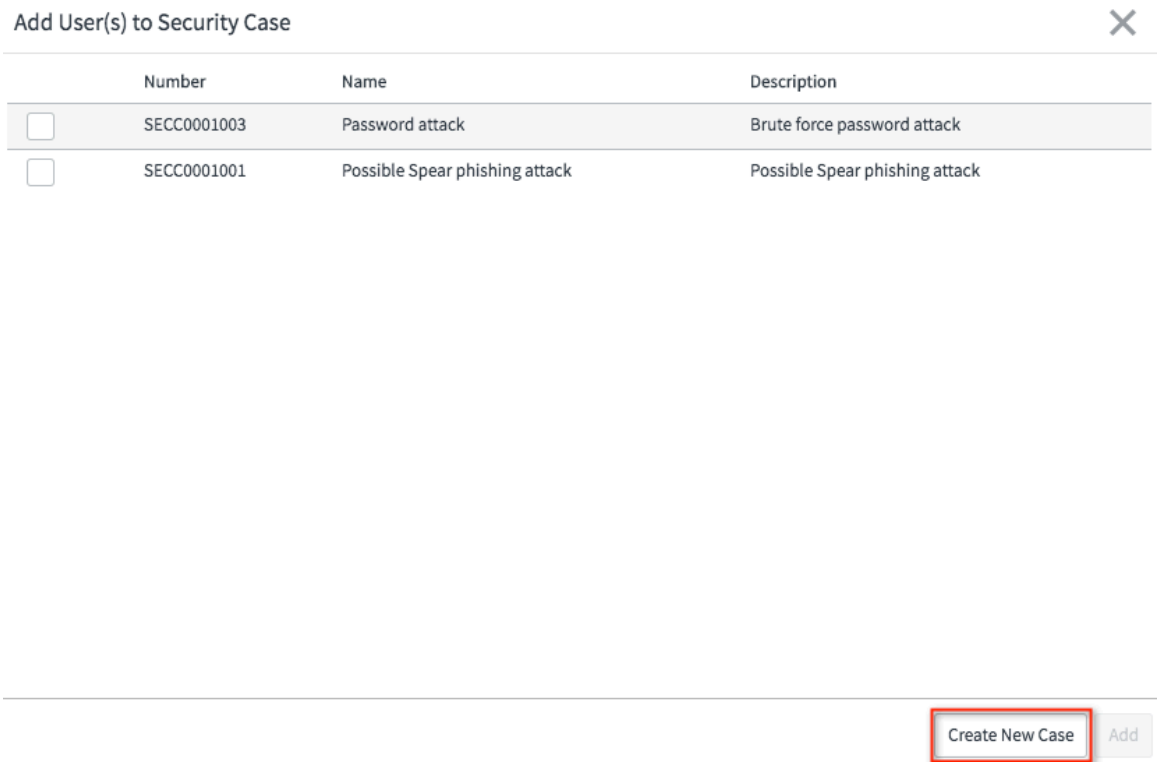
1. Accédez à la **Tout** > **Administration utilisateurs** > **Utilisateurs**.
   La liste des utilisateurs sélectionnés s'ouvre. Dans la liste, vous pouvez créer un ticket à partir d'un ou de plusieurs enregistrements utilisateur, ou sélectionner un enregistrement utilisateur spécifique et créer un nouveau ticket à partir du formulaire.
2. Dans la liste, sélectionnez les utilisateurs que vous souhaitez ajouter à un nouveau ticket.
3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.



La boîte **de dialogue Ajouter au ticket de sécurité s'ouvre** . Si des tickets vous sont déjà affectés, ils s'affichent dans la liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Créer un ticket**.
5. Renseignez les champs.

Champ	Description
Nom du ticket	Entrez un nom pour ce ticket.
Description	Entrez une description utile pour l'analyste de ticket.

6. Cliquez sur **Envoyer**.
   Un message en haut de la liste indique qu'un nouveau ticket a été créé, ainsi qu'un lien vers le ticket dans Gestion des tickets de sécurité.
7. Cliquez sur le lien pour afficher le nouveau ticket.

Ajouter des utilisateurs affectés à des tickets existants

Vous pouvez ajouter des utilisateurs affectés à un ou plusieurs tickets existants. Une fois les enregistrements utilisateur ajoutés aux tickets, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

Vous devez accéder aux enregistrements des utilisateurs que vous souhaitez ajouter aux tickets existants.

Traduction automatique

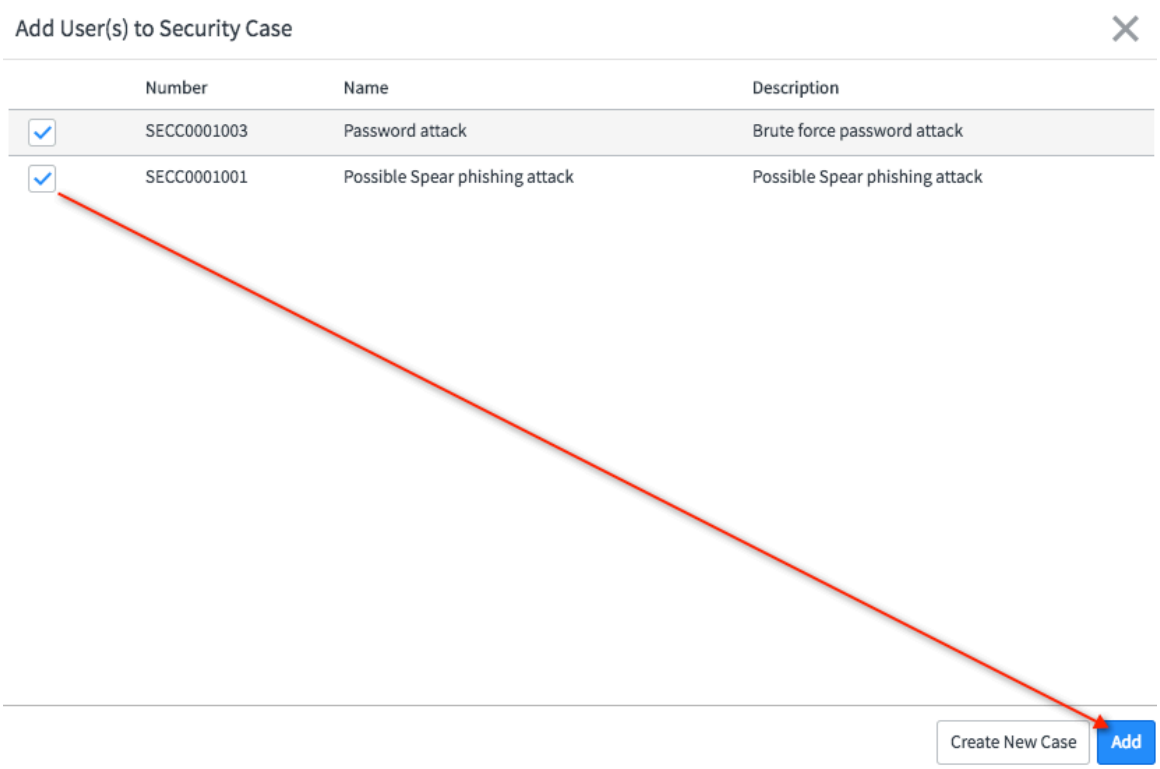
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Utilisateurs**.
   La liste des enregistrements utilisateur s'ouvre.
2. Dans la liste, sélectionnez un ou plusieurs utilisateurs à ajouter aux tickets existants.

   Remarque : Si vous sélectionnez plusieurs utilisateurs, les enregistrements des utilisateurs sélectionnés sont ajoutés à chacun des tickets sélectionnés.

3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.
   La boîte **de dialogue Ajouter au ticket de sécurité s'ouvre** et affiche les tickets qui vous sont affectés.



4. Sélectionnez les tickets dans lesquels vous souhaitez ajouter les utilisateurs sélectionnés.
5. Cliquez sur **Ajouter**.
   Un message indique que les enregistrements sélectionnés ont été ajoutés aux tickets, ainsi qu'un lien vers les tickets dans Gestion des tickets de sécurité.

Analyse des artefacts de sécurité

Une fois que vous avez créé des tickets, soit à l'aide Gestion des tickets de sécuritéde , soit à partir d'artefacts tels que des IoC, des observables, des incidents de sécurité, etc., vous pouvez continuer à ajouter des artefacts pour faciliter l'analyse des menaces identifiées.

Détails connexes pour les artefacts du ticket

Lorsque vous ajoutez des artefacts à un ticket, des détails connexes supplémentaires pour chaque artefact peuvent également être ajoutés automatiquement. Par exemple, si vous ajoutez un incident de sécurité, il peut contenir des enregistrements de CI et d'utilisateurs affectés. Vous pouvez afficher rapidement les détails connexes d'un artefact sélectionné sans quitter la liste des artefacts.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les détails connexes d'un artefact d'incident de sécurité

Si votre ticket inclut des artefacts d'incident de sécurité, vous pouvez afficher tous les détails connexes contenus dans chaque incident de sécurité référencé par le ticket.

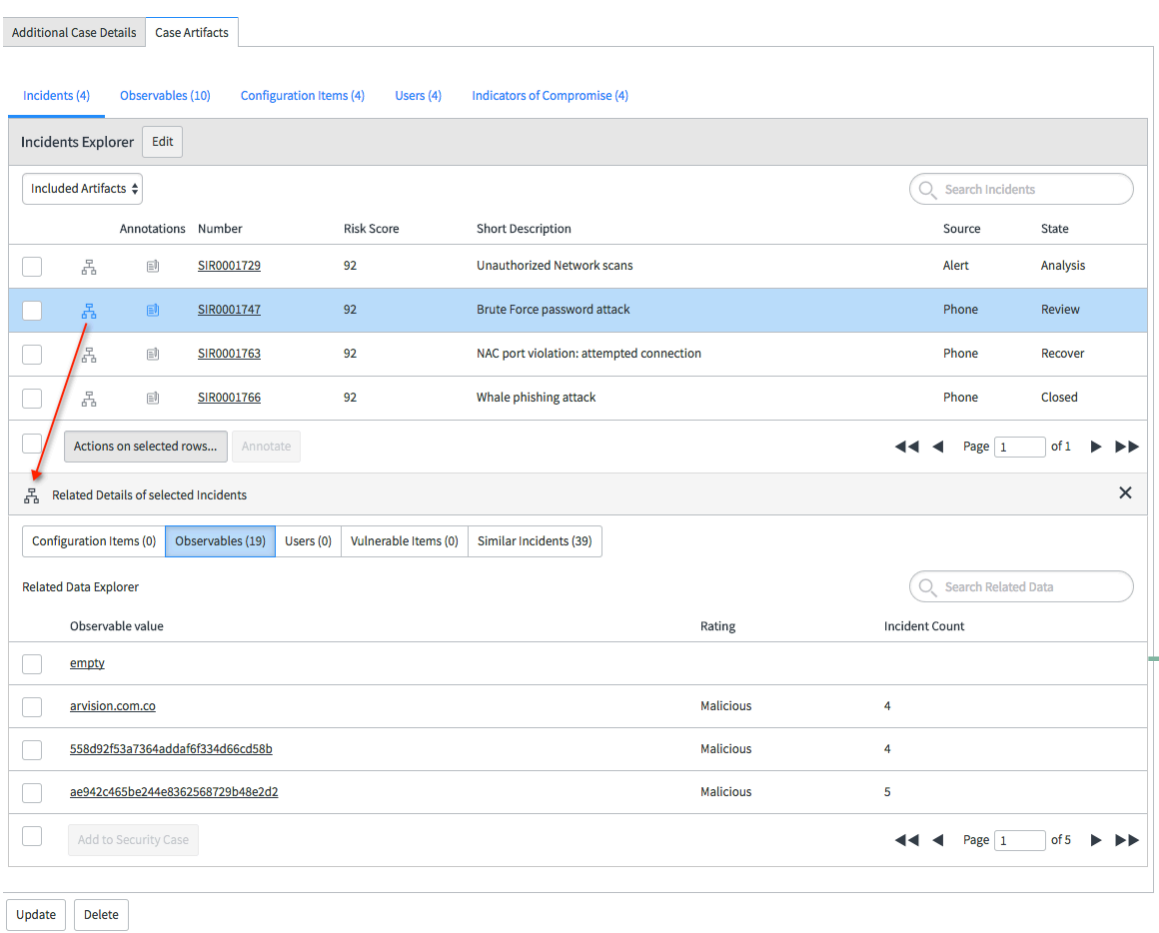
Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket qui contient des artefacts d'incident de sécurité.
2. Cliquez sur l'onglet **Incidents** .
3. Cliquez sur l'icône Détails supplémentaires de l'incident de sécurité pour lequel vous souhaitez afficher les détails connexes.



4. Cliquez sur l'un des onglets pour afficher les types spécifiques de détails de l'artefact sélectionné.
5. Vous pouvez également cliquer sur **l'onglet Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Afficher les détails connexes d'un artefact d'élément de configuration

Si votre ticket inclut des artefacts d'éléments de configuration, vous pouvez afficher tous les détails connexes contenus dans chaque CI référencé par le ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

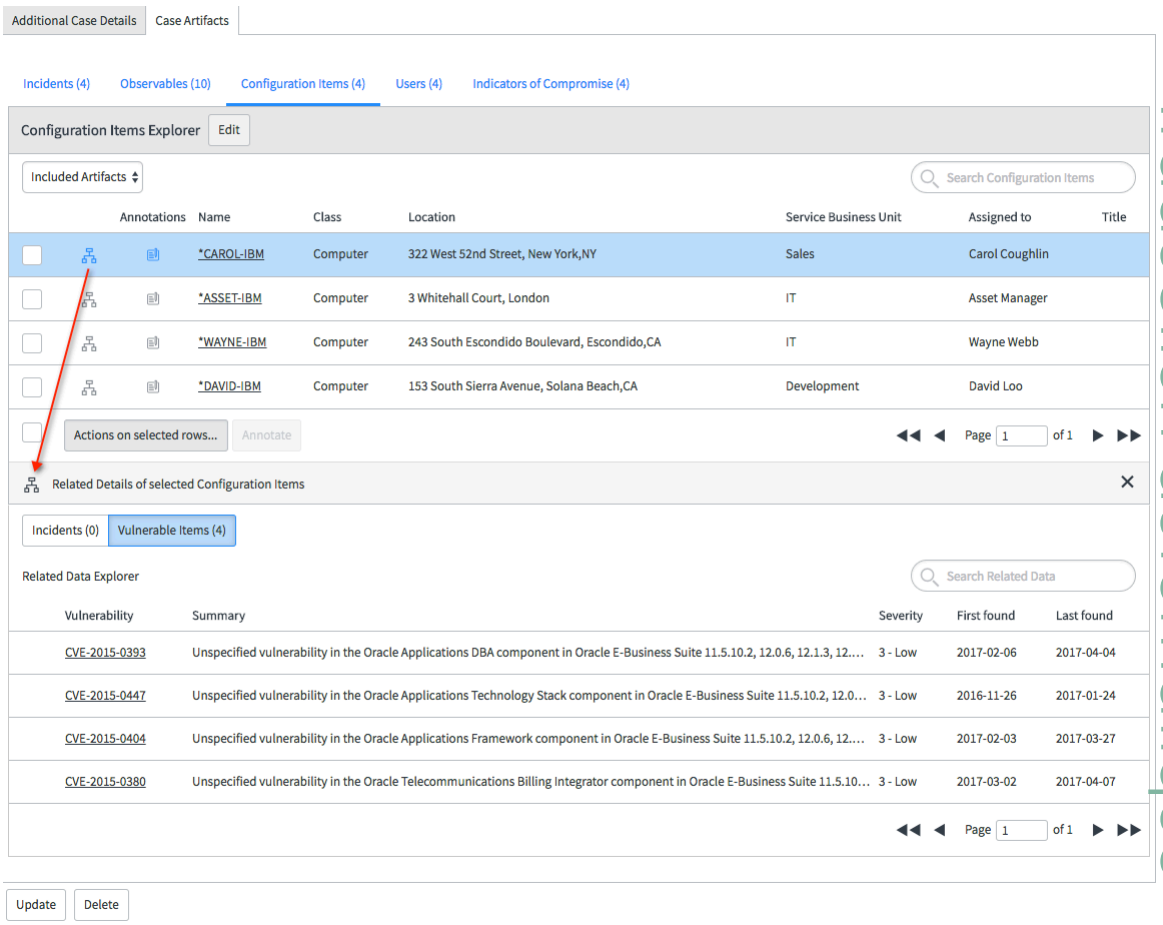
Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket qui contient des artefacts CI.
2. Cliquez sur l'onglet **Éléments de configuration** .
3. Cliquez sur Détails supplémentaires pour l'artefact CI pour lequel vous souhaitez afficher les détails connexes.



4. Cliquez sur l'un des onglets pour afficher les types spécifiques de détails de l'artefact sélectionné.
5. Vous pouvez également cliquer sur l'onglet **Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Afficher les détails connexes d'un artefact IoC

Si votre ticket inclut des artefacts d'indicateurs de compromission (IoC), vous pouvez afficher tous les détails connexes contenus dans chaque IoC référencé par le ticket.

Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

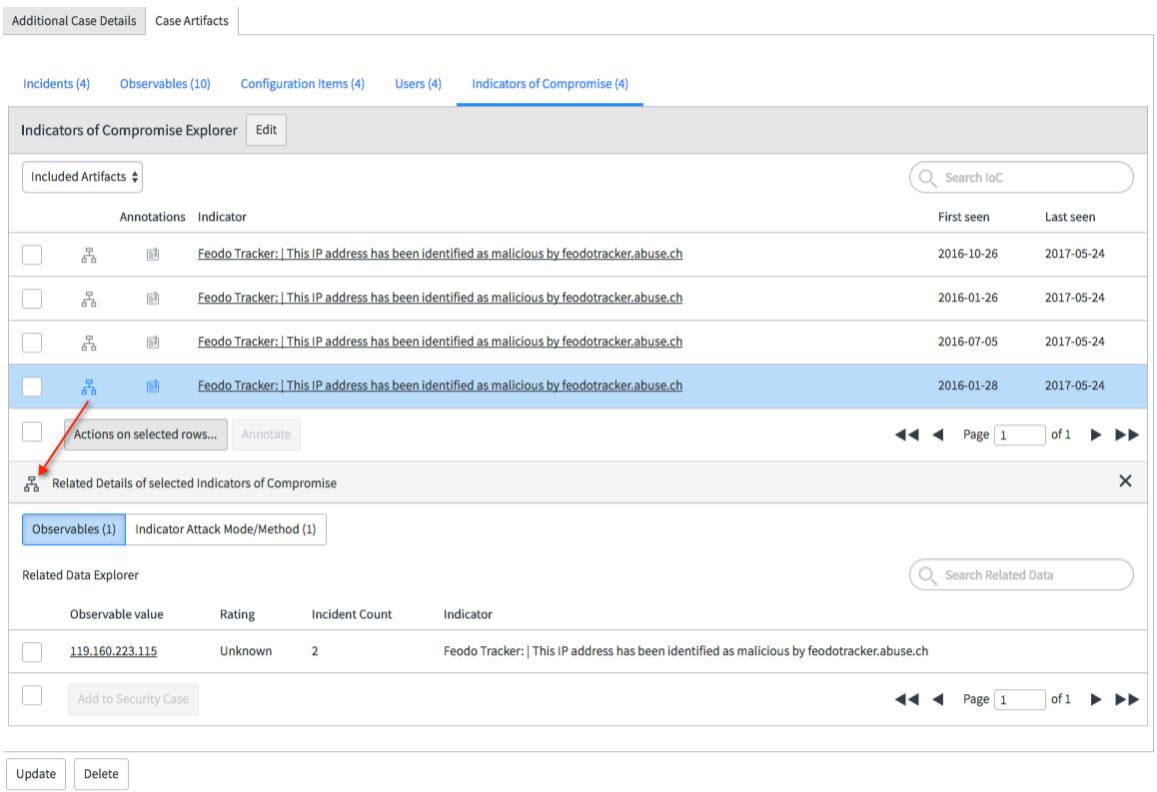
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket qui contient des artefacts IoC.
2. Cliquez sur l'onglet **Indicateurs de compromission** .
3. Cliquez sur l'icône Détails supplémentaires en regard de l'artefact IoC pour lequel vous souhaitez afficher les détails connexes.



4. Cliquez sur l'un des onglets pour afficher les types spécifiques de détails de l'artefact sélectionné.
5. Vous pouvez également cliquer sur **l'onglet Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Afficher les détails connexes d'un artefact d'utilisateur affecté

Si votre ticket inclut des artefacts d'utilisateur affectés, vous pouvez afficher tous les détails connexes contenus dans chaque utilisateur affecté référencé par le ticket.

Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

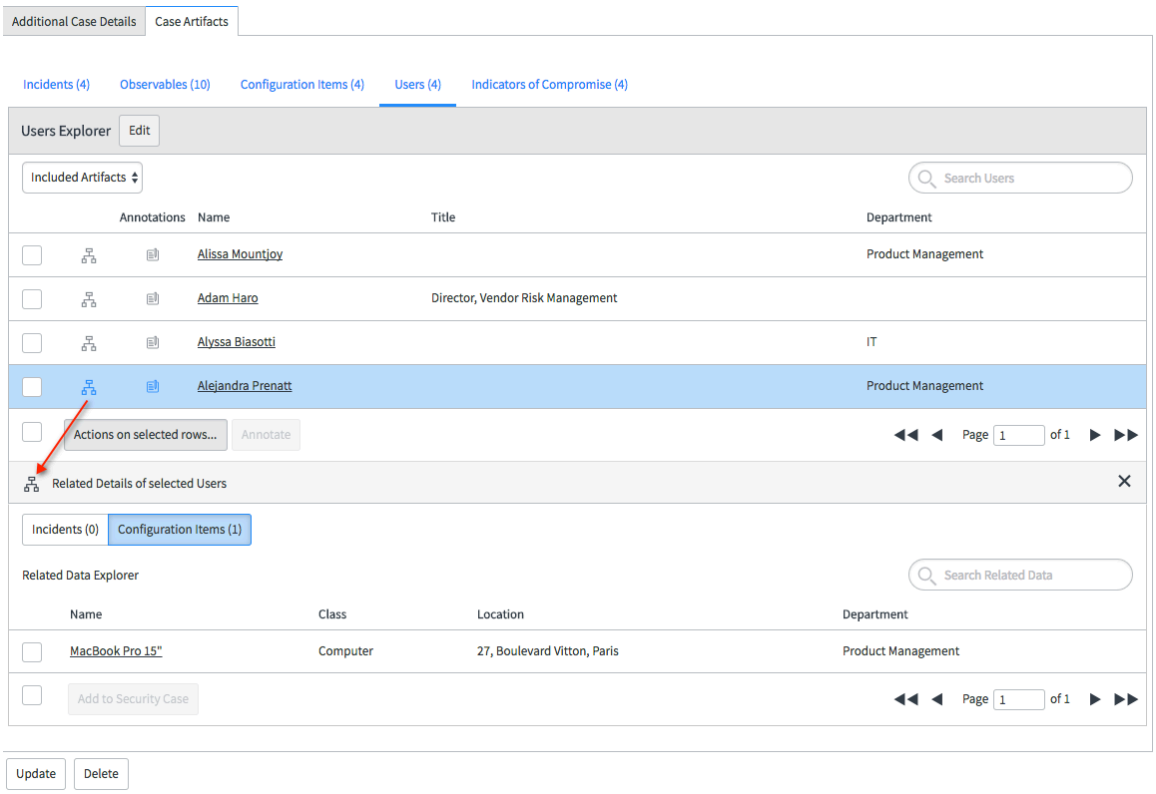
Procédure

1. Ouvrez un ticket qui contient des artefacts de l'utilisateur affecté.
2. Cliquez sur l'onglet **Utilisateurs** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur Détails connexes pour l'artefact de l'utilisateur affecté pour lequel vous souhaitez afficher les détails connexes.



4. Cliquez sur l'un des onglets pour afficher les types spécifiques de détails de l'artefact sélectionné.
5. Vous pouvez également cliquer sur **l'onglet Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Afficher les détails connexes d'un artefact observable

Si votre ticket inclut des artefacts observables, vous pouvez afficher tous les détails connexes contenus dans chaque observable référencé par le ticket.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

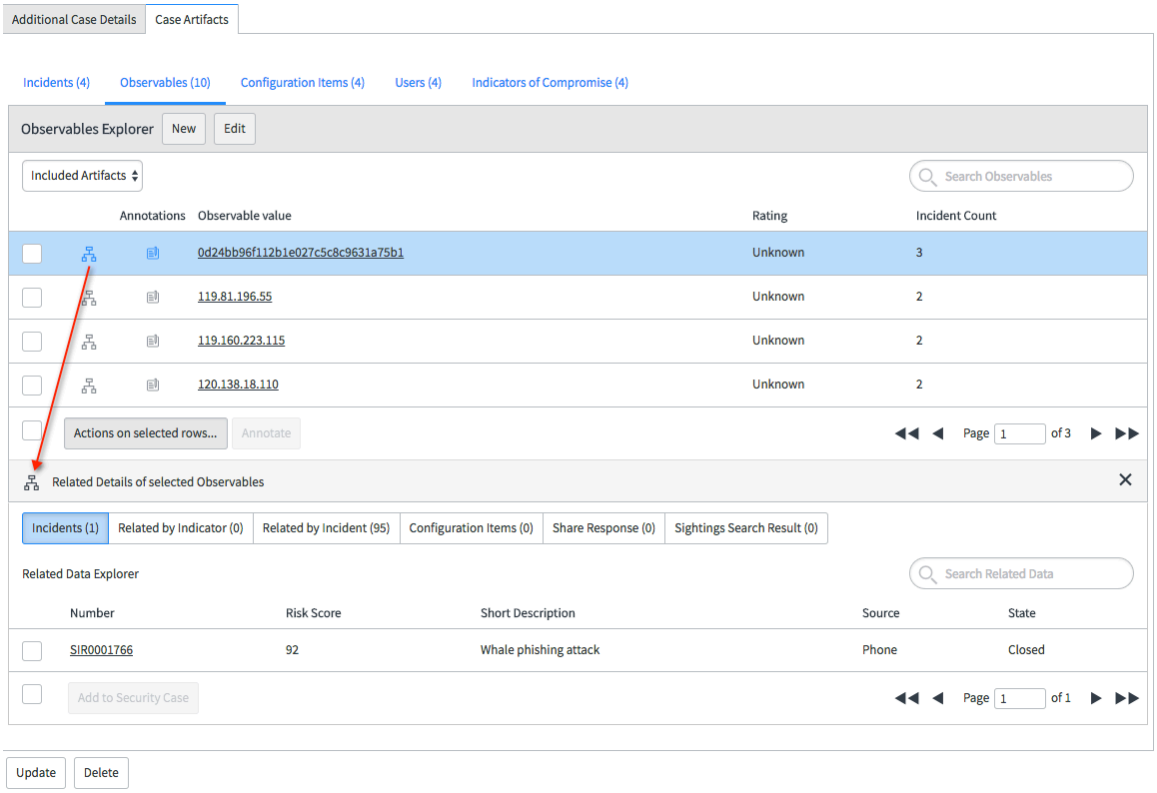
Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket qui contient des artefacts observables.
2. Cliquez sur l'onglet **Observables** .
3. Cliquez sur l'icône Détails supplémentaires pour l'artefact observable pour lequel vous souhaitez afficher les détails connexes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur l'un des onglets pour afficher les types spécifiques de détails de l'artefact sélectionné.
5. Vous pouvez également cliquer sur **l'onglet Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Exclusion et inclusion des artefacts de sécurité

Les listes d'artefacts de support affectés à un ticket peuvent parfois être longues et il peut arriver que vous souhaitiez supprimer des artefacts particuliers d'une liste. Plutôt que de supprimer définitivement les artefacts, vous pouvez les exclure de la liste et, si nécessaire, les réintégrer ultérieurement.

Exclure les artefacts de sécurité d'un ticket

Vous pouvez supprimer des artefacts des listes d'artefacts de support. Ils ne sont pas retirés définitivement et peuvent être remis dans la mallette au besoin.

Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

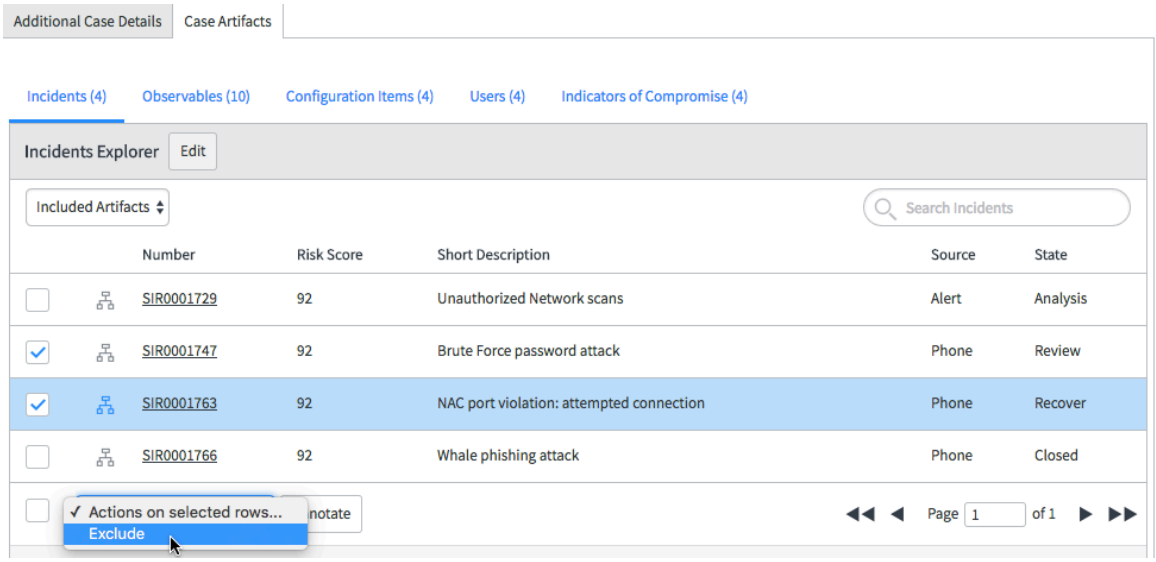
Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket contenant des artefacts que vous souhaitez exclure de la liste.
2. Cliquez sur la liste connexe **Artefacts du ticket** .
3. Cliquez sur l'onglet associé aux artefacts à exclure.
   Par exemple, cliquez sur **Incidents** pour exclure les incidents de sécurité de la liste.
4. Sélectionnez un ou plusieurs enregistrements d'artefact à exclure.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Exclure**.
6. Cliquez sur Exclure dans la zone **de** confirmation.
   Les artefacts sélectionnés sont supprimés de la liste.

Renvoyer les artefacts de sécurité exclus à un ticket

Une fois que vous avez exclu des artefacts d'une liste dans un ticket, vous pouvez les remettre dans le ticket pour continuer à travailler dessus.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

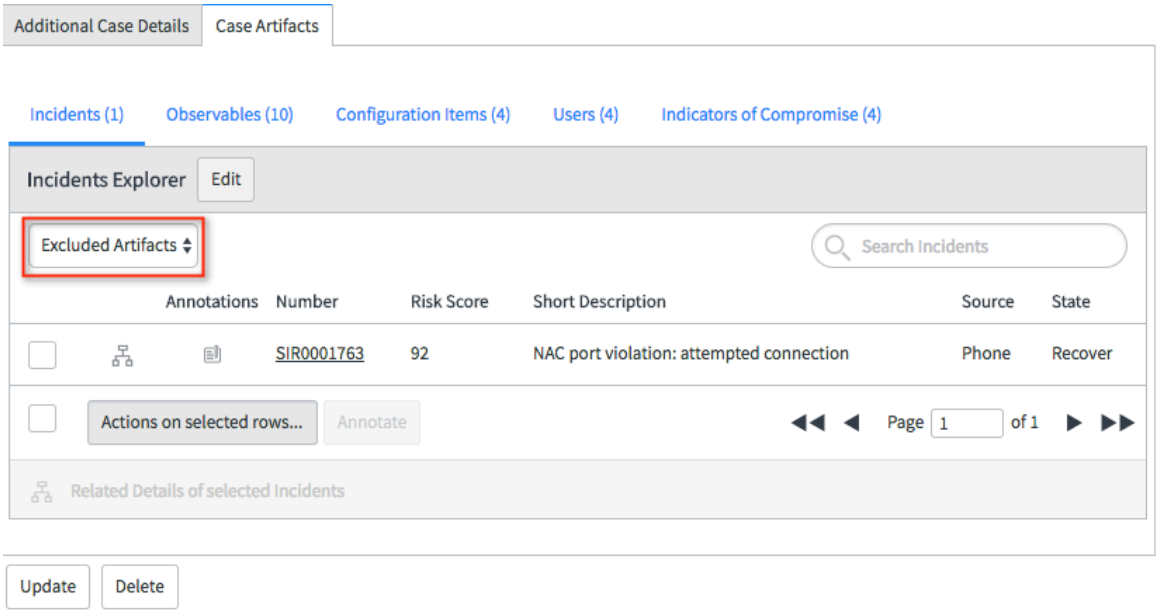
Rôle requis : sn_ti.case_user_write

Procédure

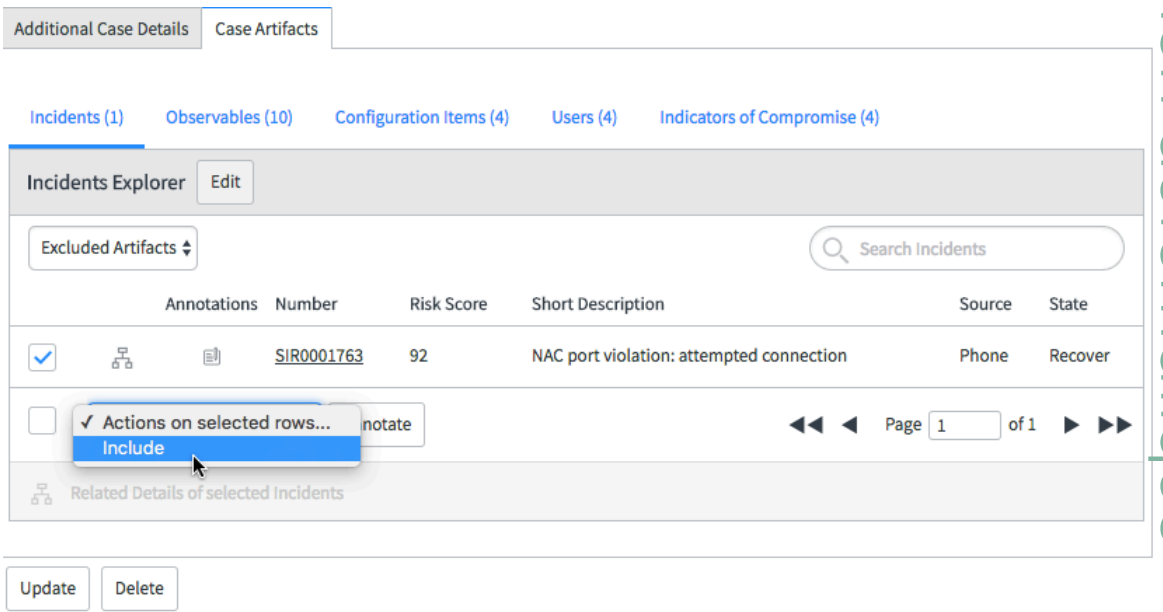
1. Ouvrez un ticket contenant des artefacts que vous avez précédemment exclus d'une liste et que vous souhaitez réintégrer dans la liste.
2. Cliquez sur la liste connexe **Artefacts du ticket** .
3. Cliquez sur l'onglet associé aux artefacts à réintégrer à la liste.
4. Cliquez sur la liste déroulante Filtre d'artefact et sélectionnez **Artefacts exclus**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Sélectionnez un ou plusieurs enregistrements d'artefacts que vous souhaitez renvoyer à la liste Inclure.
6. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Inclure**.



7. Cliquez sur **Inclure** dans la zone de confirmation.
   Les artefacts sélectionnés sont retirés de la liste des artefacts exclus et renvoyés à la liste des artefacts inclus dans le ticket.

Annoter les artefacts de sécurité

Au fur et à mesure de l'analyse d'un ticket, vous pouvez ajouter des annotations à n'importe quel artefact.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis :

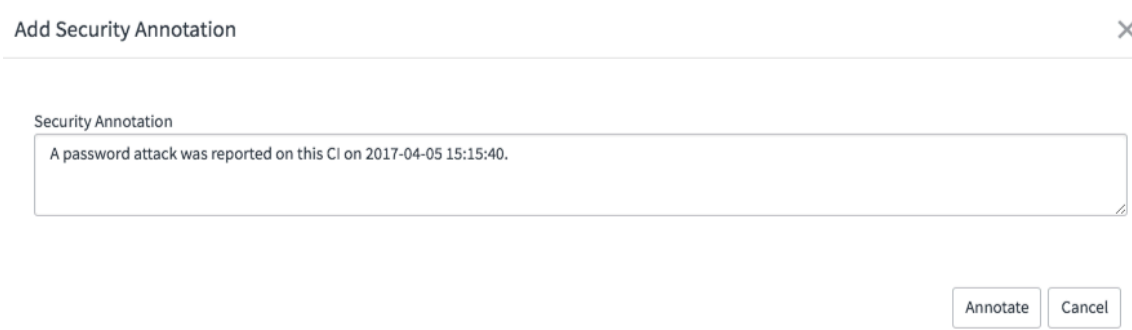
- sn_ti.case_user_write pour l'ajout d'annotations
- sn_ti.case_user_read pour afficher les annotations

Procédure

1. Ouvrez un ticket qui contient des artefacts que vous souhaitez annoter.
2. Cliquez sur la liste connexe **Artefacts du ticket** .
3. Cliquez sur l'onglet associé aux artefacts que vous souhaitez annoter.
   Par exemple, cliquez sur **Indicateurs de compromission** pour ajouter des annotations aux IoC.
4. Pour ajouter une annotation à un ou plusieurs artefacts, procédez comme suit :

   a. Sélectionnez les artefacts auxquels vous souhaitez ajouter une annotation.

   b. Cliquez sur **Annoter**.

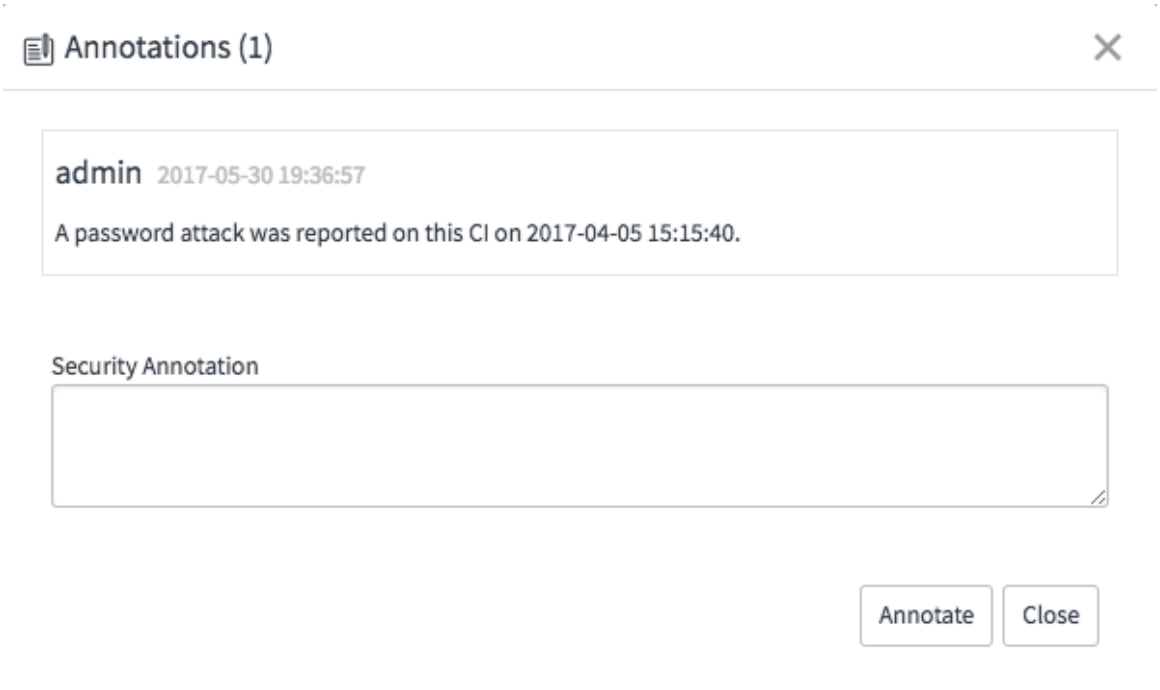


   c. Tapez l'annotation et cliquez sur **Annoter**.
   L'annotation est ajoutée aux artefacts sélectionnés.

5. Pour afficher les annotations d'un artefact, cliquez sur l'icône Afficher les).
   Les annotations existantes s'affichent dans la boîte de dialogue Annotations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Vous pouvez également entrer une nouvelle annotation pour l'artefact dans la zone **Annotation de sécurité** , puis cliquer sur **Annoter**.

Rechercher des artefacts de sécurité

Vous pouvez effectuer une recherche par mot clé sur n'importe quelle liste d'artefacts de sécurité.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour utiliser Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket qui contient des artefacts de sécurité.
2. Cliquez sur l'onglet des artefacts de sécurité sur lesquels vous souhaitez effectuer une recherche par mot clé.
3. Dans la zone **de recherche par mot-clé** , commencez à taper le nom de l'artefact que vous souhaitez localiser.
   Lorsque des artefacts correspondant à votre entrée sont trouvés, ils sont affichés.

Contrôle de la posture de sécurité

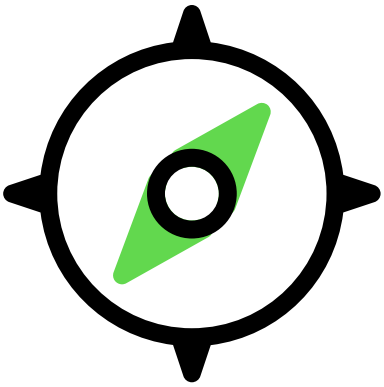
Gagnez en visibilité sur l'inventaire des actifs de votre entreprise et la couverture des outils de sécurité. Utilisez les politiques fournies avec le produit ou créez les vôtres pour identifier les actifs pour lesquels il manque des outils de sécurité clés, tels que la protection des terminaux, la gestion de la configuration et l'analyse des vulnérabilités. Surveillez les actifs pour les configurations d'outils de Security spécifiques à votre environnement et automatisez le workflow de rattrapage pour les failles de sécurité dans l'application Conformité de la configuration .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

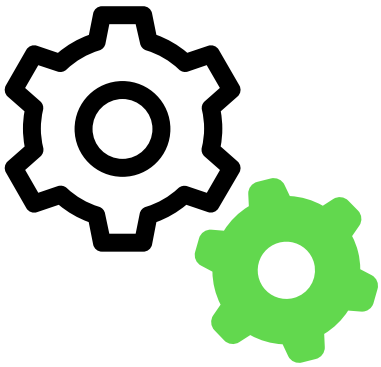
Premiers pas

Explorer



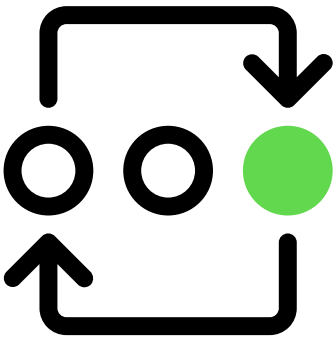
En savoir plus sur les concepts et les fonctionnalités de Security Posture Control

Installer



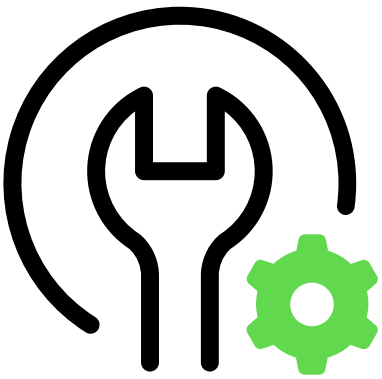
Installer les applications de contrôle de la posture de sécurité

Intégrer



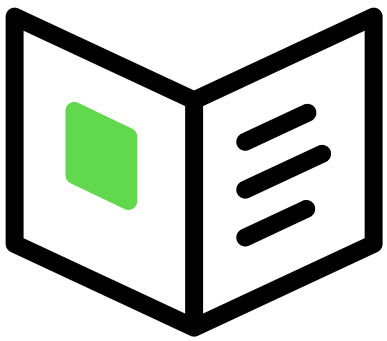
Intégrer Service Graph Connectors à Security Posture Control

Utiliser



Découvrez comment utiliser l'espace de travail pour rechercher vos actifs et identifier les failles de sécurité

Référence



Obtenez des détails sur les scénarios qui vous aident à identifier des types spécifiques d'écarts de couverture d'outils. Consultez des exemples de stratégies de base, enfants et clonées, ainsi qu'une liste des connecteurs du graphe de services matériels et logiciels pris en charge.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage et demande d'aide

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

Explorer Contrôle de la posture de sécurité

Contrôle de la posture de sécurité permet aux équipes de cybersécurité d'obtenir une visibilité sur l'inventaire complet de leurs actifs d'entreprise et de déterminer leur posture de sécurité globale.

Les analystes de sécurité obtiennent un aperçu de la façon dont les outils de sécurité sont déployés et de la couverture de leurs actifs en fonction de leur inventaire d'actifs et des données importées à partir de connecteurs du graphe de services et de produits ServiceNow tels que Gestion des actifs matériels (HAM) et ITOM Discovery.

Version	Notes de publication
Contrôle de la posture de sécurité Core v4.0, v3.0, v2.0, v1.0	Pour plus d'informations sur la compatibilité, consultez Matrice de compatibilité de KB0856498 Vulnerability Response et Changements de schéma de mise en production Notes de publication Contrôle de la posture de sécurité
Gestion de la posture de sécurité des actifs v4.0. v3.0, v2.0, v1.0	

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

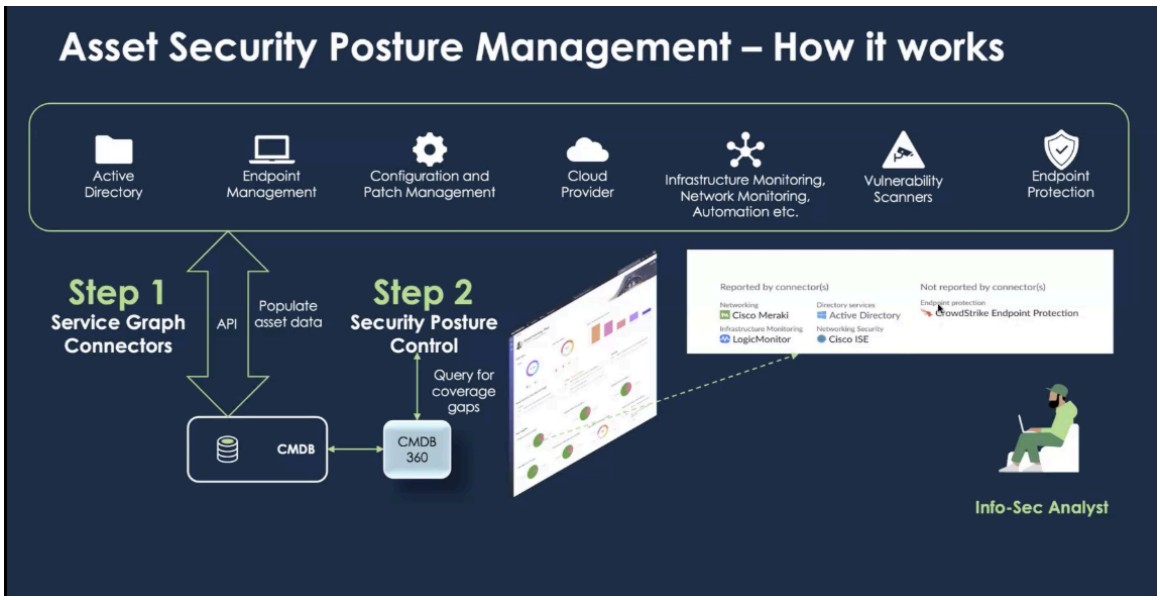
Grâce à ce SPC produit, les équipes Info-Sec peuvent effectuer les tâches suivantes :

- Surveillez vos actifs pour vérifier leur conformité aux normes internes de configuration des outils de sécurité. Par exemple, assurez-vous que la dernière version d'un produit de protection du point de terminaison est utilisée.
- Automatisez votre workflow de rattrapage des lacunes en matière de posture de sécurité que vous trouvez avec l'application ServiceNow Configuration Compliance.
- Créez des politiques et des aperçus personnalisés en fonction des métadonnées des actifs, des données de couverture des outils de sécurité et des données de vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mode de fonctionnement de Gestion de la posture de sécurité des actifs



Gestion de la posture de sécurité des actifs (ASPM) identifie les lacunes de couverture de l'outil de Security dans les actifs à l'aide d'intégrations d'API avec divers outils tiers (Connecteurs du graphe de services) ainsi qu'avec les produits ServiceNow.

Gestion de la posture de sécurité des actifs identifie les lacunes de couverture de l'outil de Security dans les actifs à l'aide d'intégrations d'API avec divers outils (Connecteurs du graphe de services) et produits ServiceNow. Les catégories comprennent, sans s'y limiter, les suivantes :

- Expérience numérique de l'employé
- Découverte
- Gestion des points de terminaison
- IT Asset Management
- Surveillance de l'infrastructure
- Réseau
- Sécurité réseau
- Network Performance Monitoring
- Configuration et gestion des correctifs
- Protection de point de terminaison
- Fournisseur de cloud
- Application Performance Monitoring
- Services de répertoire
- Évaluation de la vulnérabilité

Installer les applications prises en charge pour Contrôle de la posture de sécurité

Les applications requises pour cette intégration sont disponibles sur le ServiceNow Store. Certaines applications ont des dépendances que vous devez télécharger et installer séparément.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : admin pour le téléchargement, l'installation et l'activation de toutes les applications.

Procédure

1. Téléchargez les applications requises à partir de dans ServiceNow Store votre ServiceNow instance.
2. Une fois les applications téléchargées, accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout**.
3. Localisez les applications que vous avez téléchargées et sélectionnez **Installer** pour les activer ainsi que leurs dépendances.
   Toutes les applications dépendantes qui sont également installées automatiquement en même temps qu'une application s'affichent dans la boîte de dialogue d'installation d'application. Toutefois, si vous êtes invité à installer des modules d'extension de dépendance pendant l'installation, suivez les invites fournies. Vérifiez que toutes les applications et dépendances répertoriées dans la table précédente sont installées et activées.

   Une boîte de dialogue s'affiche après l'activation réussie d'une application.
4. Une fois les applications installées et activées, affectez les utilisateurs aux groupes de contrôle de la posture de sécurité suivants :

   Ces groupes héritent de tous les rôles nécessaires pour lire et modifier les enregistrements SPC.
5. Modifiez les sources de données CMDB de rapprochement et recalculez-les pour définir la source de vérité pour les valeurs d'attributs.

   Le tableau de bord CMDB 360 fournit des agrégations et une analyse des données CMDB 360. CMDB 360 collecte des données sur toutes les sources de découverte qui génèrent des valeurs d'attribut pour les CI. Utilisez la vue CMDB 360 dans l'espace de travail Base de données de gestion des configurations (CMDB) pour suivre les activités et identifier les problèmes potentiels liés aux sources de découverte. Consultez Vue à 360° de CMDB dans l'espace de travail CMDB pour plus d'informations.

Connecteurs du graphe de services pour Contrôle de la posture de sécurité

Contrôle de la posture de sécurité s'appuie sur les intégrations d'API ou sur Connecteurs du graphe de services en tant que source clé pour les données d'actifs utilisées pour identifier les failles de sécurité.

Contrôle de la posture de sécurité prend actuellement en charge les connecteurs du graphe de services (SGC) qui peuvent vous fournir une grande variété de données sur vos actifs. Ces applications d'intégration sont disponibles à partir du ServiceNow Storefichier .

Choisissez les connecteurs que vous souhaitez utiliser et téléchargez les applications, puis activez-les. La liste des connecteurs pris en charge dans le magasin s'allonge à mesure que Contrôle de la posture de sécurité d'autres connecteurs sont pris en charge.

Les connecteurs du graphe de services pris en charge par Contrôle de la posture de sécurité incluent actuellement les catégories suivantes :

Une fois installés, vous pouvez afficher les connecteurs et leurs catégories sur la table des connecteurs [sn_sec_spc_core_connector] de votre instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez afficher les types d'actif et leur mappage aux classes CI et aux connecteurs dans la table [sn_sec_spc_core_asset_type_connector].

Voir Service Graph Connectors pris en charge pour Contrôle de la posture de sécurité et Logiciels pris en charge Service Graph Connectors pour Contrôle de la posture de sécurité pour plus d'informations et d'exemples de ces tableaux. Bien qu'il ne s'agisse pas de listes exhaustives, vous pouvez voir comment les connecteurs pris en charge fournissent une grande variété de données.

Contrôle de la posture de sécurité prend en charge les produits ServiceNow tels que Gestion des actifs logiciels (SAM) et Gestion des actifs matériels (HAM) que vous pouvez utiliser avec les connecteurs du graphe de services pour vous aider à rechercher toute discordance qui existe entre les logiciels installés signalés par vos produits de scanner de vulnérabilité et les logiciels signalés par les analyseurs qui sont déjà pris en compte dans SAM et d'autres produits ServiceNow.

Pour plus d'informations sur le téléchargement, la configuration et l'activation des applications prises en charge pour les connecteurs du graphe de services, consultez les rubriques suivantes :

- Connecteurs Service Graph .
- .
- .

Politiques pour Contrôle de la posture de sécurité

Les politiques auditent vos actifs en fonction des données importées à partir de vos connecteurs du graphe de services pour vous aider à trouver les violations potentielles.

Politiques

Contrôle de la posture de sécurité Les politiques sont construites sur un modèle de données actif-relations-propriétés. Certaines politiques sont incluses dans l'application, et vous pouvez créer vos propres politiques pour rechercher des critères spécifiques.

Les critères des politiques peuvent être spécifiés sous la forme de conditions sur les propriétés de cet actif ou sur les propriétés d'une entité liée. Dans le créateur de politique du module Politique et résultats de l'espace de travail, vous pouvez définir des politiques pour rechercher un type d'actif (matériel, logiciel) et une connexion (signalé, non signalé par), ou une entité (source d'actif, produit Service Graph Connector ou métadonnées CMDB), ou vous pouvez faire correspondre d'autres types de critères spécifiques.

Pour vous aider à modifier ou à créer des politiques :

- Définissez vos conditions dans le module de recherche d'actifs et recherchez des actifs par produits Service Graph Connector spécifiques ou pour les actifs dont des données spécifiques sont signalées par un connecteur. Vous pouvez enregistrer vos recherches en tant que stratégies.
- Clonez les politiques incluses dans l'application pour créer des politiques plus étendues. Vous copiez, puis affinez les conditions d'une politique existante sans avoir à les saisir à nouveau.
- Créez de nouvelles politiques (politiques enfants) à l'aide des politiques de base que vous sélectionnez comme point de départ pour de nouvelles politiques.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple d'audit de politique et de remplissage des données : classes CI dans la CMDB

Si une politique tente de récupérer une classe d'actifs signalée ou non par un connecteur du graphe de services spécifique, Contrôle de la posture de sécurité mappe toutes les classes d'éléments de configuration (CI) pertinentes associées à cette classe d'actifs dans la CMDB, qui sont renseignées ou non par ce connecteur du graphe de services ou cette catégorie de connecteur.

Par exemple, supposons qu'une politique recherche tous les actifs matériels signalés par le connecteur du graphe de services Jamf Pro. La logique suivante s'applique.

1. Security Posture Control identifie les classes CI dans la CMDB qui sont mappées à la classe « Actif matériel » pour Jamf Pro.

   Remarque : Différents connecteurs du graphe de services remplissent différentes classes CI dans la CMDB, et le mappage aux classes CI à partir de « Actif matériel » varie d'un connecteur du graphe de services à l'autre.

2. Contrôle de la posture de sécurité détermine que les classes CI, Ordinateur, Serveur et Imprimante dans la CMDB sont mappés à la classe d'actifs « Actif matériel » pour Jamf Pro de Connecteur du graphe de services.
3. Contrôle de la posture de sécurité puis interroge tous les enregistrements d'actifs renseignés dans l'une de ces trois classes CI : Serveur, Ordinateur et Imprimante par le Connecteur du graphe de services Jamf Pro dans la CMDB et renvoie ces actifs.

   La colonne « Classes CI prises en charge par SPC » dans la table suivante indique quelles classes d'enregistrements CI sont prises en compte lors d'une requête par le produit Contrôle de la posture de sécurité dans le cadre d'une évaluation de stratégie. Ce tableau n'est pas une liste exhaustive, mais vous pouvez l'utiliser pour voir comment les données ingérées provenant de différentes catégories et sources sont généralement mappées et interrogées.

Création de vos propres politiques

Reportez-vous à la section Création de vos propres politiques dans l'application Contrôle de la posture de sécurité pour en savoir plus sur la façon de créer vos propres stratégies.

Pour des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfants et clonées pour Contrôle de la posture de sécurité.

Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour en savoir plus sur les étapes nécessaires à la création d'une politique.

SGC pris en charge

Pour obtenir la liste de certains des connecteurs du graphe de services pris en charge, consultez Service Graph Connectors pris en charge pour Contrôle de la posture de sécurité et Logiciels pris en charge Service Graph Connectors pour Contrôle de la posture de sécurité.

Politiques incluses avec l'application Contrôle de la posture de sécurité

Quelques politiques incluses dans l'application sont liées à des Contrôle de la posture de sécurité cas d'utilisation importants et sont finalement affichées comme des aperçus clés sur le tableau de bord de la page de destination (module d'accueil) de l'espace de travail SPC.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage des politiques

Pour afficher ces politiques, accédez à **Espaces de travail** > **Contrôle de la posture de sécurité** > **Politiques et résultats** > **Tout**.

Ces politiques sont désactivées par défaut. Vous devez les activer avant de pouvoir afficher les résultats renvoyés (résultats). Vous ne pouvez pas modifier ces stratégies, mais vous pouvez les utiliser pour vous aider à créer d'autres stratégies en clonant leurs conditions comme point de départ. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité pour plus d'informations.

Vous pouvez configurer des aperçus ou des rapports personnalisés pour les politiques clonées, ou configurer des résultats pour ces politiques clonées afin de gérer le rattrapage. Vous pouvez également créer vos propres politiques personnalisées à partir de zéro pour surveiller la couverture des contrôles de sécurité conformément à vos besoins internes.

Une fois que vous avez cloné et activé toutes les politiques que vous créez, vous devez créer votre propre enregistrement d'aperçu personnalisé dans le module Générateur d'aperçu personnalisé de l'espace de travail (le dernier module du panneau de navigation). Ce n'est qu'à ce moment-là que vous pourrez afficher les données de vos politiques sur le tableau de bord des aperçus personnalisés (la deuxième icône en partant du haut dans l'espace de travail).

Création de vos propres politiques

Reportez-vous à la section Création de vos propres politiques dans l'application Contrôle de la posture de sécurité pour en savoir plus sur la façon de créer vos propres stratégies.

Pour des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfants et clonées pour Contrôle de la posture de sécurité.

Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour en savoir plus sur les étapes nécessaires à la création d'une politique.

Création de vos propres politiques dans l'application Contrôle de la posture de sécurité

Vous pouvez créer vos propres politiques personnalisées pour surveiller les données spécifiques aux actifs de votre environnement. Vous basez ces politiques sur des données que vous importerez à partir des différents connecteurs du graphe de services que vous avez installés et activés.

Par où commencer ?

Vous pouvez cloner les politiques existantes et y ajouter d'autres conditions, ou créer une politique à partir de zéro. Pour vos politiques personnalisées, vous pouvez inclure des critères pour les propriétés CMDB communes renseignées par différents connecteurs du graphe de services.

Vous pouvez également utiliser une politique de base comme point de départ et inclure des conditions pour les exceptions approuvées avec des politiques pour l'application Gouvernance, risque et conformité (GRC), par exemple. Ces exceptions concernent les actifs que vous ne souhaitez pas surveiller et inclure dans votre nombre d'actifs.

Pour vos stratégies personnalisées, vous pouvez inclure des conditions pour les métadonnées telles que le système d'exploitation, la version du système d'exploitation et le nom de domaine complet (FQDN), par exemple pour vous aider à surveiller les actifs avec des logiciels plus anciens. Notez que ces propriétés sont des propriétés CMDB communes renseignées par divers connecteurs du graphe de services pour un actif donné.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les types d'actifs de niveau supérieur et leurs relations, consultez Politiques incluses avec l'application Contrôle de la posture de sécurité le générateur de conditions de politique pour vos politiques.

Pour des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfants et clonées pour Contrôle de la posture de sécurité.

Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour en savoir plus sur les étapes nécessaires à la création d'une politique.

Utilisation des décorateurs ET, OU dans le générateur de conditions

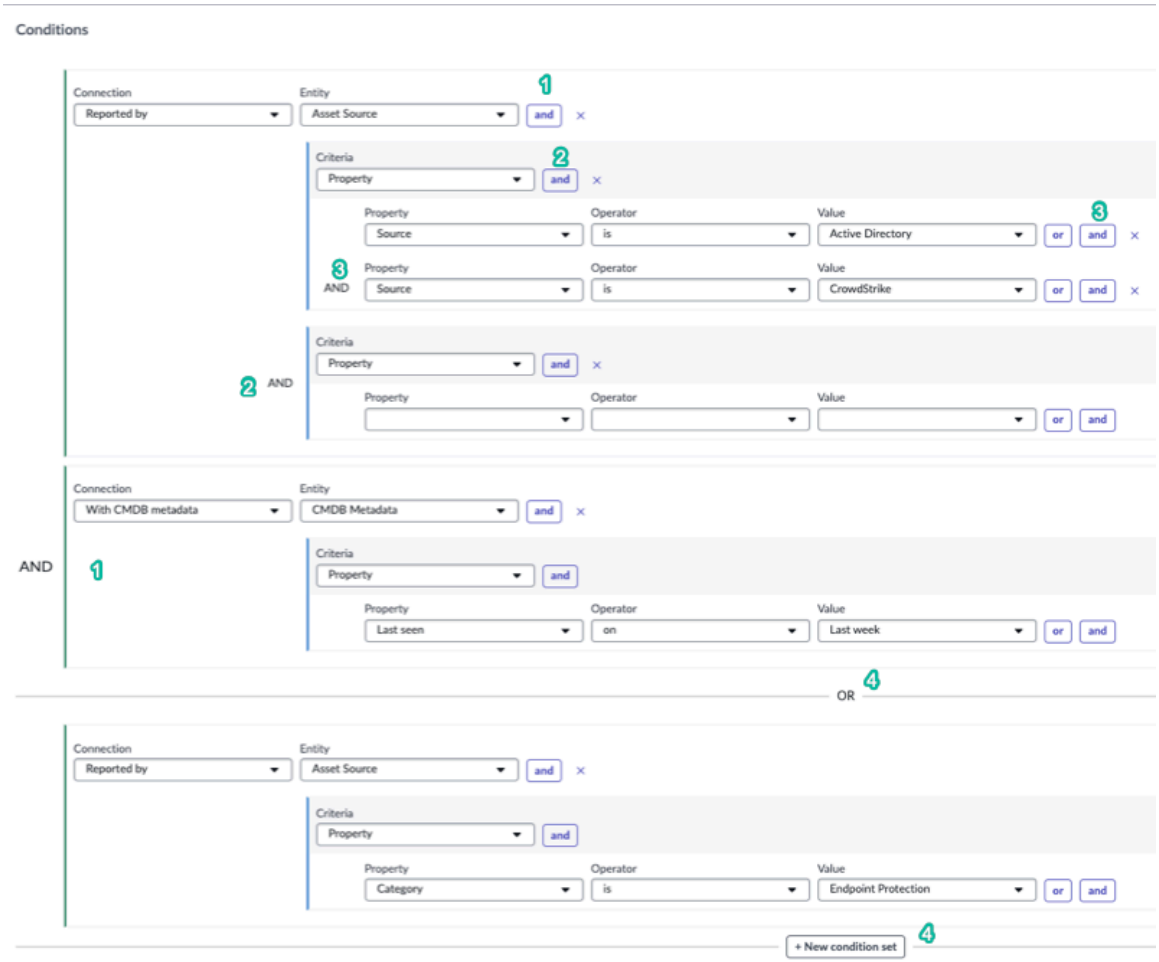
Vous naviguez des types d'actifs de niveau supérieur pour le matériel et les logiciels à leurs entités secondaires à l'aide du créateur de conditions du module Politiques et conclusions de l'espace de travail. En fonction de vos choix, des champs s'affichent pour vous et vous pouvez modifier ou ajouter des critères.

Les décorateurs AND, OR du générateur de conditions vous permettent de configurer la logique pour les données renvoyées que vous souhaitez renvoyer pour la politique.

Décorateur	Description	Numéro référencé dans l'image
Sélectionnez **ET** en regard des champs Connexion et Entité situés en haut pour le nouvel ensemble de conditions.	Ajoute un ET logique entre les critères d'entité de connexion actuels et les nouveaux critères d'une autre entité de connexion.	1
Sélectionnez **ET** à droite d'un champ Critères ou Propriété pour un nouvel ensemble de critères et de conditions de propriété.	Ajoute un ET logique entre les critères d'entité de connexion actuels et un nouveau critère sous la même entité de connexion.	2
Sélectionnez **OU/ET** à droite d'un champ de propriété pour un nouvel ensemble de conditions de propriété.	Ajoute un OR/ET logique entre la propriété actuelle et une nouvelle propriété à partir des mêmes critères d'entité de connexion.	3
Sélectionnez **+ Nouvelle condition définie** pour un nouvel ensemble de conditions.	Ajoute un OU logique entre l'ensemble de conditions de tous les critères actuels et un nouvel ensemble de conditions.	4

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Utilisation des stratégies de base, du clonage et des stratégies enfant

Vous pouvez utiliser plusieurs politiques pour évaluer vos actifs et créer vos propres aperçus personnalisés. Vous disposez des options suivantes pour vous aider à créer rapidement des politiques existantes personnalisées ou à modifier les politiques existantes :

- Cloner la politique : créer une copie d'une politique. Le nom de la politique et ses conditions sont affichés avec un « copie » dans le titre. Les conditions sont affichées et vous pouvez les modifier. Consultez Modifier une politique activée dans Contrôle de la posture de sécurité.
- Créer une politique enfant : le nom de la politique à partir de laquelle vous avez commencé s'affiche sous la forme « Politique de base » dans le nouvel enregistrement. Les conditions de votre politique de base sont héritées dans la nouvelle politique et un nouvel ensemble de conditions vide s'affiche. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité.
- Politiques d'exclusion : ajoutez des politiques à vos politiques personnalisées afin que les résultats d'actifs des politiques que vous sélectionnez soient exclus de vos résultats. Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité.

Métadonnées et filtrage CMDB

Il peut être important pour vos équipes de sécurité de surveiller les actifs dotés de logiciels plus anciens. Vous pouvez spécifier des critères de politique commençant par la connexion « Avec métadonnées CMDB » après le type d'actif matériel pour inclure les propriétés communes répertoriées ci-dessous. Il ne s'agit pas d'une liste exhaustive. Pour collecter

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ces métadonnées, les propriétés doivent être disponibles à partir de la connexion de métadonnées CMDB renseignée par vos connecteurs du graphe de services.

- RAM
- Nom d'hôte
- Numéro de série
- Domaine SE
- Version de SE
- Espace disque
- Dernier observé
- Systèmes d'exploitation
- Premier observé
- Nombre de processeurs
- Fabricant MAC
- Carte réseau
- Adresse IP
- Emplacement
- FQDN
- Masque réseau
- Version IP
- Type de numéro de série
- Service Pack du système d'exploitation

À partir de la v3.0 de Contrôle de la posture de sécurité:

La connexion « Avec les métadonnées CMDB » vous permet d'ajouter la propriété de nom d'hôte et d'utiliser l'opérateur regex des correspondances pour vous aider à saisir des expressions régulières dans vos conditions pour le type d'actif matériel. Par exemple, si vous saisissez « lp », vous pouvez rechercher tous les ordinateurs portables dont les deuxième et troisième caractères du nom d'hôte sont « lp ».

« Premier vu » : actifs qui ont été découverts pour la première fois par n'importe quelle source dans le délai que vous sélectionnez avec la propriété d'horodatage « Premier vu ».

« Dernier observé » : actifs qui ont été « Vus pour la dernière fois au cours des n derniers jours » par n'importe quelle source. Entrez le nombre de jours jusqu'à 30 comme valeur. Par exemple, entrez 3 comme valeur pour surveiller les actifs par « dernière connexion » à partir d'Active Directory au cours des trois derniers jours.

Type d'actif logiciel : recherchez les éditeurs de logiciels ou utilisez les SGC que vous avez installés pour importer les données et métadonnées logicielles que vous souhaitez si vous commencez par la connexion « Avec les détails du logiciel ».

Pour les types d'actifs matériels, vous pouvez utiliser la connexion « A des informations sur le modèle » avec la connexion « Avec métadonnées CMDB » pour les appareils en fonction de modèles et d'informations de modèle spécifiques.

Les types d'actifs matériels vous permettent également de rechercher tous les actifs signalés par une source, Qualys par exemple, mais qui ne sont pas signalés par ServiceNow ITOM Discovery.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Reportez-vous à la rubrique Politiques pour Contrôle de la posture de sécurité pour plus d'informations sur le schéma de Contrôle de la posture de sécurité stratégie.

Exceptions avec l'application Governance, Risk, and Compliance (GRC)

Une exception de Gestion intégrée des risques (IRM) est un actif avec une exception approuvée du produit Gouvernance, risque et conformité (GRC). Vous avez la possibilité, dans une stratégie, d'ajouter une condition pour une exception afin de ne pas surveiller ces actifs et de les inclure dans vos décomptes.

Par exemple, certains actifs peuvent avoir des exceptions approuvées pour certains objectifs de contrôle avec IRM. Pour réduire le nombre de correspondances renvoyées, les équipes de sécurité de l'information peuvent exclure ces actifs de la surveillance des contrôles de sécurité avec des exceptions IRM déjà approuvées.

Aperçus clés et aperçus configurés pour Contrôle de la posture de sécurité

Les aperçus clés et configurés (personnalisés) vous fournissent des rapports visuels créés et mis à jour en fonction des critères d'évaluation qui correspondent à vos actifs. Les aperçus vous aident à surveiller les mesures des contrôles de sécurité sur un tableau de bord.

Aperçus clés

Les critères utilisés pour les évaluations de vos actifs sont fournis par les polices incluses dans la demande.

- Les aperçus clés utilisent les politiques incluses dans l'application.
- Les aperçus configurés peuvent être créés à l'aide des politiques fournies avec l'application, de vos propres politiques personnalisées ou d'une combinaison des deux.

Sur la page d'accueil (page de destination) de l'espace de travail Contrôle de la posture de sécurité, la section Aperçus clés située sous la Vue d'ensemble affiche des rapports visuels créés et mis à jour par les politiques incluses dans l'application. Ces aperçus sont également inclus dans l'application et affichent les informations suivantes :

- Agent de protection du point de terminaison installé : nombre total d'actifs qui ont ou n'ont pas de protection du point de terminaison.
- Couverture des appareils gérés : nombre d'actifs gérés par rapport à ceux qui ne le sont pas.
- Couverture de l'analyse de vulnérabilité : nombre total d'actifs analysés par rapport à ceux qui ne sont pas analysés pour détecter les vulnérabilités connues par un scanner de vulnérabilité tiers.
- Actifs présentant des vulnérabilités critiques : nombre d'actifs sur le nombre total d'actifs présentant des vulnérabilités critiques.
- Éléments vulnérables par criticité : nombre total d'éléments vulnérables répartis par gravité. Une vulnérabilité connue qui correspond à un actif de votre CMDB entraîne un élément vulnérable. Cet aperçu nécessite l'installation de l'application Vulnerability Response et d'au moins une intégration de scanner : Qualys, Rapid7 ou Tenable Vulnerability Integration. Toutes ces applications sont disponibles sur le ServiceNow® Storefichier .
- 3 principales politiques par résultats : politiques qui renvoient le plus de résultats (correspondances) sur vos actifs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus configurés

Vous pouvez créer vos propres aperçus si vous souhaitez plus d'informations qui ne se trouvent pas dans les aperçus clés. Vous pouvez créer ces aperçus configurés et utiliser des politiques existantes ou vos propres politiques personnalisées pour l'évaluation. Vos aperçus configurés s'affichent dans le module Tableau de bord des aperçus configurés, la deuxième icône en partant du haut dans l'espace de travail.

Les types d'aperçus suivants peuvent être configurés.

- Tableau comparatif : comparez les résultats de plusieurs politiques à l'aide d'histogrammes.
- Widget du nombre de correspondances de politique : affichez le nombre d'appareils qui correspondent à une politique.
- Graphique des pourcentages de correspondance avec les politiques : affichez le pourcentage d'appareils qui correspondent à une politique dans un graphique à secteurs. Vous pouvez choisir le pool d'actifs total comme tous les actifs surveillés par SPC ou les actifs qui correspondent à la politique de base à partir de laquelle la politique sélectionnée actuelle est créée.
- Graphique des tendances des polices : affichez les tendances des actifs qui correspondent à différentes stratégies.

Groupes

Vous devez créer ou affecter des groupes à vos aperçus configurés lorsque vous créez de nouveaux enregistrements dans le module Générateur d'aperçu personnalisé. Les groupes vous permettent d'organiser vos rapports sur le tableau de bord Aperçus configurés.

Utilisation de l'espace de Contrôle de la posture de sécurité travail

L'espace Contrôle de la posture de sécurité de travail contient les modules que vous utilisez pour configurer, utiliser et surveiller les données importées sur vos actifs.

Les modules de l'espace de travail

Pour accéder à l'espace de travail, accédez à **Espaces de travail** > **Contrôle de la posture de sécurité** La page d'accueil (page de destination) s'affiche. L'espace Contrôle de la posture de sécurité de travail contient les modules suivants.

Modules

Module	Description
Accueil	Affichez des visualisations de données et d'autres informations dans les sections Vue d'ensemble, Aperçus clés et Couverture du cas d'utilisation clé pour vous aider à surveiller vos actifs. Les informations fournies sur cette page vous permettent de rendre compte de l'état de votre posture de sécurité globale aux responsables informatique, IT et sécurité, ainsi qu'à d'autres personnes concernées clés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modules (suite)

Module	Description
	Consultez Aperçus clés et aperçus configurés pour Contrôle de la posture de sécurité et Politiques pour Contrôle de la posture de sécurité.
Aperçus configurés	Affichez les visualisations de données relatives à vos actifs que vous créez, configurez et activez. Consultez Aperçus clés et aperçus configurés pour Contrôle de la posture de sécurité.
Recherche d'actifs	Recherchez rapidement des actifs dans votre environnement en fonction des conditions que vous définissez. Vérifiez que vous pouvez localiser les actifs avec un ensemble de conditions avant de valider ces conditions dans une politique. Vous pouvez affiner ces recherches afin d'obtenir un aperçu des ressources qui correspondent à vos critères de recherche. Lorsque vous êtes prêt, vous pouvez enregistrer vos conditions en tant que politique. Consultez Créer une recherche d'actifs dans Contrôle de la posture de sécurité.
Politiques et résultats	Créez, clonez, modifiez et activez des politiques. Certaines politiques sont incluses dans l'application, et vous pouvez créer les vôtres. Les politiques auditent vos actifs pour trouver des correspondances avec des violations potentielles. Les aperçus, les visualisations et les cas d'utilisation dépendent des politiques. Consultez Politiques pour Contrôle de la posture de sécurité. Les actifs qui correspondent aux conditions de la politique sont signalés comme des résultats et mappés à l'application pour y Conformité de la configuration remédier. Consultez Afficher les résultats pour Contrôle de la posture de sécurité.
Configuration des connecteurs et des tickets d'utilisation	Activez et consultez l'état des connecteurs du graphe de services (SGC) et des intégrations d'API installés. Connecteurs du

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modules (suite)

Module	Description
	graphe de services et intégrations d'API sont des sources que vous utilisez pour importer des données relatives à vos actifs. Une grande variété de (SGC) sont pris en charge et sont disponibles depuis le ServiceNow® Store. Configurez et surveillez les cas d'utilisation clés. Les cas d'utilisation sont différents scénarios que vous configurez pour vous aider à identifier des types spécifiques d'écarts de couverture d'outils. Chaque cas d'utilisation nécessite une ou plusieurs politiques pour auditer vos actifs afin de détecter d'éventuelles violations. Consultez Cas d'utilisation, exemples de politiques et connecteurs du graphe de services pris en charge dans Contrôle de la posture de sécurité.
Générateur d'aperçus personnalisés	Créez vos propres visualisations de données. Les aperçus personnalisés vous fournissent des rapports visuels qui sont mis à jour en fonction des résultats d'audit de vos polices et des données importées. Une fois que vous les avez activés, vos aperçus personnalisés s'affichent sur le tableau de bord dans le module Aperçus configurés. Vous pouvez déterminer où les données d'un aperçu sont affichées sur le tableau de bord à l'aide de Groupes. Consultez Créer et activer un aperçu configuré pour Contrôle de la posture de sécurité.

Utilisation des modules de l'espace de travail pour identifier les lacunes dans la couverture des outils

Pour identifier les failles des outils de Security, vous devez procéder comme suit.

1. Configurez et activez les connexions d'API avec l'un des outils que vous utilisez dans différentes catégories. Vous pouvez utiliser Connecteurs du graphe de services pour les produits disponibles dans ServiceNow Store pour les connexions d'API requises. Pour plus d'informations sur les connecteurs du graphe de services pris en charge, consultez Connecteurs du graphe de services pour Contrôle de la posture de sécurité et Connecteurs Service Graph . Les connecteurs du graphe de services pris en charge sont disponibles auprès de avec ServiceNow® Store des abonnements distincts.
2. Effectuez une ou plusieurs recherches d'actifs en fonction de critères spécifiques pour obtenir un inventaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Activez les politiques fournies avec l'application Contrôle de la posture de sécurité. Vous pouvez également créer vos propres politiques et les activer en fonction des résultats de vos recherches d'actifs.
4. Créez et activez vos propres aperçus configurés pour vous aider à surveiller vos actifs.
5. Configurez des règles pour automatiser le workflow de rattrapage dans l'application Configuration Compliance.

L'identification des failles des outils de Security implique les étapes suivantes :

1. Activez les politiques fournies avec l'application Contrôle de la posture de sécurité . Le Contrôle de la posture de sécurité produit détecte les lacunes des outils de Security en effectuant les tâches suivantes :
   a. Identifie la liste de tous les actifs uniques renseignée par divers connecteurs du graphe de services dans la CMDB.
   b. Identifie les actifs qui ne sont pas signalés par des catégories spécifiques de ce pool d'actifs, par exemple, Protection des points de terminaison. Les actifs sont identifiés en fonction de la politique active en cours d'évaluation.
   c. Les actifs identifiés comme non déclarés par des catégories spécifiques sont signalés en tant que « Résultats » ou « Résultats des tests » dans l'application Conformité de la configuration .
2. Affectez automatiquement des « résultats » à différentes équipes pour le rattrapage avec l'application Configuration Compliance.

Création de vos propres politiques

Reportez-vous à la section Création de vos propres politiques dans l'application Contrôle de la posture de sécurité pour en savoir plus sur la façon de créer vos propres stratégies.

Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour en savoir plus sur les étapes nécessaires à la création d'une politique.

Pour des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfants et clonées pour Contrôle de la posture de sécurité.

Activer une politique incluse dans l'application Contrôle de la posture de sécurité

Les politiques incluses dans l'application doivent être activées avant de Contrôle de la posture de sécurité pouvoir surveiller les actifs correspondants à cette politique. Par défaut, aucune des politiques incluses dans l'application n'est activée.

Avant de commencer

Vous devez vérifier que toutes les conditions préalables requises sont remplies avant d'activer les politiques incluses dans l'application.

- Vérifiez que Connecteur du graphe de services est activé.
- Vérifiez que toutes les applications requises, telles que Vulnerability Response, sont installées et activées, le cas échéant.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Vous ne pouvez pas modifier les stratégies incluses dans l'application, mais vous pouvez créer de nouvelles stratégies en fonction de leurs critères à l'aide des fonctionnalités **Cloner la stratégie** et **Créer une stratégie enfant** . Ces fonctionnalités sont disponibles dans le menu Plus d'options (trois points verticaux).

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Politiques et résultats** > **Tout**.

   Pour déterminer si une politique est activée, confirmez son état (`vrai` ou `faux`) dans la colonne Actif.

2. Sélectionnez un enregistrement de politique pour l'ouvrir.
3. Vous disposez des options suivantes sur les enregistrements de police qui sont inclus dans l'application :

Option	Description
Activer la politique	Activez une politique si vous souhaitez surveiller tous les actifs qui correspondent aux conditions de la politique et générer des résultats. Le cas échéant, sélectionnez Désactiver la politique pour arrêter les évaluations des actifs et la génération de résultats pour cette politique.
Configurer les résultats	Sélectionnez **Oui** dans le modal pour générer des conclusions pour la politique. Sélectionnez le lien **Configurer les règles d'affectation** pour configurer des règles d'affectation dans l'application Configuration Compliance afin d'affecter des résultats pour votre politique de résolution. **Remarque :** Pour les politiques que vous créez avec « Logiciel » comme type d'actif, vous pouvez enregistrer la politique et créer des aperçus personnalisés, mais vous ne pouvez pas configurer les résultats à partir de l'enregistrement de politique.
Cloner la politique	Créez une nouvelle politique avec toutes les conditions de la politique affichée comme point de départ.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour plus d'informations.
Créer une politique enfant	Créez une politique enfant qui hérite des conditions de la politique actuelle. Les conditions de politique actuelles sont affichées dans le champ « Politique de base » du nouvel enregistrement, et vous ajoutez d'autres conditions.
Désactiver la politique (affiché uniquement sur les politiques activées)	Désactivez une politique active si vous ne souhaitez pas que des actifs soient surveillés ou évalués par rapport à cette politique. Cette option de modification n'est visible que sur les enregistrements de politique activés.
Afficher les résultats	Ouvrez un nouvel onglet et affichez les actifs correspondants le cas échéant. Les résultats sont également référés aux CTR, ou enregistrements de résultats des tests pour la politique.

Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité

Créez vos propres polices personnalisées pour surveiller les actifs au niveau de la couverture des outils et d'autres combinaisons à haut risque.

Avant de commencer

Pour vous aider à comprendre les étapes requises pour créer une politique avec plus de détails, reportez-vous à Exemples de politiques de base, enfants et clonées pour Contrôle de la posture de sécurité. Les exemples vous guident tout au long des étapes requises pour créer une politique de base, utiliser la stratégie de base pour créer une politique enfant et cloner une politique.

Pour des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfants et clonées pour Contrôle de la posture de sécurité.

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Liste** > **Politiques** > **Tout**.
2. Sélectionnez **Nouvelle stratégie**.
3. Sélectionnez l'icône du crayon en regard du nom en haut pour modifier les métadonnées.

   Renseignez les champs.

Champ	Description
Nom	Nom unique pour votre police.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Criticité	Sélectionnez-en un dans la liste.
Description brève	Description unique de votre police.

4. Sélectionnez **Enregistrer les métadonnées**.
5. Pour Type d'actif, sélectionnez Activé dans la liste.

Option de l'entité	Description de l'entité
Matériel	Localisez les périphériques IP qui comprennent des appareils informatiques personnels, des ordinateurs virtuels dans le cloud, des serveurs, des périphériques réseau et d'autres matériels.
Logiciel	Localisez les logiciels installés sur les appareils signalés par les SGC et vos scanners de vulnérabilité.

6. Facultatif : Choisissez aucun, l'un ou les deux.

Option	Description
Politique de base	Les conditions de votre choix de politique de base sont héritées dans la nouvelle police.
Politiques d'exclusion	Sélectionnez toutes les politiques que vous souhaitez exclure des résultats d'actif pour cette politique. Les résultats de ces politiques sont ignorés.

(Optional) Les champs Connection (Connexion) et Entity (Entité) s'affichent.

7. Sélectionnez-en un dans la liste pour le champ Connexion.
Le champ Entité cible est renseigné automatiquement en fonction de votre choix. Un nouveau champ Critères s'affiche avec les champs Propriété, Opérateur et Valeur.
Pour plus d'informations sur les types d'actifs et le schéma des relations, reportez-vous à Politiques pour Contrôle de la posture de sécurité.
8. Sélectionnez-en un dans la liste des propriétés.
9. Sélectionnez **Catégorie** ou **Source**.
10. Sélectionnez un opérateur et entrez une catégorie de connecteur, par exemple, Gestion des points de terminaison, ou une catégorie nom de produit (source).
11. Facultatif : Utilisez le Créateur de conditions et ajoutez d'autres conditions ou ensembles de conditions.

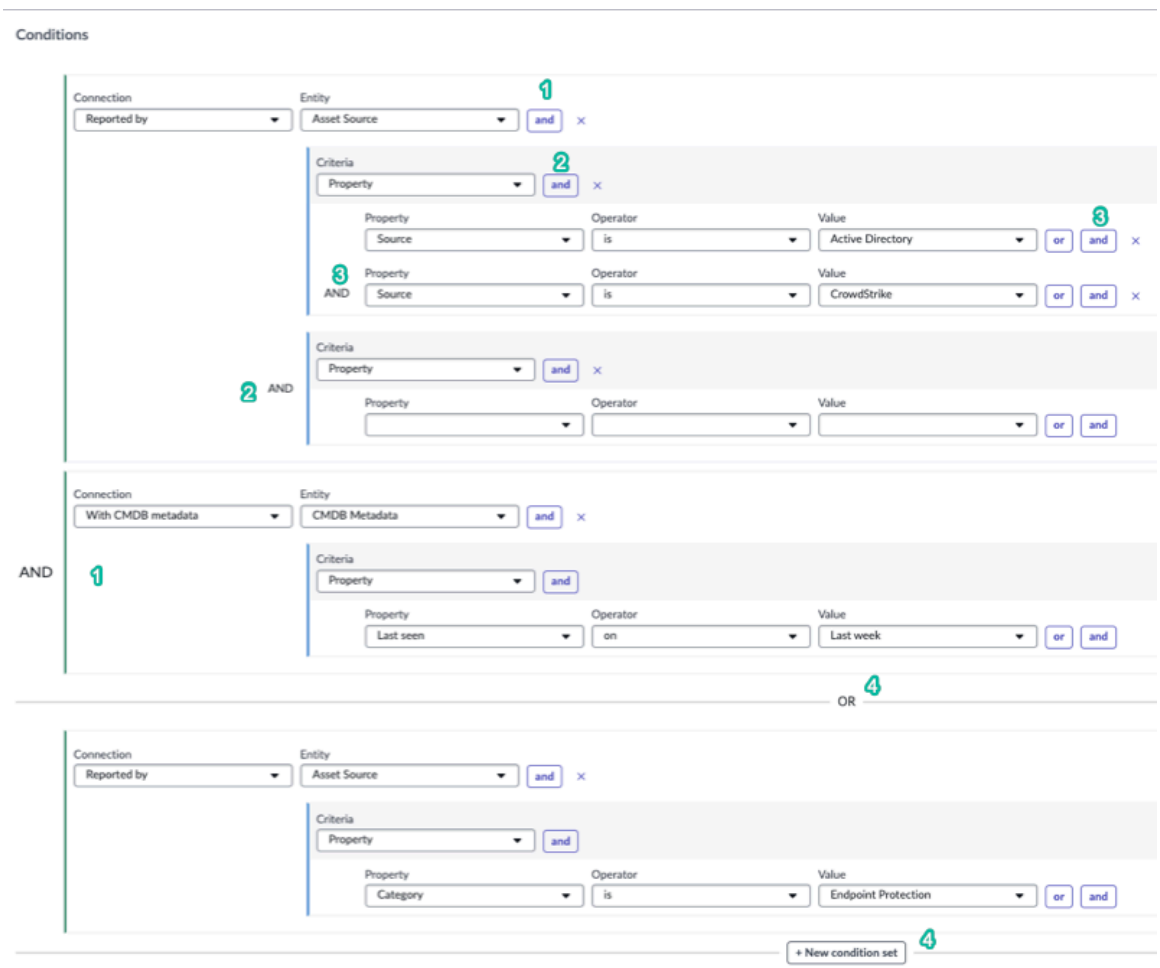
    (Optional) Vous naviguez des types d'actifs de niveau supérieur pour le matériel et les logiciels vers leurs entités secondaires à l'aide du Créateur de conditions. En fonction de vos choix, des champs s'affichent pour vous et vous pouvez modifier ou ajouter des critères.

    Les décorateurs AND, OR du générateur de conditions vous permettent de configurer la logique pour les données renvoyées que vous souhaitez renvoyer pour la politique. Reportez-vous au tableau et à l'image suivants pour plus d'informations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Décorateur	Description	Numéro référencé dans l'image
Sélectionnez **ET** en regard des champs Connexion et Entité situés en haut pour le nouvel ensemble de conditions.	Ajoute un ET logique entre les critères d'entité de connexion actuels et les nouveaux critères d'une autre entité de connexion.	1
Sélectionnez **ET** à droite d'un champ Critères ou Propriété pour un nouvel ensemble de critères et de conditions de propriété.	Ajoute un ET logique entre les critères d'entité de connexion actuels et un nouveau critère sous la même entité de connexion.	2
Sélectionnez **OU/ET** à droite d'un champ de propriété pour un nouvel ensemble de conditions de propriété.	Ajoute un OR/ET logique entre la propriété actuelle et une nouvelle propriété à partir des mêmes critères d'entité de connexion.	3
Sélectionnez **+ Nouvelle condition définie** pour un nouvel ensemble de conditions.	Ajoute un OU logique entre l'ensemble de conditions de tous les critères actuels et un nouvel ensemble de conditions.	4



12. Sélectionnez **Enregistrer la politique** une fois la modification terminée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Votre politique est enregistrée. Vous pouvez choisir de l'activer maintenant ou de revenir plus tard pour l'activer.

13. Dans le menu Autres options en regard de **Enregistrer la politique**, sélectionnez configurer les résultats.
14. Renseignez les champs.

Option	Description
Générer des conclusions pour cette politique ?	Choisissez **Oui** pour générer des résultats pour les actifs correspondants. Une fois les données importées, l'option Afficher les résultats s'affiche dans l'enregistrement de politique. Choisissez **Non** si vous ne souhaitez pas générer de résultats.
Configurer les règles d'affectation	Sélectionnez le lien pour configurer des règles d'affectation afin d'affecter des résultats pour le rattrapage dans l'application Configuration Compliance. Il existe une règle d'affectation par défaut dans la table [sn_vulc_assignment_rule_list] que vous pouvez utiliser dans Configuration Compliance.

15. Sélectionnez **Enregistrer la configuration**.

Une fois que vous avez enregistré et activé une politique, elle évalue les données importées à partir du connecteur du graphe de services planifiée lors de la prochaine exécution. Si vous souhaitez afficher les données sur le tableau de bord des aperçus configurés dans l'espace de travail, vous devez créer un nouvel aperçu dans le module Générateur d'aperçus personnalisé. Une fois que vous avez activé l'aperçu configuré, ses données sont affichées sur le tableau de bord Aperçus configurés dans l'espace de travail.

Modifier une politique activée dans Contrôle de la posture de sécurité

Vous pouvez modifier les politiques activées pour personnaliser leurs conditions afin qu'elles correspondent mieux à vos actifs.

Avant de commencer

Vous ne pouvez pas modifier les politiques incluses dans l'application, mais vous pouvez les cloner et en créer des enfants. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité.

Si vous modifiez les politiques et publiez vos changements, les versions sont suivies et les numéros de version sont affichés sur l'enregistrement de politique et ses résultats des tests associés.

Avant de modifier une stratégie activée, il peut être préférable de la désactiver afin qu'elle ne continue pas d'évaluer vos actifs pendant que vous le modifiez.

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Liste** > **Politiques** > **Tout**.
2. Sélectionnez un enregistrement de politique pour l'ouvrir.
3. Sélectionnez **Modifier la stratégie**.
   Si vous effectuez une première modification, deux boutons désactivés s'affichent à côté du bouton Quitter le **mode d'édition** actif : **Enregistrer les modifications** et **Publier les modifications**. Si vous avez déjà modifié cette politique et l'avez enregistrée en tant que brouillon, la notification « `Vous avez une modification non publiée` » s'affiche également.
4. Apportez vos modifications et choisissez-en une pour continuer.

Option	Description
Enregistrer les changements	Enregistrez vos modifications en tant que brouillon et revenez au mode d'édition. Vos changements ne sont pas publiés à ce stade, et vous pouvez revenir à la politique et continuer la modification ultérieurement.
Publier les changements	Publiez vos changements en tant que nouvelle version de la stratégie et quittez automatiquement le mode de modification. Il peut s'écouler un certain temps avant que les résultats ne s'affichent sur votre nouvelle version de la politique sur le bouton Afficher les résultats de la politique. Si vous publiez une nouvelle version d'une politique, vous avez la possibilité de fermer tous les résultats existants pour la politique que vous avez modifiée. Vous préférerez peut-être fermer les conclusions existantes de la politique d'origine si vous souhaitez uniquement afficher les conclusions de votre politique modifiée. Si vous annulez à ce stade ou si vous quittez le mode de modification, un message s'affiche indiquant que vous avez une modification non publiée pour cette politique. Si vous choisissez de fermer ses résultats des tests connexes existants (résultats), les états des résultats des tests et des tâches de rattrapage passent en fonction des processus de transition d'état de l'application Configuration Compliance. Consultez Transitions d'état des résultats des tests et des tâches de rattrapage dans

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	l'application Contrôle de la posture de sécurité pour plus d'informations.
Afficher l'historique des versions	Pour les changements publiés, les versions font l'objet d'un suivi et les numéros de version sont affichés sur l'enregistrement de politique et ses résultats des tests connexes.
Quitter le mode de modification	Quittez sans enregistrer vos changements ou enregistrez vos changements et quittez sans publier. Si vous enregistrez vos changements et ne les publiez pas, vous devez publier votre nouvelle version avant de pouvoir créer des résultats.
Désactiver la politique (affiché uniquement sur les politiques activées)	Désactivez une politique active si vous ne souhaitez pas que des actifs soient surveillés ou évalués par rapport à cette politique. Cette option de modification n'est visible que sur les enregistrements de politique actifs.
Afficher les résultats	Ouvrez un nouvel onglet et affichez les actifs correspondants le cas échéant. Les résultats sont également renvoyés aux CTR ou aux enregistrements de résultats des tests pour la politique.

5. Une fois que vous avez enregistré la politique en tant que brouillon et quitté le mode de modification, sélectionnez l'une des options suivantes :

Option	Description
Modifier la politique	Revenez au mode d'édition.
Désactiver la politique (affiché uniquement sur les politiques activées)	Désactivez une politique active si vous ne souhaitez pas que des actifs soient surveillés ou évalués par rapport à cette politique. Cette option n'est visible que sur les enregistrements de politique actifs.
Menu Autres options	
Configurer les résultats	Sélectionnez **Oui** dans le modal pour générer des conclusions pour la politique. Consultez Afficher les résultats pour Contrôle de la posture de sécurité.
Cloner la politique	Créez une copie de l'enregistrement de politique. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité.
Créer une politique enfant	Créez une nouvelle politique en utilisant cette politique comme base. Consultez Cloner une politique ou créer une politique

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	enfant dans Contrôle de la posture de sécurité.
Supprimer la politique	Supprimer l'enregistrement de politique de la liste de politiques.
Afficher les résultats	Ouvrez un nouvel onglet et affichez les actifs correspondants le cas échéant. Les résultats sont également renvoyés aux dossiers de résultats des tests (CTR) pour la politique.
Afficher les enregistrements liés	Pour les politiques publiées, affichez les aperçus personnalisés, le cas échéant. Reportez-vous à la rubrique Créer et activer un aperçu configuré pour Contrôle de la posture de sécurité.

Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité

Clonez une stratégie existante et ajoutez-y des conditions pour créer votre propre stratégie personnalisée. Vous pouvez également créer des politiques enfants à partir de politiques existantes.

Avant de commencer

Vous pouvez cloner des stratégies pour créer vos propres stratégies personnalisées. Vous pouvez cloner une politique ou créer une politique enfant en utilisant n'importe quelle politique comme base pour vous aider à étendre les politiques existantes sans avoir à saisir à nouveau les conditions. Toutes les conditions de la politique de base sont également héritées dans la politique enfant. Consultez Cloner une politique pour Contrôle de la posture de sécurité (exemple) pour plus d'informations.

Vous pouvez cloner toutes les politiques incluses dans l'application, mais les correspondances de politique ne sont pas reflétées en tant qu'aperçus clés dans le tableau de bord de la page de destination de l'accueil. Seuls les aperçus clés pour les politiques incluses dans l'application sont affichés sur la page de destination d'accueil.

Après avoir cloné et activé toutes les politiques que vous créez, vous devez créer votre propre enregistrement d'aperçu configuré dans le module Générateur d'aperçu personnalisé de l'espace de travail (le dernier module du panneau de navigation). Ce n'est qu'à ce moment-là que vous pouvez afficher les données de vos politiques sur le tableau de bord Aperçus configurés (la deuxième icône en partant du haut dans l'espace de travail).

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Liste** > **Politiques** > **Tout**.
2. Sélectionnez l'enregistrement de politique que vous souhaitez cloner.
3. Sélectionnez-en une dans le menu Autres options en regard de **Activer la stratégie**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Cloner la politique	Sélectionnez cette option si vous souhaitez utiliser les conditions d'une politique existante comme point de départ pour votre nouvelle politique. Un nouvel onglet contenant l'enregistrement de politique cloné s'affiche avec « copie » dans le nom. (Facultatif) Sélectionnez Politique de base et ajoutez-en une dans la liste pour votre nouvelle politique.
Créer une politique enfant	Sélectionnez cette option si vous souhaitez créer une nouvelle politique en utilisant la politique actuelle comme point de départ. Un nouvel onglet avec un enregistrement de politique vide avec une politique de base que vous choisissez s'affiche.

4. Facultatif : Sélectionnez **une politique de base** , puis sélectionnez une politique comme base de votre nouvelle politique.

   (Optional) Vous pouvez choisir cette option si vous souhaitez hériter des conditions d'une police existante comme point de départ pour votre nouvelle police.

5. Facultatif : Sélectionnez **Politiques d'exclusion** , puis sélectionnez les politiques que vous souhaitez exclure des conclusions de cette politique.
   Les résultats de votre nouvelle politique qui correspondent à des politiques exclues ne sont pas inclus dans vos résultats.
6. Dans le cas d'une stratégie clonée, modifiez les conditions.
   Pour plus d'informations sur les relations Ressource-connexion-entité dans le générateur de conditions, reportez-vous à la section Politiques pour Contrôle de la posture de sécurité.
   Pour plus d'informations sur les décorateurs dans le générateur de conditions, reportez-vous à la section Création de vos propres politiques dans l'application Contrôle de la posture de sécurité.
7. Modifiez et enregistrez votre stratégie à l'aide **de la commande Enregistrer les modifications**.
   Votre politique s'affiche dans la liste Tout du module Liste de l'espace de travail.
8. Pour activer une stratégie, suivez les étapes décrites à la rubrique Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité.
9. Facultatif : Sélectionnez Supprimer la politique pour supprimer une politique.
   L'option de suppression n'est pas prise en charge pour les politiques fournies avec l'application ou pour les politiques qui ont généré des résultats. Vous ne pouvez désactiver les politiques qu'avec des résultats.

Créer et activer un aperçu configuré pour Contrôle de la posture de sécurité

Vous pouvez créer vos propres aperçus. Les aperçus configurés sont des aperçus que vous pouvez créer à l'aide de politiques existantes ou de vos propres politiques personnalisées.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Vous devez créer un enregistrement d'aperçu et l'activer avant de pouvoir afficher vos données sur le tableau de bord des aperçus configurés. Vous pouvez avoir jusqu'à six aperçus et 21 graphiques sur le module de tableau de bord d'aperçus configuré dans l'espace de travail.

Toutes les politiques que vous utilisez pour un aperçu personnalisé doivent être activées.

Pour les politiques que vous créez avec « Logiciel » comme type d'actif, vous pouvez enregistrer la politique et créer des aperçus personnalisés, mais vous ne pouvez pas configurer les résultats à partir de l'enregistrement de politique.

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Générateur d'aperçus personnalisés** (dernière icône dans l'espace de travail).

   Sur cette page de destination, il y a trois onglets :

   Actif

   Vos aperçus personnalisés activés. Les aperçus personnalisés activés s'affichent sur la page de destination Aperçus configurés (deuxième icône en partant du haut dans l'espace de travail).

   Inactif

   Vos aperçus personnalisés inactifs. Les aperçus désactivés ne s'affichent pas sur la page de destination Aperçus configurés tant que les aperçus et les politiques de prise en charge qu'ils prennent en charge ne sont pas activés.

   Tout

   Tous vos aperçus configurés actifs et inactifs.

2. Sélectionnez **Nouvel aperçu** à droite de la page pour créer un nouvel enregistrement.
3. Dans le champ Type, sélectionnez un aperçu dans la liste de choix.

Option	Description
Tableau comparatif	Comparez les nombres d'actifs correspondants pour un maximum de cinq politiques.
Widget du nombre de correspondances de politique	Nombre total de vos actifs qui correspondent à une ou plusieurs politiques.
Graphique des pourcentages de correspondance avec les politiques	Pourcentage de vos actifs totaux qui correspondent ou non à une politique.
Graphique des tendances de correspondance avec les politiques	Tendance historique des actifs qui correspondent à une ou plusieurs stratégies.

4. Sélectionnez-en un.
   - Actif matériel
   - Logiciel
5. Sélectionnez des groupes pour votre aperçu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un aperçu doit appartenir à au moins un groupe. Vous devez créer ou affecter des groupes à vos aperçus configurés lorsque vous créez de nouveaux enregistrements dans le module Générateur d'aperçu personnalisé. Les groupes vous permettent d'organiser vos rapports sur le tableau de bord Aperçus configurés.

6. Sélectionnez les politiques et les étiquettes d'aperçu que vous souhaitez pour vos données d'aperçu.
7. Sélectionnez **Enregistrer**.
   Votre aperçu est enregistré dans l'onglet Aperçu inactif.
8. Pour activer votre nouvel aperçu, ouvrez l'enregistrement dans la liste Inactive et sélectionnez **Activer**.
   Les données sont collectées à partir de la prochaine importation planifiée pour les connecteurs du graphe de services associés aux politiques de l'aperçu, et les données sont affichées sur le module de tableau de bord des aperçus personnalisés dans l'espace de travail.

Afficher les résultats pour Contrôle de la posture de sécurité

Vous pouvez afficher les résultats générés par l'évaluation des politiques dans Contrôle de la posture de sécurité l'espace Contrôle de la posture de sécurité de travail.

Où afficher les résultats

Vous disposez des options suivantes pour afficher les résultats générés par l'évaluation des politiques.

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

- Accédez à la **Espace de travail pour le contrôle de la posture de sécurité** > **Politiques et résultats** > **Conclusions** > **Tout.**
- Dans un enregistrement de politique, sélectionnez **Afficher les résultats**. La liste affiche des groupes de résultats qui les organisent en catégories générales telles que « Combinaison à haut risque », « Exposition à Internet », etc., mais ces groupes ne sont pas des groupes formels pouvant être utilisés pour la correction. Vous devez configurer des règles de rattrapage et d'affectation dans Configuration Compliance pour les résultats.
- Dans l'application Configuration Compliance, sélectionnez **Résultats des tests** et filtrez les enregistrements par **La source est ServiceNow SPC**.

Le tableau de bord

Dans l'espace de travail Contrôle de la posture de sécurité, la page d'accueil (page de destination) affiche les visualisations suivantes :

Vue d'ensemble

- Actifs : nombre d'actifs surveillés sur site et dans le Cloud.
- Résultats par criticité : nombre de résultats critiques sur le total de vos actifs.
- Actifs surveillés par les 5 principales sources : cinq principaux connecteurs du graphe de services générant des rapports sur les actifs.
- Comptes dans le cloud : nombre de comptes dans le cloud surveillés par AWS et Azure.
- Conclusions ouvertes et fermées : comparaison des enregistrements encore en cours de traitement ou en attente de résolution et de ceux qui le sont déjà.

Aperçus clés

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Agent de protection du point de terminaison installé : nombre total d'actifs avec ou sans protection du point de terminaison.
- Couverture des appareils gérés : nombre d'actifs gérés par rapport à ceux qui ne le sont pas.
- Couverture de l'analyse de vulnérabilité : nombre total d'actifs analysés par rapport au nombre qui ne sont pas analysés pour détecter les vulnérabilités connues par un scanner de vulnérabilité tiers.
- Actifs présentant des vulnérabilités critiques : nombre d'actifs sur le nombre total d'actifs présentant des vulnérabilités critiques.
- Éléments vulnérables par criticité : nombre total d'éléments vulnérables répartis par gravité. Une vulnérabilité connue qui correspond à un actif de votre CMDB entraîne un élément vulnérable.
- 3 principales politiques par résultats : politiques qui renvoient le plus de résultats (correspondances) sur vos actifs.

Couverture du cas d'utilisation clé

Sélectionnez un cas d'utilisation, puis **Aider à activer** ou **Aider à améliorer** pour voir quels connecteurs du graphe de services et quelles politiques doivent être activés pour les cas d'utilisation clés.

Transitions d'état des résultats des tests et des tâches de rattrapage dans l'application Contrôle de la posture de sécurité

Les états des résultats (enregistrements de tests de configuration) et leurs tâches de rattrapage associées sont impactés si vous modifiez vos politiques dans l'application Contrôle de la posture de sécurité.

Scénarios de transitions d'états entre les résultats des tests et les tâches de rattrapage

À quelques exceptions près, les états font généralement la transition entre vos résultats (résultats des tests) et leurs tâches de rattrapage associées dans Contrôle de la posture de sécurité, de la même manière qu'ils assurent la transition entre les résultats des tests et les tâches de rattrapage dans l'application Conformité de la configuration . Toutefois, si vous modifiez vos politiques dans Contrôle de la posture de sécurité, vos changements ont un impact sur la façon dont les états transitent sur vos résultats et sur les tâches de rattrapage qui leur sont associées.

Les tableaux suivants illustrent la transition des états sur vos résultats si vous modifiez et publiez une nouvelle version (modifier), désactivez ou supprimez vos stratégies.

Pour plus d'informations sur les changements d'état dans , reportez-vous à Conformité de la configurationla section Transitions d'état des résultats des tests et des tâches de rattrapage dans l'application Conformité de la configuration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements de terminologie

Terminologie antérieure à la version 14.9	Terminologie à partir de la version 14.9
Groupe de résultats des tests	Tâche de rattrapage
Règle de groupe	Règles de la tâche de rattrapage
Politique	Groupe de tests

Les améliorations apportées aux audits de politique garantissent que les actifs mis hors service ne sont pas évalués par des politiques activées. Si l'état d'un actif passe de **Mis hors service** à **Actif**, il est inclus dans la prochaine évaluation de la politique.

Si une politique est...	Valeurs de champ sur les enregistrements de résultats existants pour...	Transition vers...
Désactivé	Résultat	Conserver les valeurs d'origine
	État	Fermé
	Résolution	Expiré

Si une politique est...	Valeurs de champ sur les enregistrements de résultats existants pour...	Transition vers...
Modifié avec l'option permettant de fermer tous les résultats existants sélectionnés	Résultat	Conserver les valeurs d'origine
	État	Fermé
	Résolution	Résultat non valide

Si une politique est...	Valeurs de champ sur les enregistrements de résultats existants pour...	Transition vers...
Modifié avec la possibilité de conserver tous les résultats existants sélectionnés	Résultat	Les scénarios de test valides (réussis) conservent les valeurs d'origine et les scénarios de test non valides (échec) sont fermés.
	État	Fermé
	Résolution	Résultat non valide

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si une politique est...	Valeurs de champ sur les enregistrements de résultats existants pour...	Transition vers...
Supprimé	Résultats	Conserver les valeurs d'origine
	État	Fermé
	Résolution	Résultat non valide

Créer une recherche d'actifs dans Contrôle de la posture de sécurité

Définissez vos conditions et recherchez des actifs par produits Service Graph Connector spécifiques ou pour les actifs dont des données spécifiques sont signalées par un connecteur.

Avant de commencer

À titre d'exemple de recherche, supposons que vous souhaitiez identifier vos actifs qui disposent de serveurs Windows et d'une version spécifique trouvée dans les détails des CrowdStrike métadonnées.

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Recherche d'actifs**.
2. Choisissez-en un.

Option	Description
Actif matériel	Recherchez n'importe quel appareil, y compris des appareils informatiques personnels, des serveurs, des appareils réseau, des ordinateurs virtuels dans le cloud et d'autres matériels.
Logiciel	Recherchez les logiciels installés sur vos actifs signalés par les connecteurs du graphe de services, vos produits de scanner de vulnérabilité et les logiciels signalés par les analyseurs qui sont déjà pris en compte dans Gestion des actifs logiciels (SAM) et d'autres produits ServiceNow.

   Pour cet exemple, sélectionnez **Actif matériel pour Type d'actif** .
3. Facultatif : Sélectionnez **Politique de base** et **Politiques d'exclusion** si vous souhaitez utiliser les conditions d'une politique existante comme point de départ et si vous souhaitez exclure les actifs qui correspondent aux politiques existantes, respectivement.
   Les politiques que vous sélectionnez s'affichent.
4. Sélectionnez **Avec les données du connecteur** pour le champ Connexion.
5. Sélectionnez les **détails de l'appareil CrowdStrike** pour l'entité.
6. Pour Property, Operator, and Value (Propriété), Operator (Propriété), Operator (Valeur), sélectionnez **[Agent Version][is]** et saisissez la version, par exemple, **6.26.14003.0**.
7. Sélectionnez l'opérateur et à droite du champ Entité avec CrowdStrike Détails de l'appareil comme valeur pour une autre condition.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Sélectionnez **Avec métadonnées CMDB** pour le champ Connexion.
   Le champ Entité est renseigné avec les métadonnées CMDB.
9. Sélectionnez la **propriété** pour le champ Critères.
10. Pour la propriété, l'opérateur et la valeur, sélectionnez **[OS] [contient]** et saisissez **serveur Windows**.
11. Sélectionnez **Afficher les actifs**.
    Après quelques instants, les résultats s'affichent dans l'onglet Actifs correspondants. Si vous ne voyez aucune correspondance, vous pouvez affiner votre recherche. Une fois que vous êtes certain d'avoir correctement défini les conditions, vous pouvez enregistrer la recherche en tant que politique et l'activer. Comme les autres stratégies, elle recherche vos actifs avec une tâche en arrière-plan en continu après son activation.

Cas d'utilisation, exemples de politiques et connecteurs du graphe de services pris en charge dans Contrôle de la posture de sécurité

Les cas d'utilisation sont différents scénarios que vous configurez pour vous aider à identifier des types spécifiques d'écarts de couverture d'outils. Chaque cas d'utilisation nécessite une ou plusieurs politiques pour auditer vos actifs afin de détecter d'éventuelles violations. Vous pouvez également définir vos propres politiques pour vous aider à répondre aux exigences de vos normes de sécurité interne spécifiques.

Cas d'utilisation

L'application Contrôle de la posture de sécurité prend en charge divers cas d'utilisation inclus dans l'application. Les cas d'utilisation vous aident à identifier des types spécifiques de lacunes dans la couverture des outils de vos actifs, l'exposition Internet des actifs dans le cloud et les combinaisons avec des vulnérabilités. Les politiques dont vous avez besoin pour les cas d'utilisation pris en charge sont également incluses dans le produit.

Vous pouvez afficher l'état de la couverture pour certains des principaux cas d'utilisation sur la page d'accueil (de destination) de l'espace de travail de contrôle de la posture de sécurité à l'adresse suivante : **Espaces de travail** > **Contrôle de la posture de sécurité** > **Accueil** dans le module d'accueil (page de destination).

Vous pouvez également afficher les connecteurs du graphe de services pris en charge et l'état de la couverture pour certains des cas d'utilisation clés dans les onglets « Connecteurs du graphe de services pris en charge » et « Configuration du cas d'utilisation clé » à l'adresse suivante : **Tout** > **Espaces de travail** > **Contrôle de la posture de sécurité** > **Configuration des connecteurs et des tickets d'utilisation** (l'icône d'engrenage).

Remarque :

L'onglet Cas d'utilisation clés des pages de destination Accueil ne répertorie pas tous les cas d'utilisation possibles. Il vous fournit quelques cas d'utilisation importants que vous activez pour vous aider à démarrer avec le déploiement du produit Contrôle de la posture de sécurité.

Avant d'activer les politiques pour les cas d'utilisation pris en charge fournis avec l'application, vérifiez que vous avez effectué les tâches suivantes.

- Vous avez installé et configuré toutes les applications requises décrites à la section Installer les applications prises en charge pour Contrôle de la posture de sécurité.
- Vous avez satisfait à un ou plusieurs des prérequis suivants pour chaque cas d'utilisation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Vous utilisez actuellement ou vous installez et activez des connecteurs du graphe de services pour différentes catégories.

   Les catégories des cas d'utilisation comprennent des connecteurs du graphe de services que vous devez activer pour obtenir des aperçus initiaux, et des connecteurs du graphe de services que vous pouvez activer pour améliorer la couverture des actifs surveillés par Security Posture Control.

2. Vous utilisez actuellement l'application Vulnerability Response ou vous installez et activez celle-ci.
3. Vous utilisez actuellement ou vous configurez l'analyse de compte cloud pour vos comptes AWS et Azure sous « Gestion de la posture de sécurité cloud ».

Les exigences spécifiques à chaque cas d'utilisation pris en charge sont décrites dans les sections suivantes. En outre, vous devez activer une ou plusieurs des politiques fournies avec Contrôle de la posture de sécurité pour un cas d'utilisation. Ce concept est également abordé dans les sections suivantes.

Exemples de politiques de base, enfants et clonées

Découvrez Exemples de politiques de base, enfants et clonées pour Contrôle de la posture de sécurité comment réutiliser les conditions d'une stratégie de base lorsque vous créez d'autres stratégies. Créez des politiques de base enfants et clonez des politiques existantes dans ces exemples. Ces exemples vous aident également à voir comment fonctionne le générateur de politiques dans le module Politiques et résultats.

Connecteurs du graphe de services pris en charge

Consultez les tables des connecteurs du graphe de services pris en charge, leurs catégories d'outils et les types de données qu'ils importent dans Service Graph Connectors pris en charge pour Contrôle de la posture de sécurité et Logiciels pris en charge Service Graph Connectors pour Contrôle de la posture de sécurité.

Contrôle de la posture de sécurité Cas d'utilisation : détection d'actifs avec la protection du point de terminaison manquante

Pour détecter les actifs sans agent de protection du point de terminaison, les prérequis suivants sont requis.

En fonction de votre cas d'utilisation, vous pouvez choisir d'activer uniquement les connecteurs requis.

1. Activez au moins un connecteur du graphe de services dans la catégorie Endpoint Protection.
2. Activez au moins un connecteur du graphe de services pour l'une des catégories suivantes.
   a. Services de répertoire (Microsoft Active Directory).
   b. Endpoint Management : Microsoft Intune ou Jamf Device and Endpoint Management.
   c. Configuration et gestion des correctifs : Microsoft SCCM ou IBM Bigfix.
   d. Fournisseur cloud : Amazon AWS Cloud, Microsoft Azure, GCP.

> **Remarque :** Si Détection dans le cloud est activé, ces produits Service Graph Connector ne sont pas requis.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. [Facultatif] Vous pouvez activer Connecteurs du graphe de services pour l'une des catégories suivantes afin d'améliorer la couverture globale, c'est-à-dire le nombre d'actifs qui sont signalés et surveillés par Contrôle de la posture de sécurité.
   a. Sécurité réseau
   b. Surveillance de l'infrastructure
   c. Réseau
   d. Gestion des points de terminaison .
   e. Surveillance des performances des applications.

Après avoir vérifié que vous remplissez ces conditions préalables, vous devez activer la stratégie suivante, Protection de point de terminaison manquante pour les actifs. Pour en savoir plus sur les stratégies, reportez-vous à Politiques pour Contrôle de la posture de sécurité.

Contrôle de la posture de sécurité Cas d'utilisation : détection des actifs manqués par les outils d'évaluation de la vulnérabilité

Pour détecter les actifs manqués par les outils d'évaluation de la vulnérabilité, les conditions préalables suivantes sont requises.

Pour chaque connecteur du graphe de services de la liste, vous pouvez voir si ce connecteur est nécessaire pour surveiller les actifs sur site ou les actifs dans le cloud. En fonction de votre cas d'utilisation, vous pouvez choisir d'activer uniquement les connecteurs requis.

1. Activez au moins un connecteur du graphe de services à partir de la catégorie d'évaluation de la vulnérabilité.
2. Activez au moins un connecteur du graphe de services pour l'une des catégories suivantes.
   a. Services de répertoire (Microsoft Active Directory).
   b. Endpoint Management : Microsoft Intune ou Jamf Device and Endpoint Management.
   c. Configuration et gestion des correctifs : Microsoft SCCM ou IBM Bigfix.
   d. Fournisseur cloud : Amazon AWS Cloud, Microsoft Azure, GCP.

      Remarque : Si Détection dans le cloud est activé, ces produits Service Graph Connector ne sont pas requis.

3. [Facultatif] Vous pouvez activer Connecteurs du graphe de services pour l'une des catégories suivantes afin d'améliorer la couverture globale, c'est-à-dire le nombre d'actifs qui sont signalés et surveillés par Contrôle de la posture de sécurité.
   a. Sécurité réseau .
   b. Réseautage.
   c. Surveillance de l'infrastructure.
   d. Surveillance des performances des applications.

Après avoir vérifié que vous remplissez ces conditions préalables, vous devez activer la politique suivante, Actifs non analysés pour détecter les vulnérabilités. Pour en savoir plus sur les politiques, reportez-vous à Politiques pour Contrôle de la posture de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôle de la posture de sécurité Cas d'utilisation : Détection d'actifs non gérés

Ce cas d'utilisation comprend deux parties : détection des actifs pour lesquels il manque des agents de configuration et de gestion des correctifs.

Pour détecter les actifs sans outils de configuration et de gestion des correctifs, les conditions préalables suivantes sont requises.

Pour chaque connecteur du graphe de services de la liste, vous pouvez voir si ce connecteur est nécessaire pour surveiller les actifs sur site ou les actifs dans le cloud.

En fonction de votre cas d'utilisation, vous pouvez choisir d'activer uniquement les connecteurs requis.

1. Activez au moins un connecteur du graphe de services dans les catégories Configuration et Gestion des correctifs.
2. Au moins un connecteur du graphe de services doit être activé pour L'UNE des catégories suivantes.
   a. Services de répertoire (Microsoft Active Directory).
   b. Endpoint Protection : CrowdStrike ou SentinelOne.
   c. Évaluation de vulnérabilité : Qualys, Rapid7ou Tenable.
   d. Configuration et gestion des correctifs : Microsoft SCCM ou IBM Bigfix.
3. [Facultatif] Vous pouvez activer Connecteurs du graphe de services pour l'une des catégories suivantes afin d'améliorer la couverture globale, c'est-à-dire le nombre d'actifs qui sont signalés et surveillés par Contrôle de la posture de sécurité.
   a. Réseautage.
   b. Surveillance de l'infrastructure
   c. Sécurité réseau
   d. Surveillance des performances des applications.

Après avoir vérifié que vous remplissez ces conditions préalables, vous devez activer au moins une des politiques suivantes. Pour toute politique qui commence par « Actifs dans le cloud », les connecteurs du graphe de services de la catégorie « Fournisseur dans le cloud » doivent être activés. Pour plus d'informations sur les politiques, consultez Politiques pour Contrôle de la posture de sécurité.

- Configuration et gestion des correctifs manquants dans les actifs.
- Configuration et gestion des correctifs manquants dans les actifs cloud.

Contrôle de la posture de sécurité Cas d'utilisation : détection des actifs manquants d'une solution de gestion des points de terminaison

Pour détecter les actifs manquants d'une solution de gestion des points de terminaison, les prérequis suivants sont requis.

En fonction de votre cas d'utilisation, vous pouvez choisir d'activer uniquement les connecteurs requis.

1. Activez au moins un connecteur du graphe de services à partir de la catégorie Gestion des points de terminaison.
2. Au moins un connecteur du graphe de services doit être activé pour L'UNE des catégories suivantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Services de répertoire (Microsoft Active Directory).

b. Endpoint Protection : CrowdStrike ou SentinelOne.

c. Évaluation de vulnérabilité : Qualys, Rapid7ou Tenable.

d. Configuration et gestion des correctifs : Microsoft SCCM ou IBM Bigfix.

Après avoir vérifié que vous avez rempli ces conditions préalables, vous devez activer la stratégie suivante, Solution de gestion des points de terminaison manquants d'actifs. Pour en savoir plus sur les politiques, reportez-vous à Politiques pour Contrôle de la posture de sécurité.

Contrôle de la posture de sécurité Cas d'utilisation : détection d'actifs présentant des vulnérabilités et des lacunes dans la couverture de l'outil de Security

Vous pouvez identifier les actifs présentant des vulnérabilités critiques et des outils de sécurité critiques manquants, tels que la protection des terminaux, afin de hiérarchiser ces actifs pour le rattrapage. Contrôle de la posture de sécurité fournit quelques politiques incluses avec le produit pour prendre en charge ce cas d'utilisation.

Ce cas d'utilisation nécessite l'installation de l'application Vulnerability Response et une intégration avec au moins un produit d'évaluation des vulnérabilités, tel que Qualys, Rapid7ou Tenable.

Les politiques suivantes sont incluses avec le produit Contrôle de la posture de sécurité pour prendre en charge ce cas d'utilisation pour les actifs présentant des vulnérabilités critiques qui ne couvrent pas non plus l'outil de sécurité.

1. Actifs avec des vulnérabilités critiques et une protection du point de terminaison manquante.
2. Actifs avec des vulnérabilités critiques et une gestion de la configuration et des correctifs manquante.
3. Actifs avec des vulnérabilités critiques et une gestion des points de terminaison manquante.

Contrôle de la posture de sécurité Cas d'utilisation : Détection de l'exposition Internet des ressources cloud et des combinaisons à haut risque

Il est essentiel de surveiller l'exposition Internet potentielle des actifs Cloud (machines virtuelles) sur différents ports afin de s'assurer que les vulnérabilités de ces actifs ne sont pas exploitées à distance. Ce cas d'utilisation vous aide à identifier ces actifs.

Contrôle de la posture de sécurité vous permet d'évaluer la configuration des ressources dans le cloud pour vous aider à identifier les ressources qui sont accessibles sur Internet, c'est-à-dire les ressources accessibles depuis n'importe où sur Internet et les ports à partir desquels elles sont exposées.

Contrôle de la posture de sécurité combine ces informations avec les lacunes de couverture de l'outil de sécurité et les données de vulnérabilité provenant d'analyseurs tiers tels que Qualys, Rapid7, ou Tenable pour identifier les combinaisons à haut risque.

Actuellement, ce cas d'utilisation prend en charge AWS et requiert les conditions préalables suivantes.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Connecteur du graphe de services pour AWS est activé pour les mêmes comptes AWS que ceux que vous avez configurés.
2. Vous avez activé une ou plusieurs des politiques incluses avec le produit dans Contrôle de la posture de sécurité.
   - Les actifs dans le cloud avec le port SSH 22 sont ouverts à Internet.
   - Les actifs dans le cloud avec le port SSH 22 sont ouverts à Internet et la protection du point de terminaison est manquante.
   - Les actifs dans le cloud avec le port HTTP 80 sont ouverts à Internet et la protection du point de terminaison est manquante.
   - Actifs dans le cloud avec des vulnérabilités critiques et port SSH 22 ouvert à Internet (nécessite Vulnerability Response).
   - Actifs dans le cloud avec des vulnérabilités critiques, une protection des points de terminaison manquante et le port SSH 22 ouvert à Internet (nécessite Vulnerability Response).
   - Ressources dans le cloud avec des ports HTTP ouverts à Internet, des vulnérabilités critiques et une protection de point de terminaison manquante (Exige Réponse aux vulnérabilités).

Service Graph Connectors pris en charge pour Contrôle de la posture de sécurité

Connecteurs du graphe de services matériels pris en charge avec la classe CI, la source (produit) et les catégories d'outils. Cette liste n'est pas exhaustive et est susceptible d'être modifiée avec l'ajout de nouveaux produits.

Pour la source de détection d'un connecteur répertorié, « SG », « SGO » ou « SGC » précède le nom de produit pour les produits tiers, par exemple, SG-AWS, SGO-Datadog ou SGC-AD (Active Directory). Pour les produits ServiceNow, « SN » ou « ServiceNow » précède le nom du produit, par exemple, SNAssetManagement pour Gestion des actifs matériels ServiceNow.

Une fois installés, vous pouvez afficher les connecteurs et leurs catégories sur la table des connecteurs [sn_sec_spc_core_connector] de votre instance.

Vous pouvez afficher les types d'actif et leur mappage aux classes CI et aux connecteurs dans la table [sn_sec_spc_core_asset_type_connector].

Connecteurs Hardware Service Graph

Type d'actif	Classe CI	Source de l'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_computer	Active Directory	Services de répertoire
Actif matériel	cmdb_ci_server	AppDynamics	Application Performance Monitoring
Actif matériel	cmdb_ci_server	Automox	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_computer	Automox	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_computer	BigFix	Configuration et gestion des correctifs

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs Hardware Service Graph (suite)

Type d'actif	Classe CI	Source de l'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_server	BigFix	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_printer	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_server	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_iot	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_hc_device	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_netgear	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_computer	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_server	CrowdStrike (en anglais seulement)	Protection de point de terminaison
Actif matériel	cmdb_ci_server	Datadog	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_server	Dynatrace	Application Performance Monitoring
Actif matériel	cmdb_ci_computer	Dynatrace	Application Performance Monitoring
Actif matériel	cmdb_ci_computer	Révélation ExtraHop (x)	Sécurité réseau
Actif matériel	cmdb_ci_hc_device	Révélation ExtraHop (x)	Sécurité réseau
Actif matériel	cmdb_ci_server	Révélation ExtraHop (x)	Sécurité réseau
Actif matériel	cmdb_ci_iot	Révélation ExtraHop (x)	Sécurité réseau
Actif matériel	cmdb_ci_printer	Révélation ExtraHop (x)	Sécurité réseau
Actif matériel	cmdb_ci_iot	Éclaireur	Sécurité réseau
Actif matériel	cmdb_ci_hc_device	Éclaireur	Sécurité réseau
Actif matériel	cmdb_ci_computer	Éclaireur	Sécurité réseau
Actif matériel	cmdb_ci_server	Éclaireur	Sécurité réseau
Actif matériel	cmdb_ci_printer	Éclaireur	Sécurité réseau
Actif matériel	cmdb_ci_server	Intune	Gestion des points de terminaison
Actif matériel	cmdb_ci_computer	Intune	Gestion des points de terminaison

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs Hardware Service Graph (suite)

Type d'actif	Classe CI	Source de l'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_printer	Jamf Pro	Gestion des points de terminaison
Actif matériel	cmdb_ci_server	Jamf Pro	Gestion des points de terminaison
Actif matériel	cmdb_ci_computer	Jamf Pro	Gestion des points de terminaison
Actif matériel	cmdb_ci_server	Balayeuse de Lansweeper	IT Asset Management
Actif matériel	cmdb_ci_computer	Balayeuse de Lansweeper	IT Asset Management
Actif matériel	cmdb_ci_printer	Balayeuse de Lansweeper	IT Asset Management
Actif matériel	cmdb_ci_hc_device	Moniteur logique	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_printer	Moniteur logique	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_server	Moniteur logique	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_vm_instance	Moniteur logique	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_iot	Moniteur logique	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_computer	Moniteur logique	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_netgear	Moniteur logique	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_server	Microsoft Defender	Protection de point de terminaison
Actif matériel	cmdb_ci_server	New Relic	Application Performance Monitoring
Actif matériel	cmdb_ci_computer	Nexthink	Expérience numérique de l'employé
Actif matériel	cmdb_ci_server	Ouvrir les données de télémétrie	Application Performance Monitoring
Actif matériel	cmdb_ci_computer	Puppet	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_server	Puppet	Configuration et gestion des correctifs

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs Hardware Service Graph (suite)

Type d'actif	Classe CI	Source de l'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_computer	Qualys	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_server	Qualys	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_vm_instance	Qualys-ServiceNow	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_server	Qualys-ServiceNow	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_hardware	Rapid7	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_computer	SCCM	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_server	SCCM	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_printer	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_iot	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_server	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_computer	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_hc_device	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_vm_instance	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_hardware	ServiceNow HAM	Gestion des actifs matériels
Actif matériel	cmdb_ci_hardware	Détection ServiceNow ITOM	Découverte
Actif matériel	cmdb_ci_server	Actif Tanium	Gestion des points de terminaison
Actif matériel	cmdb_ci_computer	Actif Tanium	Gestion des points de terminaison
Actif matériel	cmdb_ci_ups	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_industrial_sensor	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_cnc	Tenable	Évaluation de la vulnérabilité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs Hardware Service Graph (suite)

Type d'actif	Classe CI	Source de l'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_hardware	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_netgear	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_industrial_device	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ip_switch	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_hub_network	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_security	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_server	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_rtu	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_ews	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_plc	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_control	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_dcs	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_storage_server	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_hmi	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_control_module	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_industrial_robot	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_historian	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_industrial_drive	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_iot	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ip_firewall	Tenable	Évaluation de la vulnérabilité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs Hardware Service Graph (suite)

Type d'actif	Classe CI	Source de l'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_computer	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_unclassed_hardware	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ids_network	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_ied	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_printer	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_computer	VMWare Workspace ONE UEM	Gestion des points de terminaison
Actif matériel	cmdb_ci_server	VMWare Workspace ONE UEM	Gestion des points de terminaison
Actif matériel	cmdb_ci_printer	VMWare Workspace ONE UEM	Gestion des points de terminaison

Logiciels pris en charge Service Graph Connectors pour Contrôle de la posture de sécurité

Connecteurs du graphe de services logiciels pris en charge avec classe CI, source (produit) et catégories d'outils. Cette liste n'est pas exhaustive et est susceptible d'être modifiée avec l'ajout de nouveaux produits.

Une fois installés, vous pouvez afficher les connecteurs et leurs catégories sur la table des connecteurs [sn_sec_spc_core_connector] de votre instance.

Vous pouvez afficher les types d'actif et leur mappage aux classes CI et aux connecteurs dans la table [sn_sec_spc_core_asset_type_connector].

Connecteurs du graphe de services logiciels

Type d'actif	Classe CI	Source de l'actif	Catégorie de connecteur
Logiciel	cmdb_ci_spkg	BigFix	Configuration et gestion des correctifs
Logiciel	cmdb_ci_spkg	Dynatrace	Application Performance Monitoring
Logiciel	cmdb_ci_spkg	Éclaireur	Sécurité réseau
Logiciel	cmdb_ci_spkg	Intune	Gestion des points de terminaison
Logiciel	cmdb_ci_spkg	Jamf Pro	Gestion des points de terminaison

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs du graphe de services logiciels (suite)

Type d'actif	Classe CI	Source de l'actif	Catégorie de connecteur
Logiciel	cmdb_ci_spkg	New Relic	Application Performance Monitoring
Logiciel	cmdb_ci_spkg	Nexthink	Expérience numérique de l'employé
Logiciel	cmdb_ci_spkg	Qualys-ServiceNow	Évaluation de la vulnérabilité
Logiciel	cmdb_ci_spkg	SCCM	Configuration et gestion des correctifs
Logiciel	cmdb_ci_spkg	Détection ServiceNow ITOM	Découverte
Logiciel	cmdb_ci_spkg	Actif Tanium	Gestion des points de terminaison
Logiciel	cmdb_ci_spkg	VMWare Workspace ONE UEM	Gestion des points de terminaison

Exemples de politiques de base, enfants et clonées pour Contrôle de la posture de sécurité

Vous pouvez créer vos propres politiques de base qui comportent de larges ensembles de conditions que vous pouvez utiliser comme point de départ pour des politiques plus complexes.

Exemples

Les exemples suivants vous aideront à voir comment vous pouvez réutiliser les conditions d'une stratégie de base lorsque vous créez d'autres stratégies en créant des stratégies enfants ou en clonant des stratégies existantes. Ces exemples vous aident également à voir comment fonctionne le générateur de politiques dans le module Politiques et résultats.

Commencez par le premier exemple, la stratégie de base. Les autres exemples utilisent la politique de base comme point de départ.

Remarque : Le connecteur du graphe de services CrowdStrike est utilisé comme connecteur du graphe de services dans ces exemples, mais vous pouvez utiliser n'importe quel connecteur que vous avez installé. Ces exemples vous permettent de créer et d'activer les polices pour rechercher des correspondances d'actifs. Vous pouvez supprimer ces politiques à tout moment à partir du module Politiques et résultats après les avoir activées.

Créez une politique de base pour Contrôle de la posture de sécurité (exemple)

Un exemple de la façon de créer une politique de base que vous pouvez utiliser pour créer d'autres politiques.

Avant de commencer

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Espace de travail pour le contrôle de la posture de sécurité** > **Politiques et résultats**.
2. Sélectionnez **Nouvelle stratégie**.
3. Sélectionnez l'icône du stylo en haut à gauche et, dans le modal Modifier les métadonnées, renseignez les champs.

Champ	Description
Nom	Saisissez, Politique de base : appareils Windows 10.
Criticité	Sélectionnez **Faible**.
Description brève	Tapez, **Localiser les appareils sur lesquels Windows 10 est installé.**

4. Sélectionnez **Enregistrer les métadonnées**.
5. Dans Créateur de conditions, sélectionnez **Actif matériel** pour Type d'actif.

   Pour cette stratégie, laissez les options Politique de base et Politiques d'exclusion dans leurs paramètres par défaut (désactivés).

6. Pour Connexion, sélectionnez **Avec des données agrégées**.

   Pour cette stratégie, les données agrégées vous aident à localiser les actifs dans votre CMDB sur lesquels Windows 10 est installé. Par exemple, certains enregistrements peuvent présenter de légères variations dans la façon dont les différents scanners signalent « Windows 10 ». Les données agrégées garantissent que toutes ces légères variations de « Windows 10 » correspondront à cette politique.

   Les champs Entité et Critères sont renseignés automatiquement en fonction de votre sélection dans le champ Connexion.

7. Pour Propriété **, sélectionnez Système d'exploitation**.
8. Pour Valeur, tapez dans `Windows 10`.
9. Sélectionnez **Enregistrer les modifications**.
   Votre politique de base s'affiche dans la liste Tout du module Politiques et résultats, mais elle n'est pas activée.
10. Sélectionnez **Activer la politique** afin que votre politique de base surveille tous les actifs qui correspondent aux conditions de la politique et génère des conclusions.

Créez une politique enfant à partir d'une politique de base, par Contrôle de la posture de sécurité exemple :

Exemple de création d'une politique enfant à l'aide des conditions d'une politique de base.

Avant de commencer

Cette politique enfant hérite des conditions d'une politique de base, et vous allez ajouter d'autres conditions à votre politique enfant pour vous aider à vous concentrer sur des détails d'actif plus spécifiques. Vous souhaitez une nouvelle stratégie pour surveiller tous vos appareils sur lesquels Windows 10 est installé et qui sont signalés par le connecteur du CrowdStrike graphe de services, et vous souhaitez exclure tous les appareils qui correspondent à une autre stratégie. Pour cet exemple, vous allez exclure de vos conclusions les actifs qui ont été approuvés pour les exceptions de la gestion intégrée des risques (IRM).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous n'avez pas installé le CrowdStrike connecteur du graphe de services, vous pouvez en utiliser un qui est installé.

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

Procédure

1. Accédez à la **Tout** > **Espace de travail pour le contrôle de la posture de sécurité** > **Politiques et résultats**.
2. Dans la liste Actif, localisez la stratégie de base - appareils Windows 10 que vous avez créée dans le premier exemple et sélectionnez-la pour ouvrir l'enregistrement.
3. Sélectionnez le menu Autres options (trois points verticaux), puis sélectionnez **Créer une politique enfant**.
   Un nouvel onglet s'ouvre et avec un nouvel enregistrement, la stratégie de base - appareils Windows 10 s'affiche dans le champ stratégie de base.
4. Sélectionnez l'icône du stylo en haut à gauche et, dans le modal Modifier les métadonnées, renseignez les champs.

Champ	Description
Nom	Saisissez, `Politique enfant : appareils Windows avec CrowdStrike`.
Criticité	Sélectionnez **Moyen**.
Description brève	Tapez, `Localiser tous les appareils avec Windows 10 signalés par Crowd-Strike.`

5. Sélectionnez **Enregistrer les métadonnées**.
6. Dans Créateur de conditions, sélectionnez **Actif matériel** pour Type d'actif.
7. Sélectionnez le bouton à bascule Politique de base.
8. Sélectionnez la stratégie que vous avez créée pour Exemple 1, **Stratégie de base : appareils Windows 10** dans la liste.

   Cette politique enfant hérite automatiquement des conditions de la politique de base.
9. Sélectionnez le bouton à bascule Politiques d'exclusion.
10. Sélectionnez Actifs avec exception IRM approuvée dans la liste.

    Remarque : Si vous ne disposez pas de cette politique, vous pouvez sélectionner une autre politique dans la liste que vous souhaitez exclure de cette politique.

    Les actifs qui correspondent à cette politique seront exclus de votre politique enfant. Notez que vous pouvez ajouter d'autres politiques.
11. Sélectionnez **Signalé par**.
12. Sélectionnez **CrowdStrike** dans la liste.
13. Sélectionnez **Enregistrer les modifications**.
    Votre nouvelle politique s'affiche dans la liste Tout du module Politiques et conclusions, mais elle n'est pas activée.
14. Sélectionnez **Activer la politique** afin que votre politique de base surveille tous les actifs qui correspondent aux conditions de la politique et génère des conclusions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cloner une politique pour Contrôle de la posture de sécurité (exemple)

Un exemple de la façon de créer une politique qui copie les conditions d'une autre politique.

Avant de commencer

Créez une politique qui copie les conditions de la politique que vous avez créée dans l'exemple 2 afin de ne pas avoir à les saisir à nouveau. Vous clonerez ces conditions et ajouterez d'autres conditions à la copie de la politique enfant que vous avez créée. Pour cet exemple, vous souhaitez que cette stratégie localise les appareils avec Windows 10 avec CrowdStrike, excluez les actifs avec des exceptions IRM qui n'ont pas été vus au cours des 7 derniers jours.

Rôles requis : Groupe d'administrateurs SPC ou Groupe d'analystes SPC

Procédure

1. Accédez à la **Tout** > **Espace de travail pour le contrôle de la posture de sécurité** > **Politiques et résultats**.
2. Dans la liste Actif, localisez les appareils de stratégie enfant que CrowdStrike vous avez créés pour le deuxième exemple et sélectionnez-les Windows pour ouvrir l'enregistrement.
3. Sélectionnez le menu Autres options (trois points verticaux), puis sélectionnez **Cloner la stratégie**.
   Un nouvel onglet s'ouvre et le nom de la politique s'affiche dans un nouvel enregistrement avec « copie » dans le titre : Appareils Windows avec CrowdStrike-copy.
4. Sélectionnez l'icône du stylo en haut à gauche et, dans le modal Modifier les métadonnées, renseignez les champs.

Champ	Description
Nom	`Tapez, Politique clonée : Windows 10 Exceptions IRM CrowdStrike non observées pendant 7 jours.`
Criticité	Sélectionnez **Critique**.
Description brève	`Tapez, Localiser les appareils avec Windows 10 avec CrowdStrike IRM exceptions non vues au cours des 7 derniers jours.`

5. Sélectionnez **Enregistrer les métadonnées**.
6. À droite des premiers champs Connexion et Entité, sélectionnez l'opérateur **ET** pour les nouveaux champs.
   Cela ajoute un ET logique entre les critères d'entité de connexion actuels et les nouveaux critères d'une autre entité de connexion. Dans ce cas, vous souhaitez spécifier les données du connecteur pour les actifs non vus par CrowdStrike au cours des 7 derniers jours.
7. Pour Connexion, sélectionnez **Avec les données du connecteur**.
8. Pour Entité, sélectionnez **CrowdStrike : Détails de l'appareil CrowdStrike**.
   Les critères remplis sont automatiquement en fonction de votre sélection.
9. Pour Property (Propriété), sélectionnez **Last Seen Time (Heure de la dernière observation)**.
10. Pour Value (Valeur), sélectionnez **This week (Cette semaine)**.
11. Sélectionnez **Enregistrer les modifications**.

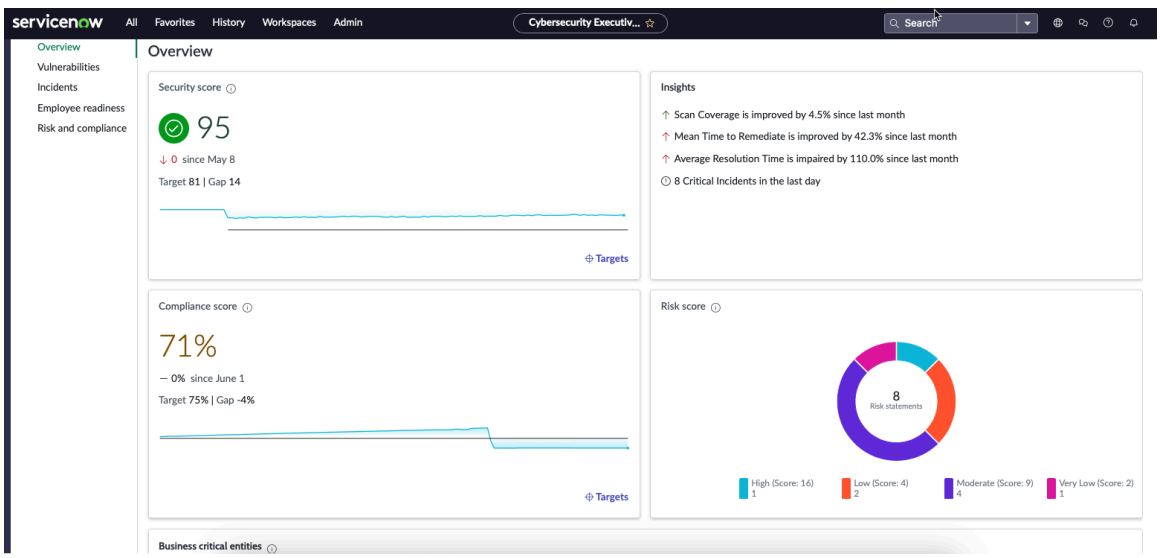
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

12. Sélectionnez **Activer la stratégie**.
    Vous pouvez supprimer ces politiques à tout moment à partir du module Politiques et résultats.

Tableau de bord de direction de cybersécurité

Le tableau de bord de direction de cybersécurité est une solution complète qui permet aux responsables de la sécurité de l'information (RSSI) et aux responsables de la cybersécurité d'avoir une visibilité sur la posture et les initiatives de sécurité de l'organisation. Le tableau de bord consolide les données issues de divers produits au sein de Security ServiceNow Operations Suite et de Governance, Risk and Compliance (GRC).



Le tableau de bord fournit les fonctionnalités suivantes :

- Score de posture de sécurité à l'échelle de l'organisation
- Scores de sécurité, de risque et de conformité par unité business
- Surveillance personnalisable
- Vue unifiée du paysage de la sécurité d'une organisation
- Benchmarking
- Interface conviviale
- Visibilité sur les mesures de simulation d'hameçonnage de KnowBe4 et Microsoft Defender pour Office 365

Ces fonctionnalités permettent une prise de décision proactive en fournissant un accès rapide aux mesures de sécurité critiques. Il s'agit donc d'un outil indispensable pour améliorer la résilience et la préparation globales en matière de sécurité.

Rôles Now Platform requis

- CISO (sn_bod.ciso) pour afficher et partager le tableau de bord.
- sn_bod.ciso_admin pour afficher, partager le tableau de bord et configurer les poids pour l'évaluation de la posture de sécurité.
- Utilisateur CISO GRC (sn_grc_dashboards.grc_ciso_user) pour afficher les rapports de conformité et de risque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accéder au tableau de bord de direction de cybersécurité

Pour ouvrir le tableau de bord, accédez à **Tout** > **Tableau de bord de direction de cybersécurité** > **Tableau de bord de direction de cybersécurité**.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Responsables de la sécurité de l'information (RSSI)	Les RSSI obtiennent des informations sur la gestion des vulnérabilités, la gestion des incidents, la posture de sécurité de l'organisation, les mesures de simulation d'hameçonnage, etc., pour leur organisation.

Visualisation des données

Remarque : Pour en savoir plus sur un widget, sélectionnez l'icône d'informations .

Cibles

Mesures	Type	Description
Cibles	Pourcentage	Affiche la cible définie à couvrir pour une mesure. L'état des cibles est indiqué par un code couleur. Il affiche toutes les cibles dont la date de révision se situe dans les 30 derniers jours ou à venir. Vous pouvez définir le nombre de jours d'affichage des cibles à l'aide de la *sn_bod.show_targets_from* propriété système. De plus, ces cibles peuvent être modifiées. Consultez Définir des cibles pour plus d'informations.

Vue d'ensemble

Mesures	Type	Description
Score de sécurité	Score unique	Score global de la posture de sécurité de l'organisation en tenant compte des éléments vulnérables, des incidents de sécurité,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble (suite)

Mesures	Type	Description
		des incidents de sécurité majeurs et des erreurs de configuration.
Aperçus	Points forts	Points forts de l'ensemble du tableau de bord.
Score de conformité	Score unique	Fournit la posture de conformité de l'organisation à l'aide du score de conformité calculé en fonction du pourcentage de contrôles conformes par rapport au nombre total de contrôles.
Score du risque	Score unique	Fournit le nombre de déclarations de risque en fonction des évaluations de risque. Il aide les organisations à comprendre l'impact potentiel et la probabilité de divers risques, ce qui leur permet de hiérarchiser et de gérer ces risques.
Entités critiques pour l'entreprise		
Unités business	Score unique	Score de sécurité global des unités business en tenant compte du risque associé aux vulnérabilités, aux erreurs de configuration, aux vulnérabilités de technologie opérationnelle (OT), aux incidents de sécurité et aux incidents de sécurité majeurs. L'étiquette d'intégrité des unités business est basée uniquement sur le score de sécurité. Pour voir comment ces étiquettes sont affectées, accédez à la table Poids du score de risque [sn_sec_cmn_risk_score_weight_list.do] et recherchez une entité commerciale. Les étiquettes telles que « Intègre » sont affectées en fonction de plages de valeurs prédéfinies. Par exemple, un

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble (suite)

Mesures	Type	Description
		score de sécurité compris entre 0 et 39 est étiqueté comme Sain. Le code couleur de ces étiquettes est spécifié dans l'include de script `UnifiedCISOutils`. Vous pouvez configurer à la fois la plage de valeurs et les couleurs des étiquettes. Pour savoir comment les noms de l'unité business et du responsable de l'unité business sont affectés, accédez à **Tout** > **Organisation** > **Unités business**. **Remarque :** Selon les modules d'extension que vous avez activés, vous pouvez accéder au score de conformité, au score de risque et au score de sécurité. Pour afficher le score de conformité et de risque, vous devez activer les modules d'extension GRC. Pour afficher le score de sécurité, vous devez activer les modules d'extension associés à Security Operations. Pour plus d'informations, reportez-vous à la section Applications à actives.
Services aux entreprises	Score unique	Score de sécurité global des services d'entreprise en tenant compte du risque associé aux vulnérabilités, aux erreurs de configuration, aux vulnérabilités de technologie opérationnelle (OT), aux incidents de sécurité et aux incidents de sécurité majeurs. Pour voir comment ces étiquettes sont affectées,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble (suite)

Mesures	Type	Description
		accédez à la table Poids du score de risque [sn_sec_cmn_risk_score_weight_list.do] et recherchez une entité commerciale. Les étiquettes telles que « Sain », « Modéré » et « Critique » sont affectées en fonction de plages de valeurs prédéfinies. Par exemple, un score de sécurité compris entre 0 et 39 est étiqueté comme Sain. Le code couleur de ces étiquettes est spécifié dans l'include de script`UnifiedCISOutils`. Vous pouvez configurer à la fois la plage de valeurs et les couleurs des étiquettes. Pour savoir comment l'unité business et le nom du responsable de l'unité business sont affectés, accédez à **Tout** > **Organisation** > **Unités business**. **Remarque :** Selon les modules d'extension que vous avez activés, vous pouvez accéder au score de conformité, au score de risque et au score de sécurité. Pour afficher le score de conformité et de risque, vous devez activer les modules d'extension GRC. Pour afficher le score de sécurité, vous devez activer les modules d'extension associés à Security Operations. Pour plus d'informations, reportez-vous à la section Applications à actives.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

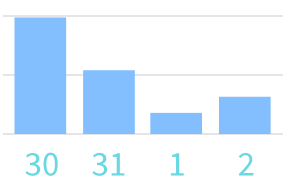
Vulnérabilités

Mesures	Type	Description
Délai moyen de résolution (mensuel)	Graphique linéaire	Temps moyen nécessaire pour fermer les vulnérabilités et les résultats des tests échoués sur l'ensemble des actifs (hôtes, conteneurs et applications) en un mois. Il fournit également les mesures suivantes : • Cible : cible définie en jours pour corriger les vulnérabilités. • Écart : différence en jours entre la cible et le temps réel nécessaire pour corriger les vulnérabilités. • Point de référence du secteur : moyenne des mesures des pairs du même secteur. • Point de référence global : Moyenne des mesures des pairs sur le marché mondial Découvrez Adhésion aux scores de point de référence comment afficher les scores de point de référence.
Âge moyen des vulnérabilités actives (mensuel)	Score unique	Âge moyen mensuel des trois types d'éléments vulnérables. Il fournit également une comparaison de l'âge du mois actuel avec le mois précédent. Il fournit également les mesures suivantes : • Point de référence du secteur : moyenne des mesures des pairs du même secteur. • Point de référence global : Moyenne des mesures des pairs sur le marché mondial • Cible : cible définie en jours pour corriger les vulnérabilités.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

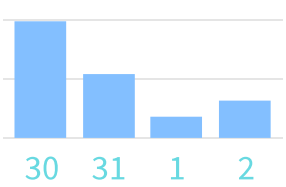
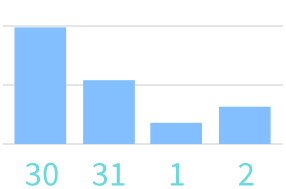
Vulnérabilités (suite)

Mesures	Type	Description
Efficacité de la résolution (mensuelle)	Score unique	Pourcentage d'éléments vulnérables fermés mensuels par rapport aux éléments vulnérables actifs mensuels. Il fournit également les mesures suivantes : • Variation en pourcentage par rapport au mois précédent. • Cible : cible définie en pourcentage pour corriger les vulnérabilités. • Écart : l'écart entre le score cible et le score actuel. • Point de référence du secteur : moyenne des mesures des pairs du même secteur. • Point de référence global : Moyenne des mesures des pairs sur le marché mondial
Âge moyen des vulnérabilités actives par groupe d'affectation	Ligne multiple	Âge moyen des vulnérabilités actives pour chaque groupe d'affectation.
Vulnérabilités par cote de risque et âge	Carte thermique	Répartition des vulnérabilités actives entre les hôtes, les conteneurs et les applications par cote de risque et par âge.
Respect de la cible de résolution par groupe d'affectation	barre verticale 	Rapport entre le nombre de vulnérabilités et d'erreurs de configuration fermés avec la cible de correction et le nombre total de vulnérabilités et d'erreurs de configuration fermées.
Couverture de l'analyse	Pourcentage	Pourcentage des actifs analysés au cours des 90 derniers jours sur l'ensemble des actifs du CMDB.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vulnérabilités (suite)

Mesures	Type	Description
Actifs numérisés et non numérisés	Barre horizontale	Répartition des actifs analysés au cours des 90 derniers jours et actifs totaux par CMDB classe CI
Actifs analysés	Barre horizontale	Actifs analysés au cours des 90 derniers jours pour détecter les vulnérabilités par rapport à la conformité de la configuration.
Tendance des résultats de vulnérabilités critiques et élevées actives	sur plusieurs lignes	Tendance quotidienne des vulnérabilités et des mauvaises configurations ayant une cote de risque critique et élevé.
Vulnérabilités par catégorie d'actifs et cote de risque	barre verticale 	Répartition des vulnérabilités actives et des mauvaises configurations par catégorie d'actifs et cote de risque (critique, élevé et moyen).
Résultats différés par motif et groupe d'affectation	barre verticale 	Répartition des vulnérabilités actives et des erreurs de configuration différées par motif de report et groupe d'affectation.
Technologie opérationnelle (OT)		
Tendance des vulnérabilités critiques et élevées actives	de ligne	Tendance quotidienne des vulnérabilités OT actives avec cote de risque critique et élevé.
Délai moyen de résolution (mensuel)	Score unique	Temps moyen nécessaire pour fermer les vulnérabilités OT. Ratio de l'âge total des vulnérabilités OT fermées par rapport au nombre total de vulnérabilités OT. Il fournit également les mesures suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vulnérabilités (suite)

Mesures	Type	Description
		• Variation en pourcentage par rapport au mois précédent. • Cible : cible définie en jours pour corriger les vulnérabilités. • Point de référence du secteur : moyenne des mesures des pairs du même secteur. • Point de référence global : Moyenne des mesures des pairs sur le marché mondial Découvrez Adhésion aux scores de point de référence comment afficher les scores de point de référence.
Vulnérabilités par cote de risque et âge	Carte thermique 	Répartition des vulnérabilités OT actives par cote de risque et par âge.
Âge moyen des vulnérabilités actives (mensuel)	Graphique en courbes	Âge moyen mensuel des éléments vulnérables OT. Il fournit également une comparaison de l'âge du mois actuel avec le mois précédent.
Vulnérabilités par état et âge	Carte thermique 	Répartition des vulnérabilités OT actives par état et par âge.

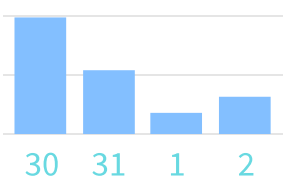
Incidents

Mesures	Type	Description
Incidents de sécurité majeurs	Score unique	Nombre d'incidents de sécurité majeurs actuellement actifs
Délai moyen de résolution des incidents de sécurité (mensuel)	Score unique	Délai de résolution moyen mensuel, en jours, des incidents de sécurité fermés. Il fournit également les mesures suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

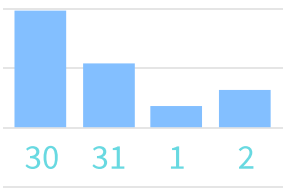
Incidents (suite)

Mesures	Type	Description
		• Variation en pourcentage par rapport au mois précédent. • Cible : cible définie en jours pour corriger les incidents de sécurité. • Écart : l'écart entre le nombre réel de jours nécessaires à la résolution et l'objectif défini pour y remédier. • Point de référence du secteur : moyenne des mesures des pairs du même secteur. • Point de référence global : Moyenne des mesures des pairs sur le marché mondial
Délai moyen pour éradiquer (mensuel)	Graphique en courbes	Résolution moyenne mensuelle en jours pour éradiquer les incidents de sécurité.
Délai moyen pour identifier (mensuel)	Score unique	Résolution mensuelle moyenne en jours pour identifier les incidents de sécurité.
Délai moyen pour contenir (mensuel)	Score unique	Résolution moyenne mensuelle en jours pour contenir les incidents de sécurité.
Incidents actifs par priorité et catégorie	Carte thermique	Nombre d'incidents de sécurité actifs, classés par priorité et catégorie.
Tendance des incidents fermés et ouverts	barre verticale 	Répartition des incidents fermés et ouverts.

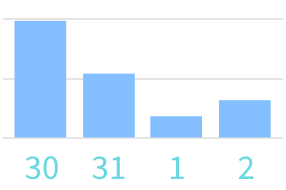
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incidents (suite)

Mesures	Type	Description
Incidents actifs par états	barre verticale 	Répartition des incidents actifs en fonction de leur état.

Préparation des employés

Mesures	Type	Description
Vue d'ensemble mensuelle de la simulation d'hameçonnage	barre verticale 	Somme des utilisateurs qui ont effectué les actions (ouverture, clic et signalement dans la simulation d'hameçonnage), ainsi que la somme du nombre total d'utilisateurs de chaque simulation au cours des six derniers mois.

Risque et conformité

Pour afficher les widgets Risk and Compliance, vous devez activer les modules d'extension GRC. Pour plus d'informations sur les plug-ins GRC, reportez-vous à la section Applications à activer. Pour en savoir plus sur les widgets GRC, reportez-vous à la section Tableau de bord des risques et de la conformité pour GRC : Mesures.

Indicateurs

SLA hôte : fermé

Cet indicateur est calculé quotidiennement. Il tient compte de l'âge total de toutes les vulnérabilités de l'hôte qui ont été fermées le jour précédent au moment du calcul.

SLA de conteneur : fermé

Cet indicateur est calculé quotidiennement. Il prend en compte toutes les vulnérabilités de conteneurs qui ont été fermées la veille au moment du calcul.

SLA de l'application : fermé

Cet indicateur est calculé quotidiennement. Il tient compte de l'âge total de toutes les vulnérabilités de l'application qui ont été fermées le jour précédent au moment du calcul.

SLA de résultat de test : réussi

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cet indicateur est calculé quotidiennement. Il prend en compte toutes les vulnérabilités des résultats des tests qui ont été transmises la veille au moment du calcul.

SLA hôte : nombre de fermetures

Cet indicateur est calculé quotidiennement. Il prend en compte le nombre de vulnérabilités de l'hôte qui ont été fermées le jour précédent au moment du calcul.

SLA de conteneur : compte fermé

Cet indicateur est calculé quotidiennement. Il prend en compte le nombre de vulnérabilités de conteneurs qui ont été fermées le jour précédent au moment du calcul.

SLA de l'application : nombre de fermetures

Cet indicateur est calculé quotidiennement. Il prend en compte le nombre de vulnérabilités d'applications qui ont été fermées le jour précédent au moment du calcul.

SLA de résultat de test : compte réussi

Cet indicateur est mesuré quotidiennement. Il prend en compte le nombre de vulnérabilités des résultats des tests qui ont été transmises pour la dernière fois le jour précédent au moment du calcul.

Actifs analysés

Cet indicateur est calculé quotidiennement. Elle tient compte de la somme des CI analysés à partir de la table sn_vul_analytics_scan_coverage_config, qui inclut ceux qui ont été analysés pour la dernière fois au cours des 90 derniers jours, dans toutes les classes de CI CMDB.

Actifs analysables

Cet indicateur est calculé quotidiennement. Elle prend en compte la somme du total des CI de sn_vul_analytics_scan_coverage_config table pour toutes les classes de CI CMDB présentes.

Éléments vulnérables

Cet indicateur est calculé quotidiennement. Il prend en compte le nombre d'éléments vulnérables actifs au moment du calcul.

Élément vulnérable de l'application

Cet indicateur est calculé quotidiennement. Il prend en compte le nombre d'éléments vulnérables actifs de l'application au moment du calcul.

Élément vulnérable de conteneur

Cet indicateur est calculé quotidiennement. Il prend en compte le nombre d'éléments vulnérables actifs du conteneur au moment du calcul.

Âge cumulé des éléments vulnérables

Cet indicateur est calculé quotidiennement. Il tient compte de l'âge cumulé des éléments vulnérables actifs au moment du calcul.

Âge cumulé des éléments vulnérables de l'application

Cet indicateur est calculé quotidiennement. Il tient compte de l'âge cumulé des éléments vulnérables actifs de l'application au moment du calcul.

Éléments vulnérables ouverts

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables ouverts au moment du calcul.

Éléments vulnérables du conteneur ouverts

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables du conteneur ouvert au moment du calcul.

Éléments vulnérables de l'application ouverts

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables de l'application ouverts au moment du calcul.

VIT différés

Cet indicateur est calculé quotidiennement. Il possède une source d'indicateur en tant qu'élément vulnérable de l'hôte.

AVIT différés

Cet indicateur est calculé quotidiennement. Il dispose d'une source d'indicateur en tant qu'élément vulnérable de l'application.

CVIT différés

Cet indicateur est calculé quotidiennement. Il a une source d'indicateur en tant qu'élément vulnérable de conteneur.

Résultats des tests différés

Cet indicateur est calculé quotidiennement. Il prend en compte les résultats des tests qui étaient dans un état différé.

Éléments vulnérables actifs en attente d'implémentation

Cet indicateur est calculé quotidiennement. Il considère les éléments vulnérables qui ont un état comme en attente d'implémentation au moment du calcul.

Problèmes de configuration ouverts : résultats des tests

Cet indicateur est calculé quotidiennement. Il dispose d'une source d'indicateur comme résultat de test pour le tableau de bord de Vulnerability Response unifié.

SI - Délai moyen d'identification

Cet indicateur est calculé quotidiennement. Il prend en compte l'incident de sécurité où définition est le temps à identifier au moment du calcul.

SI : durée moyenne

Cet indicateur est calculé quotidiennement. Il prend en compte l'incident de sécurité dont la définition est la durée de l'état de l'incident au moment du calcul.

Nombre d'incidents de sécurité majeurs ouverts

Cet indicateur est calculé quotidiennement. Il prend en compte les incidents de sécurité majeurs ouverts au moment du calcul.

Nombre d'incidents de sécurité clôturés

Cet indicateur est calculé quotidiennement. Il prend en compte les incidents de sécurité fermés au moment du calcul.

Éléments vulnérables d'application clôturés

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables de l'application fermés au moment du calcul.

Éléments vulnérables du conteneur fermés

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables du conteneur fermés au moment du calcul.

Éléments vulnérables clôturés

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cet indicateur est calculé quotidiennement. Il tient compte des éléments vulnérables fermés au moment du calcul.

Obtenir le score de risque maximal pour les éléments vulnérables

Cet indicateur est calculé quotidiennement. Il tient compte du score de risque maximal pour les éléments vulnérables au moment du calcul.

Obtenir le score de risque maximal pour l'élément vulnérable du conteneur

Cet indicateur est calculé quotidiennement. Il prend en compte le score de risque maximal pour les éléments vulnérables du conteneur au moment du calcul.

Obtenir le score de risque maximal pour les éléments vulnérables de l'application

Cet indicateur est calculé quotidiennement. Il prend en compte le score de risque maximal pour les éléments vulnérables de l'application au moment du calcul.

Score de risque cumulé des VIT

Cet indicateur est calculé quotidiennement. Il tient compte de la somme des scores de risque des éléments vulnérables au moment du calcul.

Score de risque cumulé des AVI

Cet indicateur est calculé quotidiennement. Il tient compte de la somme des scores de risque des éléments vulnérables de l'application au moment du calcul.

Score de risque cumulé des CVI

Cet indicateur est calculé quotidiennement. Il prend en compte la somme des scores de risque des éléments vulnérables du conteneur au moment du calcul.

Obtenir le score de risque maximal pour les incidents SI

Cet indicateur est calculé quotidiennement. Il prend en compte le score de risque maximal des incidents de sécurité au moment du calcul.

Obtenir le score du risque maximal pour les résultats des tests de configuration incorrecte

Cet indicateur est calculé quotidiennement. Il prend en compte les scores de risque maximaux pour une mauvaise configuration des résultats des tests au moment du calcul.

Obtenir le score du risque moyen pour les résultats des tests de configuration incorrecte

Cet indicateur est calculé quotidiennement. Il prend en compte les scores de risque moyen de mauvaise configuration des résultats des tests au moment du calcul.

Nombre d'incidents de sécurité ouverts

Cet indicateur est calculé quotidiennement. Il prend en compte les incidents de sécurité ouverts au moment du calcul.

Vue d'ensemble de l'hameçonnage

Cet indicateur est calculé quotidiennement. Il prend en compte le nombre de mesures de simulation de sécurité au moment du calcul.

Regrouper MTTR

Calcule le temps moyen nécessaire pour fermer les vulnérabilités (hôtes, conteneurs et applications) et le temps nécessaire pour fermer les résultats des tests en jours. [[SLA hôte : fermé]] + [[SLA d'application : fermé]] + [[SLA de conteneur : fermé]] + [[SLA de résultat de test : réussi]]) / ([[SLA hôte : nombre de fermetures]] + [[SLA d'application : nombre de fermetures]] + [[SLA de résultat de test : nombre de réussites]] + [[SLA de conteneur : nombre de fermetures]])

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Couverture de l'analyse actuelle

Calcule le pourcentage en utilisant le rapport entre le nombre d'éléments analysés et le nombre total d'éléments éligibles à l'analyse au cours de la même période. var scannedItems =[[Actifs analysés]] ; var scannableItems = [[Actifs analysables]] ; var res ; if (scannedItems == 0)res = 0 ; elseres = scannedItems / scannableItems * 100 ; si (res > 100)res = 100 ; Res;

Âge moyen des éléments vulnérables actifs

Calcule l'âge moyen de tous les éléments vulnérables actifs (hôtes, conteneurs et applications) en jours. ([[Âge cumulé des éléments vulnérables]] + [[Âge cumulé des éléments vulnérables de l'application]] + [[Âge cumulé des éléments vulnérables du conteneur]]) / ([[Éléments vulnérables]] + [[Éléments vulnérables de l'application]] + [[Éléments vulnérables du conteneur]])

VIT actives par âge et cote de risque

Calcule le nombre total de tous les éléments vulnérables actifs (hôtes, conteneurs et applications) classés par âge et niveau d'évaluation des risques. [[Éléments vulnérables ouverts]] + [[Éléments vulnérables du conteneur ouvert]] + [[Éléments vulnérables de l'application ouvert]]

Problèmes différés

Calcule le nombre total de tous les éléments vulnérables (hôtes, conteneurs, applications et résultats des tests) avec l'état « Différé ». [[VIT différés]] + [[AVIT différés]] + [[Résultats des tests différés]] + [[CVIT différés]]

Délai moyen de résolution des incidents de sécurité clôturés

Calcule le délai moyen nécessaire pour fermer les incidents de sécurité en jours. ([[Durée cumulée des incidents de sécurité fermés]] / [[Nombre d'incidents de sécurité fermés]]) /24

Score de sécurité

Calcule quotidiennement les évaluations de sécurité globales. Il est calculé en fonction du score de risque cumulé. var secPostureRating = 100 - [[Score de sécurité]] ; secPostureRating ;

Score de sécurité (unités business)

Calcule le score de risque cumulé final où le score de risque cumulé des éléments vulnérables, des erreurs de configuration, des incidents de sécurité et des incidents de sécurité majeurs est multiplié par les poids respectifs qui sont extraits de la table de déploiement de la posture de sécurité. var numMajorIncidents = [[Nombre d'incidents de sécurité majeurs ouverts]], majorSIRiskScore, rollUpRiskScore ; if(numMajorIncidents > 0) majorSIRiskScore = 100 ; sinon majorSIRiskScore = 0 ; rollUpRiskScore = ([[Score de risque déployé de vulnérabilité et d'erreur de configuration]] * 20 + [[Score de risque déployé de vulnérabilité OT]] * 20 + [[Obtenir le score de risque maximal pour les incidents SI]] * 20 + majorSIRiskScore * 40)/100 ; rollUpRiskScore ;

Score de sécurité (services d'entreprise)

Calcule le score de risque cumulé final où le score de risque cumulé des éléments vulnérables, des erreurs de configuration, des incidents de sécurité et des incidents de sécurité majeurs est multiplié par les poids respectifs qui sont extraits de la table de déploiement de la posture de sécurité. var numMajorIncidents = [[Nombre d'incidents de sécurité majeurs ouverts - Services]], majorSIRiskScore, rollUpRiskScore ; if(numMajorIncidents > 0) majorSIRiskScore = 100 ; sinon majorSIRiskScore = 0 ; rollUpRiskScore = ([[Score de risque déployé de vulnérabilité et d'erreur de configuration - Services]] * 20 + [[Score de risque déployé de vulnérabilité OT - Services]] * 20 + [[Obtenir le

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

score de risque maximal pour les incidents SI - Services]] * 20 + majorSIRiskScore * 40)/100 ; rollUpRiskScore ;

Score de risque déployé de vulnérabilité

Calcule le score de risque déployé de vulnérabilité où le score de risque maximal, le score de risque moyen des éléments vulnérables et le nombre d'éléments vulnérables sont multipliés par leurs poids respectifs. var maxRiskScore = 100 ; var count = [[VIT actives par âge et cote de risque]] ; var countRiskScore ; if (0 == count) countRiskScore = 0 ; sinon si (nombre > 10000) countRiskScore = maxRiskScore ; sinon si (nombre > 1000) countRiskScore = (maxRiskScore * 0.80) ; sinon si (nombre > 100) countRiskScore = (maxRiskScore * 0.60) ; else if (count > 10) countRiskScore = (maxRiskScore * 0.40) ; sinon countRiskScore = (maxRiskScore * 0.20) ; var vulRiskScore = ([[Obtenir le score maximal de tous les éléments vulnérables]] * 0 + [[Score de risque moyen de tous les éléments vulnérables]] * 100 + countRiskScore * 0)/100 ; vulRiskScore ;

Obtenir le score maximal pour tous les éléments vulnérables

Calcule le score de risque déployé de vulnérabilité où le score de risque maximal, le score de risque moyen des éléments vulnérables et le nombre d'éléments vulnérables sont multipliés par leurs poids respectifs. var maxScoreForVI = [[Obtenir le score de risque maximal pour les éléments vulnérables]], maxScoreForCVI = [[Obtenir le score de risque maximal pour l'élément vulnérable du conteneur]], maxScoreForAVI = [[Obtenir le score de risque maximal pour les éléments vulnérables de l'application]], maxScore ; si (maxScoreForVI >= maxScoreForCVI & maxScoreForVI >= maxScoreForAVI) maxScore = maxScoreForVI ; sinon si (maxScoreForCVI >= maxScoreForVI & maxScoreForCVI >= maxScoreForAVI) maxScore = maxScoreForCVI ; sinon maxScore = maxScoreForAVI ; maxScore ;

Scores de risque moyen de tous les éléments vulnérables

Calcule le score de risque moyen de tous les éléments vulnérables (hôtes, conteneurs et applications). var summedRiskScore = [[Cumul des scores de risque des VIT]] + [[Cumul des scores de risque des AVI]] + [[Cumul des scores de risque des VI]], avgRiskScore ; var totalVulCount = [[Éléments vulnérables ouverts]] + [[Éléments vulnérables de l'application ouverte]] + [[Éléments vulnérables du conteneur ouvert]] ; if(summedRiskScore == 0) avgRiskScore = 0 ; sinon si(totalVulCount .=0) avgRiskScore = summedRiskScore / totalVulCount ; avgRiskScore ;

Score de risque déployé des mauvaises configurations

Calcule le score de risque déployé de mauvaise configuration à l'aide des résultats des tests classés comme Échec, Erreur ou Inconnu. var maxRiskScore = 100 ; var count = [[Problèmes de configuration ouverts - Résultats des tests]] ; var countRiskScore ; if (0 == count) countRiskScore = 0 ; sinon si (nombre > 10000) countRiskScore = maxRiskScore ; sinon si (nombre > 1000) countRiskScore = (maxRiskScore * 0.80) ; sinon si (nombre > 100) countRiskScore = (maxRiskScore * 0.60) ; else if (count > 10) countRiskScore = (maxRiskScore * 0.40) ; sinon countRiskScore = (maxRiskScore * 0.20) ; var misRiskScore = ([[Obtenir le score de risque maximal pour les résultats des tests de configuration incorrecte]] * 0 + [[Obtenir le score de risque moyen pour les résultats des tests de configuration incorrecte]] * 100 + countRiskScore * 0)/100 ; misRiskScore ;

Délai moyen pour éradiquer

Calcule le temps moyen nécessaire pour éradiquer les incidents de sécurité en jours [[SI : durée moyenne > l'état d'incident de sécurité = éradiquer]] / 1 440

Délai moyen pour identifier

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calcule le temps moyen nécessaire pour identifier les incidents de sécurité en jours. [[SI - Délai moyen d'identification]] / 1440

Délai moyen pour contenir

Calcule le temps moyen nécessaire pour contenir les incidents de sécurité en jours. [[SI : durée moyenne >état d'incident de sécurité = contenir]] / 1 440

Respect de l'objectif de remédiation

Calcule le pourcentage mensuel d'adhésion à la cible de rattrapage à partir des résultats des tests, des éléments vulnérables, des éléments vulnérables de conteneurs et des éléments vulnérables de l'application. Le respect de l'objectif est déterminé par le nombre d'éléments qui ont atteint l'objectif fixé. ([[SLA de résultat de test : nombre de réussites > État de rattrapage (unifié) = Cible atteinte]] + [[SLA de conteneur : nombre de fermetures > État de rattrapage (unifié) = Cible atteinte]] + [[SLA d'application : nombre de fermetures > État de rattrapage (unifié) = Cible atteinte]] + [[SLA hôte - Nombre de fermetures > État de rattrapage (unifié) = Cible atteinte]]) / ([[SLA de résultat de test - Nombre de réussites]] + [[SLA de conteneur - Nombre de fermetures]] + [[SLA d'application - Nombre de fermetures]] + [[SLA hôte - Nombre de fermetures]]) * 100

Efficacité de la remédiation mensuelle (Tous les éléments vulnérables)

Calcule le pourcentage mensuel des éléments vulnérables fermés, des éléments vulnérables de conteneurs et des éléments vulnérables de l'application par rapport aux éléments nouvellement identifiés. var closedItems = [[SLA hôte - Nombre de fermetures]] + [[SLA de conteneur - Nombre de fermetures]] + [[SLA de l'application - Nombre de fermetures]] + [[SLA de résultat de test - Nombre de réussites]] ;

var newItems = [[VIT d'hôte ouverts/rouverts hier]] + [[VIT de conteneur ouverts/rouverts hier]] + [[VIT d'application ouverts/rouverts hier]] + [[Résultats des tests ouverts/rouverts hier]] ;

var res = 0 ; si (closedItems == 0) res = 0 ; else if (newItems .=0)res = closedItems / newItems * 100 ; si (res > 1000) res = 1000 ; Res;

VIT d'hôte ouverts/rouverts hier

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables de l'hôte qui ont été ouverts pour la dernière fois le jour précédent au moment du calcul.

VIT d'application ouverts/rouverts hier

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables de l'application qui ont été ouverts pour la dernière fois le jour précédent au moment du calcul.

VIT de conteneur ouverts/rouverts hier

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables du conteneur qui ont été ouverts pour la dernière fois le jour précédent au moment du calcul.

Résultats des test ouverts/rouverts hier

Cet indicateur est calculé quotidiennement. Il prend en compte les résultats des tests qui ont été vus pour la dernière fois la veille au moment du calcul.

Éléments vulnérables OT

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables OT actifs présents au moment du calcul.

Durée cumulée des vulnérabilités fermées OT

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cet indicateur est calculé quotidiennement. Il tient compte de l'âge total de toutes les vulnérabilités OT qui sont fermées le jour du calcul.

Éléments vulnérables OT fermés

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables OT qui sont fermés le jour du calcul.

Âge moyen des éléments vulnérables actifs OT

Calcule l'âge moyen des éléments vulnérables OT ([[Âge cumulé des éléments vulnérables OT]] / [[Éléments vulnérables OT]])

Répartitions

- Unité business
- Services d'entreprise
- Cote de risque
- Tranche d'âges
- Groupe d'affectation (unifié)
- État de la cible de rattrapage (fermé)
- Classe d'actifs
- Catégorie d'actif
- Évaluation du risque (unifiée)
- Raison de l'ajournement (unifiée)
- État de l'incident de sécurité
- Priorité de l'incident de sécurité
- Catégorie d'incident de sécurité
- Événement d'hameçonnage
- Raison de l'ajournement Non fermé (unifié)

Applications à activer

Vous devez activer les applications suivantes pour renseigner le score dans les widgets. En fonction de l'application que vous utilisez, vous devez activer les applications dépendantes.

Si vous utilisez	Activer
Réponse aux vulnérabilités	• Performance Analytics pour Vulnerability Response • Vulnerability Response commun • Réponse aux vulnérabilités • Vulnerability Response et Configuration Compliance pour les conteneurs • Configuration Compliance
Operational Technology	Vulnerability Response pour Operational Technology

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous utilisez	Activer
Intégrations de l'hameçonnage	• Intégration de la simulation et de la formation de sécurité pour les opérations de sécurité • Intégration KnowBe4 pour SecOps • Intégration de Microsoft Defender pour Office 365 pour SecOps
Réponse aux incidents de sécurité	• Analyse des performances pour Réponse aux incidents de sécurité • Réponse aux incidents de sécurité • Gestion des incidents de sécurité majeurs
Gouvernance, risque et conformité	• GRC : éléments communs du tableau de bord • GRC : Espace de travail Gestion des risques • GRC: Advanced Risk • GRC : Espace de travail pour la gestion de Compliance

Travaux planifiés pour la collecte de données

Les travaux planifiés suivants sont exécutés pour collecter automatiquement les scores sur de nouvelles données.

Tâche planifiée	Fréquence	Description
Charger les scores de point de référence	Sur demande	Collecte les scores de l'instance et les publie sur l'instance centrale. Les algorithmes d'analyse comparative calculent les meilleurs scores de l'industrie.
Télécharger les scores de point de référence	Sur demande	Télécharger les scores de point de référence. Il est disponible dans la table Scores de point de référence [sn_bm_client_score_list].

Adhésion aux scores de point de référence

Obtenez des scores de point de référence en inscrivant votre instance sur l'instance ServiceNow centrale. Ce dernier conserve des informations sur plusieurs industries pour fournir le score de référence.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Pour enregistrer votre instance auprès de l'instance centrale, procédez comme suit :

   a. Accédez à la **Tout** > **Propriétés système** > **Toutes les propriétés**.

   b. Sélectionnez la *sn_bm_client.central_instance_url* propriété système.

   c. Dans le champ **Valeur** , saisissez l'URL de l'instance centrale de point de référence.

   > **Remarque :** Si l'instance est mise en service, vos détails sont automatiquement transmis à l'instance centrale.

   d. Sélectionnez **Opt-in (Opt-in**) à partir du widget pour valider et établir une connexion avec l'instance centrale.

2. Pour charger votre score sur l'instance centrale, procédez comme suit :

   a. Accédez à la **Tout** > **Planificateur système** > **Travaux planifiés**

   b. Sélectionnez la *Upload the benchmark scores* tâche planifiée.

   c. Sélectionnez **Mettre à jour**.
   Les scores sont téléchargés dans l'instance centrale. Toutefois, les travaux planifiés par l'instance centrale s'exécutent une fois par mois pour mettre à jour les scores sur les widgets du tableau de bord.

3. Pour télécharger la partition à partir de l'instance centrale, procédez comme suit :

   a. Accédez à la **Tout** > **Planificateur système** > **Travaux planifiés**

   b. Sélectionnez la *Download the benchmark scores* tâche planifiée.

   c. Sélectionnez **Exécuter maintenant**.
   Les scores sont disponibles dans la table Scores de point de référence [sn_bm_client_score_list], qui est reflétée dans les widgets du tableau de bord.

Définir des cibles

Définissez des cibles en jours pour corriger les vulnérabilités, les incidents de sécurité et les erreurs de configuration.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Sélectionnez **Cibles** dans le widget ou sélectionnez l'icône **Cibles** sur la page Détails des KPI.
2. Sélectionnez le bouton **Pour tout le monde** .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

3. Dans le champ **Nouvelle valeur** , saisissez le nombre de jours pendant lesquels vous souhaitez atteindre l'objectif.
4. Sélectionnez la date de début de la cible.
5. Sélectionnez la date d'examen cible.
6. Sélectionnez **Mettre à jour**.

Intégration de la simulation et de la formation de sécurité pour les opérations de sécurité

Renforcez la défense de votre organisation contre les principales menaces de cybersécurité en intégrant des intégrations d'hameçonnage au tableau de bord de direction de cybersécurité. Les intégrations d'hameçonnage améliorent le tableau de bord de direction de cybersécurité en incorporant de manière transparente des données provenant d'outils de simulation d'hameçonnage tiers tels que KnowBe4 et Microsoft Defender pour Office 365.

Les intégrations suivantes améliorent les capacités du tableau de bord de direction de cybersécurité, en offrant une perspective unifiée sur la posture de sécurité de votre organisation, la préparation des employés et la vulnérabilité aux attaques de phishing :

- Intégration KnowBe4
- Intégration de Microsoft Defender pour Office 365

Configurer l'intégration Knowbe4

Obtenez des informations immédiates sur la vulnérabilité de votre personnel aux attaques de phishing en l'intégrant à KnowBe4, une plateforme de formation de sensibilisation à la cybersécurité de premier plan. Grâce à l'intégration de KnowBe4, identifiez les tendances et les domaines d'amélioration dans vos programmes de formation à la cybersécurité, surveillez la résilience globale du phishing et renforcez de manière proactive les mesures de sécurité de votre organisation.

Avant de commencer

Rôle requis : sn_sec_phish.admin et sn_sec_phish_kb4.kb4_admin

Procédure

1. Accédez à la **Tout** > **Intégration KnowBe4** > **KnowBe4 Configurations**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs suivants du formulaire :

Formulaire de configuration KnowBe4

Champ	Description
Instance d'intégration	Nom de l'instance d'intégration. Sélectionnez l'instance d'intégration à l'aide de l'icône de recherche.
URL de base	URL à intégrer à KnowBe4.
Clé API	Clé API acquise à partir du compte KnowBe4.
Page	Numéro de page à partir duquel les simulations doivent être extraites.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Taille de page	Nombre de simulations à inclure.

a. Sélectionnez **Nouveau** si aucune instance d'intégration n'est disponible.

b. Renseignez les champs suivants du formulaire :

Formulaire Instance d'intégration

Champ	Description
Nom	Nom de l'instance d'intégration.
Application	Nom de l'application (Intégration KnowBe4 pour SecOps).
Intégration	KnowBe4 est la valeur par défaut.
Actif	La valeur par défaut est activée (sélectionnée). Si elle est décochée, l'instance n'est pas active.
Description	Brève description de l'instance d'intégration.

4. Sélectionnez **Soumettre**.
5. Accédez à la **Tout** > **Simulation et formation de sécurité** > **Intégrations**.
6. Sélectionnez l'intégration Knowbe4.
7. Sélectionnez **Exécuter maintenant** pour exécuter et collecter des données à partir de KnowBe4.

Configurer l'intégration de Microsoft Defender pour Office 365

Obtenez des informations précieuses sur les mesures de simulation d'hameçonnage directement dans le tableau de bord de direction de cybersécurité grâce à une intégration transparente avec Microsoft Defender pour Office 365.

Avant de commencer

Rôle requis : sn_sec_phish_msatk.ms_admin

Procédure

1. Accédez à la **Tout** > **Intégration des attaques Microsoft** > **Configurations d'attaques Microsoft**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs suivants du formulaire :

Formulaire de configuration des attaques Microsoft

Champ	Description
Instance d'intégration	Nom de l'instance d'intégration. Sélectionnez l'instance d'intégration à l'aide de l'icône de recherche.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID de locataire	ID de locataire de l'application créée sur le portail Microsoft Azure.
ID client	ID client de l'application créée sur le portail Microsoft Azure.
Secret client	Secret client de l'application créée sur le portail Microsoft Azure.
Signet	Date à partir de laquelle les simulations doivent être extraites.
URL de jeton	URL de base à partir de laquelle le jeton est créé pour accéder à l'API de simulations Microsoft.
Toutes les URL de simulation	URL de base de l'API de simulations Microsoft.

a. Sélectionnez **Nouveau** si aucune instance d'intégration n'est disponible.

b. Renseignez les champs suivants du formulaire :

Formulaire Instance d'intégration

Champ	Description
Nom	Nom de l'instance d'intégration.
Application	Nom de l'application (Microsoft Defender pour Office 365).
Intégration	Référence d'intégration tierce (Microsoft Attack Integration).
Actif	La valeur par défaut est activée (sélectionnée). Si elle est décochée, l'instance n'est pas active.
Description	Brève description de l'instance d'intégration.

4. Sélectionnez **Soumettre**.

5. Accédez à la **Tout** > **Simulation et formation de sécurité** > **Intégrations**.

6. Sélectionnez Microsoft Attack Integration.

7. Sélectionnez **Exécuter maintenant** pour exécuter et collecter des données à partir de Microsoft.

Tableau de bord des risques et de la conformité pour GRC : Mesures

Le tableau de bord des risques et de la conformité fournit aux utilisateurs de la conformité et des risques une vue d'ensemble complète des informations relatives aux risques et à la conformité dans un tableau de bord unique qui les aide dans leurs décisions clés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez accéder au tableau de bord Risque et conformité à partir de l'unifié Tableau de bord de direction de cybersécurité unique pour afficher les mesures de risque et de conformité des Gouvernance, risque et conformité applications.

Le tableau de bord fournit des fonctionnalités telles que :

- Vue d'ensemble de la conformité
- Vue d'ensemble du risque
- Vue d'ensemble de la confidentialité
- Vue d'ensemble de la continuité d'activité
- Risque de tiers
- Vue d'ensemble de l'audit

Conditions préalables pour accéder au tableau de bord des risques et de la conformité

Important : Vous devez disposer d'un accès primaire à pour Tableau de bord de direction de cybersécurité activer le module d'extension fonctionnel Cybersécurité et risque avec lequel vous pouvez accéder au tableau de bord des risques et de la conformité.

Un nouveau domaine fonctionnel est introduit pour séparer les données liées à la cybersécurité et aux risques. Vous pouvez activer le module d'extension de cybersécurité et de risque en sélectionnant le bouton d'action d'interface utilisateur **Activer** . Par défaut, ce domaine fonctionnel est inactif.

Rôles Now Platform requis

Le rôle d'utilisateur principal GRC est le sn_grc_dashboards.grc_ciso_user, qui peut afficher les rapports sur le tableau de bord des risques et de la conformité. Ce rôle contient :

- sn_compliance.reader
- sn_risk.reader

Remarque : Toutefois, vous devez disposer du rôle sn_bod.ciso pour vous connecter, afficher et partager le tableau de bord de direction de cybersécurité à partir duquel vous pouvez accéder au tableau de bord des risques et de la conformité.

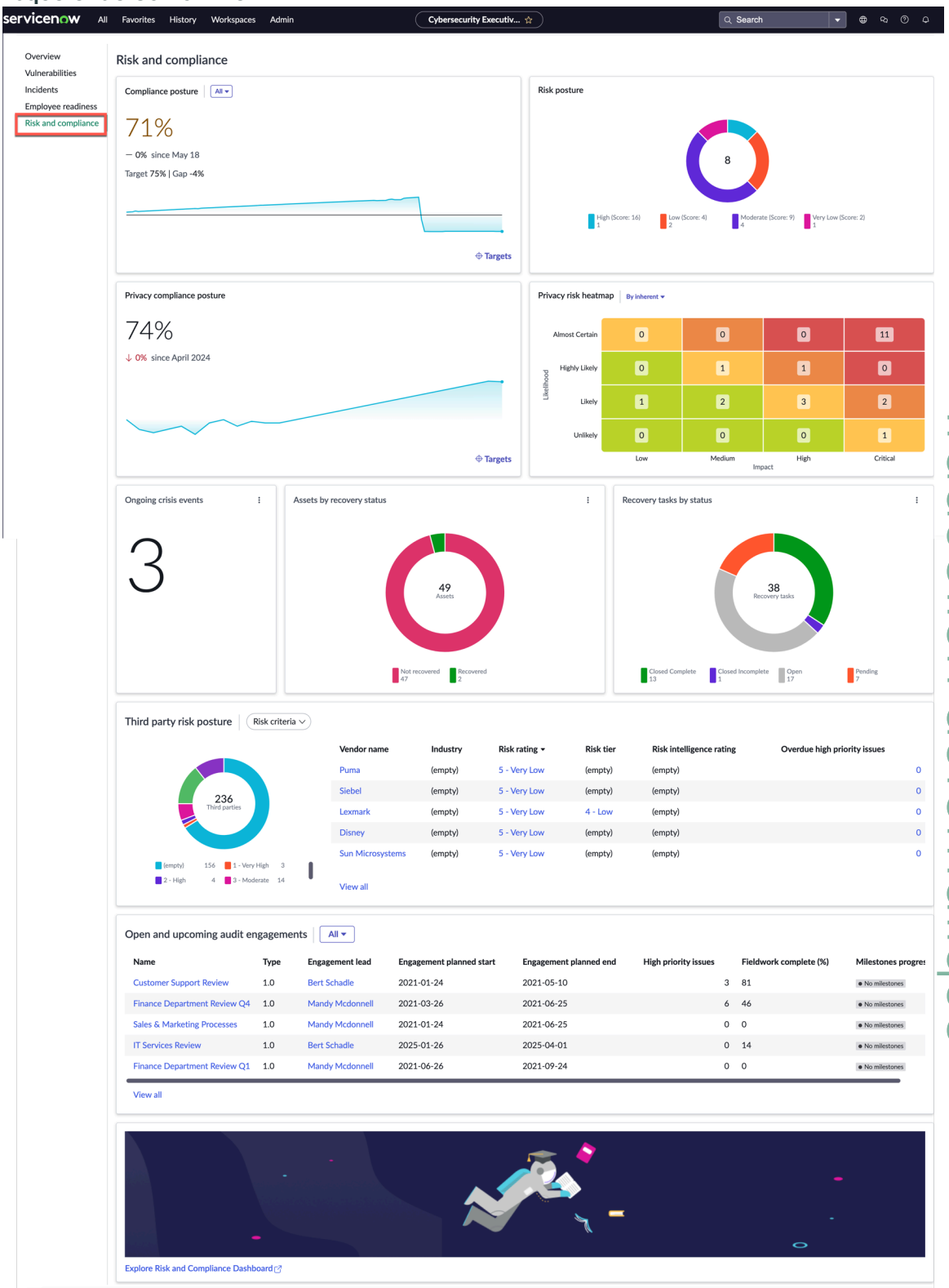
Accéder au tableau de bord des risques et de la conformité

1. Pour accéder au tableau de bord des risques et de la conformité, accédez à **Tout** > **Tableau de bord de direction de cybersécurité** > **Tableau de bord de direction de cybersécurité**.
2. Sélectionnez **Étiquette de risque et de conformité** dans la liste située à gauche du tableau de bord.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau de bord unifié de direction de cybersécurité pour les mesures de risque et de conformité



Traduction automatique

3. Pour visualiser vos données et afficher les rapports et les solutions disponibles sur le tableau de bord conçu pour l'utilisateur, sélectionnez l'étiquette Explorer le tableau de bord Risk and Compliance.

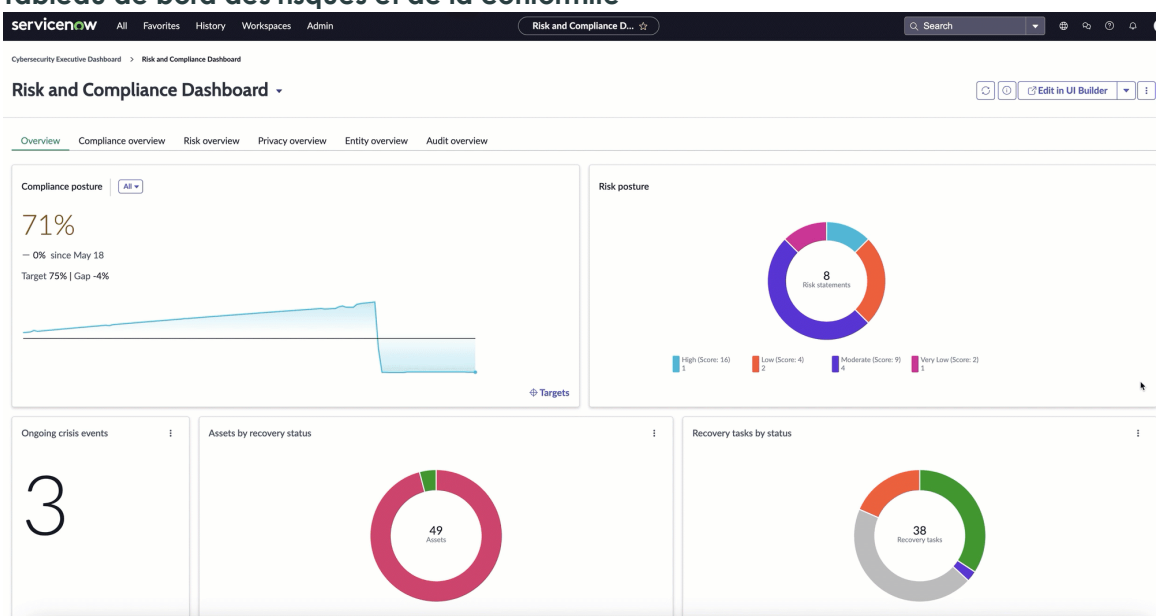
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Risque et conformité Rapports et solutions de tableau de bord

Le tableau de bord des risques et de la conformité est un tableau de bord unifié qui fournit au responsable de la sécurité de l'information une analyse complète des rapports disponibles à partir des principales applications GRC afin de comprendre la posture de l'organisation en matière de conformité et de risque. Le tableau de bord consolide les données de divers produits au sein de la ServiceNow GRC suite d'applications.

Remarque : Tous les rapports ne sont disponibles que lorsque les espaces de travail correspondants sont installés.

Tableau de bord des risques et de la conformité



Rôles Now Platform requis

Pour les rapports associés à la conformité

L'utilisateur doit disposer du rôle sn_grc_dashboards.grc_ciso_user et du rôle sn_bod.ciso.

Pour les rapports associés aux risques

L'utilisateur doit disposer du rôle sn_grc_dashboards.grc_ciso_user et du rôle sn_bod.ciso.

Pour les rapports associés à Business Continuity Management

L'utilisateur doit avoir les rôles sn_bcm.viewer et sn_bod.ciso.

Pour les rapports liés aux risques liés aux tiers

L'utilisateur doit disposer du rôle sn_vdr_risk_asmt.vendor_assessment_reviewer et du rôle sn_bod.ciso.

Pour les rapports relatifs à la confidentialité

L'utilisateur doit avoir le rôle sn_privacy.analyst et le rôle sn_bod.ciso.

Pour les rapports associés à l'audit

L'utilisateur doit avoir le rôle sn_audit_ws.auditor et le rôle sn_bod.ciso.

Accéder au tableau de bord Risk and Compliance

Pour ouvrir le tableau de bord, accédez à **Tout** > **Tableau de bord de direction de cybersécurité** > **Tableau de bord de direction de cybersécurité**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indicateurs

Posture de conformité

- Pourcentage de conformité : indicateur de formule qui représente la posture de conformité.
- Tous les contrôles : indicateur automatisé qui prend en charge l'indicateur de formule.
- Contrôles conformes : indicateur automatisé qui prend en charge l'indicateur de formule.

Posture de conformité de la confidentialité

Indicateur PA : pourcentage du score de conformité de l'activité de traitement.

Répartitions

Domaine fonctionnel.

Rapports

Remarque : Tous les rapports ne sont disponibles que lorsque les espaces de travail correspondants sont installés.

Onglet Vue d'ensemble

Titre	Type	Table source	Description
Posture de conformité	Graphique en courbes	Contrôle [sn_compliance_control]	Fournit aux gestionnaires de conformité un état de cybersécurité et de gestion des risques, ainsi qu'une posture de risque informatique et de conformité basée sur l'analyse des données.
Situation vis-à-vis du risque		Les tables sources sont les suivantes : • Risque [sn_risk_risk] • Risque agrégé détaillé [sn_risk_advanced_risk_assessment_result] (lorsque l'application est installée et que l'évaluation Risque avancé avancée des risques est activée)	Fournit le nombre de risques en fonction des évaluations de risques.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble (suite)

Titre	Type	Table source	Description
Événements de crise en cours	Score unique	Événement de reprise [sn_recovery_event] où le type d'événement est réel	Affiche le nombre total d'événements de crise en cours qui ne sont ni approuvés ni fermés.
Actifs par état de reprise		Actifs [sn_recovery_event_asset]	Fournit le nombre total d'actifs pour les événements de crise en cours regroupés par état de reprise, y compris les actifs qui ont été récupérés et ceux qui ne l'ont pas été.
Tâches de reprise par état		Tâches de reprise [sn_recovery_event_task]	Fournit l'état des tâches de reprise dans différents états pour les événements de crise en cours.

Onglet Vue d'ensemble de la conformité

Titre	Type	Table source	Description
Documents de référence		Source de référence [sn_compliance_authority_document]	Fournit des données sur les documents de référence conformes et non conformes dans le graphique. La liste fournit des détails sur les documents de référence, leur score de conformité individuel en pourcentage, le nombre de problèmes de priorité élevée et d'exceptions à risque élevé sur les documents de référence, ainsi que le nombre de tickets de conformité.
Politiques		Politique [sn_compliance_policy]	Fournit le nombre de politiques conformes et non conformes dans le graphique. La liste fournit des détails sur les politiques, leur score de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble de la conformité (suite)

Titre	Type	Table source	Description
			conformité individuel en pourcentage, le nombre de problèmes de priorité élevée et d'exceptions de risque soulevés pour chaque politique, ainsi que le nombre de tickets de conformité.

Onglet Vue d'ensemble du risque

Titre	Type	Table source	Description
Situation vis-à-vis du risque		Les tables sources sont les suivantes : • Risque [sn_risk_risk] • Risque agrégé détaillé [sn_risk_advanced_risk_assessment_result] (lorsque l'application est installée et que l'évaluation Risque avancé Advanced Risk est activée)	Fournit le nombre de risques en fonction des évaluations de risques.
Situation vis-à-vis du risque		État du contenu GRC [sn_grc_content_report]	Fournit la cote de risque pour chaque risque organisationnel afin de comprendre les résultats globaux de l'évaluation des risques. Ces évaluations aident les organisations à comprendre l'impact potentiel et la probabilité de divers risques, ce qui leur permet de hiérarchiser et de gérer ces risques. La carte Situation vis-à-vis du risque met également en évidence les informations

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble du risque (suite)

Titre	Type	Table source	Description
			suivantes pour chaque risque : • **Appétence au risque** : valeur de l'appétence au risque définie. • **Problèmes de priorité élevée** : le nombre de problèmes de priorité élevée est défini comme élevé. • **Tâches de réponse aux risques en retard** : nombre de tâches de réponse aux risques en retard. • **% de violation des KRI** : pourcentage d'indicateurs de risques clés (KRI) qui ont dépassé leurs seuils ou limites prédéfinis.
Situation vis-à-vis des tiers		Risques de tiers [sn_grc_dashboards_third_party_risk]	Fournit la cote de risque par risk chaque tiers. La note de risque est la note d'évaluation globale qui prend en compte les scores et les évaluations de toutes les évaluations effectuées pour un tiers ou un fournisseur. La carte Situation vis-à-vis des risques des tiers met également en évidence les informations suivantes pour chaque tiers ou fournisseur : • **Critères de risque** : groupe de domaines de risque (parfois appelés

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble du risque (suite)

Titre	Type	Table source	Description
			domaines de risque dans d'autres fonctionnalités de la plateforme) qui s'appliquent à un type particulier de tiers. • **Niveau de risque** : valeur déterminée en fonction des réponses recueillies après l'achèvement d'une évaluation des risques inhérents (IRQ). • **Cote des renseignements** sur les risques : agrégat de tous les scores collectés auprès des fournisseurs de renseignements sur les risques. • **Tâches de réponse aux risques en retard** : nombre de tâches de réponse aux risques en retard.

Onglet Vue d'ensemble de la confidentialité

Titre	Type	Table source	Description
Posture de conformité de la confidentialité	Ligne	Indicateur PA : pourcentage du score de conformité de l'activité de traitement [pa_indicators]	Indique la posture de conformité par mois et est tracé en se référant au score de conformité global pour toutes les activités de traitement.
Questions de haute priorité en retard	Score unique	Problèmes [sn_grc_issue]	Fournit une vue d'ensemble ciblée de tous les problèmes hautement prioritaires liés à la confidentialité en retard, permettant

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble de la confidentialité (suite)

Titre	Type	Table source	Description
			une identification et une résolution rapides des tâches critiques pour garantir la conformité et la protection des données.
Carte thermique des risques de confidentialité	Carte thermique	Méthodologie d'évaluation des risques [sn_risk_advanced_risk_assessment_methodology]	Fournit les données d'évaluation des risques pour la confidentialité sous la forme d'une carte thermique. Les évaluations des risques pour la confidentialité sont des évaluations détaillées qui sont effectuées si le score de criticité est élevé. Évaluez chaque risque associé à l'activité de traitement et connaissez le score de risque agrégé sur l'activité de traitement. Après avoir évalué les risques pour la confidentialité, vous pouvez afficher la situation en matière de risque pour la confidentialité sur la carte thermique des risques.

Onglet Vue d'ensemble de l'entité

Titre	Type	Table source	Description
Entités		État de conformité de l'entité [sn_compliance_entities_respects]	Fournit le résumé des risques directement associés à l'entité qui contribuent à la notation globale des risques de l'entité. La liste affiche également le score de conformité des entités, ainsi que

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble de l'entité (suite)

Titre	Type	Table source	Description
			les problèmes de priorité élevée et les exceptions de risque soulevés en raison des contrôles non conformes associés à l'entité.

Onglet Vue d'ensemble de l'audit

Titre	Type	Table source	Description
Engagements d'audit ouverts et à venir		Engagement [sn_audit_engagement]	Fournit une liste des missions d'audit ouvertes et à venir. La liste fournit également des détails sur le responsable de la mission pour chaque document de référence, les dates de début et de fin prévues de chaque mission, les questions hautement prioritaires, le pourcentage de travail sur le terrain terminé et les jalons en cours.

Filtres

Nom	Type	Description
Critères de risque	Rapport	En fonction des critères de risque que vous sélectionnez, le graphique en anneau et la liste affichent les tiers ou fournisseurs qui se trouvent dans ces domaines de risque.

Threat Intelligence Security Center

La Centre de sécurité des renseignements sur les menaces plate-forme (TISC) fournit une solution technologique pour l'agrégation, la gestion et l'opérationnalisation de la connaissance des menaces.

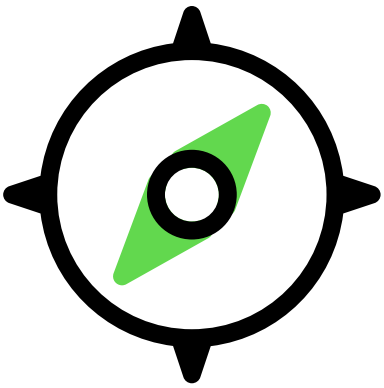
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Premiers pas

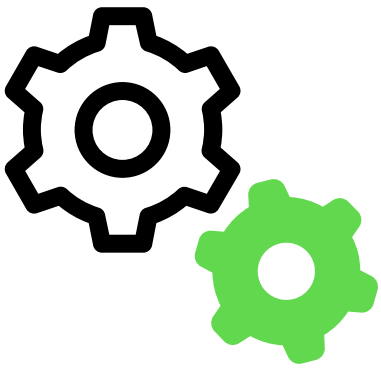
Cliquez sur une tuile pour commencer.

Explorer



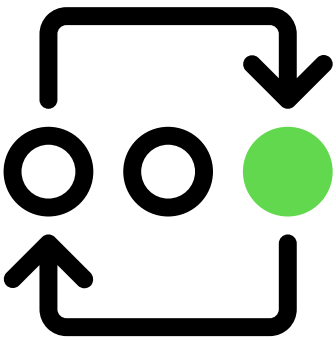
Découvrez comment Threat Intelligence Security Center peut vous aider avec ses principales fonctionnalités et avantages.

Configurer



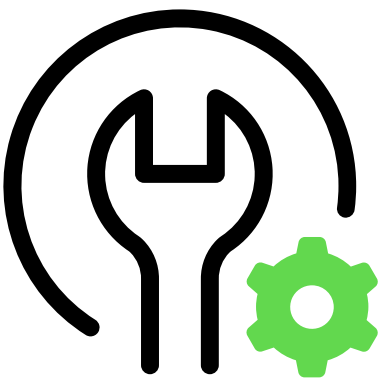
Installez et configurez Threat Intelligence Security Center pour répondre à vos besoins spécifiques.

Intégrer



Intégrer à Threat Intelligence Security Center

Administrer



Gérez et personnalisez votre centre de sécurité Renseignements sur les menaces.

Utiliser



Gérez votre bibliothèque et vos objets du Centre de sécurité des renseignements sur les menaces.

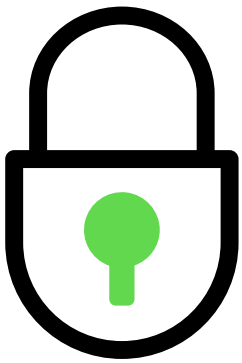
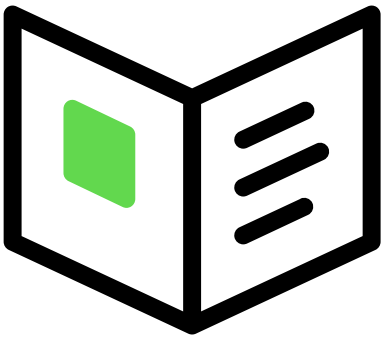
Modèles de rapports



Gérez et personnalisez vos rapports de gestion des tickets.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Référentiel MITRE ATT&CK	Archive	Référence
		
Gérez les données du référentiel MITRE ATT&CK.	Gérer l'archivage des données et les règles de destruction.	Obtenir des informations supplémentaires sur le Centre de sécurité des renseignements sur les menaces.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

L'installation Centre de sécurité des renseignements sur les menaces de (sn_sec_tisc) installe automatiquement toutes les applications dépendantes à partir de ServiceNow Store.

Plus de ressources

Visitez le Réponse aux incidents de sécurité forum sur le ServiceNow Community.

Dépannage et demande d'aide

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

Explorer Centre de sécurité des renseignements sur les menaces

Centre de sécurité des renseignements sur les menaces (TISC) vous permet de collaborer avec les équipes de renseignements sur les menaces et dispose de plusieurs options pour collecter et traiter divers flux de renseignements sur les menaces, ainsi que d'un espace de travail pour analyser, collaborer, agir et partager les informations nécessaires.

Threat Intelligence Security Center est amélioré avec des options pour gérer la collecte de données, le traitement des données telles que la déduplication, la normalisation et l'agrégation, l'analyse des renseignements sur les menaces, la diffusion des renseignements sur les menaces, ainsi que l'espace de travail qui fournit les tâches d'administration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalités principales

Voici les principales fonctionnalités du Centre de sécurité des renseignements sur les menaces (TISC) qui sont expliquées en détail dans les sections suivantes :

- Collecte de données à partir de différentes sources et dans divers formats.
- Agrégation de données provenant de divers flux, y compris STIX, XML, JSON et OpenIOC.
- Options d'enrichissement, impliquant la suppression des faux positifs, la confiance/la notation des indicateurs, la validation des indicateurs et l'ajout d'informations contextuelles.
- Un calculateur de score de menace personnalisé pour une évaluation nuancée des menaces.
- Intégration de l'intelligence interne englobant VR, SIR, Assets, Services et CMDB.
- Chasse aux menaces avec des fonctionnalités de gestion des tickets et de tâches.
- Tableaux de bord spécifiques à l'utilisateur, adaptés aux profils Threat Intel.
- Outils de visualisation graphique pour comprendre les données Threat Intel.
- Un espace de travail Threat Intelligence Analyst Workspace dédié pour rationaliser les opérations.
- Règles de corrélation pour établir automatiquement des relations entre les observables.
- Le système a la capacité d'identifier et d'extraire automatiquement tous les observables des fichiers chargés.
- Intégration de flux premium pour améliorer la connaissance des menaces.
- Permettre aux utilisateurs d'associer des informations MITRE ATT&CK à des enregistrements dans la bibliothèque Threat Intelligence et la gestion des tickets.
- Intégration avec SIR et options de migration de données de Threat Intelligence vers Threat Intelligence Security Center.

Terminologie clé TISC

Les termes définis ci-dessous sont utilisés dans l'ensemble du Centre de sécurité des renseignements sur les menaces (TISC).

Définitions terminologiques

Terminologie	Définition
Traitement des données	Une plateforme de renseignements sur les menaces (TIP) est une solution technologique qui collecte, agrège et organise des données de renseignements sur les menaces provenant de diverses sources et modèles. Les renseignements sur les menaces sont les données qui sont collectées, traitées et analysées pour comprendre les cibles et les comportements d'attaque d'un acteur de menace.
Observables	Les observables représentent des propriétés avec état (telles que le hachage MD5 d'un fichier ou la valeur d'une clé de Registre) ou des événements mesurables (tels que la création d'une clé de registre ou la suppression d'un fichier) qui sont pertinents

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définitions terminologiques (suite)

Terminologie	Définition
	pour le fonctionnement des ordinateurs et des réseaux. Pour plus d'informations, consultez Observables.
Indicateurs	Les indicateurs contiennent un modèle qui peut être utilisé pour détecter les cyberactivités suspectes ou malveillantes. Par exemple, un indicateur peut être utilisé pour représenter un ensemble de domaines malveillants et utiliser le langage de modélisation STIX pour spécifier ces domaines. L'indicateur SDO contient une description textuelle simple, les phases de kill chain dans lesquelles il détecte le comportement, une fenêtre de temps indiquant quand l'indicateur est valide ou utile, et une propriété de **modèle** requise pour capturer un modèle de détection structuré. Pour plus d'informations, consultez Indicateurs.
Objets	Définit l'ensemble des objets de domaine STIX (SDO), chacun d'entre eux correspondant à un concept unique couramment représenté dans Cyber Threat Intelligence (CTI). En utilisant les SDO et les objets relationnels STIX (OAR) comme éléments constitutifs, les individus peuvent créer et partager des renseignements sur les cybermenaces vastes et complets. Pour plus d'informations, consultez Référentiel de la bibliothèque TISC.
Relations	Une relation est un lien entre deux observables ou deux SDO ou un observable et un SDO qui décrit la manière dont les objets sont liés. Les relations peuvent être représentées à l'aide d'un objet de relation STIX (SRO) externe ou, dans certains cas, par le biais de certaines propriétés qui stockent une référence d'identificateur qui comprend une relation imbriquée. Pour plus d'informations, consultez Objets de relations.

Traduction automatique

Séparation de domaine et Threat Intelligence Security Center

Centre de sécurité des renseignements sur les menaces prend en charge Séparation de domaine. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Standard

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

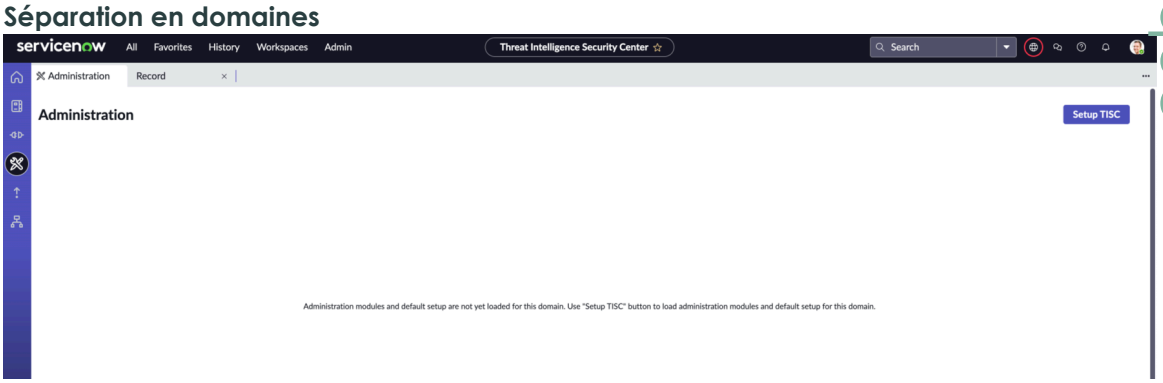
Vue d'ensemble

L'application Séparation de domaine est activée pour toutes les fonctionnalités de Centre de sécurité des renseignements sur les menaces.

Comment fonctionne Séparation de domaine dans Centre de sécurité des renseignements sur les menaces

- Tous les enregistrements liés à la configuration qui sont mis en service dans le système de base sont expédiés dans le domaine global. Dans le cas où l'instance est séparée par domaine, les utilisateurs verront un bouton explicite **Configurer TISC** sous le module **Administration** de l'espace de travail TISC. Cliquez sur ce bouton pour cloner les configurations de domaine global mises en service par le système de base dans les domaines respectifs.

Séparation en domaines



Remarque : Les utilisateurs doivent uniquement activer ou modifier les enregistrements de configuration spécifiques à un domaine et ne doivent pas activer ou modifier les enregistrements de configuration dans le domaine global.

- Deux règles de notification de plateforme (sysevent_email_action) sont mises en service dans le système de base. Ces règles de notification doivent être clonées dans les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

domaines requis et seules les règles de notification spécifiques au domaine doivent être activées.

Remarque : Pour plus d'informations sur les notifications de règles, accédez à **Notification système** > **Notifications** et filtrez toutes les règles de notification de domaine globales définies dans les tables commençant par le *nom sn_sec_tisc* afin de comprendre comment les utilisateurs peuvent identifier les règles de notification de base qui sont mises en service dans le système de base.

- Toutes les configurations et les données ingérées seront spécifiques à chaque domaine, ce qui signifie que les utilisateurs d'un domaine ne pourront pas accéder aux données d'un autre domaine.
- Configurez un environnement séparé par domaine avec cette application en installant le module d'extension Domain Support - Domain Extensions Installer .
- Des colonnes de domaine sont ajoutées pour toutes les tables d'application du système de base.
- À l'aide de la fonctionnalité fournie par la plateforme, les domaines de locataire gèrent leurs propres données d'application.
- La logique métier et les processus qui peuvent être séparés par domaine par le propriétaire de l'instance sont identiques à ceux pris en charge par Platform.
- La logique métier et les processus qui peuvent être administrés par le domaine du locataire sont identiques à ceux pris en charge par la plateforme.
- Vous pouvez accéder à la page Configuration à partir de la section Administration. Cliquez sur le lien fourni dans la section Administration pour afficher la vue Séparation de domaine.
- Pour prendre en charge Séparation de domaine pour les widgets à l'aide d'indicateurs Analyse des performances (PA) dans le tableau de bord d'accueil TISC, consultez l'article de la base de connaissances KB1647990 la procédure détaillée.

Tables séparées par domaine

Toutes les tables sont séparées par domaine.

Cas d'utilisation

Toutes les fonctionnalités de cette application sont séparées par domaine.

Information associée

Séparation de domaine pour les fournisseurs de services

Configurer Threat Intelligence Security Center

Avant d'utiliser le Centre de sécurité des renseignements sur les menaces, vous devez le télécharger à partir du ServiceNow Store.

Rôles installés

Examinez les informations suivantes et vérifiez que vous avez effectué toutes les tâches pour une intégration fluide. Vous trouverez ci-dessous la liste des différents profils d'utilisateur définis pour accéder à l'application et travailler avec elle :

- Analyste Threat Intelligence (sn_sec_tisc.analyst)
- Administrateur Threat Intelligence (sn_sec_tisc.admin)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisations applicables pour les rôles TISC

Configuration	Description
Affectez et vérifiez les rôles requis Now Platform et Threat Intelligence Security Center.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • En tant qu'administrateur, vous devez installer l'application TISC à partir du ServiceNow Store et affecter le rôle sn_sec_tisc.admin. • Ce rôle sn_sec_tisc.admin effectue les tâches suivantes : ◦ Configure les sources de données pour ingérer les données. Pour plus d'informations, consultez Flux Threat Intelligence. ◦ Configurer les intégrations requises pour l'enrichissement des données observables dans TISC. Pour plus d'informations, consultez Intégrations de l'enrichissement TISC. ◦ Configure les rôles d'approbation d'importation de données pour l'importation de données à l'aide de l'assistant d'importation. Pour plus d'informations, consultez Utilisation des importations de données. ◦ Configure le calculateur de score de menace à l'aide des critères requis pour le calcul automatique du score de menace des observables. Pour plus d'informations, consultez Définir le calculateur de score de menace. ◦ Configure les taxonomies et valeurs de taxonomie requises. Pour plus d'informations, consultez Création de taxonomies. ◦ Configurez le référentiel MITRE ATT&CK pertinent pour votre organisation. Pour plus d'informations, consultez MITRE-ATT&CK Dépôt. **Remarque :** En tant que sn_sec_tisc.admin, vous pouvez également affecter le rôle sn_sec_tisc.analyst. • Le rôle sn_sec_tisc.analyst effectue les tâches suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisations applicables pour les rôles TISC (suite)

Configuration	Description
	◦ Affiche la vue d'ensemble des données dans le système à l'aide de la page d'accueil du produit. Pour plus d'informations, consultez Afficher la page d'accueil de Threat Intelligence Security Center. ◦ Importez des données dans le système à l'aide du bouton Import Intelligence de la page bibliothèque de menaces. Pour plus d'informations, consultez Centre de sécurité des renseignements sur les menaces Bibliothèque. ◦ ▪ Effectuez une recherche dans les données présentes dans l'application à l'aide de la recherche fournie sur la page Bibliothèque de menaces. ▪ Gère les données ingérées à partir de diverses sources dans la bibliothèque de menaces. ▪ Effectue diverses actions d'enrichissement sur les observables. ▪ Crée et gère les tickets. Pour plus d'informations, consultez Création de tickets à l'aide de Threat Analyst Workbench.

Modules d'extension de dépendance

Module d'extension	Description
Les applications suivantes sont requises pour l'installation de cette application : • Composants de l'espace de travail commun de Gestion des tickets de sécurité [com.snc.escm.ws_commons]. • Support commun de Threat Intelligence [com.snc.threat].	Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant de configurer cette intégration.

Afficher la page d'accueil de Threat Intelligence Security Center

Utilisez la page d'accueil TISC qui est la page de destination, pour visualiser les données associées à Threat Intelligence.

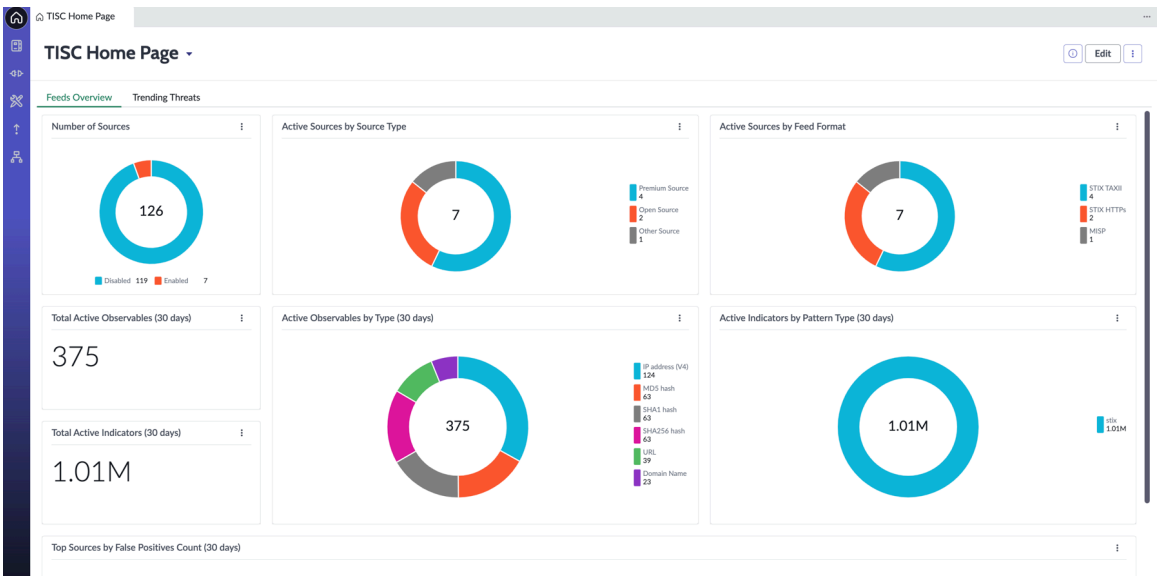
Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Espaces de travail** > **Threat Intelligence Security Center**.
   La page d'accueil TISC s'affiche.



2. Affichez la page d'accueil TISC avec différentes données de widgets.
   La vue de la page d'accueil se compose de deux **onglets différents : Vue d'ensemble des flux** et **Tendances des menaces**. Le contenu de la page d'accueil provient de diverses sources telles que des observables, des indicateurs et des flux de données.

   a. **Vue d'ensemble des flux** : cet onglet fournit une vue d'ensemble de haut niveau des différentes sources auxquelles les données sont ingérées et des sources configurées pour l'ingestion de données.

Vue d'ensemble des flux

Nom du widget	Description	Action
Nombre de sources	Affiche le nombre de sources par état tel que brouillon, activé et désactivé dans le système.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Sources actives par type de source	Affiche la distribution des sources actives par type de source.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Sources actives par format de flux	Affiche le nombre de sources activées par type de flux.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Nombre total d'observables actifs (30 jours)	Affiche les 10 premières sources par volume d'enregistrements de renseignement qui ont été créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom du widget	Description	Action
Observables actifs par type	Affiche le volume total principal d'agrégats observables qui ont été créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Indicateurs actifs par type de modèle	Affiche le volume total d'agrégats d'indicateurs par type de modèle qui ont été créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Nombre total d'indicateurs actifs (30 jours)	Affiche le volume total d'agrégats d'indicateurs qui ont été créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Principales sources par nombre de faux positifs (30 jours)	Affiche le volume total par des observables de faux positif qui ont été créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.

b. Tendances des menaces : cet onglet fournit une vue d'ensemble de haut niveau des tendances des menaces.

Vue d'ensemble des flux

Nom du widget	Description	Action
Rapports les plus récents (les 10 principaux)	Affiche la liste des rapports et des liens : les 10 premiers classés par date de publication.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Derniers flux RSS (les 10 principaux)	Affiche la liste des flux RSS et des liens : 10 principaux classés par date de publication.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Observables actifs par plage de score de menace (30 jours)	Affiche le nombre d'observables qui ont été créés au cours des 30 derniers jours, répartis par plage de scores de menace.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Observables actifs par réputation (30 jours)	Affiche le nombre d'observables qui ont été créés au cours des 30 derniers jours, répartis par réputation.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Principales balises (30 jours)	Affiche les principales balises sur les enregistrements créés au cours des 30 derniers jours	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom du widget	Description	Action
	en fonction de la fréquence d'utilisation.	
Secteurs les plus ciblés (30 jours)	Affiche les 10 principaux secteurs classés selon les activités signalées qui ont été créées au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.

Intégration de Threat Intelligence Security Center

Utilisez cette section pour comprendre les Centre de sécurité des renseignements sur les menaces intégrations.

La section **Intégrations comprend les** sous-modules suivants.

Intégrations

Nom du module	Description
Catalogue	Tous les flux de renseignements sur les menaces et les intégrations d'enrichissement disponibles sont affichés ici sous forme de tuiles/cartes. Les utilisateurs n'auront aucune possibilité de créer un nouveau flux ou une intégration à partir de cette section.
Flux de menaces	Cette section contient les détails relatifs aux flux Threat Intelligence uniquement. Les utilisateurs auront la possibilité de configurer de nouveaux flux Threat Intelligence à partir de cette section.
Intégrations des enrichissements	Cette section contient uniquement les détails relatifs aux intégrations d'enrichissement et les utilisateurs auront la possibilité de configurer les intégrations d'enrichissement disponibles à partir de cette section. **Remarque :** La section Intégrations d'enrichissement n'est visible que si au moins un module d'extension d'intégration d'enrichissement est installé.

Centre de sécurité des renseignements sur les menaces Catalogue

Le Centre de sécurité des renseignements sur les menaces catalogue est une liste organisée des flux Threat Intelligence et des intégrations d'enrichissement disponibles dans l'application pour que vous puissiez les activer après avoir ajouté les informations requises et planifier le flux pour ingérer automatiquement les données Threat Intelligence à une fréquence définie.

En tant que sn_sec_tisc.admin, vous pouvez également rechercher et modifier les configurations sources existantes, activer ou désactiver et supprimer les configurations du

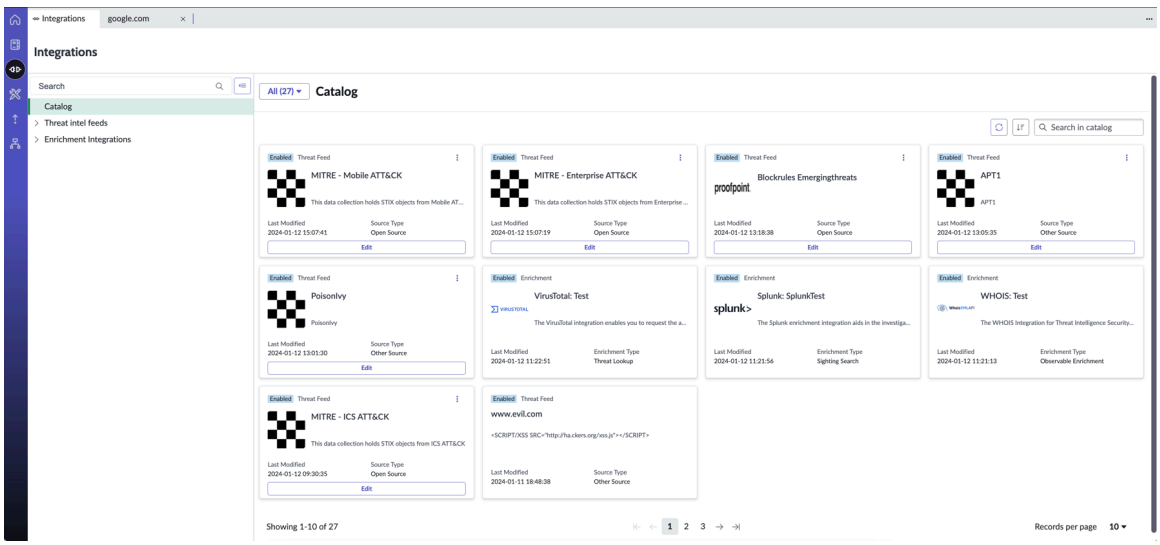
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

catalogue. Toute nouvelle source de données est ajoutée au catalogue, qui s'affiche sous la forme d'une nouvelle carte de configuration dans le catalogue.

Rôle requis :

- sn_sec_tisc.admin (créer/mettre à jour)
- sn_sec_tisc.analyste (lire)



Remarque : Les cartes du catalogue sont différenciées par son libellé qui se trouve en haut de la carte Flux de menaces/Enrichissement.

Actions sur la vue du catalogue

La vue Catalogue vous permet d'effectuer les actions suivantes.

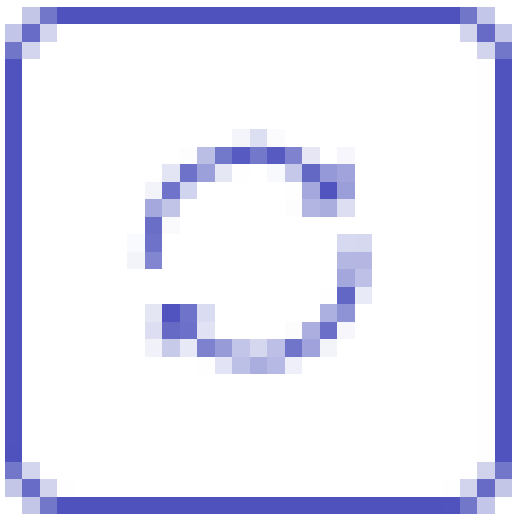
Actions sur la vue du catalogue

Action	Description
Tout	Utilisez ce menu déroulant pour filtrer les flux et les intégrations en fonction de leur état actuel. Vous pouvez filtrer en fonction des états suivants : • **Tout** : affiche tous les flux et intégrations de la page. Il s'agit de l'option par défaut. • **Activé** : affiche tous les flux et intégrations qui sont à l'état activé. • **Désactivé** : affiche tous les flux et intégrations qui sont à l'état désactivé. • **Brouillon** : affiche tous les flux et intégrations qui se trouvent à l'état de brouillon.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions sur la vue du catalogue (suite)

Action	Description
	Utilisez cette action pour actualiser le catalogue.
	Utilisez cette action pour trier tous les flux et intégrations en fonction des éléments suivants : • **Dernière modification (récente)** • **Dernière modification (la plus ancienne)** • **Nom (A-Z)** • **Nom (de Z à A)**
Rechercher dans le catalogue	Utilisez cette action pour rechercher des flux/intégrations en fonction du nom et de la description dans le catalogue.

Flux Threat Intelligence

Utilisez les flux Threat Intelligence pour ajouter, modifier ou supprimer une source de données du flux Threat Intelligence.

Les flux de sources de données sont disponibles dans le catalogue Threat Intelligence dans la section Intégrations.

Le catalogue des flux Threat Intelligence est conçu pour afficher les sources de données de flux disponibles sous forme de tuiles et permet de filtrer, rechercher et accéder aux détails de la configuration source et d'effectuer diverses actions.

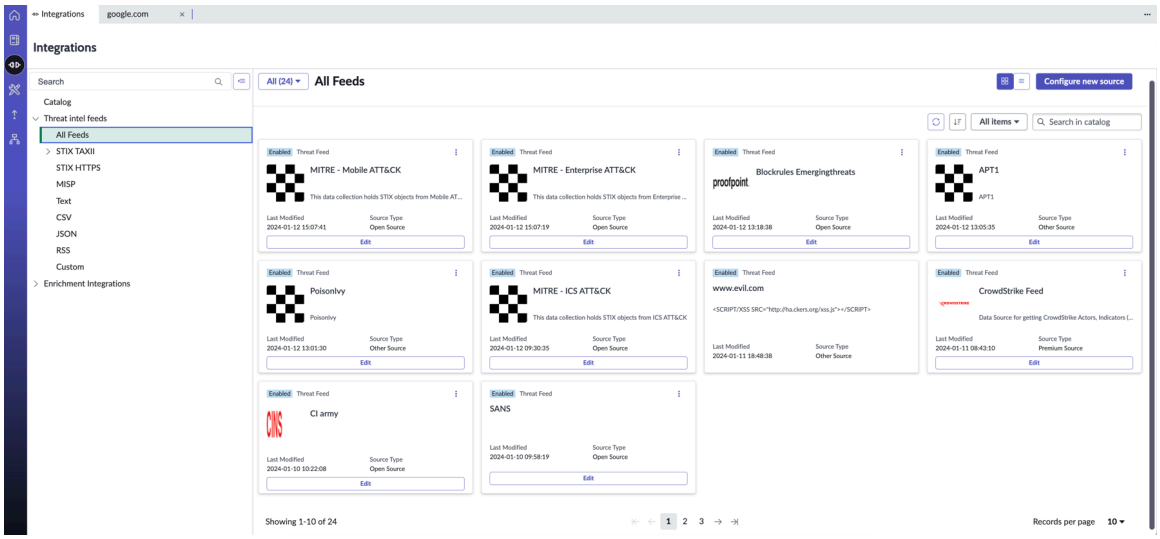
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tous les flux

Le système de base comprend une série de cartes pour chacun des flux que vous pouvez activer et utiliser.

Les flux peuvent être affichés en accédant à **Espaces de travail** > **Threat Intelligence Security Center** > **Intégrations** > **Flux de connaissance des menaces** > **Tous les flux**.



Actions sur la vue Tous les flux

La section Tous les flux vous permet d'effectuer les actions suivantes.

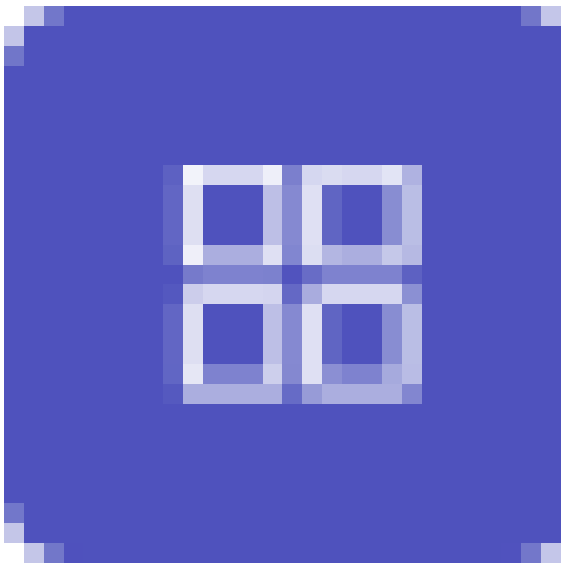
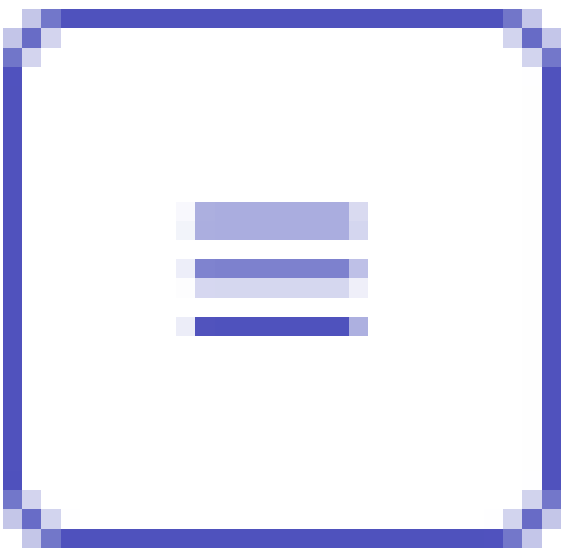
Vue Actions sur toutes les intégrations

Action	Description
Tout	Ce menu déroulant permet de filtrer les flux en fonction de leur état actuel. Vous pouvez filtrer en fonction des états suivants : • **Tout** : affiche tous les flux de la page. Il s'agit de l'option par défaut. • **Activé** : affiche tous les flux qui sont dans un état activé. • **Désactivé** : affiche tous les flux qui sont dans un état désactivé. • **Brouillon** : affiche tous les flux qui sont à l'état de brouillon.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

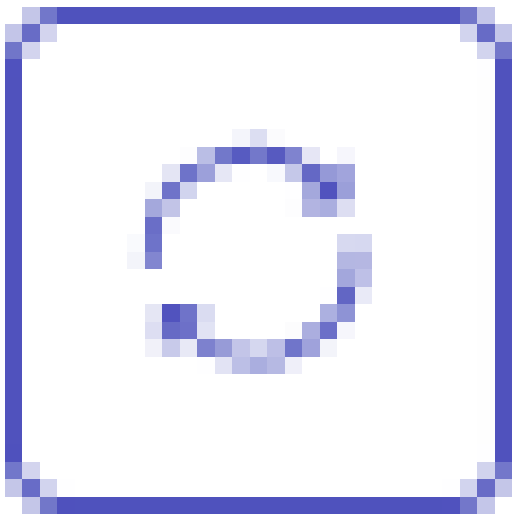
Vue Actions sur toutes les intégrations (suite)

Action	Description
	Utilisez cette action pour afficher tous les flux sous forme de cartes.
	Utilisez cette action pour afficher tous les flux sous la forme d'une vue de liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue Actions sur toutes les intégrations (suite)

Action	Description
	Utilisez cette action pour actualiser la page.
	Utilisez cette action pour trier toutes les intégrations en fonction des éléments suivants : • **Dernière modification (récente)** • **Dernière modification (la plus ancienne)** • **Nom (A-Z)** • **Nom (de Z à A)**
Tous les éléments	Utilisez cette action pour filtrer et répertorier les vignettes du flux Threat Intelligence par type de source ou type de flux. **Type de source** : • Source ouverte • Autre source • Source premium **Type de flux** : • CSV • Flux personnalisé • JSON

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

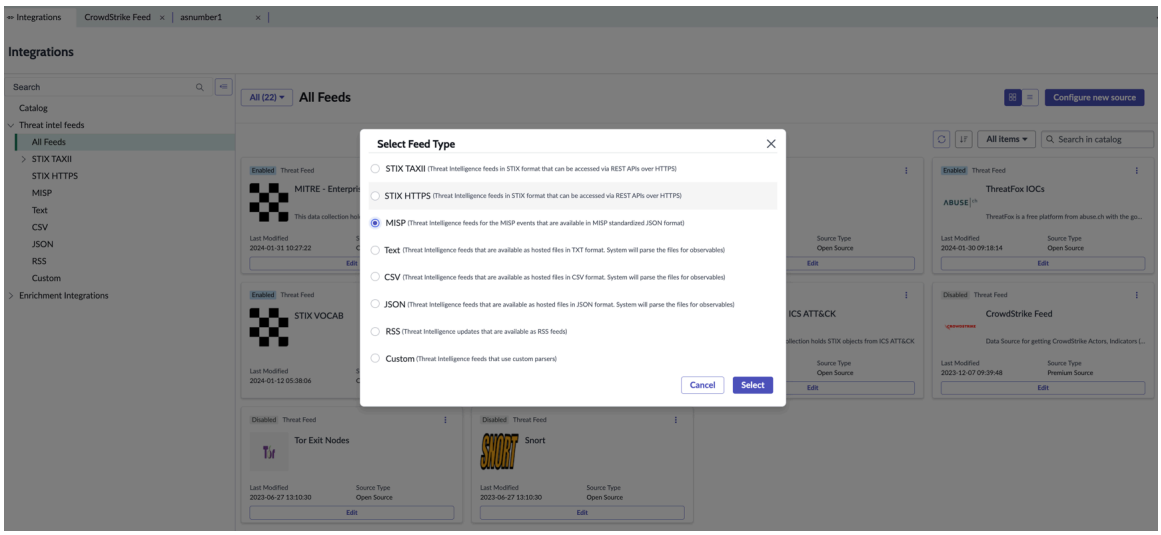
Vue Actions sur toutes les intégrations (suite)

Action	Description
	• MISP • RSS • STIX HTTPs • Texte
Rechercher dans le catalogue	Utilisez cette action pour rechercher des flux en fonction du nom et de la description dans le catalogue.

Configurer une nouvelle source de données du flux Threat Intelligence

Pour configurer une nouvelle source de données de flux Threat Intelligence, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionner **Flux de connaissance des menaces** > **Tous les flux**.
4. Cliquez sur **Configurer une nouvelle source**. Les différents types de flux s'affichent.



5. Sélectionnez le type de flux correspondant. Par exemple, MISP.
6. Cliquez sur **Sélectionner**.
7. Renseignez les champs du formulaire.

Créer une source de données

Champ	Description
Nom	Donnez un nom au flux.
Description	Description du flux.
Type de flux	Type de flux. Par exemple, MISP.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par défaut, cette valeur s'affiche en fonction du type de flux que vous avez sélectionné dans le catalogue.
Logo	Joignez le logo du flux source.
Secteur	Sélectionnez la catégorie de secteur à laquelle la source de données de flux s'applique, par exemple Aérospatiale, Agriculture, etc.
Type de source	Sélectionnez le type de source dans la liste des types de sources disponibles. La liste des sources disponibles est la suivante : ◦ Gouvernement ◦ ISACs ◦ Source ouverte ◦ Source premium ◦ Autre source

Renseignez les champs de la section Configuration, selon vos besoins.

Configuration

Champ	Description
Période d'expiration (jours)	Saisissez la période d'expiration du flux en jours. Par exemple, 180 jours. **Remarque :** Quelles que soient les données ingérées à partir de la source, elles expirent 180 jours après l'ingestion.
Utiliser le message REST	Cochez **la case Utiliser le message REST** si vous devez utiliser la fonctionnalité Message REST/Méthode REST fournie par Now Platform. Si cette case n'est pas cochée, l'application utilise le point de terminaison fourni dans **l'URL du point de terminaison REST** pour extraire les données du flux. Pour plus d'informations, consultez Service Web REST sortant dans la Now Platform documentation. **Remarque :** Les champs Message REST et Méthode REST sont obligatoires lorsque vous sélectionnez le message REST.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Message REST	Sélectionnez l'enregistrement de message REST dans la liste des enregistrements de message REST qui sont déjà configurés dans l'instance. Pour plus d'informations, consultez Service Web REST sortant dans la documentation de Now Platform. **Remarque :** Sélectionnez cette valeur lorsque vous avez besoin d'afficher des en-têtes spécifiques et de définir les enregistrements connexes REST à l'aide de l'option de message REST.
Méthode REST	Sélectionnez la méthode REST dans la liste des méthodes REST disponibles configurées pour le message REST sélectionné. Pour plus d'informations, consultez Service Web REST sortant dans la documentation de Now Platform.
Fiabilité	Définissez le score de confiance pour tous les enregistrements applicables qui sont ingérés via ce flux spécifique. **Remarque :** Définissez la confiance entre 0 et 100 pour cette source.
URL du point de terminaison REST	Entrez l'URL du point de terminaison REST où les données sont hébergées par la source de données.
Authentification requise	Cochez cette case si l'authentification est requise pour votre nouvelle source de données. **Remarque :** Ajoutez une déclaration mentionnant que cela ne s'applique que lorsque l'URL du point de terminaison REST est utilisée pour récupérer les données.
Type d'authentification	Type d'authentification pour le flux source. Voici les types d'authentification configurés et approvisionnés au sein du système de base pour les utilisateurs : ◦ ID API / Clé API ◦ ID de l'API/Secret de l'API ◦ Clé API ◦ Clé API/Secret API

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Nom d'utilisateur / Mot de passe API / Clé API ◦ Authentification de base **Remarque :** Les types d'authentification dans le système de base pour le type de flux source personnalisé sont ID client et Secret client.
En-têtes à transmettre avec la demande	Tous les en-têtes à transmettre avec les demandes peuvent être fournis dans le mappage d'en-tête de demande. L'en-tête doit être fourni dans une paire clé-valeur séparée par deux-points (' :'). Chaque paire clé-valeur d'en-tête doit être fournie dans une nouvelle ligne. Pour fournir des paramètres d'authentification en tant que valeurs d'en-tête, encadrez l'étiquette d'authentification requise avec « ${ » et « }$ ». Par exemple, x-api-key :${API Key}$.
Avancés	Cochez cette case pour définir un script d'intégration personnalisé et un script de processeur de rapport. **Remarque :** Lorsque vous cochez cette case, les champs **Script d'intégration** et **Processeur de rapport** s'affichent pour vous permettre de sélectionner les scripts personnalisés.
Script d'intégration	Le script d'intégration appelle un appel à l'URL du point de terminaison REST à l'aide des paramètres d'authentification et des en-têtes configurés dans le flux, puis le script récupère les données disponibles à partir du flux spécifique. Dans le système de base, les scripts personnalisés inclus sont les suivants, qui sont mis en service dans l'application pour les scripts d'intégration : ◦ FeedDatasourceIntegrationBase ◦ MITRESourceIntegration ◦ RSSFeedDatasourceIntegration (en anglais seulement) ◦ SimpleFeedDatasourceIntegration (en anglais seulement) ◦ SimpleMISPFeedDatasourceIntegration

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Le script d'intégration par défaut est basé sur le type de flux que vous sélectionnez. Par exemple, si vous sélectionnez le type de flux MISP, qui est un format standard pour traiter et extraire les données, le script d'intégration est **SimpleFeedDatasourceIntegration**. **Remarque :** Pour les scripts d'intégration personnalisés, vous pouvez créer un include de script en étendant **FeedDatasourceIntegrationBase** et en remplaçant les méthodes requises.
Script de processeur de rapport	Le script de processeur de rapport traite les données extraites du flux à l'aide d'un script d'intégration. Dans le système de base, les scripts personnalisés inclus sont les suivants, qui sont mis en service dans l'application pour les scripts d'intégration : ◦ FeedDatasourceResponseProcessor ◦ MITRECollectionDataProcessor ◦ RSSFeedDatasourceResponseProcessor ◦ SimpleFeedDatasourceResponseProcessor ◦ SimpleMISPFeedDatasourceResponseProcessor ◦ TAXIIV2CollectionDataProcessor Le processeur de rapport par défaut pour STIX HTTPS est **TAXIIV2CollectionDataProcessor**. Par défaut, cette option s'affiche et vous ne pouvez pas modifier ou sélectionner un autre processeur de rapport.

Renseignez les champs de la section Planification, comme il convient.

Ordonnancement

Champ	Description
Exécuter	Définissez la fréquence à laquelle vous souhaitez ingérer les enregistrements. Le flux s'exécutera et s'exécutera en fonction de l'intervalle de tâche de planification. Les intervalles de tâches disponibles sont les suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Quotidien ◦ Hebdomadaire ◦ Mensuel ◦ Périodiquement ◦ Une fois ◦ Sur demande ◦ Calendrier d'entreprise : début de l'entrée ◦ Calendrier d'entreprise : fin de l'entrée **Remarque :** Par défaut, la fréquence est définie sur Sur demande. Pour plus d'informations, consultez Travaux planifiés et Exécution automatique d'un script de votre choix.
Extraire les données de	Date de début à partir de laquelle les données doivent être extraites. Ce champ doit être défini avec l'heure à partir de laquelle les données doivent être ingérées à partir de la source correspondante. Une fois ce champ défini, l'exécution d'ingestion suivante extrait les données à partir de l'heure configurée et les exécutions d'ingestion consécutives récupèrent les données incrémentielles. Par exemple, la source est planifiée pour ingérer les données toutes les heures. L'utilisateur définit **Extraire les données du** 12 janvier à 6h00 le 12 janvier à 9h30, le déclenchement de l'ingestion le 12 janvier à 10h00 récupérerait les données du 12 janvier à 6h00 au 12 janvier à 10h00. La prochaine ingestion qui se déclenche à 11h00 récupère uniquement les données incrémentielles du 12 janvier à 10h00 au 12 janvier à 11h00. **Remarque :** Cela signifie que les exécutions planifiées extrairont les données de manière incrémentielle à partir de la date spécifiée.

Balises

Champ	Description
Sélectionner des balises	Utilisez les balises pour annoter ou marquer les enregistrements qui sont ingérés dans le système à partir de cette source.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Commencez à saisir le nom de la balise dans la barre **de recherche** pour choisir les balises disponibles dans l'application ou saisissez un nouveau nom de balise et cliquez sur **Ajouter** pour l'attribuer à la source.

8. Cliquez sur l'action **Enregistrer** pour stocker et créer le flux.

   Les détails fournis sont validés et, par défaut, l'état des flux est désactivé.

9. (Facultatif) Cliquez sur l'action **Enregistrer en tant que brouillon** pour ne stocker les configurations de flux qu'en tant que brouillons. Les utilisateurs ne peuvent pas activer un flux lorsqu'il est enregistré à l'état de brouillon.

   Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez remplir les informations restantes dans la version brouillon et la créer.

10. Pour activer le flux, cliquez sur **Activer**.

    Le flux est activé avec succès. Vous pouvez également activer, désactiver ou supprimer un flux particulier à l'aide du menu **Actions** de la vignette du flux requis sur la page **Catalogues** ou **Flux Intel de menaces** .

    Remarque : Si la fréquence **d'exécution** est définie sur **Sur demande** dans la section **Planification** de la page du formulaire de source de données, chaque fois que vous activez l'intégration, une invite de message s'affiche pour avertir les utilisateurs qu'ils ont activé la source avec succès. Vous devez modifier la fréquence d'exécution pour activer la configuration source et ingérer automatiquement les données.

11. Cliquez sur **Activer** pour activer l'enregistrement.

    Une fois que l'enregistrement de source de données de flux est activé, vous pouvez exécuter l'enregistrement pour exécuter l'intégration.

    Remarque : L'enregistrement de la source de données est étiqueté et indiqué comme **activé**. De même, vous pouvez désactiver le flux de source de données en cliquant sur le bouton **Désactiver** .

12. Cliquez sur **Supprimer** pour supprimer l'enregistrement de source de données de flux.
13. Sélectionnez **la section Exécutions d'intégrations** pour vérifier les détails de l'exécution.

Remarque : La procédure de configuration de la source de données de flux ci-dessus est la même pour tous les autres types de sources de données de flux, à l'exception de STIX TAXII. Pour plus d'informations sur la configuration de STIX TAXII, reportez-vous à la section Configurer un nouveau flux TAXII.

Types de menaces Flux Intel

Les types de flux de renseignements sur les menaces qui peuvent être configurés et activés sont les suivants :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux Threat Intelligence

Type	Description
Flux TAXII	Flux disponibles au format de collections STIX/TAXII.
STIX HTTPS	Les flux Threat Intelligence au format STIX sont accessibles via des API REST sur le protocole HTTPS.
MISP	Flux au format MISP.
Texte	Flux disponibles en tant que fichiers hébergés au format texte. **Remarque :** Le système analyse uniquement les fichiers pour déterminer l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP.
CSV	Flux disponibles en tant que fichiers hébergés au format CSV. **Remarque :** Le système analyse uniquement les fichiers pour déterminer l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP.
JSON	Flux disponibles en tant que fichiers hébergés au format JSON. **Remarque :** Le système analyse uniquement les fichiers pour déterminer l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP.
RSS	Flux disponibles au format RSS. L'application stockera les données sous forme d'enregistrements de flux RSS.
Personnalisé	Flux configurés à l'aide d'analyseurs personnalisés. **Remarque :** Le système analyse uniquement les fichiers pour déterminer l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP.

Pour les étapes suivantes de la procédure, reportez-vous à la section respective pour configurer un type de flux spécifique. Flux Threat Intelligence.

Afficher les flux Intel de menaces

Cette section vous fournit les flux de connaissance des menaces configurés dans le système de base.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voir les flux STIX TAXII

Affichez les flux STIX TAXII configurés dans le système de base.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **STIX TAXII.**
   Les flux MISP du système de base sont décrits dans le tableau suivant.

Flux de menaces	Description	URL
Cyware TAXII	Cyware Threat Intelligence eXchange (CTIX) est une plateforme conçue pour faciliter le partage de renseignements sur les cybermenaces entre les organisations.	https://threatfeed.cyware.com/ctixapi/ctix21/
RecordedFuture TAXII	Recorded Future est une plateforme cloud indépendante de renseignements sur les menaces qui permet aux organisations d'identifier et d'atténuer les menaces dans les domaines de la cybersécurité, de la chaîne d'approvisionnement, du physique et de la fraude.	https://api.recordedfuture.com/taxii2
Pulsedive TAXII	Pulsedive est une plateforme de renseignements sur les menaces qui fournit une large gamme de services et d'outils de renseignements sur les cybermenaces aux organisations.	https://pulsedive.com/taxii2/api/

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher les flux HTTPs STIX

Affichez les flux HTTPs STIX configurés dans le système de base.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **STIX HTTPs**.
   Le tableau suivant décrit les flux HTTPs STIX dans le système de base.

Flux de menaces	Description	URL
MITRE - Mobile ATT&CK	Cette collection de données contient des objets STIX de Mobile ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json
MITRE - ICS ATT&CK	Cette collection de données contient des objets STIX d'ICS ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
MITRE : entreprise ATT&CK	Cette collection de données contient des objets STIX d'Enterprise ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

4. Cliquez sur **Modifier** pour modifier le flux et effectuer les mises à jour nécessaires.

Afficher les flux MISP

Affichez les flux MISP configurés dans le système de base.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **MISP**.
   Les flux MISP du système de base sont décrits dans le tableau suivant.

Flux de menaces	Description	URL
Menace DigitalSide Flux INT Intel	Source de données permettant d'extraire des informations Open Source Cyber Threat Intelligence à partir du flux OSINT DigitalSide Threat-Intel, qui est principalement basé sur l'analyse des logiciels malveillants et les URL, adresses IP et domaines compromis.	https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/manifest.json

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
URLhaus IOC	URLhaus est un projet de abuse.ch dont l'objectif est de partager les URL malveillantes utilisées pour la distribution de logiciels malveillants.	https://urlhaus.abuse.ch/downloads/misp/manifest.json
Bazar de logiciels malveillants	MalwareBazaar est un projet de abuse.ch dont l'objectif est de partager des échantillons de logiciels malveillants avec la communauté de sécurité de l'information, les fournisseurs d'antivirus et les fournisseurs de renseignements sur les menaces.	https://bazaar.abuse.ch/downloads/misp/manifest.json
IOC ThreatFox	ThreatFox est une plateforme gratuite de abuse.ch dont l'objectif est de partager les indicateurs de compromission (IOC) associés aux logiciels malveillants avec la communauté de sécurité de l'information, les fournisseurs d'antivirus et les fournisseurs de renseignements sur les menaces.	https://threatfox.abuse.ch/downloads/misp/manifest.json

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher les flux de texte

Affichez les flux de texte configurés dans le système de base.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionner **l'option Texte** .
   Vous trouverez ci-dessous la liste des flux de texte configurés dans le système de base.

Flux de menaces	Description	URL
Les adresses IP par force brute de Haley	Fournit une liste des adresses IP des machines attaquantes au cours des 2 dernières années, triées par adresse IP	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
Règles de blocage Menaces émergentes	Emerging Threat Intelligence (ET) Intelligence fournit des flux de renseignements exploitables sur les menaces afin d'identifier les adresses IP impliquées dans des activités suspectes et malveillantes.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Nuug Pop3 Groper Web	Liste des hôtes qui ont essayé et échoué à se connecter au service pop3 à bsdly.net.	https://home.nuug.no/%7Epeter/pop3gropers.txt
Nœuds de sortie Tor	Les nœuds de sortie Tor peuvent être utilisés pour détecter le trafic provenant du réseau TOR.	https://www.dan.me.uk/torlist/?exit
Liste noire des adresses IP de Talos Intelligence	Talos a été formé en combinant l'équipe de recherche sur les vulnérabilités de SourceFire, le groupe de recherche et de communications sur les menaces de Cisco et le groupe d'applications sécurisées de Cisco. L'expertise combinée s'appuie sur une infrastructure sophistiquée et sur la télémétrie inégalée des données de Cisco qui s'étend sur les réseaux, les terminaux, les environnements cloud, les systèmes virtuels et le trafic Web et de courrier électronique quotidien.	https://www.talosintelligence.com/documents/ip-blacklist
SANS	ISC fournit un service gratuit d'analyse et d'alerte à des milliers d'internautes et d'organisations.	https://isc.sans.edu/feeds/topips.txt
Snort	Snort est le premier système de prévention des intrusions (IPS) Open Source au monde. Snort IPS utilise une série de règles qui aident à définir l'activité malveillante du réseau.	https://snort.org/downloads/ip-block-list
Armée CI	La liste CINS Army est un sous-ensemble de l'ensemble de règles CINS Active Threat Intelligence	https://cinsscore.com/list/ci-badguys.txt

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
	et se compose d'adresses IP qui répondent à l'un des deux critères de base suivants : 1) le récent facteur de score Rogue Packet de l'adresse IP est très faible, ou 2) l'adresse IP a déclenché un nombre désigné d'alertes « de confiance » sur un nombre donné de leurs Sentinelles déployées dans le monde entier.	
Point de preuve	Adresses IP brutes pour les listes de blocs de pare-feu. Ceux-ci proviennent de : Spam nets identifiés par Spamhaus (www.spamhaus.org), Top Attackers répertoriés par DShield (www.dshield.org) et Abuse.ch	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
Liste de blocage Greensnow	GreenSnow est une équipe composée des meilleurs spécialistes de la sécurité informatique, GreenSnow récolte un grand nombre d'IP à partir de différents ordinateurs situés dans le monde entier. GreenSnow est comparable à SpamHaus.org pour les attaques de toutes sortes, à l'exception du spam.	https://blocklist.greensnow.co/greensnow.txt
Armée CI	La liste CINS Army est un sous-ensemble de l'ensemble de règles CINS Active Threat Intelligence et se compose d'adresses IP qui répondent à l'un des deux critères de base suivants : 1) le récent facteur de score Rogue Packet de l'adresse IP est très faible, ou 2) l'adresse IP a déclenché un nombre désigné d'alertes « de confiance » sur un nombre donné de leurs Sentinelles déployées dans le monde entier.	https://cinsscore.com/list/ci-badguys.txt
Liste de blocs	www.blocklist.de s'agit d'un service gratuit et	https://lists.blocklist.de/lists/all.txt

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
	volontaire fourni par un spécialiste de la fraude et de l'abus, dont les serveurs sont souvent attaqués via des services SSH, Mail-Login, FTP, Webserver et autres.	
Nœuds de sortie Tor	Les nœuds de sortie Tor peuvent être utilisés pour détecter le trafic provenant du réseau TOR.	https://www.dan.me.uk/torlist/?exit
IP BOT Botscout	BotScout permet d'empêcher les scripts Web automatisés, connus sous le nom de « bots », de s'inscrire sur les forums, de polluer les bases de données, de diffuser du spam et d'abuser des formulaires sur les sites Web.	http://botscout.com/last_caught_cache.txt
Plan de données VNC RFB	Adresses IP identifiées comme initiatrices de sessions de mémoire tampon de trame distante VNC.	https://dataplane.org/signals/vncrfb.txt
Connexion TELNET au plan de données	Adresses IP identifiées comme tentant de se connecter via l'authentification par mot de passe TELNET.	https://dataplane.org/signals/telnetlogin.txt
Authentification par mot de passe SSH du plan de données	Adresses IP identifiées comme tentant de se connecter via l'authentification par mot de passe SSH.	https://dataplane.org/signals/sshpwauth.txt
Connexion client SSH du plan de données	Adresses IP identifiées comme effectuant des négociations de protocole client SSH.	https://dataplane.org/signals/sshclient.txt
Règles de blocage Menaces émergentes	Emerging Threat Intelligence (ET) Intelligence fournit des flux de renseignements exploitables sur les menaces afin d'identifier les adresses IP impliquées dans des activités suspectes et malveillantes.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Message d'accueil SMTP du plan de données	Adresses IP identifiées comme des clients SMTP émettant des commandes	https://dataplane.org/signals/smtpgreet.txt

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
	HELO ou EHLO non sollicitées.	
Requête SIP du plan de données	Les adresses IP identifiées comme envoyant des requêtes SIP OPTIONS.	https://dataplane.org/signals/sipquery.txt
Protocole IP de plan de données 41	Adresses IP identifiées comme relais de protocole IPv4 41 ouvert (c'est-à-dire IPv6 sur IPv4).	https://dataplane.org/signals/proto41.txt
Invitation SIP Dataplane	Adresses IP identifiées comme envoyant des opérations SIP INVITE.	https://dataplane.org/signals/sipinvitation.txt
Plan de données DNS CH, TXT version.bind	Adresses IP identifiées comme envoyant DNS CH TXT VERSION. LIER les requêtes.	https://dataplane.org/signals/dnsversion.txt
Plan de données DNS TCP	Les adresses IP identifiées comme envoyant des requêtes DNS sur le port TCP 53.	https://dataplane.org/signals/dnstcp.txt
Récursivité DNS du plan de données souhaitée DANS N'IMPORTE QUEL	Les adresses IP identifiées comme envoyant un DNS récursif dans n'importe quelle requête.	https://dataplane.org/signals/dnsrdany.txt
Récursivité DNS du plan de données souhaitée	Adresses IP identifiées comme envoyant des requêtes DNS récursives.	https://dataplane.org/signals/dnsrd.txt
Base de données Hameçonnage de GitHub Liens d'hameçonnage actifs	Source de données pour l'extraction des liens d'hameçonnage actifs à partir de la base de données d'hameçonnage disponible sur GitHub.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-links-ACTIVE.txt
Base de données Hameçonnage de GitHub Domaines actifs	Source de données pour l'extraction des domaines actifs à partir de la base de données d'hameçonnage disponible sur GitHub.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt
Base de données d'hameçonnage à partir des adresses IP actives GitHub	Source de données pour l'extraction des adresses IP actives à partir de la base de données d'hameçonnage disponible sur GitHub.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-IPs-ACTIVE.txt
Liste de blocage des bots	Toutes les adresses IP qui ont été signalées au cours des dernières 48 heures comme ayant exécuté des attaques	https://lists.blocklist.de/lists/bots.txt

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
	sur les attaques RFI, REG-Bots, IRC-Bots ou BadBots.	
Liste de blocage des attaques Apache	Toutes les adresses IP qui ont été signalées au cours des dernières 48 heures comme ayant exécuté des attaques sur le service Apache, Apache-DDOS, RFI-Attacks.	https://lists.blocklist.de/lists/apache.txt
Liste noire Voip par Scopserv	Récupérer la liste des adresses IP sur liste de blocage à partir de la liste noire Voip.	http://voipbl.org/update/?dm=bl
Liste de blocage du domaine Threatview	Domaines malveillants identifiés pour l'hameçonnage/la diffusion de programmes malveillants/la commande et le contrôle.	https://threatview.io/Downloads/DOMAIN-High-Confidence-Feed.txt
Liste de blocage de hachage MD5 Threatview	Hachages MD5 de fichiers malveillants ou associés à des logiciels malveillants, des rançongiciels, des outils de piratage, des bots, etc.	https://threatview.io/Downloads/MD5-HASH-ALL.txt
Liste de blocage de l'URL de Threatview	URL malveillantes au service de logiciels malveillants, d'hameçonnage, de botnets et de C2.	https://threatview.io/Downloads/URL-High-Confidence-Feed.txt
Liste de blocage de hachage de fichier SHA Threatview	Hachages SHA de fichiers connus ou liés à l'exécution de logiciels malveillants.	https://threatview.io/Downloads/SHA-HASH-FEED.txt
Liste de blocage des adresses IP Threatview	Liste de blocage des adresses IP malveillantes pour les adresses IP incorrectes connues.	https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
Flux de chasse C2 Threatview	Infrastructure hébergeant les serveurs de commande et de contrôle trouvés pendant la recherche proactive par Threatview.io	https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt
OSINT Threatview Flux de menaces	Indicateurs malveillants de compromission recueillis à partir de la source OSINT : Twitter et Pastebin.	https://threatview.io/Downloads/Experimental-IOC-Tweets.txt

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher les flux CSV

Affichez les flux CSV configurés dans le système de base.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **CSV**.
   Les flux CSV du système de base sont expliqués dans le tableau suivant.

Flux de menaces	Description	URL
Liste noire des certificats SSL Abuse.ch	La liste noire des certificats SSL (CSV) est un fichier CSV qui contient l'empreinte SHA1 de tous les certificats SSL figurant sur la liste noire sur SSLBL.	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
Liste noire d'adresses IP du botnet C2	Un certificat SSL peut être associé à un ou plusieurs serveurs (combinaison adresse IP :port). SSLBL collecte les adresses IP qui s'exécutent avec un certificat SSL sur liste noire sur SSLBL. Il s'agit généralement de serveurs de commande et de contrôle (C&C) de botnet. SSLBL publie donc une liste noire contenant ces adresses IP qui peuvent être utilisées pour détecter le trafic C2 du botnet des machines infectées vers Internet, quittant votre réseau.	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
Phishtank en ligne	N/A	https://data.phishtank.com/data/online-valid.csv

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher le flux personnalisé

Affichez les flux personnalisés expédiés dans le système de base.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **Personnalisé**.
   La table suivante répertorie les flux personnalisés prêts à l'emploi.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
Flux CrowdStrike	Source pour obtenir les données d'acteurs, d'observables et de rapports CrowdStrike.	https://api.crowdstrike.com

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher le flux de menaces Premium pour CrowdStrike

Affichez le flux de menaces premium récemment ajouté pour le type de flux personnalisé. Chaque flux premium utilisant un gestionnaire de sources de données nécessite des intégrations ponctuelles.

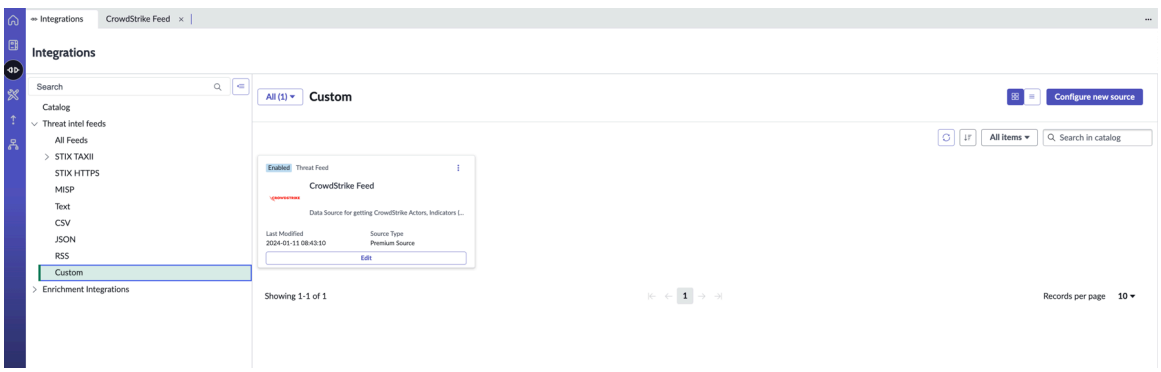
Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **Personnalisé**.
4. Cliquez sur la carte du **flux CrowdStrike** .

> **Remarque :** Par défaut, le flux CrowdStrike est désactivé, vous devez modifier les configurations pour activer le flux.



5. Explorez la section Détails de la **configuration** .
6. Saisissez **l'URL de base**, l'ID **client** et la **clé secrète du client**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

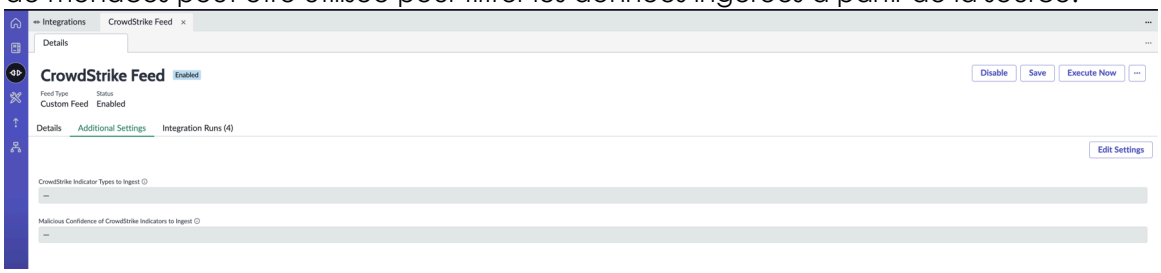
a. **URL de base** : chaque cloud CrowdStrike a une URL de base différente. Lorsque vous effectuez des demandes à l'API CrowdStrike, utilisez l'URL de base qui correspond au cloud où CrowdStrike est hébergé.

b. Vous devez générer votre ID client et votre secret client au cas où vous ne les auriez pas. Pour plus d'informations sur l'ID client et le secret client, consultez la section Définition de votre premier client d'API .

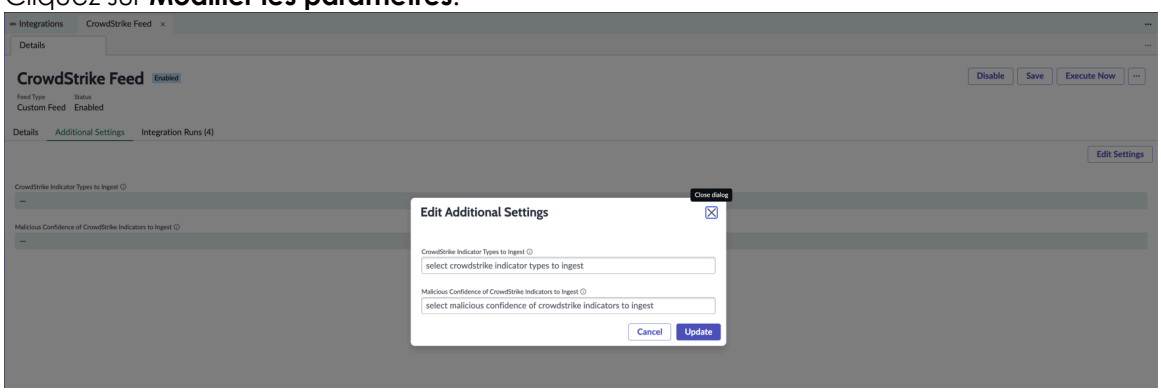
c. Obtenir l'ID client et le secret client à partir de CrowdStrike pour les champs d'application requis. Vous trouverez ci-dessous les champs d'application requis pour l'ID client et le secret client de Crowdstrike :

- Indicateurs (intelligence Falcon)
- Acteurs (Falcon Intelligence)
- Rapports (Falcon Intelligence)

7. Accéder aux **paramètres supplémentaires** spécifiques à CrowdStrike L'intégration du flux de menaces peut être utilisée pour filtrer les données ingérées à partir de la source.



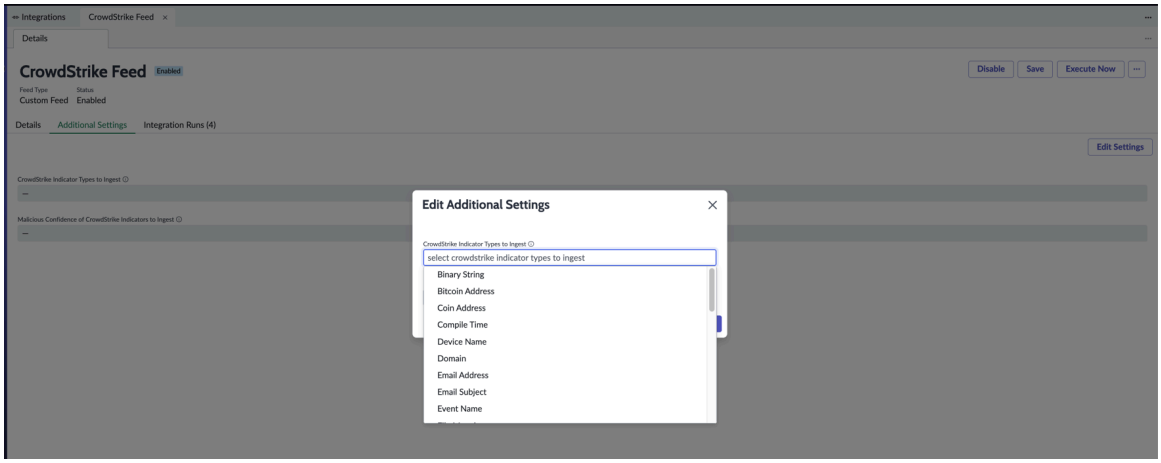
8. Cliquez sur **Modifier les paramètres**.

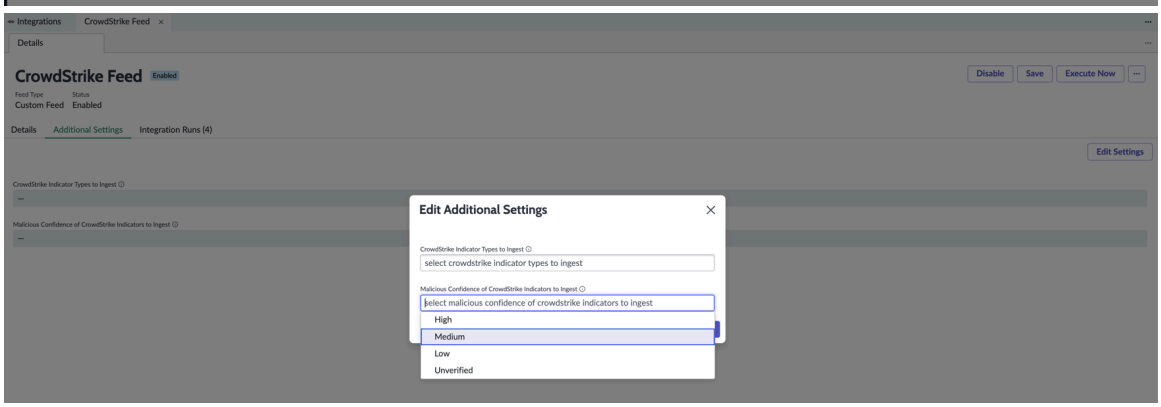


9. Sélectionnez l'une des options suivantes : **Types d'indicateurs Crowd Strike à ingérer** ou **Confiance malveillante des indicateurs CrowdStrike à ingérer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





Remarque :

a. **Types d'indicateurs CrowdStrike à ingérer** : seuls les types d'indicateurs sélectionnés seront ingérés à partir de CrowdStrike lors de l'extraction des indicateurs mis à jour (les indicateurs sur CrowdStrike sont mappés aux observables dans TISC). S'ils sont laissés vides, les indicateurs de tous types seront ingérés.

b. **Fiabilité malveillante des indicateurs CrowdStrike à ingérer** : seul l'indicateur sélectionné avec la confiance malveillante sélectionnée sera ingéré à partir de CrowdStrike lors de l'extraction des indicateurs mis à jour (les indicateurs sur CrowdStrike sont mappés aux observables dans TISC). S'ils sont laissés vides, des indicateurs de confiance malveillante seront ingérés.

10. Sélectionnez les valeurs requises pour chaque option, en fonction de cela, les indicateurs correspondants seront ingérés.
11. Cliquez sur **Mettre à jour**.
12. Cliquez sur **Activer**.

Remarque : Le flux premium est identique aux autres flux, à l'exception de la réponse qui est analysée pendant la configuration. Une réponse spécifique est analysée dans CrowdStrike en ajoutant l'ID client et le secret client.

Quel type de données est récupéré à partir de CrowdStrike ?

a. Indicateurs de CrowdStrike qui sont mis à jour après le délai d'ingestion configuré. Ces indicateurs de CrowdStrike seront ensuite mappés aux observables dans TISC. Voici les types d'indicateurs qui sont ingérés dans TISC :

- Hachage SHA256
- Hachage MD5

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Hachage SHA1
- URL
- Domaine
- Adresse IP
- Nom Mutex
- Nom du fichier
- Adresses e-mail
- Nom d'utilisateur
- Bloc d'adresses IP

b. Acteurs de menace de CrowdStrike qui sont mis à jour après le délai d'ingestion configuré. Ces acteurs de CrowdStrike seront mappés aux acteurs de menace dans notre système.

c. Rapports de CrowdStrike qui sont mis à jour après le délai d'ingestion configuré. Ces rapports de CrowdStrike seront mappés aux rapports de menace dans notre système.

d. Nous récupérons également les données ci-dessous en plus des entités mentionnées ci-dessus.

i. Acteurs/rapports/indicateurs de menace liés aux indicateurs ingérés ci-dessus.

ii. Acteurs/indicateurs de menace associés à tous les rapports ingérés dans le cadre de l'ingestion actuelle.

Propriétés système pour CrowdStrike

Ce qui suit détaille les propriétés système de CrowdStrike.

1. sn_sec_tisc.crowdstrike_actor_batch_size : indique le nombre d'acteurs à extraire dans un seul appel d'API. Remarque : applicable uniquement lorsque l'intégration ne détecte pas la présence des éléments nécessaires dans le système.

- Type : nombre entier
- Valeur : 250

2. sn_sec_tisc.crowdstrike_api_limit : nombre d'enregistrements à extraire simultanément à partir de CrowdStrike. Plus le nombre est élevé, plus la mémoire consommée pour le traitement de la charge utile est élevée.

- Type : nombre entier
- Valeur : 1000

3. sn_sec_tisc.crowdstrike_indicator_batch_size : indique le nombre d'indicateurs à extraire dans un seul appel d'API. Remarque : applicable uniquement lorsque l'intégration ne détecte pas la présence des éléments nécessaires dans le système.

- Type : nombre entier
- Valeur : 150

4. sn_sec_tisc.crowdstrike_offset_limit_total : total autorisé du décalage et de la limite par l'API CrowdStrike.

- Type : nombre entier
- Valeur : 50000

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. sn_sec_tisc.crowdstrike_report_batch_size : indique le nombre de rapports à extraire dans un seul appel d'API. Remarque : applicable uniquement lorsque l'intégration ne détecte pas la présence des éléments nécessaires dans le système.
   - Type : nombre entier
   - Valeur : 50

Comprendre STIX TAXII

Structured Threat Information Expression (STIX) est un langage et un format de sérialisation utilisés pour échanger des renseignements sur les cybermenaces (CTI). Le protocole TAXII (Trusted Automated Exchange of Intelligence Information) est un protocole utilisé pour échanger des renseignements sur les cybermenaces (CTI) sur HTTPS.

Avec STIX, tous les aspects de la suspicion, de la compromission et de l'attribution sont représentés sous forme d'objets et de relations descriptives. Les informations STIX peuvent être représentées visuellement pour un analyste ou stockées au format JSON pour être rapidement lisibles par machine.

Cyber Threat Intelligence (CTI) a été créé pour définir un ensemble de représentations d'informations et de protocoles afin de répondre au besoin de modéliser, d'analyser et de partager des renseignements sur les cybermenaces. Le CTI est principalement axé sur le développement et la normalisation de l'expression structurée d'informations sur les menaces (STIX) et de l'échange automatisé et fiable d'informations sur les indicateurs (TAXII).

Configurer un nouveau flux TAXII

Vous pouvez gérer des flux TAXII pour partager des informations au format STIX. Chaque flux TAXII contient une ou plusieurs collections TAXII.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionner **Flux de connaissance des menaces** > **STIX TAXII** > **Flux TAXII**.

   Remarque : Configurez le flux TAXII pour qu'il serve de profil pour toutes les collections TAXII qu'il contient.

4. Cliquez sur **Configurer une nouvelle source**.
   La page Configure new TAXII Feed (Configurer un nouveau flux TAXII) s'affiche.
5. Renseignez les champs du formulaire.

Créer une source de données

Champ	Description
Nom	Donnez un nom au flux.
Description	Description du flux.
Type de source	Type de source fourni pour le flux, par exemple Open Source, Source Premium, etc. Les types de sources disponibles sont les suivants :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Gouvernement ◦ ISACs ◦ Source ouverte ◦ Source premium ◦ Autre source
Logo	Joignez le logo du flux source.
Secteur	Sélectionnez la catégorie de secteur à laquelle la source de données de flux s'applique, par exemple Aérospatiale, Agriculture, etc.

Renseignez les champs de la section Configuration, selon vos besoins.

Configuration

Champ	Description
Version TAXII	Sélectionnez la version TAXII du serveur TAXII qui doit être configurée. Les versions prises en charge sont 2.0 et 2.1.
Type de configuration	Fournissez un type de configuration pour extraire les collectes TAXII. Les valeurs disponibles sont les suivantes : ◦ **URL du service Discovery** : choisissez l'URL du service Discovery pour extraire les collections de toutes les racines d'API disponibles dans le service Discovery du serveur TAXII. ◦ **URL racine de l'API** : choisissez l'URL racine de l'API pour extraire les collections de la racine d'API spécifique du serveur TAXII.
Authentification	Sélectionnez l'option requise dans la liste déroulante si l'authentification est requise. Les options disponibles sont les suivantes : ◦ **Aucun** : sélectionnez cette option si aucune authentification n'est requise. ◦ **Basique** : sélectionnez cette option pour fournir un nom d'utilisateur et un mot de passe. ◦ **Clé API** : sélectionnez cette option pour fournir une clé API. ◦ **Choisissez un message REST** : sélectionnez cette option pour tout autre type d'authentification. Les options de message REST sont les suivantes :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ **Utiliser le message REST** : cochez cette case si vous avez besoin d'un message REST pour créer un message REST prédéfini. Si vous ne sélectionnez pas, la valeur du champ de point de terminaison sera utilisée. Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste. ▪ **Méthode REST** : cochez cette case si vous avez besoin d'une méthode REST. Cliquez sur l'icône de recherche et sélectionnez la méthode REST dans la liste. **Remarque :** Les champs Message REST et Méthode REST deviennent disponibles lorsque l'option de message REST est sélectionnée.
URL	Entrez l'URL du service de découverte du serveur TAXII ou l'URL racine de l'API spécifique en fonction du type de configuration sélectionné.
Section avancée	
Avancés	Cochez la case pour choisir un script d'intégration et un processeur de rapport différents. Assurez-vous que les scripts choisis sont compatibles avec la version TAXII sélectionnée. En fonction de la version et de l'authentification TAXII, ces scripts sont renseignés automatiquement par défaut.
Script d'intégration	Invoque un appel à l'API REST Endpoint URL à l'aide des paramètres d'authentification tels que le type d'authentification : nom d'utilisateur/mot de passe/clé API et les en-têtes à transmettre avec la demande, puis le script récupère les données STIX des observables ou des indicateurs disponibles pour le flux spécifique.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Les données extraites sont uniquement des données brutes (aucun enregistrement n'est créé) qui sont jointes au processus d'intégration et peuvent ensuite être visualisées dans la section **Exécution de l'intégration** . Dans le système de base, les scripts personnalisés inclus sont les suivants, qui sont mis en service dans l'application pour les scripts d'intégration : ◦ TAXIIV2_0QueryParamAPIKeyIntegrationScript ◦ TAXIIV2_0BasicAuthIntegrationScript ◦ TAXIIV2_1QueryParamAPIKeyIntegrationScript ◦ TAXIIV2_1BasicAuthIntegrationScript Le script d'intégration par défaut est basé sur le type de flux que vous sélectionnez. L'include de script exécute un appel REST simple, enregistre la réponse en tant que pièce jointe, puis renvoie la pièce jointe au processeur.
Script de processeur de rapport	Le processeur de rapport appelle un appel à l'URL du point de terminaison REST. Dans le système de base ci-dessous se trouvent les includes de scripts personnalisés, qui sont mis en service dans l'application pour les scripts d'intégration, **TAXIIV2CollectionDataProcessor**.

Renseignez les champs de la section Planification, comme il convient.

Ordonnancement

Champ	Description
Fréquence d'exécution des collectes	Intervalle de planification qui sera appliqué aux enregistrements de collecte TAXII. La fréquence d'exécution d'une collecte TAXII peut être modifiée dans la vue du formulaire de collecte TAXII si nécessaire. **Remarque :** Ce paramètre sera appliqué par défaut à toutes les collections TAXII qui sont extraites. Il existe une option permettant de remplacer le paramètre dans TAXII Collections si nécessaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Pour plus d'informations, consultez Travaux planifiés et Exécution automatique d'un script de votre choix .
Extraire les données de	Date de début à partir de laquelle les données doivent être extraites. Ce champ doit être défini avec l'heure à partir de laquelle les données doivent être ingérées à partir de la source correspondante. Une fois ce champ défini, l'exécution d'ingestion suivante extrait les données à partir de l'heure configurée et les exécutions d'ingestion consécutives récupèrent les données incrémentielles. Par exemple, la source est planifiée pour ingérer les données toutes les heures. L'utilisateur définit **Extraire les données du** 12 janvier à 6h00 le 12 janvier à 9h30, le déclenchement de l'ingestion le 12 janvier à 10h00 récupérerait les données du 12 janvier à 6h00 au 12 janvier à 10h00. La prochaine ingestion qui se déclenche à 11h00 récupère uniquement les données incrémentielles du 12 janvier à 10h00 au 12 janvier à 11h00. **Remarque :** Cela signifie que les exécutions planifiées extrairont les données de manière incrémentielle à partir de la date spécifiée.

6. **Cliquez sur Valider la connexion**
   Un message d'information s'affiche indiquant que la connexion du flux TAXII a réussi. Pour extraire les collections, passez à l'étape suivante.
7. Cliquez sur **Get TAXII Collections (Obtenir les collections TAXII)**.

   Remarque : En cas d'erreur, un message d'erreur s'affiche indiquant qu'une erreur s'est produite lors de l'extraction des collectes TAXII et vérifiez les journaux pour plus de détails.

   Les collections TAXII sont affichées dans la section Collections TAXII et sont désactivées par défaut.
8. Activez les collections TAXII pour récupérer les objets STIX disponibles dans ces collections TAXII.

Intégrations de l'enrichissement TISC

Le Centre de sécurité des renseignements sur les menaces système de base n'inclut aucune intégration préconfigurée. Cette section fournit des instructions pour configurer les intégrations et ServiceNow celles de tiers.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

Assurez-vous d'avoir installé les intégrations d'applications tierces requises. Vous pouvez voir les détails des observables, de la recherche de perception et de la recherche de menaces uniquement pour les applications tierces installées.

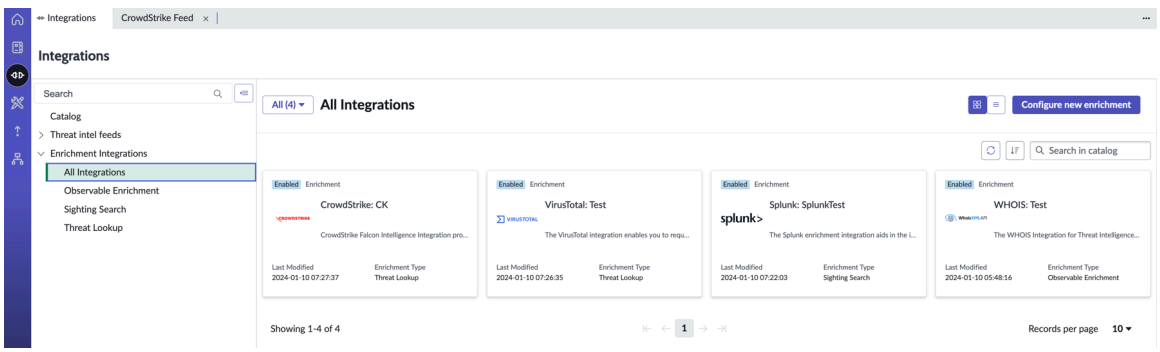
Toutes les configurations d'intégration

Toutes les intégrations sont des applications distinctes qui doivent être installées. TISC prend en charge les intégrations avec des fournisseurs tiers. Toutes les intégrations installées peuvent être configurées ici.

Cette section affiche des cartes pour chacune des implémentations d'intégration configurées que vous pouvez activer et utiliser.

La section de chaque type d'enrichissement n'est visible que si au moins une des intégrations correspondantes pour ce type d'enrichissement est installée. Par exemple, la section **Recherche de menaces n'est** visible sous **Intégrations d'enrichissement** que si au moins une intégration Recherche de menaces est installée.

Vous pouvez afficher les cartes d'intégration configurées en accédant à **Espaces de travail** > **Threat Intelligence Security Center** > **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.



Actions sur la vue Toutes les intégrations

La vue Toutes les intégrations vous permet d'effectuer les actions suivantes.

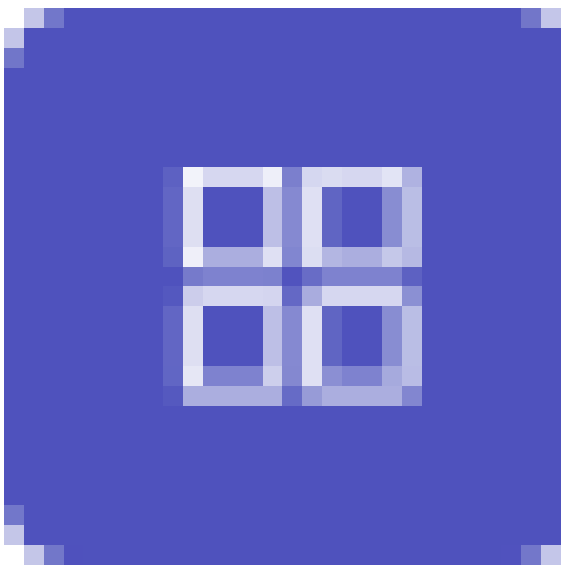
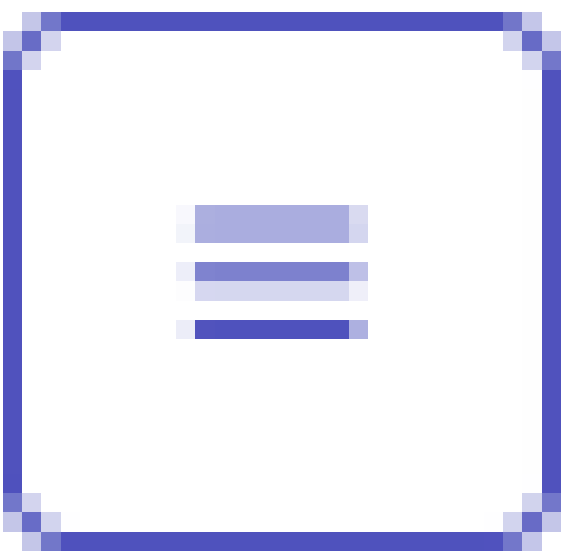
Vue Actions sur toutes les intégrations

Action	Description
Tout	Utilisez ce menu déroulant pour filtrer les intégrations en fonction de leur état actuel. Vous pouvez filtrer en fonction des états suivants : • **Tout** : affiche toutes les intégrations de la page. Il s'agit de l'option par défaut. • **Activé** : affiche toutes les intégrations qui sont dans un état activé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

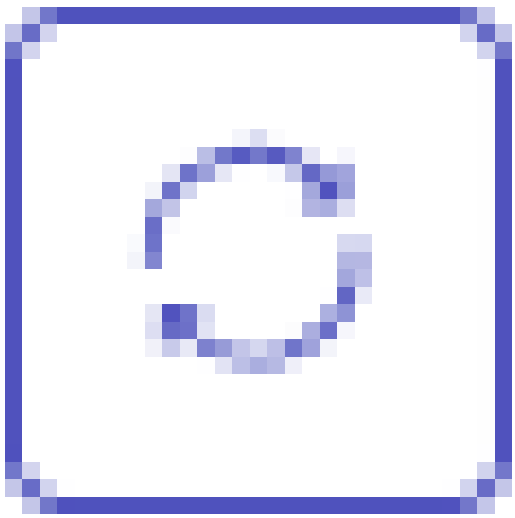
Vue Actions sur toutes les intégrations (suite)

Action	Description
	• **Désactivé** : affiche toutes les intégrations qui sont à l'état désactivé. • **Brouillon** : affiche toutes les intégrations qui sont à l'état de brouillon.
	Utilisez cette action pour afficher toutes les intégrations sous forme de cartes.
	Utilisez cette action pour afficher toutes les intégrations sous forme de listes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue Actions sur toutes les intégrations (suite)

Action	Description
	Utilisez cette action pour actualiser la page Toutes les intégrations.
	Utilisez cette action pour trier toutes les intégrations en fonction des éléments suivants : • **Dernière modification (récente)** • **Dernière modification (la plus ancienne)** • **Nom (A-Z)** • **Nom (de Z à A)**
Rechercher dans le catalogue	Utilisez cette action pour rechercher des intégrations configurées en fonction du nom et de la description dans le catalogue.

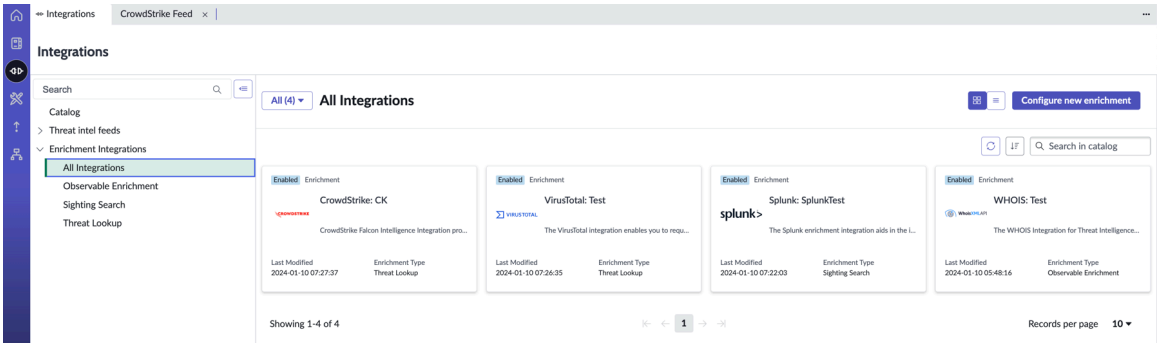
Traduction automatique

Configurer un nouvel enrichissement à partir de la vue Toutes les intégrations

Vous pouvez configurer de nouveaux enrichissements à partir de la vue Toutes les intégrations ou directement à partir des sections Enrichissement des observables, Recherche de perception ou Recherche de menace, respectivement. Pour configurer le nouvel enrichissement à partir de la vue Toutes les intégrations, procédez comme suit.

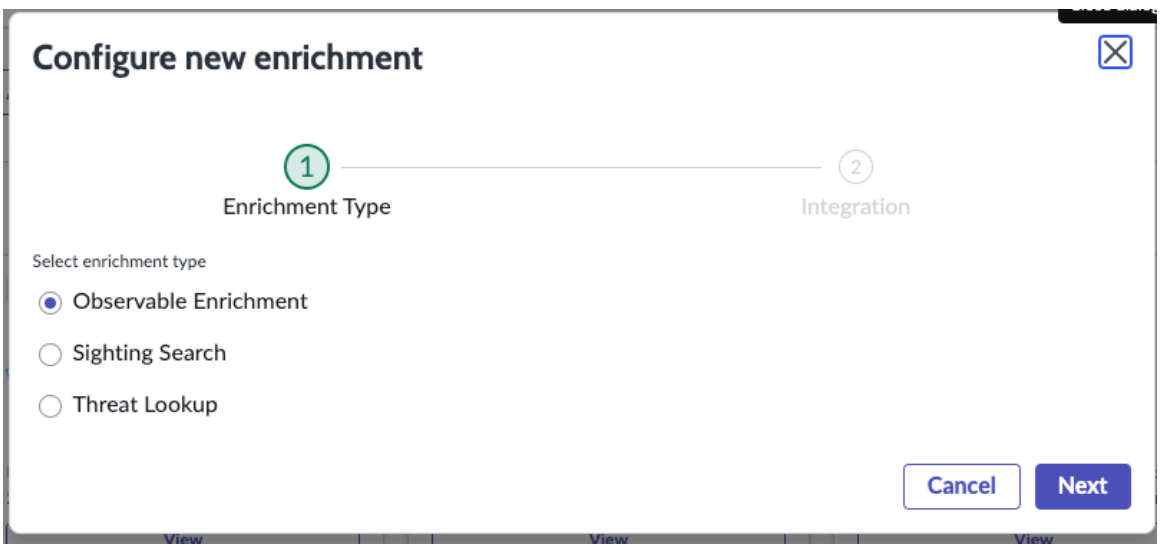
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Intégrations** , puis sélectionnez la section **Toutes les intégrations** .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur l'action **Configurer un nouvel enrichissement** .

   La fenêtre contextuelle Configurer un nouvel enrichissement apparaît avec trois types d'enrichissement : Enrichissement des observables, Recherche de perception ou Recherche de menace. Vous devez choisir le type d'enrichissement que vous souhaitez configurer.



4. Sélectionnez un type d'enrichissement, puis cliquez sur **Suivant**.

   Vous accédez alors à la fenêtre contextuelle qui affiche les intégrations disponibles. Vous devez choisir l'intégration que vous souhaitez configurer.

5. Sélectionnez une intégration dans la liste des intégrations disponibles, puis cliquez sur **Sélectionner**.

   Vous accédez alors à la page Créer une intégration d'enrichissement de l'intégration sélectionnée. Par défaut, cette page est pré-remplie avec les détails de l'intégration sélectionnée. Par exemple, l'intégration WHOIS.

6. Renseignez les champs du formulaire Créer une intégration.

Configurer le nouveau formulaire d'intégration d'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration d'enrichissement. Par exemple, `WHOIS1`.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont pré-remplis par défaut. Par exemple, `WHOIS`.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Enrichissement des observables. Les détails du type d'intégration sélectionné sont pré-remplis par défaut. Les types d'intégration suivants sont pris en charge : ◦ Enrichissement des éléments observables ◦ Recherche de perception ◦ Recherche de menace
Description	Entrez une description unique pour la nouvelle intégration d'enrichissement.

7. Dans la section Configuration de l'intégration, configurez les détails d'intégration en fonction de vos besoins.

   La section Configuration de l'intégration inclut des détails de configuration tels que la clé API, l'ID ou le secret du client API, le nom d'utilisateur, le mot de passe, etc., que vous devez renseigner. Ces détails de configuration varient selon les intégrations.

8. Cliquez sur l'action **Enregistrer** pour stocker et créer la configuration de l'intégration d'enrichissement.

   Les détails fournis sont validés et, par défaut, l'état de l'intégration de l'enrichissement est désactivé.

9. (Facultatif) Cliquez sur l'action **Enregistrer comme brouillon** pour stocker uniquement les configurations d'intégration en tant que brouillons. Les utilisateurs ne peuvent pas activer une intégration lorsqu'elle est enregistrée à l'état de brouillon

   Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez remplir les informations restantes dans la version brouillon et la créer.

10. Pour activer l'intégration de l'enrichissement, cliquez sur **Activer**.

    L'intégration de l'enrichissement est activée.

11. Vous pouvez également activer, désactiver ou supprimer une intégration d'enrichissement particulière à l'aide du menu Actions de la vignette d'intégration requise sur la page Catalogue ou sur la page Intégrations d'enrichissement.

Configurer l'enrichissement des éléments observables

Vous pouvez enrichir la connaissance des menaces sur un ou plusieurs observables pour déterminer s'ils sont associés à des menaces de sécurité connues. Les implémentations qui s'exécutent dépendent de celles que vous avez activées.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prend Centre de sécurité des renseignements sur les menaces en charge l'enrichissement des observables uniquement pour l'intégration WHOIS à partir de maintenant. Pour plus d'informations, consultez Configurer et activer l'intégration Whois.

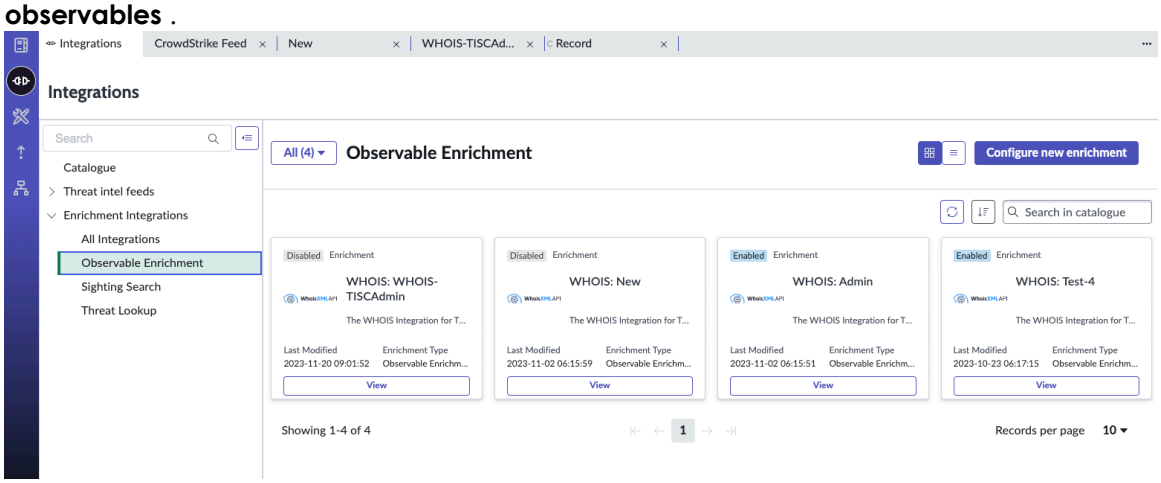
Remarque : Le module d'intégrations d'enrichissement n'est affiché que si au moins une des intégrations prenant en charge l'une des fonctionnalités est installée dans l'application.

Pourquoi et quand exécuter cette tâche

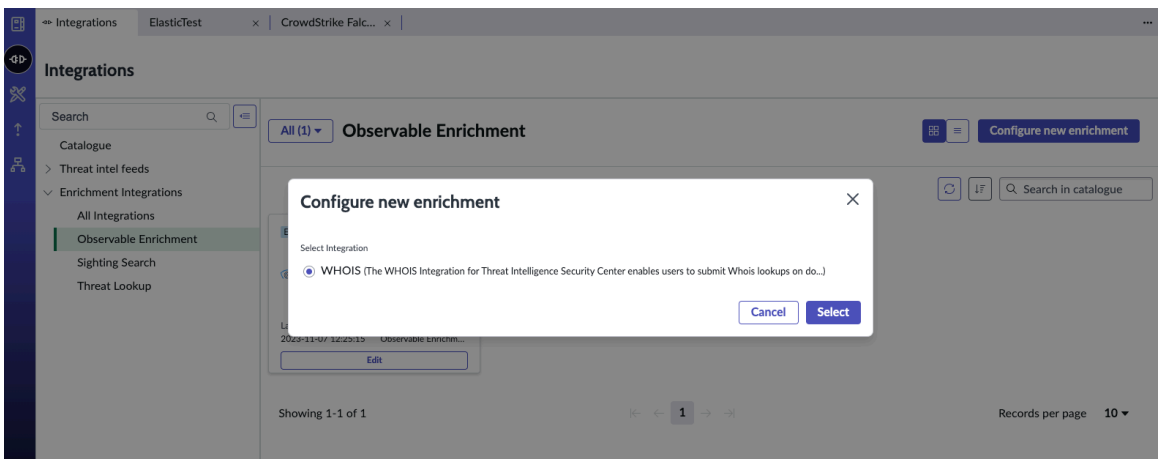
La section Enrichissement des observables contient uniquement les intégrations dont le type d'intégration est Enrichissement des observables. Cette section affiche des cartes pour chacune des implémentations d'intégration configurées que vous pouvez activer et utiliser.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Intégrations** , puis sélectionnez la section **Enrichissement des observables** .



3. Cliquez sur l'action **Configurer un nouvel enrichissement** .
   Vous accédez alors à la fenêtre contextuelle qui affiche les intégrations disponibles. Vous devez choisir l'intégration que vous avez à configurer.
4. Sélectionnez une intégration dans la liste des intégrations disponibles, puis cliquez sur **Sélectionner**.
   Vous accédez alors à la page Créer une intégration d'enrichissement de l'intégration sélectionnée. Par défaut, cette page est pré-remplie avec les détails de l'intégration sélectionnée. Par exemple, l'intégration WHOIS.

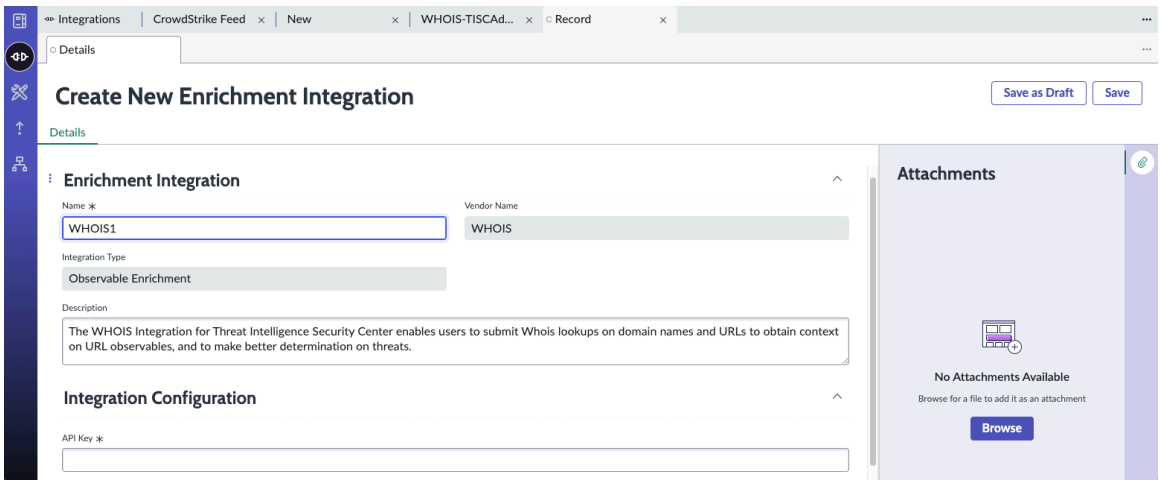


5. Renseignez les champs du formulaire Créer une intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Intégration de l'enrichissement	
Nom	Entrez un nom pour la nouvelle intégration d'enrichissement. Par exemple, `WHOIS1`.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont pré-remplis par défaut. Par exemple, `WHOIS`.
Type d'intégration	Type d'intégration que vous avez sélectionné, à savoir Enrichissement des observables. Les détails du type d'intégration sélectionné sont pré-remplis par défaut.
Description	Entrez une description unique pour la nouvelle intégration d'enrichissement.



6. Dans la section Configuration de l'intégration, configurez les détails d'intégration en fonction de vos besoins.
   La section Configuration de l'intégration inclut des détails de configuration tels que la clé API, l'ID ou le secret du client API, le nom d'utilisateur, le mot de passe, etc., que vous devez renseigner. Ces détails de configuration varient selon les applications.
7. Cliquez sur l'action **Enregistrer** pour stocker et créer la nouvelle configuration de l'intégration d'enrichissement.
   Une fois que vous avez cliqué sur l'action **Enregistrer** ou **Activer** , l'intégration est validée à l'aide des configurations d'intégration fournies. Par défaut, l'état de l'intégration de l'enrichissement est défini sur Désactivé.
8. Cliquez sur **l'action Enregistrer comme brouillon** pour stocker uniquement les mises à jour apportées à la configuration d'enrichissement et ne pas la créer.
   Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez remplir les informations restantes dans la version brouillon et la créer.
9. Pour activer l'intégration de l'enrichissement, cliquez sur **Activer**.
   L'intégration de l'enrichissement est activée. Vous pouvez également activer, désactiver ou supprimer une intégration d'enrichissement particulière à l'aide du menu Actions de la vignette d'intégration requise sur la page Catalogue ou sur la page Intégrations d'enrichissement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la recherche de perception

Vous pouvez effectuer une recherche de perception sur un ou plusieurs observables pour déterminer le nombre de fois que les observables sont vus dans les journaux de votre organisation. Vous pouvez effectuer une recherche de perception sur les observables dans un certain nombre de jours ou dans une plage de dates.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Remarque : Le module d'intégrations d'enrichissement n'est affiché que si au moins une des intégrations prenant en charge l'une des fonctionnalités est installée dans l'application.

Le Centre de sécurité des renseignements sur les menaces prend en charge la recherche de perception uniquement pour les intégrations suivantes :

- Recherche Splunk
- Elasticsearch

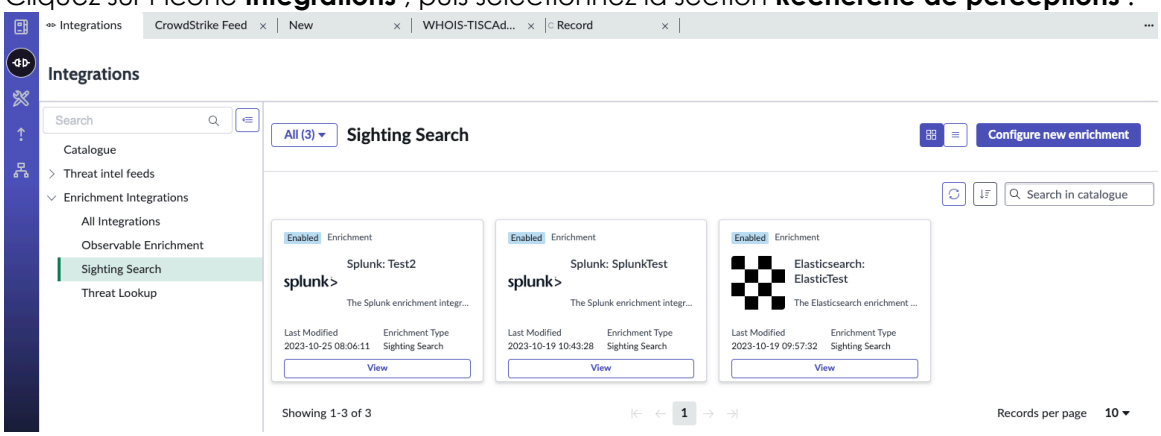
Pourquoi et quand exécuter cette tâche

La section Recherche de perceptions contient uniquement les intégrations dont le type d'intégration est Recherche de perceptions.

Cette section affiche des cartes pour chacune des implémentations d'intégration configurées que vous pouvez activer et utiliser.

Procédure

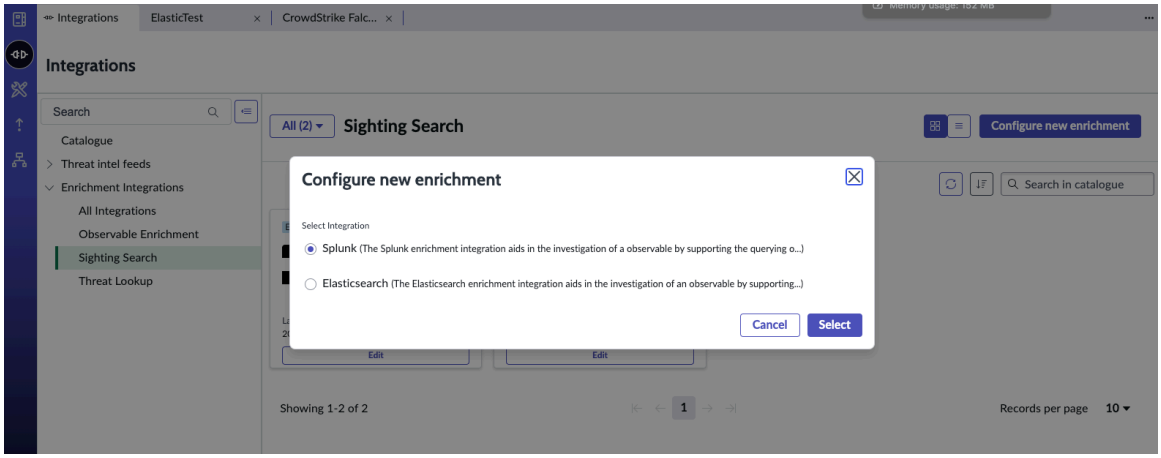
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Intégrations** , puis sélectionnez la section **Recherche de perceptions** .



3. Cliquez sur l'action **Configurer un nouvel enrichissement** .
   Vous accédez alors à la fenêtre contextuelle qui affiche les intégrations disponibles. Vous devez choisir l'intégration que vous avez à configurer.
4. Sélectionnez une intégration dans la liste des intégrations disponibles, puis cliquez sur **Sélectionner**.
   Vous accédez alors à la page Créer une intégration d'enrichissement de l'intégration sélectionnée. Par défaut, cette page est pré-remplie avec les détails de l'intégration sélectionnée. Par exemple, Intégration Splunk.

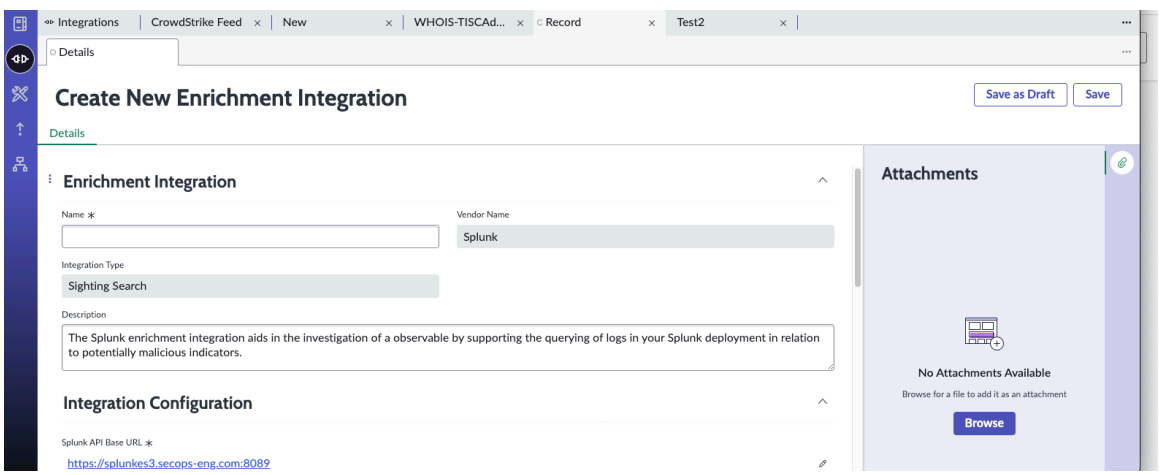
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Renseignez les champs du formulaire Créer une intégration.

Champ	Description
Intégration de l'enrichissement	
Nom	Entrez un nom pour la nouvelle intégration d'enrichissement. Par exemple, `Splunk-1`.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont pré-remplis par défaut. Par exemple, `Splunk`.
Type d'intégration	Type d'intégration que vous avez sélectionné, à savoir Recherche de perceptions. Les détails du type d'intégration sélectionné sont pré-remplis par défaut.
Description	Entrez une description unique pour la nouvelle intégration d'enrichissement.



6. Dans la section Configuration de l'intégration, configurez les détails d'intégration en fonction de vos besoins.
La section Configuration de l'intégration inclut des détails de configuration tels que la clé API, l'ID ou le secret du client API, le nom d'utilisateur, le mot de passe, etc., que vous devez renseigner. Ces détails de configuration varient selon les applications.

7. Cliquez sur l'action **Enregistrer** pour stocker et créer la nouvelle configuration de l'intégration d'enrichissement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les détails fournis sont validés et, par défaut, l'état de l'intégration de l'enrichissement est désactivé.

8. Cliquez sur **l'action Enregistrer comme brouillon** pour stocker uniquement les mises à jour apportées à la configuration d'enrichissement et ne pas la créer.
   Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez remplir les informations restantes dans la version brouillon et la créer.
9. Pour activer l'intégration de l'enrichissement, cliquez sur **Activer**.
   L'intégration de l'enrichissement est activée. Vous pouvez également activer une intégration d'enrichissement particulière à l'aide du menu Actions de la vignette d'intégration requise sur la page Catalogue ou sur la page Toutes les intégrations.

Définir des requêtes pour la recherche de perception

Vous pouvez utiliser des configurations de recherche de perception pour définir les requêtes utilisées pour trouver la récurrence des observables dans votre environnement dans le cadre des enquêtes sur les observables.

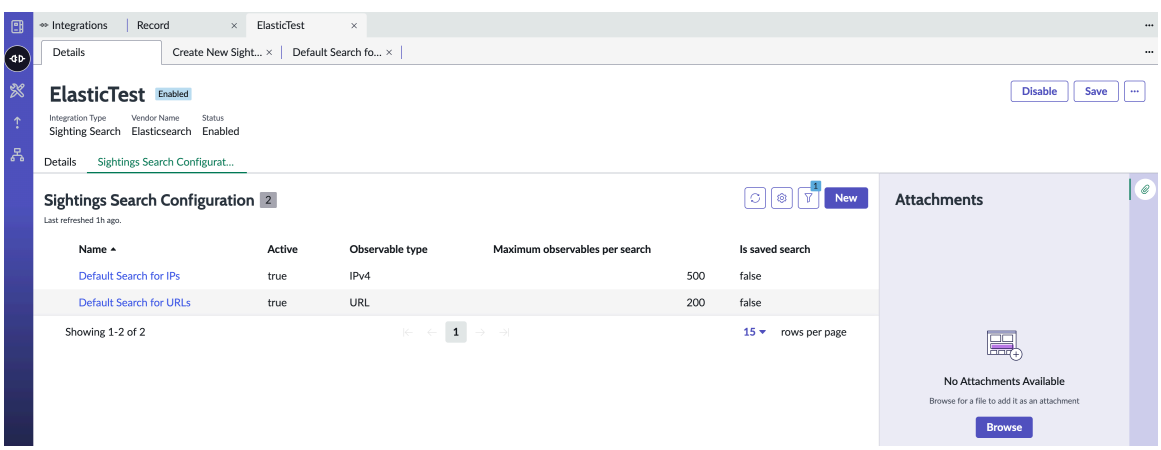
Afficher les requêtes pour la recherche de perception

Rôle requis : sn_sec_tisc.admin

Pour afficher les configurations de recherche de perception, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Intégrations**.
2. Sur la page Intégrations, accédez à **Intégrations de l'enrichissement** > **Recherche de perception**.
3. Recherchez l'intégration pour laquelle vous souhaitez afficher la configuration de recherche de perceptions, puis cliquez sur **Modifier**.
4. Sélectionnez l'onglet **Configurations de recherche de perceptions** .

   Vous pouvez afficher la liste des configurations de recherche de perception.



5. Cliquez sur la configuration de recherche de perception requise pour afficher les détails de la configuration.
6. Pour générer une requête de recherche de perceptions de test, cliquez sur l'action **Générer une requête de recherche de perceptions de test** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'action **Générer une requête de recherche de perception de test** ne fonctionnerait que si vous aviez configuré des paramètres de requête de recherche de perception. Pour plus d'informations, consultez Utilisation des paramètres de recherche de perception.

7. Dans la fenêtre contextuelle Générer une requête de recherche de perceptions de test, saisissez ou collez plusieurs observables à l'aide de virgules, de retours à la ligne, d'onglets ou de séparateurs de barres verticales pour générer une requête de test.
8. Cliquez sur **Générer** pour générer la requête de recherche de perception de test.
9. Vous pouvez également effectuer les actions suivantes dans l'onglet Configurations de recherche de perceptions :
   a. Pour actualiser la liste des configurations de recherche de perception, cliquez sur l'icône de .
   b. Pour effectuer une action de liste sur les configurations de recherche de perception, cliquez sur l'icône .

      Vous pouvez effectuer les deux actions de liste suivantes :

      - **Modifier les colonnes** : vous pouvez utiliser cette action pour ajouter ou supprimer des colonnes existantes et modifier l'ordre en fonction de vos besoins.
      - **Réinitialiser les largeurs** : vous pouvez utiliser cette action pour réinitialiser les largeurs des colonnes.

   c. Pour filtrer les configurations de recherche de perceptions en fonction des conditions, cliquez sur l'icône .

      La valeur 1 indique qu'une condition est utilisée pour le filtrage.

Créer des configurations de recherche Soupir

Rôle requis : sn_sec_tisc.admin

```
Maximum observables per search = "maximum number of observables that can
 be substituted in a single search query"

Search = "Search query that should be executed in sighting search source.
Search query can contain substitution variables that would be substituted
 with observables of specific type as configured in sighting search
 parameters when sighting search query is formed"
```

Pour créer une configuration de recherche de perception, procédez comme suit :

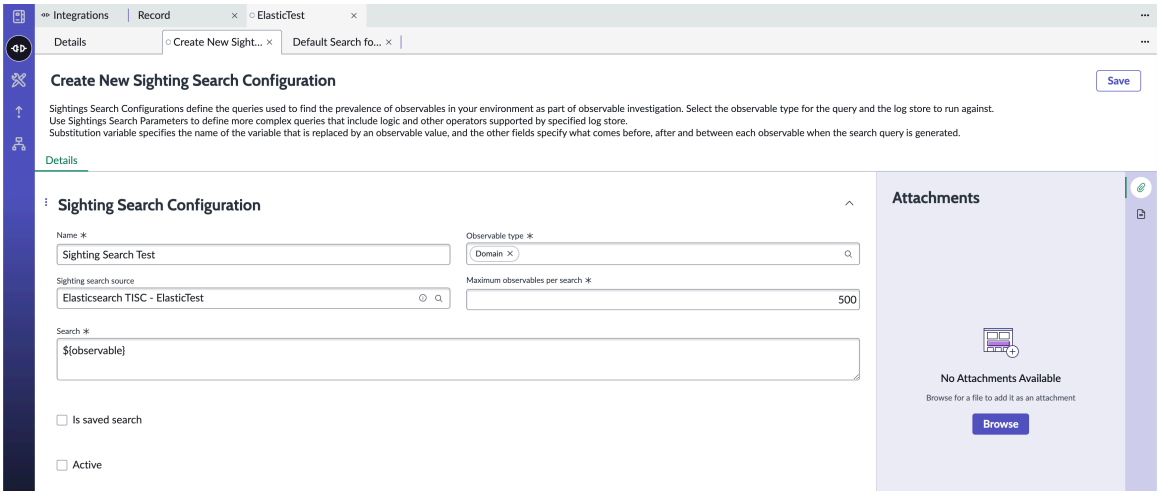
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Intégrations**.
2. Sur la page Intégrations, accédez à **Intégrations de l'enrichissement** > **Recherche de perception**.
3. Recherchez l'intégration pour laquelle vous souhaitez afficher la configuration de recherche de perceptions, puis cliquez sur **Modifier**.
4. Sélectionnez l'onglet **Configurations de recherche de perceptions** .

   Vous pouvez afficher la liste des configurations de recherche de perception.

5. Pour créer une configuration de recherche de perceptions, cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Renseignez les champs du formulaire.

Créer une configuration de recherche de perceptions

Champ	Description
Nom	Nom de la configuration de recherche de perceptions.
Type d'observable	Définit le type de catégorie de l'observable.
Source de recherche de perceptions	Définit la source configurée pour l'intégration.
Nombre maximum d'observables par recherche	Le nombre d'observables avant que la requête de recherche ne soit fractionnée en plusieurs requêtes. Définissez cette valeur sur `500` pour cette intégration.
Rechercher	Ajoutez une chaîne de recherche native pour former une requête. Par exemple, `${observable}`.
Est une recherche enregistrée	Exécute une recherche enregistrée, c'est-à-dire que le champ Nom doit correspondre au nom de la recherche enregistrée.
Actif	La requête s'exécute uniquement si l'option active est sélectionnée.

7. Cliquez sur **Enregistrer**.

Utilisation des paramètres de recherche de perception

Vous pouvez utiliser des paramètres de recherche de perception qui définissent des requêtes plus complexes, qui incluent la logique et d'autres opérateurs pris en charge par le magasin de journaux spécifié.

Afficher les paramètres de recherche de perception

Rôle requis : sn_sec_tisc.admin

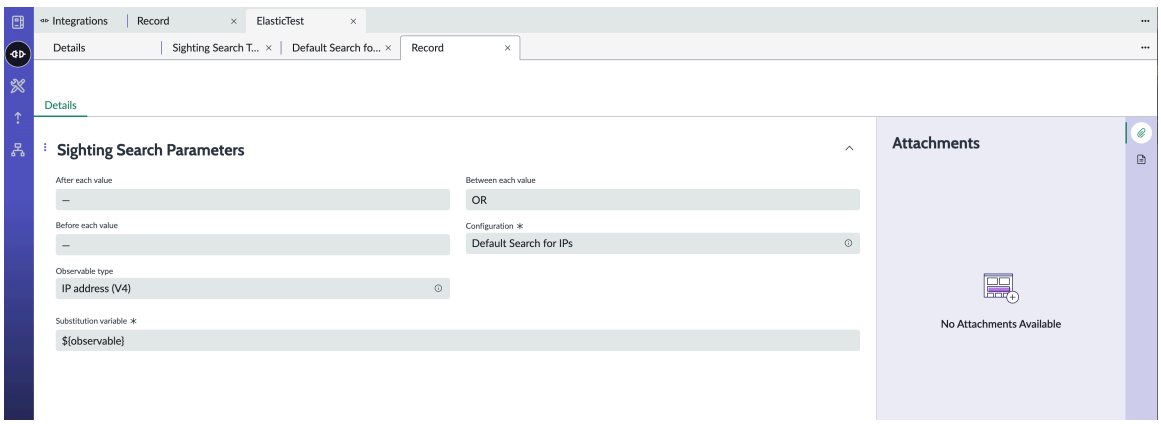
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour afficher les paramètres de recherche de perception, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Intégrations**.
2. Sur la page Intégrations, accédez à **Intégrations de l'enrichissement** > **Recherche de perception**.
3. Recherchez l'intégration pour laquelle vous souhaitez afficher la configuration de recherche de perceptions, puis cliquez sur **Modifier**.
4. Sélectionnez l'onglet **Configurations de recherche de perceptions** .

   Vous pouvez afficher la liste des configurations de recherche de perception.

5. Cliquez sur la configuration de recherche de perception requise pour afficher les détails de la configuration.



6. Sélectionnez l'onglet **Paramètres de recherche de perceptions** .

   Vous pouvez afficher la liste des paramètres de recherche de perception.

7. Cliquez sur le paramètre de recherche de perception requis pour afficher les détails du paramètre.
8. Vous pouvez également effectuer les actions suivantes dans l'onglet Paramètres de recherche de perception :
   a. Pour actualiser la liste des paramètres de recherche de perception, cliquez sur l'icône .
   b. Pour effectuer une action de liste sur les paramètres de recherche de perception, cliquez sur l'icône liste.

      Modifier les colonnes : vous pouvez utiliser cette action pour ajouter ou supprimer des colonnes existantes et modifier l'ordre en fonction de vos besoins.

   c. Pour filtrer les paramètres de recherche de perception en fonction des conditions, cliquez sur l'icône .

      La valeur 1 indique qu'une condition est utilisée pour le filtrage.

Créer un paramètre de recherche de perceptions

`Exemple de génération de requête`

```
Configured Query: ${Observable}

Observables Substitutes for Sightings search: Obs1 , Obs2
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

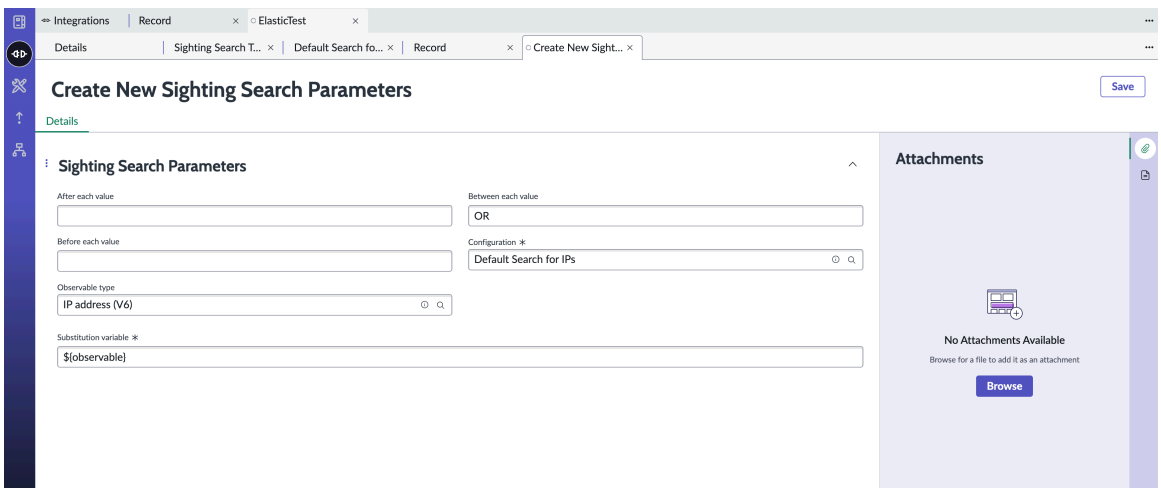
```
Query: {Before each Value}Obs1{After each Value}{Between each
 value}{Before each Value}Obs2{After each Value}


Let observables are: 172.32.31.41 & 192.168.10.12

Query Formed with below configuration will be: "ip_address = 172.32.31.41
 OR ip_address = 192.168.10.12"
```

Pour créer un paramètre de recherche de perception, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Intégrations**.
2. Sur la page Intégrations, accédez à **Intégrations de l'enrichissement** > **Recherche de perception**.
3. Recherchez l'intégration pour laquelle vous souhaitez afficher la configuration de recherche de perceptions, puis cliquez sur **Modifier**.
4. Sélectionnez l'onglet **Configurations de recherche de perceptions** .

   Vous pouvez afficher la liste des configurations de recherche de perception.
5. Cliquez sur la configuration de recherche de perception requise pour afficher les détails de la configuration.
6. Sélectionnez l'onglet **Paramètres de recherche de perceptions** .

   Vous pouvez afficher la liste des paramètres de recherche de perception.
7. Pour créer un paramètre de recherche de perception, cliquez sur **Nouveau**.



8. Renseignez les champs du formulaire.

Créer un paramètre de recherche de perception

Champ	Description
Après chaque valeur	Paramètre de recherche de perception après chaque observable lorsque la requête de recherche est générée.
Entre chaque valeur	Paramètre de recherche de perception entre chaque observable lorsque la

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	requête de recherche est générée. Par exemple, OU.
Avant chaque valeur	Paramètre de recherche de perception avant chaque observable lorsque la requête de recherche est générée.
Configuration	Détails de configuration du paramètre de recherche.
Type d'observable	Définit le type de catégorie de l'observable.
Variable de substitution	Spécifie le nom de la variable qui est remplacée par une valeur observable.

9. Cliquez sur **Enregistrer**.

Configurer la recherche de menace

Vous pouvez configurer la recherche de menace pour effectuer une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par Threat Intelligence, les observables sont analysés à la recherche de programmes malveillants et les résultats sont renvoyés. Vous pouvez effectuer une recherche de menace sur un ou plusieurs observables pour déterminer la malveillance d'un observable.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Remarque : Le module d'intégrations d'enrichissement n'est affiché que si au moins une des intégrations prenant en charge l'une des fonctionnalités est installée dans l'application.

Le Centre de sécurité des renseignements sur les menaces prend en charge la recherche de menace uniquement pour les intégrations suivantes :

- VirusTotal
- CrowdStrike Intelligence

Pour plus d'informations, consultez Recherche de menace.

Pourquoi et quand exécuter cette tâche

La section Recherche de menace contient uniquement les intégrations dont le type d'intégration est Recherche de menace.

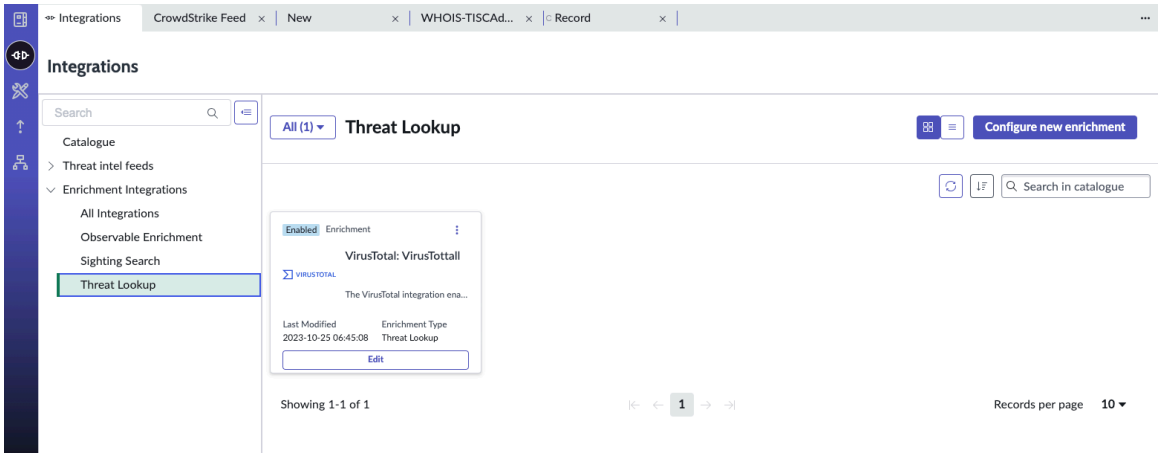
Cette section affiche des cartes pour chacune des implémentations d'intégration configurées que vous pouvez activer et utiliser.

Procédure

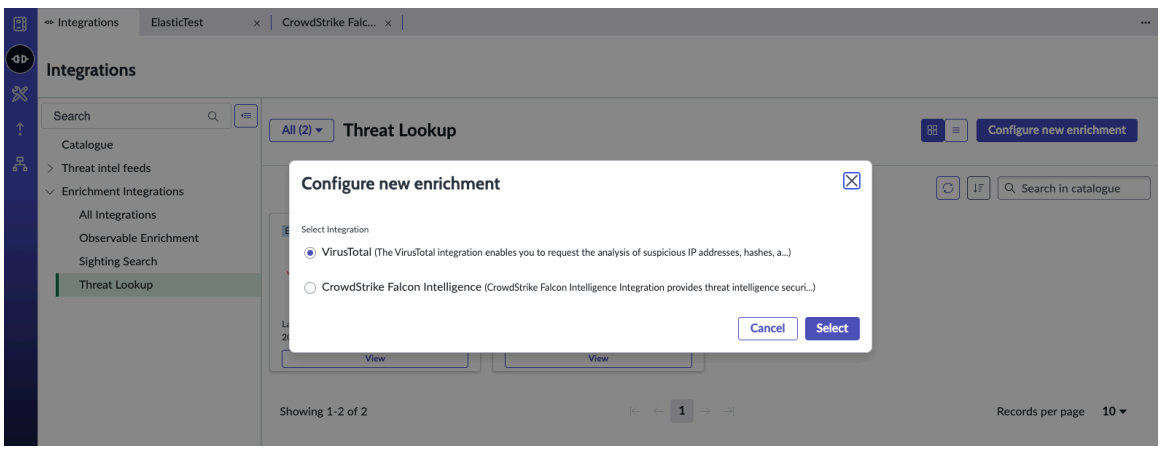
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Intégrations** , puis sélectionnez la section **Recherche de menace** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur l'action **Configurer un nouvel enrichissement** .
   Vous accédez alors à la fenêtre contextuelle qui affiche les intégrations disponibles. Vous devez choisir l'intégration que vous avez à configurer.
4. Sélectionnez une intégration dans la liste des intégrations disponibles, puis cliquez sur **Sélectionner**.
   Vous accédez alors à la page Créer une intégration d'enrichissement de l'intégration sélectionnée. Par défaut, cette page est pré-remplie avec les détails de l'intégration sélectionnée. Par exemple, l'intégration de VirusTotal.

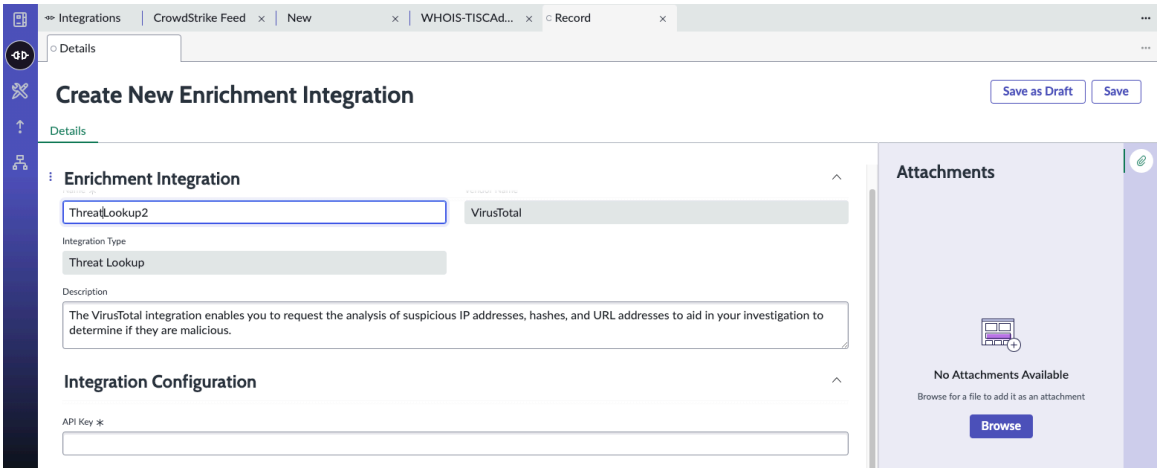


5. Renseignez les champs du formulaire Créer une intégration.

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration d'enrichissement. Par exemple, `VirusTo-tal-1`.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont pré-remplis par défaut. Par exemple, `VirusTotal`.
Type d'intégration	Type d'intégration que vous avez sélectionné, à savoir Recherche de menace. Les détails du type d'intégration sélectionné sont pré-remplis par défaut.
Description	Entrez une description unique pour la nouvelle intégration d'enrichissement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Dans la section Configuration de l'intégration, configurez les détails d'intégration en fonction de vos besoins.
   La section Configuration de l'intégration inclut des détails de configuration tels que la clé API, l'ID ou le secret du client API, le nom d'utilisateur, le mot de passe, etc., que vous devez renseigner. Ces détails de configuration varient selon les applications.
7. Cliquez sur l'action **Enregistrer** pour stocker et créer la nouvelle configuration de l'intégration d'enrichissement.
   Les détails fournis sont validés et, par défaut, l'état de l'intégration de l'enrichissement est désactivé.
8. Cliquez sur **l'action Enregistrer comme brouillon** pour stocker uniquement les mises à jour apportées à la configuration d'enrichissement et ne pas la créer.
   Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez remplir les informations restantes dans la version brouillon et la créer.
9. Pour activer l'intégration de l'enrichissement, cliquez sur **Activer**.
   L'intégration de l'enrichissement est activée. Vous pouvez également activer, désactiver ou supprimer une intégration d'enrichissement particulière à l'aide du menu Actions de la vignette d'intégration requise sur la page Catalogue ou sur la page Intégrations d'enrichissement.

Afficher les calculateurs de réputation de la recherche de menaces

Vous pouvez afficher le calculateur de résultat de la recherche de menaces pour calculer les résultats observables pour votre intégration.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

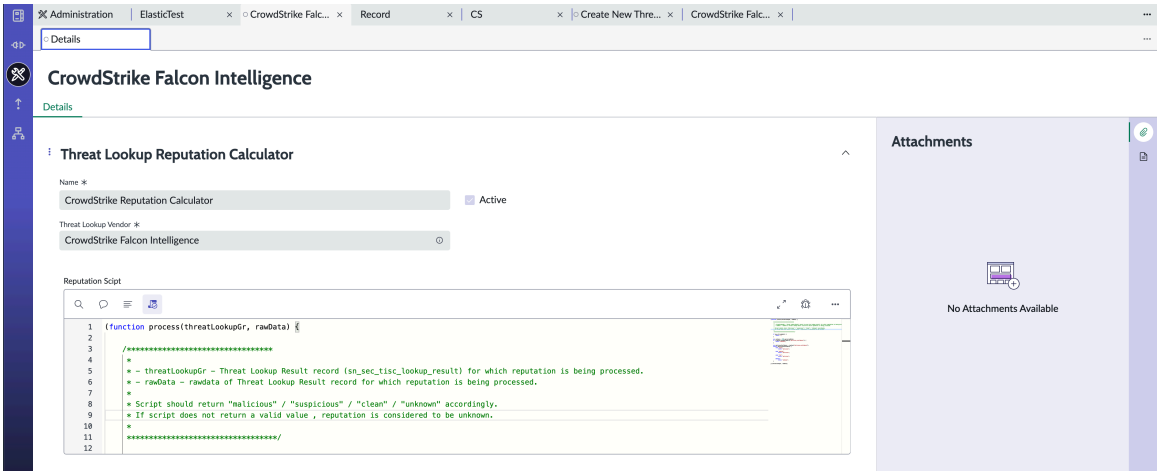
Pour en savoir plus sur les calculateurs de réputation de recherche de menaces, reportez-vous à la section Gestion du calculateur de réputation de la recherche de menaces.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionnez la section **Calculateur de réputation de la recherche de menaces** .
   Vous pouvez afficher la liste des calculateurs de réputation de recherche de menace.
3. Cliquez sur le calculateur de réputation de recherche de menaces requis pour afficher les détails du calculateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Vous pouvez également effectuer les actions suivantes dans la section Calculateur de réputation de la recherche de menaces :

   a. Pour actualiser la liste des calculateurs de réputation de la recherche de menaces, cliquez sur l'icône de .

   b. Pour effectuer une action de liste sur les calculateurs de réputation de recherche de menaces, cliquez sur l'icône .

      Vous pouvez effectuer les deux actions de liste suivantes :

      - **Modifier les colonnes** : vous pouvez utiliser cette action pour ajouter ou supprimer des colonnes existantes et modifier l'ordre en fonction de vos besoins.
      - **Réinitialiser les largeurs** : vous pouvez utiliser cette action pour réinitialiser les largeurs des colonnes.

   c. Pour filtrer les calculateurs de réputation de la recherche de menaces en fonction des conditions, cliquez sur l'icône .

      La valeur 1 indique qu'une condition est utilisée pour le filtrage.

Références API TISC

La table suivante fournit les références des points de terminaison d'API qui aident aux enrichissements.

API TISC

API	Description
API TISC : POST/sn_sec_tisc/ threat_intel_data/OBSERVABLES	Cette API récupère les données des observables, y compris les relations entre les observables et d'autres données Threat Intelligence associées.
API TISC : POST /sn_sec_tisc/ threat_intel_data/add_observables	Cette API ajoute des observables valides à l'application Centre de sécurité des renseignements sur les menaces (TISC) en créant des enregistrements sources d'observables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les points de terminaison de l'API TISC, consultez API TISC sous la section de référence de l'API REST sur l'implémentation de l'API et référence sur docs.servicenow.com.

Intégrations TISC

Cette section fournit des instructions pour configurer et activer les intégrations de Threat Intelligence.

Enrichissement des éléments observables

Le workflow Enrichir les observables WhoIs effectue un enrichissement sur les observables sélectionnés. Si les observables sont d'un type reconnu par l'intégration de l'API WhoisXML, les observables sont enrichis.

Remarque : Threat Intelligence Security Center ne prend en charge l'enrichissement des observables que pour l'intégration WHOIS.

Intégration Whois

L'intégration Whois vous permet de soumettre des recherches Whois sur les noms de domaine et les URL afin d'obtenir un contexte sur les observables d'URL et de mieux déterminer les menaces.

Configurer et activer l'intégration Whois

Avant d'utiliser l'intégration Whois, vous devez la télécharger à partir de ServiceNow Store et disposer d'un compte Whois valide.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Les modules d'extension Threat Intelligence Security Center et Whois observable integration sont requis.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Téléchargez l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à **Espaces de travail** > **Threat Intelligence Security Center**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Enrichissement des éléments observables**.
6. Dans la carte **WHOIS** , cliquez sur **Configurer un nouvel enrichissement** pour configurer l'intégration **WHOIS** .
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration d'enrichissement. Par exemple, le WHOIS.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, le WHOIS.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.
Description	Entrez la description de la nouvelle intégration d'enrichissement. Par exemple, la description de l'intégration WHOIS est la suivante : L'intégration WHOIS pour Centre de sécurité des renseignements sur les menaces permet aux utilisateurs de soumettre des recherches Whois sur les noms de domaine et les URL afin d'obtenir un contexte sur les observables d'URL et de mieux déterminer les menaces.

8. Explorez la section **Configuration de l'intégration** .
9. Entrez (ou collez) la **clé API** que vous avez acquise sur le site WHOIS.
10. Cliquez sur **Enregistrer**.
    Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration WHOIS est désactivé.
11. Cliquez sur **Activer** pour activer l'intégration du WHOIS.

Résultats
Une fois configuré, le WHOIS peut être sélectionné pour effectuer des enrichissements sur les observables dans Centre de sécurité des renseignements sur les menaces.

Intégration Shodan

Shodan est un moteur de recherche qui analyse les informations des bannières de service à partir d'appareils connectés dans le monde entier.

L'intégration Shodan effectue un enrichissement sur les observables suivants :

- Adresses IP
- URL
- Domaines

Configurer et activer l'intégration Shodan

Avant d'utiliser l'intégration Shodan, vous devez la télécharger à partir de la ServiceNow boutique.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Téléchargez l'intégration à partir de ServiceNow Store.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

3. Une fois l'installation terminée, accédez à **Espaces de travail** > **Threat Intelligence Security Center**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Enrichissement des éléments observables**.
6. Dans la carte **Shodan** , cliquez sur **Configurer un nouvel enrichissement** pour configurer l'intégration.
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration d'enrichissement. Par exemple, Shodan.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés automatiquement et, par défaut, ce champ est en lecture seule. Par exemple, Shodan.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Enrichissement des observables.
Description	Entrez la description de la nouvelle intégration d'enrichissement. Par exemple, la description de l'intégration Shodan est la suivante : Shodan vous aide à analyser les informations de bannière à partir d'appareils connectés dans le monde entier.

8. Explorez la section **Configuration de l'intégration** .
9. Entrez (ou collez) la **clé API** que vous avez acquise à partir du portail Shodan.
10. Cliquez sur **Enregistrer**.
    Les détails de l'intégration sont validés et, par défaut, l'état est désactivé.
11. Cliquez sur **Activer** pour activer l'intégration.

Recherche de perception

Cette section décrit les intégrations TISC Sighting Search et Elastic Search.

Premiers pas avec l'intégration Elasticsearch

L'intégration d'enrichissement Elasticsearch recherche vos journaux et ajoute des informations de perception pertinentes à vos observables.

Configurer et activer l'intégration d'Elasticsearch

Elasticsearch est un moteur de recherche et d'analyse distribué et RESTful qui s'intègre facilement à Security Operations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Avant de pouvoir utiliser Elasticsearch, vous devez le télécharger à partir du ServiceNow Store.

Rôle requis : sn_sec_tisc.admin

- Le module d'extension Threat Intelligence Security Center doit être installé et activé avant de pouvoir utiliser l'intégration Elasticsearch.
- Obtenez l'URL de base de l'API Elasticsearch, l'URL de base Kibana, le nom d'utilisateur et le mot de passe sous votre profil Elasticsearch.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Téléchargez l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à **Espaces de travail** > **Threat Intelligence Security Center**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Recherche de perception**

   Remarque : Les intégrations configurées apparaissent sous la forme d'une série de cartes.

6. Dans la carte **Elasticsearch** , cliquez sur **Configurer un nouvel enrichissement** pour configurer **Elasticsearch** Integration.
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la configuration de la recherche de perceptions.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, Elasticsearch.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.
Description	Saisissez la description de l'intégration Elasticsearch. Par exemple, l'intégration d'enrichissement Elasticsearch facilite l'enquête sur un observable en prenant en charge l'interrogation des journaux dans votre déploiement Elasticsearch.
Configuration de l'intégration	
URL de base de l'API Elasticsearch	L'URL de base que vous avez acquise sur le site Elasticsearch.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL de base Kibana	URL de base Kibana. [Facultatif] Liens vers une instance Kibana, lorsqu'elle est disponible.
Nom d'utilisateur	Votre nom d'utilisateur Intel Elasticsearch.
Mot de passe	Votre mot de passe Intel Elasticsearch.
Index Elasticsearch	L'index Elasticsearch. Ceux-ci contiendront à leur tour des documents uniques à chaque index. Les index sont identifiés par des noms en minuscules qui font référence à des actions effectuées (telles que la recherche et la suppression).
Champ de plage de dates	Horodatage de la configuration.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend du paramètre que vous définissez sur le nombre de lignes de la propriété de données brutes dans les propriétés de Réponse aux incidents de sécurité .
Serveur MID	Sélectionnez N'importe lequel pour utiliser n'importe quel Serveur MID actif ou sélectionnez un nom de Serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à l'éditeur de workflow.

8. Cliquez sur **Enregistrer**.
   Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration Elasticsearch est désactivé.
9. Cliquez sur **Activer** pour activer l'intégration d'Elasticsearch.

Résultats

Une fois qu'il est configuré, Elasticsearch peut être sélectionné pour effectuer une recherche de perception sur les observables dans Threat Intelligence Security Center.

Introduction à l'intégration de la recherche Splunk

Le logiciel Splunk recherche, surveille et analyse les données volumineuses générées par les machines et s'intègre facilement aux opérations de sécurité. Avant de pouvoir utiliser l'intégration de la recherche d'observations Splunk, vous devez la télécharger à partir du ServiceNow Store.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer et activer l'intégration Splunk

L'intégration d'enrichissement Splunk recherche vos journaux et ajoute des informations d'observation pertinentes.

Avant de commencer

Avant de pouvoir utiliser la recherche Splunk, vous devez la télécharger à partir du ServiceNow Store.

Rôle requis : sn_sec_tisc.admin

- Le module d'extension Threat Intelligence Security Center doit être installé et activé avant de pouvoir utiliser l'intégration de la recherche Splunk.
- Procurez-vous Splunk et obtenez la recherche Splunk et obtenez l'URL de base de l'API, l'URL du lien, le nom d'utilisateur et le mot de passe de votre instance Splunk.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Téléchargez l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à **Espaces de travail** > **Threat Intelligence Security Center**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Recherche de perception**
   Les intégrations configurées apparaissent sous la forme d'une série de cartes.
6. Sur la carte **Splunk Search** , cliquez sur **Configurer un nouvel enrichissement** pour configurer **l'intégration de Splunk Search** .
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la configuration de la recherche de perceptions.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, Splunk.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.
Description	Saisissez la description de l'intégration Splunk. Par exemple, l'intégration d'enrichissement de Splunk facilite l'examen d'un observable en prenant en charge l'interrogation des journaux dans votre déploiement Splunk en ce qui concerne les indicateurs potentiellement malveillants.
Configuration de l'intégration	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL de Base de l'API Splunk	L'URL de base que vous avez acquise sur le site Splunk.
URL de lien	[Facultatif] URL du lien qui renvoie à l'interface Web de Splunk, lorsqu'elle est disponible.
Nom d'utilisateur	Votre nom d'utilisateur Intel Elasticsearch.
Mot de passe	Votre mot de passe Intel Elasticsearch.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend du paramètre que vous définissez sur le nombre de lignes de la propriété de données brutes dans les propriétés de Réponse aux incidents de sécurité .
Déploiement sur site	Environnement de déploiement sur site.
Serveur MID	Sélectionnez N'importe lequel pour utiliser n'importe quel Serveur MID actif ou sélectionnez un nom de Serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à l'éditeur de workflow.

8. Cliquez sur **Enregistrer**.
   Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration Splunk est désactivé.
9. Cliquez sur **Activer** pour activer l'intégration Splunk.

Résultats

Une fois configuré, Splunk peut être sélectionné pour effectuer une recherche de perception sur des observables dans Centre de sécurité des renseignements sur les menaces.

Recherche de menace

Le workflow Recherche de menace - VirusTotal et CrowdStrike Falcon Intelligence effectue une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par VirusTotal et CrowdStrike, les observables sont analysés à la recherche de programmes malveillants et les résultats sont renvoyés.

Intégration TISC VirusTotal

L'intégration TISC VirusTotal vous permet de demander l'analyse des adresses IP, des fichiers, des hachages de fichiers et des adresses URL suspects afin d'aider à déterminer s'ils sont malveillants.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer et activer l'intégration de VirusTotal

Avant de pouvoir utiliser l'intégration de VirusTotal, vous devez la télécharger à partir du ServiceNow Storefichier .

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Le module d'extension Threat Intelligence Security Center est requis pour activer l'intégration de VirusTotal.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Téléchargez l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à VirusTotal et obtenez la clé API sous votre profil VirusTotal.
4. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
5. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
6. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Recherche de menace**
7. Cliquez sur **Configurer un nouvel enrichissement pour configurer l'intégrationde VirusTotal** .
8. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration d'enrichissement. Par exemple, VirusTotal.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, VirusTotal.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.
Description	Entrez la description de la nouvelle intégration d'enrichissement.

9. Explorez la section **Configuration de l'intégration** .
10. Entrez (ou collez) la **clé API** que vous avez acquise sur le site VirusTotal.
11. Cliquez sur **Enregistrer**.
    Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration VirusTotal est désactivé.
12. Cliquez sur **Activer** pour activer l'intégration de VirusTotal.

Résultats

Une fois configuré, VirusTotal peut être sélectionné pour effectuer des recherches sur les observables dans Centre de sécurité des renseignements sur les menaces.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration TISC CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence fournit des renseignements de cybersécurité qui s'intègrent facilement aux opérations de sécurité.

Remarque :

Le module d'extension Threat Intelligence Security Center est requis pour implémenter l'intégration de CrowdStrike Falcon Intelligence.

Configurer et activer l'intégration de CrowdStrike Falcon Intelligence

Avant de pouvoir utiliser CrowdStrike Falcon Intelligence, vous devez le télécharger à partir du ServiceNow Store et ajouter l'ID client et le secret client appropriés.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

- L'application Centre de sécurité des renseignements sur les menaces doit être installée et activée.
- Obtenez l'ID du client API et le secret du client API sous votre profil CrowdStrike Falcon Intelligence.
- Dans les périmètres d'API du portail CrowdStrike Falcon Intelligence, activez le paramètre de lecture pour les indicateurs (Falcon Intelligence).

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Téléchargez l'intégration à partir de ServiceNow Store.
3. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Recherche de menace**.
6. Cliquez sur **Configurer un nouvel enrichissement** pour configurer l'intégration de **CrowdStrike Falcon Intelligence** .
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration d'enrichissement. Par exemple, CrowdStrike Falcon Intelligence.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, CrowdStrike Falcon Intelligence.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Entrez la description de la nouvelle intégration d'enrichissement.
Configuration de l'intégration	
ID client	L'ID client que vous avez obtenu à partir de CrowdStrike.
Secret client	La clé secrète du client que vous avez obtenue à partir de CrowdStrike.

8. Cliquez sur **Enregistrer**.
   Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration de CrowdStrike Falcon Intelligence est désactivé.
9. Cliquez sur **Activer** pour activer l'intégration de CrowdStrike Falcon Intelligence.

Résultats
Une fois configuré, CrowdStrike Falcon Intelligence peut être sélectionné pour effectuer des recherches sur les observables dans Threat Intelligence Security Center.

Intégration de TISC à l'espace de travail SIR

L'intégration TISC au SIR associe automatiquement le contexte aux observables dans l'espace de travail d'incident de sécurité pour les analystes de sécurité. Tous les nouveaux observables de SIR peuvent être envoyés à TISC pour analyse plus approfondie par l'équipe CTI à l'aide des actions d'interface utilisateur fournies sur les écrans.

En outre, tous les résultats d'enrichissement produits à partir d'intégrations disponibles uniquement dans SIR peuvent également être transmis par push à l'aide des actions d'interface utilisateur fournies dans l'espace de travail.

Administration

Utilisez le volet de navigation de gauche pour accéder au module Administration dans Centre de sécurité des renseignements sur les menaces et afficher les modules suivants de l'administration des données TISC afin de définir des règles de filtrage, des règles d'approbation, de définir le score de menace et de gérer les notifications.

Administration des données

Module	Description
Moteur de règles	Cette section comprend les règles suivantes requises lors de la gestion des données : 1. **Importations de données Règles d'approbation** : définissez les règles d'approbation et intégrez le flux d'approbation dans la section Connaissance de l'importation après avoir soumis l'importation de données. 2. **Règles de filtrage entrant** : créez des règles de filtrage afin de filtrer les données des enregistrements sources entrants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Administration des données (suite)

Module	Description
	3. **Règle de définition du score de menace** : personnalisez le calculateur de score de menace qui affecte le score de menace aux observables.
Listes des contrôles de sécurité	Ce module vous aide avec les contrôles de sécurité : 1. **Liste d'autorisation** 2. **Liste de refus** 3. **Liste de surveillance**
Taxonomies	Ce module vous aide à créer des taxonomies pour les enregistrements sources de données.
Notifications	Ce module définit comment gérer les notifications par e-mail.
Modèles	Ce module explique comment créer des modèles de rapport au moment de la conception et de l'expérience d'exécution.

Définition des règles d'approbation des importations de données

Utilisez cette section pour définir les règles d'approbation et intégrer le flux d'approbation dans la section Intelligence d'importation après avoir soumis l'importation de données.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Administration** dans l'espace de travail.
3. Accéder à **Moteur de règles** > **Importations des données pour les règles d'approbation**.
4. Sélectionnez **la règle d'approbation pour les importations de données**.

   Dans le système de base, la **règle d'approbation pour les importations de données** est la règle d'approbation par défaut mise en service pour permettre aux utilisateurs d'activer le workflow d'approbation.

5. Entrez au moins un nom d'utilisateur ou un groupe d'utilisateurs pour chacune des sections **Sélectionner un ou plusieurs utilisateurs nécessitant une approbation** et **Sélectionner un ou plusieurs approbateurs** .
6. Cliquez sur le bouton **Activer** pour activer le flux d'approbation pour les importations de données.

   Lorsque cette option est activée, les importations de données se trouvent dans la file d'attente d'approbation pour que l'approbateur approuve ou rejette le traitement des

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

données. L'approbateur examine les changements apportés par l'analyste, puis approuve ou rejette la demande d'importation de données.

Remarque : Une notification par e-mail est envoyée au(x) utilisateur(s) ou au(x) groupe(s) d'utilisateurs indiquant que la tâche d'importation est traitée et approuvée ou rejetée.

Définition des règles d'expiration

Définissez des règles d'expiration pour divers observables ou une combinaison de divers objets sources sources ou d'indicateurs créés dans TISC.

Avant de commencer

Chaque source créée dans l'application a une période d'expiration. Les flux de données utilisent des techniques telles que la période d'expiration basée sur le temps pour stimuler l'ingestion de données. Dans TISC, les règles d'expiration définissent le délai d'expiration d'un ensemble particulier de sources de données, d'un ensemble de types d'objets ou de types d'observables.

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Règles d'expiration**.
   La page Règles d'expiration s'affiche.
3. Cliquez sur **Nouveau**.

Champ	Description
Nom	Donnez un nom à la règle d'expiration.
Description	Entrez une description pour la règle d'expiration.
Période d'expiration (jours)	Spécifiez la durée après laquelle les données ingérées doivent expirer ou être considérées comme obsolètes. Saisissez la période d'expiration de l'observable en jours. Par exemple, 100 jours. **Remarque :** Quelles que soient les données ingérées à partir de la source, elles expirent 100 jours après l'ingestion.
Sources de données	Indique la règle d'expiration pour la source de données actuelle. Sélectionnez la liste des sources de données de la recherche. **Remarque :** Ne sélectionnez pas ce champ et veillez à le laisser vide si vous souhaitez sélectionner toutes les sources de données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si vous souhaitez sélectionner l'indicateur en tant qu'objet, vous devez sélectionner l'objet, puis sélectionner la valeur **Type d'enregistrements en tant qu'indicateur**. **Remarque :** Par défaut, un exemple de règle d'expiration sn_sec_tisc_-m2m_entity_rules est mis en service pour les utilisateurs du système de base. Pour les observables, cet exemple de règle d'expiration sera à l'état désactivé. Vous devez activer et activer la règle. Pour appliquer la règle aux enregistrements sources, vous devez activer la règle.
Catégorie	Indique le type de catégorie de la règle d'expiration pour la source de données actuelle. Sélectionnez le type de catégorie dans la liste déroulante, par exemple observable ou objet.
Type d'enregistrements	Sélectionnez le type d'enregistrements.

4. Cliquez sur **Activer** pour activer la règle d'expiration après avoir créé une nouvelle règle. Si vous n'activez pas la règle d'expiration, elle ne sera pas appliquée à l'enregistrement source.

   Remarque :

   - Chaque fois que vous activez une règle d'expiration, une vérification de duplication se produit en arrière-plan pour vérifier s'il existe une règle en double dans le système avec la même combinaison de sources de données et de type d'enregistrements. Si tel est le cas, l'application invite un message d'information indiquant que la règle contient déjà la même combinaison de source de données et de catégorie d'objets et que vous devez modifier la combinaison existante pour activer la règle.
   - Un exemple de règle d'expiration est mis en service pour les utilisateurs du système de base et cet **exemple de règle d'expiration** pour l'observable est désactivé par défaut et vous devez activer et activer la règle.

5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Supprimer** si vous souhaitez supprimer une règle d'expiration.

Règles d'expiration pour les enregistrements sources

Les règles d'expiration sont essentiellement utiles pour définir le délai d'expiration des enregistrements sources. L'enregistrement d'agrégat hérite du délai d'expiration le plus élevé de ses enregistrements sources correspondants.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mode d'application des règles

Example: Le type d'enregistrement source entrant est Programme malveillant du type de source de données CrowdStrike

Processus d'évaluation des règles basé sur les règles prévues pour l'application des délais d'expiration aux enregistrements sources :

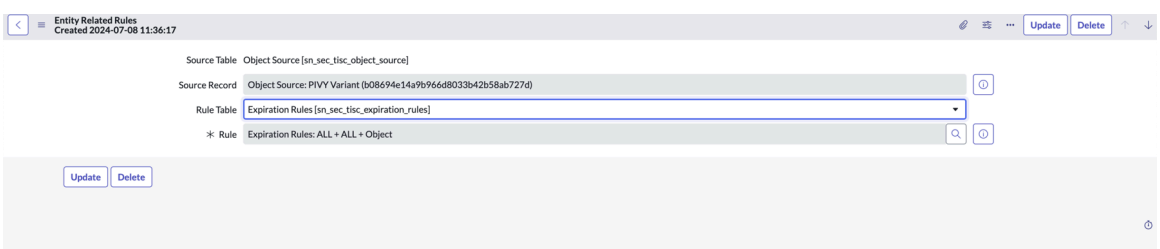
1. **Extraire toutes les règles activées :** L'application commence par vérifier toutes les règles actuellement activées.
2. Recherchez une combinaison de règles spécifique :

   Recherchez une règle qui correspond spécifiquement à la combinaison des éléments suivants :

   - **Type de source de données** : CrowdStrike
   - **Type d'enregistrements** : programme malveillant
3. **Priorité basée sur les combinaisons de règles correspondantes :**

   S'il existe une règle où le type de source de données est **CrowdStrike** et le type d'enregistrement est Logiciel **malveillant**, cette règle prévaut. Le délai d'expiration spécifié dans cette règle sera appliqué.

4. **Règles de secours :**
   a. Si aucune règle ne correspond à la combinaison **de CrowdStrike et de programme malveillant** , le système recherche une règle dans laquelle le type de source de données est **CrowdStrike** et le type d'enregistrement est **Tous**.
   b. Si aucune règle n'est encore trouvée, il recherche alors une règle dans laquelle le type de source de données est **Toutes** et le type d'enregistrement est **Logiciel malveillant**.
   c. Enfin, si aucune des règles ci-dessus n'existe, la règle par défaut est définie sur une règle où le type de source de données et le type d'enregistrement sont **tous**.
5. Si aucune de ces règles n'existe dans le système, aucune règle d'expiration n'est alors appliquée aux enregistrements sources. Dans ce cas, accédez au tableau ci-dessous (illustré dans la capture d'écran) pour vérifier la combinaison de règles qui ont été appliquées aux objets.



6. **Suppression des sources de données :**

   Supposons que si une source de données associée à des règles d'expiration est supprimée, la suppression peut être restreinte ou interdite jusqu'à ce que ces règles soient traitées. Cela garantit qu'il n'y a pas d'incohérences dans l'application des politiques d'expiration.

Définition de règles de filtrage

Créez des règles de filtrage afin de filtrer tout type de données ou tout type de données d'enregistrements sources entrants. À l'aide du gestionnaire de sources de données,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

plusieurs flux tels que les données STIX et les flux RSS sont configurés et pour filtrer les données à partir des flux configurés, vous devez définir certaines règles de filtrage.

Avant de commencer

Lorsque vous définissez une règle de filtrage, cette règle s'applique uniquement à l'ensemble de données sources dans lequel une règle est appliquée pour filtrer les enregistrements pendant l'ingestion et l'importation des données.

Rôle requis : sn_sec_tisc.admin

Pourquoi et quand exécuter cette tâche

Des règles de filtrage sont créées et appliquées à un enregistrement source pour traiter les étapes suivantes. Le système de base fournit **l'exemple de règle de filtrage** pour les utilisateurs avec une règle prédéfinie pour filtrer les observables, les données d'indicateur ou les entités/objets ingérés.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Administration**.
2. Explorer jusqu'à **Moteur de règles** > **Règles de filtrage entrant**.
3. Cliquez sur **Nouveau** pour définir des règles de filtrage.
   La page Créer de nouvelles règles de filtrage entrant s'affiche.
4. Renseignez les champs du formulaire.

Définir des règles de filtrage

Champ	Description
Nom	Nom de la nouvelle règle de filtrage.
Description	Brève description de la règle de filtrage.
Ordre	Priorité de la règle de filtrage. Ce champ indique l'ordre dans lequel les règles de filtrage sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle de filtrage associée au numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100 pour la règle de filtrage du système de base.
Sources de données	Sélectionnez le type de source de données dans la liste de recherche.
Table	Sélectionnez le type de table auquel vous souhaitez appliquer le filtre. Par exemple, Source d'observable, Source d'indicateur et Source d'objet.
Type de filtre (uniquement lorsque la table sélectionnée est Source d'observables)	Types de filtres contient deux options sur lesquelles vous pouvez appliquer le filtre.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Filtre basé sur une condition ◦ Filtre basé sur une liste
Type de filtre (filtre basé sur une condition)	Conditions de filtre dans le générateur de conditions. Ces conditions sont basées sur la table source. Par exemple, Source d'indicateur et Source d'objet n'a qu'un seul type de filtre : Filtre basé sur la condition. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouvel ensemble de conditions**.
Type de filtre (filtre basé sur la liste)	Si les observables entrants correspondent aux entrées de la liste, les éléments sélectionnés sont filtrés. **Remarque :** Ces règles de filtrage ne s'appliquent pas aux importations de données utilisant l'intelligence d'importation et les options disponibles sont Liste d'autorisation, Liste de refus et Liste de surveillance.

Une fois la règle de filtrage activée sur les données ingérées, le résultat peut être affiché dans les onglets suivants sous la forme de différents enregistrements filtrés.

a. **Enregistrements d'observables filtrés** : filtre et répertorie les enregistrements d'observables.

b. **Enregistrements d'indicateurs filtrés** : filtre et répertorie les enregistrements d'indicateurs.

c. **Enregistrements d'objets filtrés** : filtre et répertorie les enregistrements d'objets.

Remarque : Pour appliquer les règles de filtrage en fonction des balises ajoutées aux enregistrements sources, sélectionnez l'option **Balises TISC** dans le générateur de conditions de filtre.

Calculateur de score de menace personnalisé dans TISC

Le calculateur de score de menace personnalisé vous permet de définir et de calculer le score de gravité d'un observable en fonction des critères définis par l'utilisateur, ce qui permet d'obtenir un score d'intelligence transparent des observables. Le score de menace est calculé automatiquement pour les enregistrements d'observables.

Définir le calculateur de score de menace

Définissez le score de menace pour les enregistrements d'observables qui sont générés en fonction des paramètres définis par l'utilisateur. Le système de base est doté d'une règle de notation des menaces, qui peut être personnalisée et activée en conséquence.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Remarque : Par défaut, la règle de notation des menaces sera inactive, vous devez activer la règle pour voir la notation des observables.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Administration**.
2. Accéder à **Règle de notation de menace**.
   La page Calculateur de score de menace s'affiche.

Important :

- Dans l'application, au sein du système de base, il existe une règle de notation qui est mise en service pour permettre aux utilisateurs d'afficher, de modifier ou de modifier le score de menace, mais l'utilisateur ne peut ni créer une nouvelle règle ni supprimer la règle de notation de menace prédéfinie.
- Les changements s'appliqueront à tous les nouveaux observables ou mises à jour des observables à partir de ce moment-là. Pour retraiter les scores historiques, ils doivent utiliser l'option recalculer.

3. Dans le formulaire, les champs suivants contiennent les valeurs prédéfinies.

Calculateur score de menace

Champ	Description
Nom	Nom de la valeur de score de menace. Par exemple, Calculateur de score de menace.
Description	Description de l'enregistrement du score de menace. Par exemple, calcule le score de menace en fonction de la somme pondérée des scores de critères prédéfinis.
Pondération globale (applicable au générateur de critères)	Ce champ n'est pas modifiable et affiche la pondération globale calculée par le système en fonction du poids correspondant aux critères activés.
Critères de notation	Indique les critères de notation pour un observable. Les deux options disponibles pour définir les critères de score de menace sont les suivantes : ◦ **Générateur de critères** : Utilisez cette option pour ajouter, modifier ou supprimer, activer et désactiver les critères qui contribuent au calcul du score de menace et vous assurer que la pondération totale agrégée est égale à 100 %.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ **Utiliser script (avancé)** : la fonctionnalité de scripting est une fonctionnalité avancée permettant de créer un script personnalisé qui doit renvoyer le score de menace dans une plage comprise entre 0 et 100.

Vous trouverez ci-dessous les options disponibles pour définir les **critères de notation** :

◦ Générateur de critères

◦ Utiliser le script (avancé)

Voici la procédure pour le générateur de critères :

Remarque : Vous pouvez modifier les critères existants ou en ajouter un nouveau.

a. Sélectionnez le type de critères.
Par exemple, ajoutez un nouveau critère.

b. Sélectionnez la **table** pour laquelle les critères sont configurés.
La liste des valeurs de la liste déroulante est Observables, Acteur de menace, Campagne, Emplacement, Identité, Vulnérabilité, Événement de menace, Incident de sécurité et Agrégats. Lorsque vous sélectionnez l'une de ces options dans la liste déroulante, une condition est appliquée. Cette condition garantit que seuls les enregistrements associés à la valeur sélectionnée sont affichés ou calculés.

Remarque :

- Si l'observable est sélectionné, la condition sera appliquée à l'enregistrement d'observable pour lequel le score de menace sera calculé. Si la table sélectionnée n'est pas observable, la condition ne sera appliquée que si les enregistrements sont associés à l'observable pour lequel le score de menace sera calculé.
- Une table Agrégats supplémentaire est ajoutée pour définir les scores en fonction du nombre de relations associées aux observables. Par exemple, sélectionnez la table : Agrégats et la valeur de champ : Acteurs de menace Ensuite, pour un observable, s'il y a plus de deux acteurs de menace, définissez le score et appliquez les conditions le cas échéant.
- Par exemple, si vous souhaitez définir un score pour un ou plusieurs acteurs de menace associés à un observable, sélectionnez le champ Nombre d'acteurs de menace, définissez le score souhaité et appliquez les conditions le cas échéant.

c. Sélectionnez le **champ** dans la table sélectionnée ci-dessus.

d. Entrez la **pondération** des critères entre 0 et 100.
La pondération globale de tous les critères doit être de 100 %.

e. Entrez le nom et une brève description des critères.

f. Cochez la case **Activer les critères de notation** pour activer les critères de notation.

g. Définissez les **conditions** et définissez le score pour les conditions.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

h. Vous pouvez également ajouter de nouvelles conditions à l'aide du bouton **Nouvelle condition** et supprimer la condition à l'aide de l'icône **Supprimer les critères** .

i. Cliquez sur **Ajouter** pour ajouter les critères configurés.

Voici un exemple de définition d'une condition pour un score de menace :

```
Table: Vulnerability

Field: CVSS2.0

Weightage: 30%

Condition-1: CVSS2.0 > 7, Score = 80

Condition-2: CVSS2.0 > 4 AND CVSS2.0 < 7, Score = 50

Condition-3: CVSS2.0 < 4, Score = 10
```

4. Cliquez sur le bouton **Recalculer l'historique** pour recalculer le score de menace.
Si des modifications sont apportées à la règle de définition du score de menace, vous devez réappliquer la règle de notation aux observables pour lesquels le score de menace a déjà été calculé dans le passé. Utilisez le bouton **Recalculer l'historique** pour déclencher la tâche de recalcul.

Remarque :

- Un message de confirmation s'affiche pour vous permettre d'effectuer l'action. `Il s'agit d'un processus de longue durée qui s'exécute en arrière-plan. Vous ne serez pas en mesure d'apporter des changements tant que le processus n'est pas terminé. Voulez-vous vraiment exécuter cette action ?`
- Pour tous les événements de mise à jour qui sont générés pour les observables dans le cadre de **Recalculer l'historique**, le traitement des webhooks est désactivé et, si vous souhaitez l'activer, modifiez cette propriété système `webhook_ignore_threat_score_reapply`.

5. Cliquez sur **OK**.

Important : Cette action déclenchera une tâche de longue durée et le système ne vous permettra pas d'apporter d'autres modifications à la règle de notation des menaces tant que la tâche n'est pas terminée. Pour plus d'informations sur la façon dont la configuration des tâches en arrière-plan est configurée, consultez Configuration du cadre de travail des tâches en arrière-plan de Vulnerability Response .

Le script Utiliser le **script (avancé)** est le suivant : utilisez ce script pour créer un script personnalisé qui doit renvoyer le score de menace dans une plage comprise entre 0 et 100.

Le champ de script avancé est renseigné automatiquement avec une fonction qui prend les paramètres **actuels** et **agrégés** , et cette fonction doit renvoyer le score de menace dans la plage de 0 à 100.

Ici, le paramètre actuel est l'objet GlideRecord de l'entité (observable) pour laquelle le score de menace est calculé. Pour les observables, il correspond au GlideRecord de

Traduction automatique

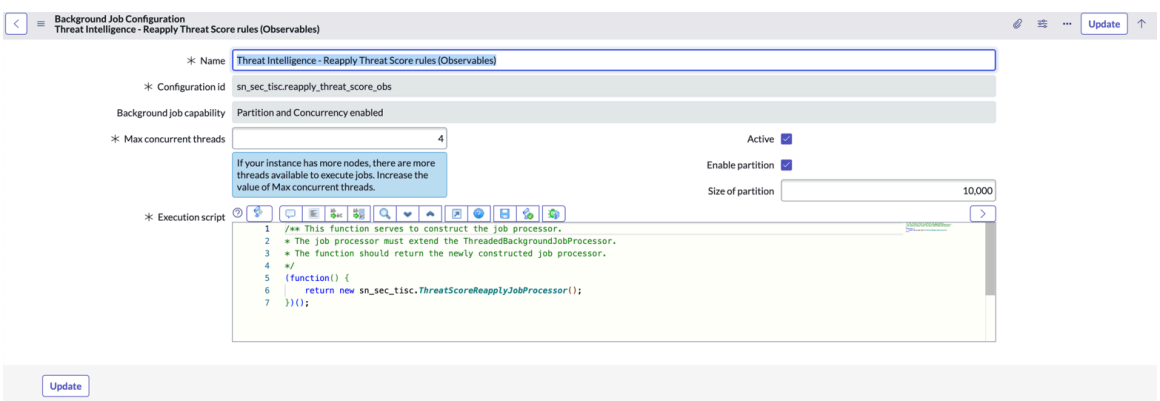
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

la table sn_sec_tisc_observable. Le paramètre aggregates est un objet GlideRecord de l'enregistrement de la table sn_sec_tisc_aggregates qui est utilisé pour accéder aux nombres d'enregistrements des différents types d'enregistrements associés (tels que les campagnes ou les identités) à l'entité principale (observable).

Exemple de script dans l'option avancée :

```
answer = (function threatScoreCalculator(current, aggregates) {

    // return the threat score in the range of 0-100
    var threatSeverity = current.getValue("threat_severity");
    if(threatSeverity == "high")
     return 80;
    else {
        let associatedCampaigns =
 aggregates.getValue("num_of_campaigns");
        if(associatedCampaigns > 0)
            return 50;
    }
    return 0;

})(current, aggregates);
```

À titre de référence, vous trouverez ci-dessous la capture d'écran qui vous montre le processus de configuration de la tâche en arrière-plan du score de menace.



Définition des listes de contrôle de sécurité

Utilisez cette fonctionnalité pour ajouter ou supprimer des observables en bloc.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Administration**.
2. Accéder à **Listes des contrôles de sécurité**.
   Par exemple, ajouter des observables à la liste d'autorisation, puis passer à l'option de liste d'autorisation.
3. Sélectionnez **Liste d'autorisation**.
4. Sélectionnez le type d'observables tel que l'adresse IP, le fichier, etc., à ajouter à la liste d'autorisation.
5. Cliquez sur **Ajouter**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La **liste Sélectionner des observables pour l'autorisation** s'affiche.

6. Sélectionnez tous les observables qui doivent être ajoutés à la liste d'autorisation.
7. Cliquez sur **Ajouter à la liste d'autorisation**.
   Les observables sélectionnés sont ajoutés.
8. De même, sélectionnez **Ajouter à la liste de refus** pour ajouter les observables à la liste supprimée.
9. Sélectionnez **Ajouter à la liste de surveillance** pour ajouter les observables à la liste de surveillance.

   Remarque : Vous pouvez ajouter directement les observables à la liste d'autorisation, à la liste de refus ou à la liste de surveillance directement à partir de la page de vue du formulaire Observables, qui est disponible au-dessus de la bannière du formulaire.

10. Pour vérifier, accédez à **la bibliothèque Threat Intel**.
11. Sélectionnez le type d'observable qui a été ajouté à la liste d'autorisation.
    L'observable est indiqué comme ajouté à la liste d'autorisation.

    Remarque : La liste d'autorisation et la liste de refus s'excluent mutuellement et le système s'assure automatiquement qu'un observable figurant dans la liste d'autorisation ne fait pas partie de la liste de refus et vice-versa.

Création de taxonomies

Créez des taxonomies pour les enregistrements sources de données.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Administration** > **Taxonomies**.
2. Cliquez sur **Nouveau**.
3. Saisissez le **nom**.
4. Activez ou désactivez le **statut** de taxonomie à l'aide des actions de formulaire Activer ou désactiver.

   Remarque : Les taxonomies désactivées ne seront pas disponibles pour la sélection d'enregistrements où des taxonomies sont applicables.

5. Accédez à la section **Valeurs de taxonomie** pour ajouter des valeurs de taxonomie.
6. Cliquez sur **Nouveau** pour ouvrir la nouvelle vue du formulaire de valeur de taxonomie et entrez la **taxonomie** et la **valeur**.
7. Cliquez sur **Enregistrer**.
8. Par exemple, accédez à **Bibliothèque Intel de menaces** > **Observables** pour vérifier les taxonomies pour l'enregistrement des observables.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Accédez à la section **Balises et taxonomies** dans n'importe quelle page de formulaire d'observable et sélectionnez la taxonomie nouvellement créée.

Remarque : Vous pouvez également ajouter des balises et des taxonomies à partir de la vue de liste de la bibliothèque Threat Intel.

Gestion du calculateur de réputation de la recherche de menaces

Vous pouvez utiliser le calculateur de résultat de la recherche de menaces pour calculer les résultats observables en fonction des réponses reçues du fournisseur de recherche de menaces.

Vous pouvez créer un calculateur de résultat de recherche de menace pour votre intégration et utiliser un script pour déterminer comment vous souhaitez identifier les différents résultats observables. Le calculateur de résultat de la recherche de menaces inclut un exemple de script fourni avec le système de base, que vous pouvez utiliser pour identifier les résultats observables ou modifier ce script en fonction de vos besoins.

Pour les intégrations tierces qui fournissent les résultats calculés, le calculateur de résultat de la recherche de menaces mappe les résultats aux résultats pris en charge dans le système de base.

Résultats de la recherche de menace de déploiement

Lorsque vous avez plusieurs résultats de recherche de menaces pour un observable des différents fournisseurs d'intégration, les résultats récents de la recherche de menaces de tous les fournisseurs sont pris en compte, et les résultats observables globaux sont marqués comme suit :

Déployer les résultats de la recherche de menace

Dernier résultat observable	Résultat observable global
Malveillant	Si l'un des fournisseurs d'intégration signale l'observable comme malveillant, le résultat observable global est alors marqué comme malveillant.
Suspect	Si aucun des fournisseurs d'intégration ne signale l'observable comme malveillant, l'un d'entre eux le signale comme suspect, puis le résultat global de l'observable est marqué comme suspect.
Nettoyer	Si tous les fournisseurs d'intégration signalent l'observable comme Propre, le résultat global de l'observable est marqué comme Propre.
Inconnu	Si aucun des fournisseurs d'intégration ne signale l'observable comme malveillant ou suspect et que l'un d'entre eux le signale comme inconnu, le résultat global de l'observable est marqué comme inconnu.

Afficher les calculateurs de réputation de la recherche de menaces

Vous pouvez utiliser le calculateur de résultats de la recherche de menaces pour déterminer comment la réputation de l'observable est calculée en fonction de la réponse d'un fournisseur spécifique de recherche de menaces.

Rôle requis : sn_sec_tisc.admin

Traduction automatique

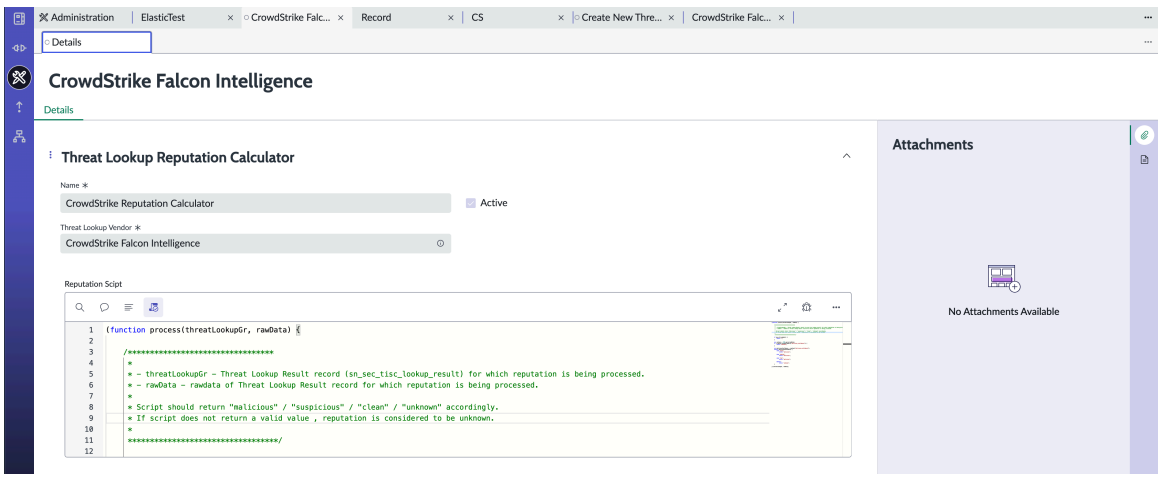
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour afficher le calculateur de réputation de la recherche de menaces, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionnez la section **Calculateur de réputation de la recherche de menaces** .

   Vous pouvez afficher la liste des calculateurs de réputation de recherche de menace.

3. Cliquez sur le calculateur de réputation de recherche de menaces requis pour afficher les détails du calculateur.



Créer un calculateur de réputation de recherche de menaces

Rôle requis : sn_sec_tisc.admin

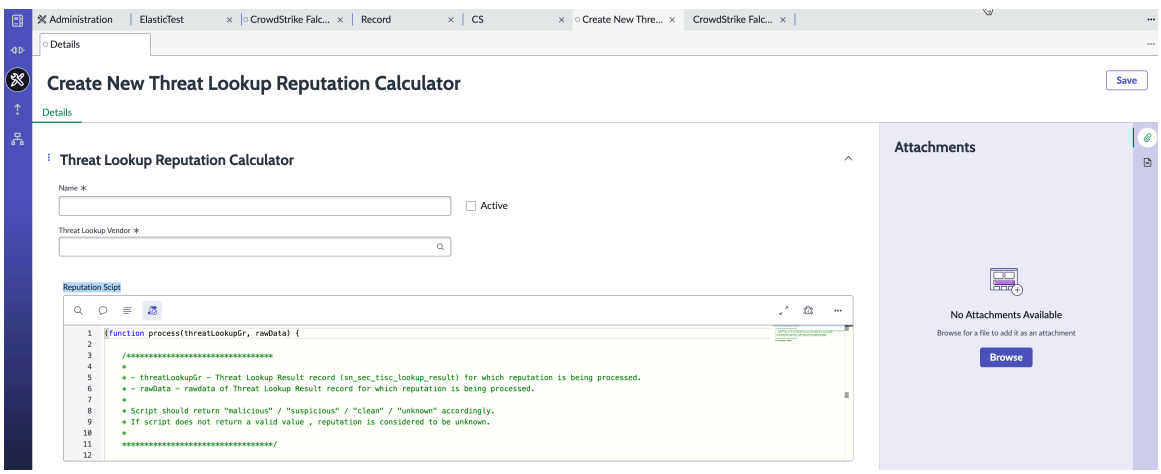
Remarque : Un seul calculateur de recherche de menaces peut être actif à un moment donné par fournisseur de recherche de menaces.

Pour créer un calculateur de réputation de recherche de menaces, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionnez la section **Calculateur de réputation de la recherche de menaces** .

   Vous pouvez afficher la liste des calculateurs de réputation de recherche de menace.

3. Pour créer un calculateur de réputation de recherche de menaces, cliquez sur **Nouveau**.



4. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un calculateur de réputation de recherche de menaces

Champ	Description
Nom	Nom du calculateur de réputation de la recherche de menaces.
Actif	Le calcul de la recherche de menace s'exécute uniquement si l'option Actif est sélectionnée.
Fournisseur de la recherche de menace	Nom du fournisseur de la recherche de menaces. Par exemple, `CrowdStrike Falcon Intelligence`.
Script de réputation	Éditeur de script permettant de déterminer comment identifier les différents résultats observables. Chaque intégration de recherche de menaces est accompagnée d'un script de base pour calculer la réputation de la recherche de menaces.

5. Cliquez sur **Enregistrer**.

Gérer les notifications par e-mail

Utilisez ServiceNow les notifications pour créer et gérer les notifications par e-mail système et afficher les journaux d'e-mails.

Notifications par e-mail

Utilisez les notifications par e-mail pour envoyer aux utilisateurs sélectionnés des notifications par e-mail concernant des tâches spécifiques au sein de l'application, telles que les mises à jour des observables/indicateurs/divers autres objets.

Rôle requis : administrateur

Remarque : En tant qu'administrateur système, vous pouvez afficher, créer ou modifier les détails de la règle de notification par e-mail dans la vue classique de l'application.

Centre de sécurité des renseignements sur les menaces Fournit des notifications par e-mail pilotées par des règles qui sont envoyées à des adresses e-mail individuelles ou à une liste d'adresses e-mail. Habituellement, les informations relatives à la diffusion des renseignements sur les menaces aux utilisateurs internes sont généralement envoyées sous la forme d'un e-mail. Le processus consiste à fournir les données de renseignements sur les menaces aux utilisateurs en fonction du format et des chronologies spécifiés.

Les notifications par e-mail permettent aux administrateurs de spécifier :

- Quand envoyer la notification
- Qui reçoit la notification
- Quel est le contenu de la notification

Remarque : Si vous souhaitez apporter des modifications, vous devez configurer le destinataire de l'e-mail en modifiant les règles du système de base en fonction de vos besoins.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

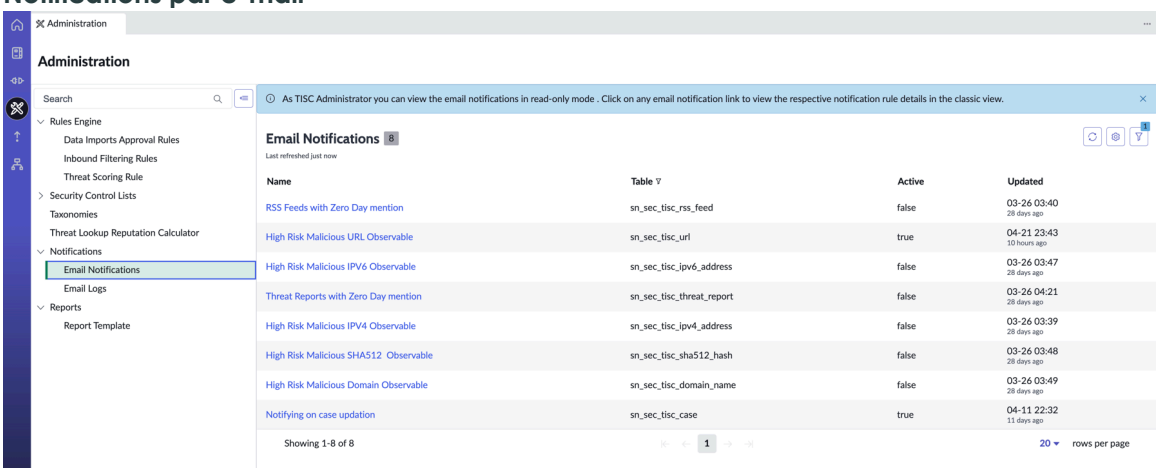
Pour plus d'informations, consultez la section Créer une notification par e-mail dans la Administration de la Now Platform documentation.

La table suivante détaille les règles de notification par e-mail qui sont mises en service dans le système de base.

Notifications par e-mail

Nom	Table
Flux RSS avec mention Zero Day	sn_sec_tisc_rss_feed
Observable d'URL malveillante à risque élevé	sn_sec_tisc_url
Observable IPV6 malveillant à risque élevé	sn_sec_tisc_ipv6_address
Rapports de menace avec mention Zero Day	sn_sec_tisc_threat_report
Observable IPV4 malveillant à risque élevé	sn_sec_tisc_ipv4_address
Observable SHA512 malveillant à risque élevé	sn_sec_tisc_sha512_hash
Observable de domaine malveillant à risque élevé	sn_sec_tisc_domain_name
Notifier lors de la mise à jour du ticket	sn_sec_tisc_case

Notifications par e-mail



Remarque : Cliquez sur chaque notification par e-mail pour accéder à l'interface utilisateur classique, afin que vous puissiez effectuer les actions nécessaires, telles que l'affichage, la modification ou la création des notifications.

Journaux d'e-mails

Cette section fournit une visibilité claire aux administrateurs TISC sur les e-mails envoyés à l'aide des règles de notification par e-mail configurées.

Notifications par e-mail et journaux

TISC offre différents champs d'application pour accéder, afficher ou modifier les notifications par e-mail et les journaux en fonction de différents profils.

Remarque :

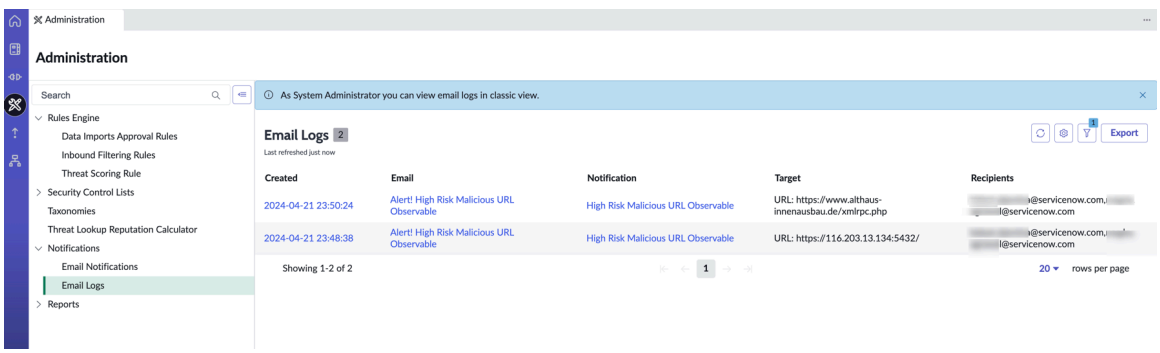
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Profil	Niveaux d'accès
Administrateur TISC (sn_sec_tisc.admin)	En tant que sn_sec_tisc.admin, vous ne pouvez afficher que les notifications par e-mail configurées pour TISC. **Remarque :** Cliquez sur les liens hypertexte des journaux d'e-mails pour accéder à l'interface utilisateur classique et afficher ces notifications.
Administrateur système (admin)	En tant qu'administrateur, vous pouvez créer, afficher et modifier les notifications dans l'interface utilisateur classique. **Remarque :** Cliquez sur les liens hypertexte des journaux d'e-mails pour accéder à l'interface utilisateur classique afin d'afficher et de créer ces notifications.

Remarque : L'administrateur TISC et l'administrateur système peuvent tous deux utiliser les filtres et rechercher les journaux d'e-mails.

Journaux d'e-mails



Modèles de rapports

Définit la possibilité de réutiliser les modèles de rapport qui peuvent être partagés au sein du groupe d'utilisateurs pour générer des rapports rapidement et de façon cohérente.

Utilisez cette fonctionnalité pour créer différents types de modèles de rapport, qui peuvent être appliqués à des tickets qui fournissent le statut d'une enquête en cours pertinente pour toute menace pour votre organisation et aident à générer des rapports sur celle-ci.

Cette section explique comment implémenter la génération de rapports CTI au niveau d'un ticket et fournit également les expériences de l'administrateur (conception du modèle) et de l'analyste (exécution).

Vous pouvez ajouter au modèle de rapport des champs de formulaire de tâche de ticket personnalisés ou des listes connexes accessibles par points. En outre, vous pouvez formater et configurer le rapport en fonction de vos besoins à l'aide de divers éléments de rapport.

Rôle requis : sn_sec_tisc.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le tableau suivant explique quelques modèles de rapport mis en service dans le système de base.

Modèle de rapport

Nom	Description
Rapport d'état de ticket : profil d'acteur de menace	Le rapport est conçu pour fournir un état d'avancement de l'enquête en cours sur un cas lié à un auteur de menace qui tente de comprendre le contexte et la pertinence de la menace pour l'organisation ; le comportement de l'adversaire et les objectifs potentiels ; l'enrichissement du CIO ; les logiciels malveillants et les outils associés ; TTP observés ; Différence par rapport aux TTP existants – nouvelles capacités nettes, légères modifications, etc.
Résumé analytique	Le rapport est conçu pour informer les décideurs de haut niveau sur un risque particulier. L'accent est mis sur les publics de cadres et sur les problèmes stratégiques en expliquant pourquoi et comment, plutôt que quoi et quand. Les détails techniques et les annexes à l'appui de la rédaction narrative de longue durée ne seront pas inclus dans ce rapport.
Résumé post-enquête : profil d'acteur de menace	Le rapport est conçu pour fournir le contexte et la pertinence de la menace pour l'organisation ; le comportement de l'adversaire et les objectifs potentiels ; l'enrichissement du CIO ; les logiciels malveillants et les outils associés ; TTP observés ; Différence par rapport aux TTP existants – nouvelles capacités nettes, légères modifications, etc.

Remarque : Par défaut, ces rapports sont à l'état Publié et seront en mode lecture seule. Comme les modèles de rapport seront en mode lecture seule, les utilisateurs ne pourront apporter aucune modification aux modèles et les analystes ne seront pas en mesure de générer les rapports, car les modèles de rapport seront désactivés.

Créer un nouveau modèle de rapport

Créez un nouveau modèle de rapport de ticket en fonction des besoins professionnels de votre organisation.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Rapports** > **Modèle de rapport**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette section affiche les modèles disponibles dans le système de base, ainsi que les modèles publiés. Vous pouvez choisir n'importe quel modèle pour travailler avec les rapports.

Remarque : À partir de cette section, vous pouvez également supprimer les modèles, si nécessaire.

3. Cliquez sur **Nouveau**.
4. Saisissez le nom et la description du modèle.
5. Cliquez sur **Enregistrer**.
   La section Contenu du modèle s'affiche.

Remarque : Chaque fois que vous créez un nouveau modèle de rapport, le modèle est à l'état de brouillon, ce qui signifie que la création du modèle est un travail en cours et que tout autre utilisateur ne peut pas afficher le modèle de rapport tant qu'il n'est pas terminé.

6. Développez le **contenu du modèle** pour insérer les champs souhaités dans le corps du modèle.

Remarque :

- Le modèle que vous modifiez vous permet de définir le corps du modèle et de sélectionner les variables requises à ajouter à la section de l'éditeur de modèle. Les modèles sont pris en charge par l'éditeur de texte enrichi (RTE) afin que vous puissiez contrôler diverses fonctions disponibles telles que l'indentation, la taille de la police, la création de tableaux, l'ajout d'images et diverses autres fonctionnalités de mise en forme.
- Vous pouvez également insérer des images dans vos modèles de rapport, pour cela vous devez copier et coller l'image directement dans le modèle. Lorsque vous ajoutez une image, cette image est chargée en tant que pièce jointe.
- Vous pouvez télécharger ou joindre une image jusqu'à 698 pixels, si l'image est supérieure à la taille définie, elle sera automatiquement ajustée à la taille d'origine. Cette restriction de la taille des pixels aidera la génération de rapports PDF à s'afficher dans un format approprié et les images ne seront pas tronquées dans le rapport.

7. Ajoutez les éléments requis du ticket.
8. Cliquez sur **Enregistrer le contenu** pour enregistrer le contenu de votre nouveau modèle de rapport.
9. Cliquez sur **Aperçu** pour prévisualiser le format de votre rapport et également pour voir comment un rapport est généré lorsque vous générez un rapport de ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- **Champs de ticket** : chaque fois que vous modifiez votre ou vos modèles de rapport, prévisualisez le contenu ajouté au modèle. Par exemple, lorsque vous générez un rapport de ticket et que vous souhaitez ajouter un champ appelé Description brève, vous pouvez sélectionner ce champ dans les champs du ticket, puis ce champ est ajouté en tant que variable dans le modèle de rapport. Lorsqu'un rapport est généré pour l'analyste, quelle que soit la brève description du cas, cette description sera affichée dans le rapport.
- **Enregistrements** : dans le modèle de rapport, vous pouvez également ajouter les enregistrements connexes de ce ticket particulier qui s'affichent en tant qu'artefacts du ticket. Par exemple, si vous souhaitez afficher des observables malveillants dans le rapport à partir des listes connexes Observables, vous pouvez les ajouter à votre modèle de rapport. Ces enregistrements connexes sont affichés au format table
- **Scripts** : chaque fois que vous souhaitez voir la date et l'heure du rapport, vous pouvez ajouter les scripts **Date et heure** actuelles à votre modèle de rapport, ce qui ajoutera la date et l'heure de création du rapport.
- **MITRE ATT&CK** : affiche les techniques associées à la carte MITRE dans votre rapport.

Une fois que vous avez ajouté tous les champs liés au ticket requis à votre modèle de rapport, vous devez publier votre modèle de rapport.

10. Cliquez sur **Publier** pour publier le modèle.
    Un message de confirmation s'affiche si vous souhaitez publier le modèle de rapport.

    Remarque : Lorsque vous publiez un modèle de rapport, ce modèle est activé pour tous les utilisateurs. S'il est obsolète et que vous souhaitez restreindre l'affichage du rapport pour les utilisateurs, vous pouvez désactiver le rapport publié, ce qui signifie que le modèle de rapport sera masqué pour les utilisateurs. Vous devez réactiver le rapport publié pour que les utilisateurs puissent le voir et l'utiliser jusque-là, il sera masqué à l'affichage.

11. Cliquez sur **Supprimer** pour supprimer le modèle de rapport au cas où vous ne voudriez pas ce modèle de rapport.
    Si vous souhaitez renommer votre modèle de rapport, cliquez sur **Éditer** et modifiez les champs souhaités.

Propriétés système pour les rapports

Les propriétés système des rapports sont expliquées ci-dessous.

Propriété	Description	Valeur
sn_sec_reporting.max_list_columns_allowed	Limite le nombre de colonnes qui peuvent être ajoutées lors de l'affichage des listes dans les PDF de rapport. Cela utilisera les colonnes depuis le début, de la vue jusqu'à la limite autorisée.	5
sn_sec_reporting.report_default_styles_object	Utilisez cette propriété pour contrôler le css des champs de formulaire libre,	(objet JSON)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur
	du panneau de gauche, des listes de rapports.	
sn_sec_reporting.load_all_records	Charge tous les enregistrements des listes du rapport créé à partir d'un modèle. true : charge tous les enregistrements et false : charge un nombre spécifique d'enregistrements défini par la propriété sn_sec_reporting.reporting_list_records_count.	Faux
sn_sec_reporting.reporting_list_records_count	Charge un nombre spécifique d'enregistrements dans l'éditeur de rapports.	20
sn_sec_tisc.sn_sec_tisc_case.defang_records_urls	Contrôle si les URL des listes sont neutralisées ou non.	Vrai
sn_sec_tisc.show_all_tactics_reporting	Si vrai, affiche toutes les tactiques (y compris celles qui n'ont aucune technique associée au ticket) pour les listes MITRE rendues dans le rapport.	Faux
sn_sec_tisc.reporting_email_template_sn_sec_tisc_case	ID système du modèle de client de messagerie pour la table Ticket (sn_sec_tisc_case) qui sera utilisé dans le rapport de partage.	b55e22c54324021060eee0ea78b8f2df
sn_sec_tisc.sn_sec_tisc_case.exclude_fields	Champs exclus du ticket dans les options de menu rapport/modèle pour remplacer un champ.	(Liste de tous les champs de tickets exclus
sn_sec_tisc.sn_sec_tisc_case.ctx_menu_field_helper	Cette propriété est utilisée pour obtenir l'enregistrement de message d'interface utilisateur correspondant pour l'étiquette des champs de ticket dans les options de menu du rapport/modèle.	sn_sec_tisc_case_reporting_ctx_menu_field_h

Modifier un modèle de rapport publié

Modifiez les modèles de rapport.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > > **Administration**.
2. Sélectionner **Rapports** > **Modèle de rapport**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez le modèle de rapport requis.
4. Cliquez sur le bouton **Modifier** qui s'affiche dans le modèle de rapport.

Remarque :

Un message de confirmation s'affiche indiquant que vous modifiez un modèle publié et que vous devez republier le modèle pour le rendre disponible sous Rapports de tickets. Voulez-vous poursuivre la modification ? ce qui signifie que vous devez republier le modèle modifié après avoir apporté les modifications nécessaires.

5. Cliquez sur **Modifier** dans la boîte de dialogue de confirmation.
6. Apportez les modifications nécessaires en ajoutant les champs de contenu requis ou la liste connexe.
7. Cliquez sur **Enregistrer le contenu**.
8. Cliquez sur le bouton **Publier** pour publier les modifications.

Remarque :

a. Vous pouvez également prévisualiser le contenu du modèle de rapport avant de publier le modèle de rapport.

b. Un message de confirmation affiche le message « Êtes-vous sûr de vouloir publier ce modèle ? » Cliquez sur **Publier** pour continuer la publication du modèle de rapport.

c. Si vous souhaitez supprimer le modèle de rapport, vous pouvez cliquer sur **Supprimer** pour supprimer le modèle de rapport.

Dupliquer un modèle de rapport

Dupliquer un modèle de rapport Si vous souhaitez ajouter des mises à jour incrémentielles, vous pouvez créer une copie du modèle de rapport.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > > **Administration**.
2. Sélectionner **Rapports** > **Modèle de rapport**.
3. Sélectionnez le modèle.
4. Cliquez sur **Dupliquer**.
   Le contenu du modèle sélectionné est dupliqué et une copie de ce modèle s'affiche. Le modèle sera à nouveau à l'état Brouillon, vous pouvez personnaliser le contenu, puis renommer le modèle selon vos besoins.
5. Éditez ou modifiez le contenu du modèle copié.

Remarque : Vous pouvez également supprimer les modèles de rapport au cas où vous n'en auriez plus besoin et créer de nouveaux modèles.

Utilisation des webhooks

Un webhook est une requête HTTP, déclenchée par un événement dans le système source (TISC) et envoyée à un système de destination (où se trouve l'URL du point de terminaison), avec une charge utile de données d'événement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ces webhooks dans Centre de sécurité des renseignements sur les menaces sont utiles pour notifier l'application de destination chaque fois que des événements se produisent.

Dans TISC, vous pouvez effectuer les opérations suivantes :

- Configurer les webhooks
- Gérer les déclencheurs
- Mécanisme de nouvelle tentative
- Effectuer la validation
- Gérer les abonnements

Propriétés système pour les webhooks

Les propriétés système des webhooks sont expliquées ci-dessous.

Nom de la propriété	Description	Type	Valeur
sn_sec_tisc.webhook_ignore_threat_score_recalculation	Ignorer les événements webhook déclenchés par le score de menace Recalculer l'historique.	Vrai/Faux	Vrai
sn_sec_tisc.webhook_max_event_batch_size	Nombre maximal d'événements à envoyer dans le cadre d'une demande webhook. La taille du lot sera limitée à 2 000 même si une valeur plus élevée est définie dans cette propriété.	Entier	1 000
sn_sec_tisc.webhook_retry_count	Nombre de fois qu'une demande ayant échoué doit être réessayée avant de la marquer comme erreur et de passer au lot d'événements suivant. Le nombre de nouvelles tentatives sera limité à 10 même si un nombre plus élevé est défini dans cette propriété.	Entier	5
sn_sec_tisc.webhook_retry_interval	Nombre de secondes à attendre avant de retenter un lot ayant échoué.	Entier	30

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété	Description	Type	Valeur
	Cette valeur augmentera de façon exponentielle en fonction du nombre de nouvelles tentatives. Par exemple, si retry_count est 3 et retry_interval 30, les nouvelles tentatives sont déclenchées après 30, 60 et 120 s. L'intervalle entre les tentatives initiales est limité à 300 secondes, même si une valeur supérieure est définie dans cette propriété.		

Configurer les webhooks

Configurez un webhook pour vous abonner à des événements dans Centre de sécurité Renseignements sur les menaces.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Pourquoi et quand exécuter cette tâche

Les webhooks TISC permettent de s'intégrer à des outils de sécurité tels que SIEM. Les utilisateurs peuvent ensuite s'abonner à divers événements liés à différents artefacts tels que des observables ou des indicateurs, des programmes malveillants ou des acteurs de menace. TISC informe les outils de Security (tels que SIEM) lorsqu'une nouvelle connaissance des menaces est disponible ou que des données existantes de la veille sur les menaces sont mises à jour ou supprimées dans TISC.

Par exemple, chaque fois qu'un nouvel observable est ajouté dans Threat Intelligence, une demande de charge utile est envoyée à la configuration de l'URL Webhook. Cette demande de charge utile collecte généralement les informations observables et les fournit en tant qu'informations supplémentaires aux outils de Security (tels que SIEM).

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Webhooks**.
   La page Webhooks s'affiche.
3. Cliquez sur **Nouveau**.

Champ	Description
Nom	Saisissez un nom de webhook.
Description	Ajoutez la description du webhook.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Détails de la configuration	
Utiliser le message REST	Cochez **la case Utiliser le message REST** si vous devez utiliser la fonctionnalité Message REST/Méthode REST fournie par Now Platform. Si cette case n'est pas cochée, l'application utilise le point de terminaison fourni dans l'URL Webhook pour envoyer les informations sur l'événement. Pour plus d'informations, consultez Service web REST sortant sur la documentation Now Platform.
Message REST	Sélectionnez l'enregistrement de message REST dans la liste des enregistrements de message REST qui sont déjà configurés dans l'instance. Pour plus d'informations, consultez Service Web REST sortant dans la documentation de Now Platform. **Remarque :** Les champs Message REST et Méthode REST sont obligatoires lorsque vous sélectionnez le message REST.
Méthode REST	Sélectionnez la méthode REST dans la liste des méthodes REST disponibles configurées pour le message REST sélectionné. Pour plus d'informations, consultez Service Web REST sortant dans la documentation de Now Platform. **Remarque :** Seules les méthodes REST POST sont prises en charge pour les webhooks.
URL webhook	Un point de terminaison Webhook est une URL qui reçoit des notifications d'événements Webhook.
Authentification requise	Cochez cette case si l'authentification est requise. **Remarque :** Cela ne s'applique que lorsque l'URL Webhook est utilisée pour récupérer les données.
Type d'authentification	Type d'authentification pour le webhook. **Remarque :** Pour l'instant, seul le type d'authentification de base est pris en charge.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom d'utilisateur	Attribuez un nom d'utilisateur à votre type d'authentification.
Mot de passe	Attribuez un mot de passe à votre type d'authentification.
En-têtes à transmettre avec la demande	Tous les en-têtes à transmettre avec les demandes peuvent être fournis dans le mappage d'en-tête de demande. L'en-tête doit être fourni dans une paire clé-valeur séparée par deux-points (' :'). Chaque paire clé-valeur d'en-tête doit être fournie dans une nouvelle ligne. Pour fournir des paramètres d'authentification en tant que valeurs d'en-tête, encadrez l'étiquette d'authentification requise avec « ${ » et « }$ ». Par exemple, username :${Username}$.

4. Cliquez sur **Valider et enregistrer**.
   Si vos détails de configuration sont incorrects, le système validera automatiquement la connexion si les détails de configuration sont modifiés, puis l'application affichera un message d'avertissement indiquant que la validation du webhook a échoué et que vous devez vérifier les détails de la configuration et les modifier en conséquence.

Remarque :

- Pour la validation du webhook, la charge utile de la demande vide est envoyée au point de terminaison et l'utilisateur doit s'assurer que le point de terminaison envoie le code de réponse correct (200) lorsque la demande vide est transmise au point de terminaison du webhook configuré.
- Par défaut, tout webhook créé sera à l'état désactivé. Vous devez activer le webhook et l'activer. Un exemple de webhook est mis en service dans le système de base en tant que référence pour les utilisateurs.

S'abonner aux déclencheurs

Affichez la liste de tous les déclencheurs de webhook abonnés pour le webhook actuel.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Webhooks**.
   La page Webhooks s'affiche.
3. Sélectionnez le webhook.
   La section Déclencheurs abonnés s'affiche.
4. Cliquez sur le bouton **S'abonner** dans la section Déclencheur abonné.
   La vue de liste affiche tous les déclencheurs de webhook activés dans l'instance.
5. Sélectionnez les déclencheurs de webhook souhaités et cliquez sur **S'abonner** dans la boîte de dialogue Déclencheurs de webhook.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un message de confirmation s'affiche indiquant que le webhook est abonné avec succès au(x) déclencheur(s) sélectionné(s). À partir de là, vous pouvez également créer directement un nouveau déclencheur et vous abonner au webhook.

Remarque : Vous pouvez également **désabonner** le webhook du ou des déclencheurs sélectionnés.

Afficher les journaux d'erreurs Webhook

Utilisez cette section de journaux d'erreurs pour afficher toutes les entrées d'audit qui sont marquées comme erreur dans l'état d'un webhook particulier.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Pourquoi et quand exécuter cette tâche
Les journaux d'audit permettent aux utilisateurs d'approfondir l'enquête, de déboguer l'exécution et d'identifier la cause première de l'échec de l'exécution.

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Webhooks**.
   La page Webhooks s'affiche.
3. Sélectionnez le webhook.
4. Accédez aux **journaux d'erreurs**.
5. Affichez les journaux d'erreurs.
   La vue de liste affiche tous les journaux d'erreurs à partir d'un webhook particulier.
6. Accéder à la colonne **Lot**
7. Cliquez sur **n'importe quel ID de lot**.

   Remarque : Chaque journal d'erreurs est associé à un lot et à l'aide de l'ID de lot (de la colonne Lot), vous pouvez afficher l'enregistrement de lot associé. Cliquez sur l'un des ID de lot et cela s'ouvrira dans un onglet séparé. Chaque ID de lot contient le numéro de lot webhook, le message d'erreur, le code d'état de la réponse, le nombre de nouvelles tentatives, les données de charge utile réelles et la liste des événements qui seront envoyés au webhook.

8. Cliquez sur **Réessayer le lot** pour réessayer les lots ayant échoué.
   Lorsque vous cliquez sur ce bouton, cela envoie une charge utile de demande (de ces informations de lot particulières) au point de terminaison Webhook configuré.

   Remarque : Cette action n'est disponible que pour les enregistrements de lots présentant des erreurs d'exécution ou terminés avec succès et les enregistrements qui sont à l'état de nouvelle tentative seront automatiquement réessayés.

Afficher les lots de webhooks

Un enregistrement de lot Webhook est créé pour chaque exécution de Webhook.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Afin de réduire le nombre d'appels d'API envoyés aux points de terminaison Webhook, le traitement par lots d'événements est implémenté dans les webhooks. Pour chaque webhook, si plusieurs événements sont déclenchés presque en même temps, tous ces événements sont envoyés dans le cadre de la même demande au point de terminaison webhook.

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Webhooks**.
   La page Webhooks s'affiche.
3. Sélectionnez le webhook.
4. Accédez aux **journaux d'erreurs**.
5. Affichez les journaux d'erreurs.
   La vue de liste affiche tous les journaux d'erreurs à partir d'un webhook particulier.
6. Accéder à la colonne **Lot**
7. Cliquez sur **n'importe quel ID de lot**.
   La page Lot Webhook s'affiche.

Remarque : Tous les lots sont stockés dans la `table sn_sec_tisc_webhook_batch`.

Voici l'exemple de format de charge utile reçu par le point de terminaison webhook :


```
{
    "batch_id": "06eeb3693b6bca10f6f82a60c5e45a7b",
    "events": [
        {
            "record": "Observable",
            "record_fields": {
                "is_false_positive": "false",
                "reputation": "malicious",
                "sys_updated_on": "2024-07-22T14:31:26.000Z",
                "type": "url",
                "sys_updated_by": "admin",
                "sys_created_on": "2024-07-04T06:45:20.000Z",
                "id": "url--1e77adb7eb8b06107750fa86cad0cd70",
                "is_defanged": "false",
                "sys_created_by": "SecCommon.System",
                "tags": "Enriched",
                "taxonomies": "T1: V1",
                "domain": "urlhaus.abuse.ch",
                "status": "active",
                "source_count": "1",
                "threat_score": "20",
                "sys_id": "da77adb7eb8b06107750fa86cad0cd70",
                "value": "https://urlhaus.abuse.ch/url/2578255/",
                "confidence": "89",
                "expiration_time": "2025-10-07T07:13:18.000Z",
                "tlp": "CLEAR"
            },
            "trigger": {
                "name": "Observable Update",
                "type": "UPDATE",
```


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
                "trigger_time": "2024-07-22T14:31:26.000Z",
                "trigger_fields": [
                    {
                        "field_name": "reputation",
                        "previous_value": null,
                        "current_value": "malicious"
                    }
                ]
            }
        },
        {
            "record": "Observable",
            "record_fields": {
                "is_false_positive": "false",
                "reputation": "malicious",
                "sys_updated_on": "2024-07-22T14:31:19.000Z",
                "type": "url",
                "sys_updated_by": "admin",
                "sys_created_on": "2024-07-04T06:45:20.000Z",
                "id": "url--9a77adb7eb8b06107750fa86cad0cd6f",
                "is_defanged": "false",
                "sys_created_by": "SecCommon.System",
                "tags": "Enriched",
                "taxonomies": "T1: V1",
                "domain": "urlhaus.abuse.ch",
                "status": "active",
                "source_count": "1",
                "threat_score": "20",
                "sys_id": "5a77adb7eb8b06107750fa86cad0cd6f",
                "value": "https://urlhaus.abuse.ch/url/2578264/",
                "confidence": "89",
                "expiration_time": "2025-10-07T07:13:18.000Z",
                "tlp": "CLEAR"
            },
            "trigger": {
                "name": "Observable Update",
                "type": "UPDATE",
                "trigger_time": "2024-07-22T14:31:19.000Z",
                "trigger_fields": [
                    {
                        "field_name": "reputation",
                        "previous_value": null,
                        "current_value": "malicious"
                    }
                ]
            }
        }
    ]
}
```


La table suivante répertorie la structure de charge utile par lots et ses attributs qui seront envoyés aux utilisateurs en tant que charge utile webhook :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres dans la charge utile par lots	Type	Description
batch_id	Chaîne	Spécifie un identificateur unique pour un lot.
Événements	Tableau d'objets	Contient un tableau d'événements déclenchés dans le cadre de ce webhook. Chaque événement contient l'instantané des valeurs de champ au moment de la génération de l'événement et contient également les informations du déclencheur. **Remarque :** Pour plus d'informations sur l'affichage des paramètres dans l'objet d'événement, reportez-vous à la section Déclencheurs de webhook.

Remarque :

8. Cliquez sur le bouton **Réessayer le lot** pour réessayer le lot ayant échoué.

Remarque : Vous pouvez également déclencher le lot de nouvelles tentatives pour les lots terminés.

Déclencheurs de webhook

Les déclencheurs Webhook sont utilisés pour filtrer les entités Threat Intelligence qui doivent être suivies pour tout changement d'événement tel que Créer, Mettre à jour et Supprimer.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Déclencheurs**.
   La page Déclencheurs de webhooks s'affiche.
3. Cliquez sur **Nouveau**.

Champ	Description
Nom	Saisissez un nom de déclencheur webhook.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Ajoutez la description du déclencheur de webhook.
Table	Sélectionnez la table pour le déclencheur webhook.
Type de déclencheur	Définit si le déclencheur de webhook configuré est créer/mettre à jour/supprimer un événement sur la table spécifiée. **Champs de déclencheur** : ceci s'affiche lorsque vous sélectionnez le **type de déclencheur : Mettre à jour**. Il s'agit de la liste des champs de l'enregistrement pour lesquels l'événement de mise à jour doit être suivi. Si ce champ est vide, l'événement est pris en compte pour tout changement de champ dans l'enregistrement. Par exemple, si les champs de déclencheur sont **Confiance** et **Réputation** pour la table **Observables** , ce déclencheur n'est pris en compte que lorsque les champs Confiance ou Réputation sont mis à jour. **Remarque :** Les champs sélectionnés dans les champs d'exclusion ne seront pas disponibles dans la sélection des champs de déclencheur. **Supprimer** : si le **type de déclencheur : Supprimer** , les champs d'exclusion ne sont pas visibles.
Champs d'exclusion	Il s'agit de l'ensemble des champs qui sont exclus de la charge utile du déclencheur webhook.
Conditions de filtre	Conditions facultatives qui peuvent être appliquées pour filtrer les enregistrements de correspondance pour n'importe quel déclencheur d'événement. Par exemple, si la gravité de la menace est élevée et que le type de déclencheur est défini comme Mettre à jour dans la table Observable, seuls les observables qui sont modifiés et où la gravité de la menace est élevée sont envoyés à l'URL Webhook.

4. Cliquez sur **Enregistrer**.
   Par défaut, le déclencheur est créé à l'état désactivé.
5. Cliquez sur **Activer** pour activer le déclencheur et ce déclencheur sera disponible pour que les webhooks s'abonnent.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Cliquez sur **Désactiver** pour désactiver le déclencheur activé. Sa désactivation désabonnera tous les webhooks associés à ce déclencheur.

6. Cliquez sur **Afficher l'exemple de charge utile** pour sélectionner l'enregistrement. Affichez l'exemple de payload de ce déclencheur webhook particulier. En fonction de la table sélectionnée, les enregistrements de cette table spécifiée seront renseignés dans la liste déroulante **Sélectionner un enregistrement** . Sélectionnez l'enregistrement pour afficher l'exemple de charge utile. L'exemple de charge utile est affiché au format JSON. Les champs de la charge utile sont répertoriés ci-dessous.
7. Sélectionnez le type d'enregistrement dans la liste déroulante. La charge utile sera automatiquement modifiée en fonction de l'enregistrement sélectionné.


```
{
    "record": "Observable",
    "record_fields": {
        "additional_context": "This could be a potential malicious IP.
 ",
        "attack_phases": "Lockheed Martin: Command and Control",
        "author": "Anomali",
        "confidence": "50",
        "description": "This could be a potential malicious IP. ",
        "expiration_time": "2024-12-01T00:00:00.000Z",
        "first_observed": "2024-01-01T00:00:00.000Z",
        "first_seen": "2024-01-01T00:00:00.000Z",
        "id": "ipv4-addr--70526b0a436a02102164e0ea78b8f210",
        "is_defanged": "false",
        "is_false_positive": "false",
        "last_observed": "2024-01-01T00:00:00.000Z",
        "last_seen": "2024-01-01T00:00:00.000Z",
        "reputation": "suspicious",
        "source_count": "1",
        "status": "active",
        "sys_created_by": "SecCommon.System",
        "sys_created_on": "2024-06-04T00:00:00.000Z",
        "sys_id": "30526b0a436a02102164e0ea78b8f210",
        "sys_updated_by": "system",
        "sys_updated_on": "2024-06-15T00:00:00.000Z",
        "tags": "critical",
        "taxonomies": "MITRE: T121",
        "threat_level": "medium",
        "threat_score": "24",
        "threat_severity": "medium",
        "tlp": "CLEAR",
        "type": "ip_v4_address",
        "usage_categories": "APT",
        "value": "116.98.170.70"
    },
    "trigger": {
        "name": "Observable Update",
        "type": "UPDATE",
        "trigger_time": "2024-07-26T07:27:29.000Z",
        "trigger_fields": [
            {
                "field_name": "confidence",
```


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
                "previous_value": "30",
                "current_value": "50"
            }
        ]
    }
}
```

Liste des paramètres dans la charge utile du déclencheur

Paramètre dans la charge utile du déclencheur	Type	Description
enregistrement	Chaîne	Spécifie le type d'enregistrement, par exemple Observable ou Indicateur.
record_fields	Objet	Spécifie l'instantané des champs d'enregistrement lorsque l'événement est généré. Pour obtenir la liste des champs pris en charge, consultez le tableau dans la section ci-dessous.
déclencher	Objet	Spécifie les informations sur le déclencheur correspondant.
trigger.name	Chaîne	Spécifie le nom du déclencheur
type.déclencheur	Chaîne	Spécifie le type du déclencheur. Les valeurs valides sont CREATE, UPDATE, DELETE.
trigger.trigger_time	Date (au format ISO avec le fuseau horaire UTC)	Spécifie l'heure à laquelle l'événement s'est produit sur l'enregistrement.
trigger_fields	Tableau d'objets	Cette option n'est disponible que pour le type de déclencheur UPDATE. Il spécifie la liste des champs de déclencheur qui ont été modifiés dans le cadre de l'événement qui s'est produit. Les paramètres **à l'intérieur trigger_fields** sont les suivants :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre dans la charge utile du déclencheur	Type	Description
		◦ **field_name** : fournit le nom du champ qui a été modifié ◦ **previous_value** : fournit la valeur précédente du champ. ◦ **current_value** : fournit la valeur actuelle du champ.

Liste des champs pris en charge pour la création et la mise à jour de déclencheurs

Table	Nom de colonne	Étiquette de colonne
Campagne	Alias	Alias
Campagne	description	Description
Campagne	first_seen	Premier vu
Campagne	last_seen	Dernier observé
Campagne	name	Nom
Campagne	objectif	Objectif
Indicateur	additional_context	Contexte supplémentaire
Indicateur	attack_phases	Phases d'attaque
Indicateur	auteur	Auteur
Indicateur	fiabilité	Fiabilité
Indicateur	description	Description
Indicateur	expiration_time	Délai d'expiration
Indicateur	first_detected	Premier détecté
Indicateur	first_observed	Premier observé
Indicateur	first_seen	Premier vu
Indicateur	id	ID
Indicateur	indicator_types	Types des indicateurs
Indicateur	ioc_classification	Classification IOC
Indicateur	last_observed	Derniers observés
Indicateur	last_seen	Dernier observé
Indicateur	name	Nom
Indicateur	modèle	Modèle
Indicateur	pattern_type	Type de modèle
Indicateur	pattern_version	Version du modèle
Indicateur	Plates-formes	Plateformes
Indicateur	Révoqué	Révoqué

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Nom de colonne	Étiquette de colonne
Indicateur	source_count	Nombre de sources
Indicateur	spec_version	Version de spéc.
Indicateur	statut	Statut
Indicateur	balises	Balises TISC
Indicateur	Taxonomies	Taxonomies
Indicateur	threat_level	Niveau de menace
Indicateur	threat_severity	Gravité de la menace
Indicateur	Tlp	TLP
Indicateur	usage_categories	Catégories d'utilisation
Indicateur	valid_from	Date de début de validité
Indicateur	valid_until	Fin de validité
Programme malveillant	Alias	Alias
Programme malveillant	attack_phases	Phases d'attaque
Programme malveillant	description	Description
Programme malveillant	executable_process_architectures	Architectures de processus
Programme malveillant	first_seen	Premier vu
Programme malveillant	implementation_languages	Langues d'implémentation
Programme malveillant	is_family	Est la famille
Programme malveillant	last_seen	Dernier observé
Programme malveillant	malware_capabilities	Options de logiciel malveillant
Programme malveillant	malware_types	Types de programmes malveillants
Programme malveillant	name	Nom
Objet (champs d'objets communs)	additional_context	Contexte supplémentaire
Objet (champs d'objets communs)	fiabilité	Fiabilité
Objet (champs d'objets communs)	expiration_time	Délai d'expiration
Objet (champs d'objets communs)	id	ID
Objet (champs d'objets communs)	Révoqué	Révoqué
Objet (champs d'objets communs)	source_count	Nombre de sources
Objet (champs d'objets communs)	spec_version	Version de spéc.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Nom de colonne	Étiquette de colonne
Objet (champs d'objets communs)	statut	Statut
Objet (champs d'objets communs)	balises	Balises TISC
Objet (champs d'objets communs)	Taxonomies	Taxonomies
Objet (champs d'objets communs)	threat_level	Niveau de menace
Objet (champs d'objets communs)	threat_severity	Gravité de la menace
Objet (champs d'objets communs)	Tlp	TLP
Observable	additional_context	Contexte supplémentaire
Observable	attack_phases	Phases d'attaque
Observable	auteur	Auteur
Observable	fiabilité	Fiabilité
Observable	description	Description
Observable	expiration_time	Délai d'expiration
Observable	first_observed	Premier observé
Observable	first_seen	Premier vu
Observable	id	ID
Observable	is_defanged	Est neutralisé
Observable	is_false_positive	Est un faux positif
Observable	last_observed	Derniers observés
Observable	last_seen	Dernier observé
Observable	réputation	Réputation
Observable	source_count	Nombre de sources
Observable	statut	Statut
Observable	balises	Balises TISC
Observable	Taxonomies	Taxonomies
Observable	threat_level	Niveau de menace
Observable	threat_score	Score de menace
Observable	threat_severity	Gravité de la menace
Observable	Tlp	TLP
Observable	type	Type
Observable	usage_categories	Catégories d'utilisation
Observable	valide	Valeur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Nom de colonne	Étiquette de colonne
Acteur de menace	Alias	Alias
Acteur de menace	description	Description
Acteur de menace	first_seen	Premier vu
Acteur de menace	objectifs	Objectifs
Acteur de menace	last_seen	Dernier observé
Acteur de menace	name	Nom
Acteur de menace	personal_motivations	Motivations personnelles
Acteur de menace	primary_motivation	Motivation principale
Acteur de menace	resource_level	Niveau de ressource
Acteur de menace	secondary_motivations	Motivations secondaires
Acteur de menace	sophistication	Sophistication
Acteur de menace	threat_actor_roles	Rôles d'acteur de menace
Acteur de menace	threat_actor_types	Types d'acteurs de menace
Rapport de menace	description	Description
Rapport de menace	name	Nom
Rapport de menace	publié	Publié
Rapport de menace	report_types	Types de rapports
Vulnérabilité	affected_software	Logiciel affecté
Vulnérabilité	description	Description
Vulnérabilité	exploitation_status	État d'exploitation
Vulnérabilité	exploit_exists	Un exploit existe
Vulnérabilité	name	Nom
Vulnérabilité	publié	Publié
Vulnérabilité	record_last_modified	Dernière modification de l'enregistrement
Vulnérabilité	severity	Gravité

Vous trouverez ci-dessous la liste des champs système applicables, communs à toutes les entités, et pris en charge dans la charge utile du déclencheur Webhook pour les déclencheurs Créer et Mettre à jour.

- sys_id (ID système)
- sys_created_on (créé)
- sys_created_by (créé par)
- sys_updated_on (mis à jour)
- sys_updated_by (Mis à jour par)

Remarque : Pour la suppression, seul sys_id (ID système) est envoyé à l'URL du point de terminaison Webhook dans le cadre de la charge utile et les autres champs système ne sont pas pris en charge.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste des champs pris en charge pour Supprimer le déclencheur

Table	Nom de colonne	Étiquette de colonne
Observable	type	Type
Observable	valide	Valeur
Indicateur	name	Nom
Indicateur	modèle	Modèle
Indicateur	pattern_type	Type de modèle
Indicateur	valid_from	Début de validité
Campagne	name	Nom
Programme malveillant	is_family	Est la famille
Programme malveillant	name	Nom
Acteur de menace	name	Nom
Rapport de menace	name	Nom
Rapport de menace	publié	Publié
Vulnérabilité	name	Nom
Vulnérabilité	severity	Gravité

Travailler avec des flux automatisés

Utilisez ces étapes définies pour apprendre à utiliser les flux automatisés dans TISC et ses options.

Créez des flux qui s'exécutent avec les rôles TISC. Dans TISC, les flux sont créés pour les éléments suivants :

- Enrichissement IOC automatisé
- Analyser, évaluer et diffuser sur les IoC liés à la menace
- Analysez, évaluez les IoC liés à la menace et créez un incident.
- Prise en charge de la gestion des vulnérabilités.
- Suivi des vulnérabilités zero-day.

Remarque : Tous les flux sont des modèles qui sont expédiés à l'état de brouillon pour que les utilisateurs puissent les personnaliser ou les copier en fonction de leurs propres besoins.

Actions réutilisables

Action de flux	Description
Ajouter une balise à l'entité	Ajout d'une balise à une entité qui la prend en charge (observable/indicateur/objet).
Supprimer la balise de l'entité	Suppression de la balise vers une entité qui la prend en charge (observable/indicateur/objet).

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action de flux	Description
Vérifier si l'adresse IP se trouve dans la plage CIDR	Vérification si une adresse IP se trouve à l'intérieur d'une plage CIDR.
Vérifier si l'adresse IP est dans la plage	Vérification si une adresse IP se trouve entre la plage de départ et la plage d'arrivée.

Enrichissement IOC automatisé

Découvrez comment automatiser l'enrichissement des IOC à l'aide de flux lorsqu'ils répondent à un certain critère.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (afficher)

Pourquoi et quand exécuter cette tâche

Automatiser l'enrichissement des déclencheurs d'IOC uniquement lorsque :

- le type de l'observable est un nom de domaine, une adresse IPv4 ou une adresse IPv6.
- L'observable est dans un état Traité.
- l'observable n'a pas les balises enrichies ou Ignorer l'enrichissement.

Procédure

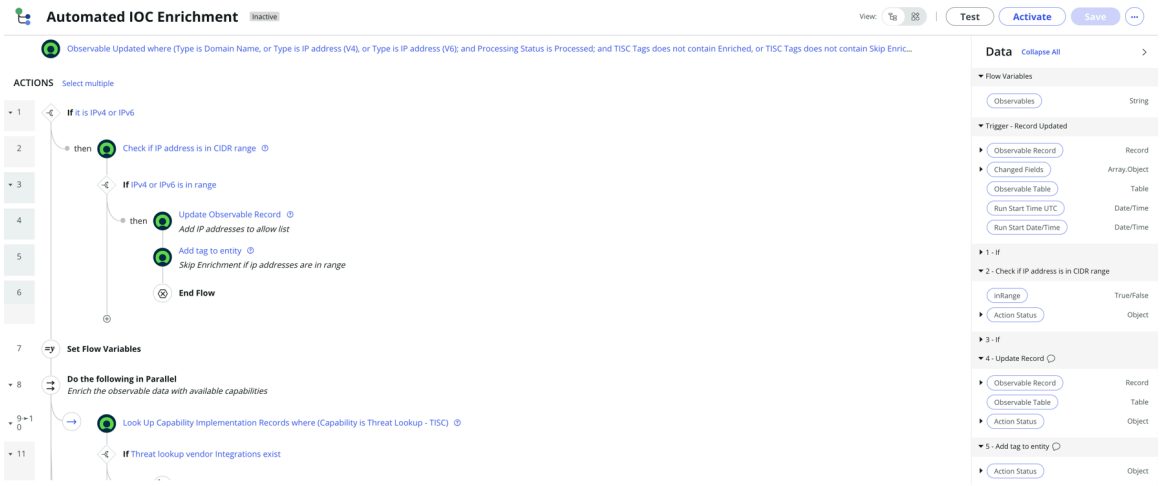
1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez le lien **de l'action d'enrichissement IOC automatisé** pour afficher les détails de la règle respective dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

```
Observable Updated where (Type is Domain Name, or Type is IP address
 (V4), or Type is IP address (V6); and Processing Status is Processed;
 and TISC Tags does not contain Enriched, or TISC Tags does not contain
 Skip Enrichment, or TISC Tags does not contain Potential New Threat)
```

5. **Si l'observable est une adresse IPv4 ou IPv6 et qu'il se trouve dans une plage CIDR autorisée, alors :**
   a. Ajoutez l'observable à la liste d'autorisation.
   b. Mettez à jour les balises des observables pour ignorer l'enrichissement.
   c. Mettez fin au flux pour cet observable.
6. **Sinon, enrichissez les données observables avec les options disponibles :**
   a. Effectuer une recherche de menace et une recherche de perception pour recueillir des informations supplémentaires sur l'observable.
   b. Mettez à jour l'observable avec des données enrichies.
   c. Ajoutez une balise **Enrichi** pour indiquer que le CIO a été traité.
7. **De plus, si la réputation des observables est irréprochable, alors :**
   a. Marquez l'observable comme faux positif et inactif.
8. **Sinon, si la réputation de l'observable est inconnue**

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Ajouter une balise **Non menace potentielle et Enrichi** pour indiquer qu'il ne s'agit pas d'une menace.



Analyser, évaluer et diffuser les observables

Apprenez à analyser et à diffuser les observables liés à la menace.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (afficher)

Pourquoi et quand exécuter cette tâche

Chaque fois qu'un enrichissement de la recherche d'observations est demandé, il est renvoyé sans aucune observation.

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez **le lien Analyser, évaluer et diffuser sur les IoC liés à l'action de menace** pour afficher les détails des règles respectives dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

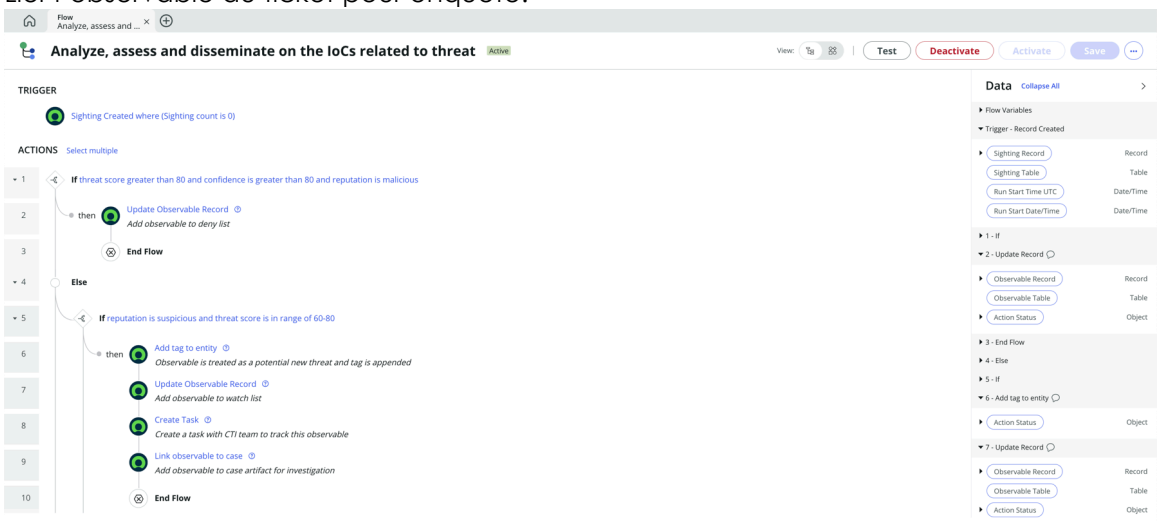
```
Sighting Created where (Sighting count is 0)
```

5. **L'observable a un score de menace supérieur à 80, une fiabilité supérieure à 80 et une réputation malveillante :**
   a. Ajoutez l'observable à la liste de refus.
   b. Mettez fin au flux pour cet observable.
6. **Sinon, la réputation de l'observable est suspecte et le score de menace est compris entre 60 et 80 :**
   a. Ajoutez une balise appelée Nouvelle menace potentielle.
   b. Ajoutez l'observable à la liste de surveillance.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Créez une tâche de ticket avec l'équipe CTI pour suivre cet observable et poursuivre l'analyse.

d. Lier l'observable au ticket pour enquête.



Analyser et évaluer les IoC de menace

Apprenez à analyser un IOC qui constitue une menace et à en informer l'équipe responsable des incidents de sécurité.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (afficher)

Pourquoi et quand exécuter cette tâche

Chaque fois qu'un enrichissement de la recherche de perception est demandé :

- si l'observable est vu (nombre > 0) et
- La réputation de l'observable est malveillante et
- Le score de menace de l'observable est > 80 et
- Fiabilité des observables > 80

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez **le lien d'action Analyser, évaluer les IoC liés à la menace et créer un incident** pour afficher les détails des règles respectives dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

```
Sighting Created where (Sighting count greater than 0, and Observable.
 Reputation is Malicious, and Observable. Threat Score greater than 80,
 and Observable. Confidence greater than 80)
```

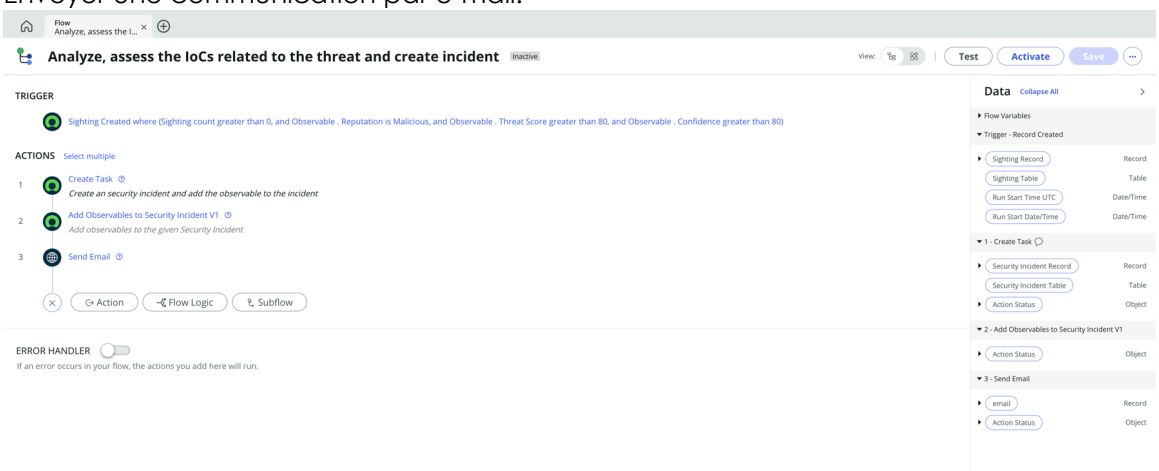

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Si la perception est créée où (nombre de perception supérieur à 0 et observable. La réputation est malveillante et observable. Score de menace supérieur à 80 et observable. Fiabilité supérieure à 80), alors :**

   a. Créez un incident de sécurité et ajoutez l'observable à l'incident.

   b. Ajouter des observables à l'incident de sécurité V1.

   c. Envoyer une communication par e-mail.



Prise en charge de la gestion des vulnérabilités

Découvrez comment une nouvelle vulnérabilité est créée dans TISC avec une vulnérabilité connexe dans VR.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (afficher)

Pourquoi et quand exécuter cette tâche

Lorsqu'une nouvelle vulnérabilité est créée dans TISC et qu'il existe une vulnérabilité connexe dans VR.

- Si le score de vulnérabilité VR (v2) est > 8 OU si le score de vulnérabilité VR (v3) est > 8.
- Le total des VI qui lui sont associés est supérieur à 0.

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez le lien de l'action **de prise en charge de la gestion des vulnérabilités** pour afficher les détails de la règle respective dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

```
When new vulnerability is created in TISC and there is a related
 vulnerability in VR.
```

5. **Si le pourcentage de VI totaux rattrapés qui sont associés à cette vulnérabilité est de 100 %, alors :**

Traduction automatique

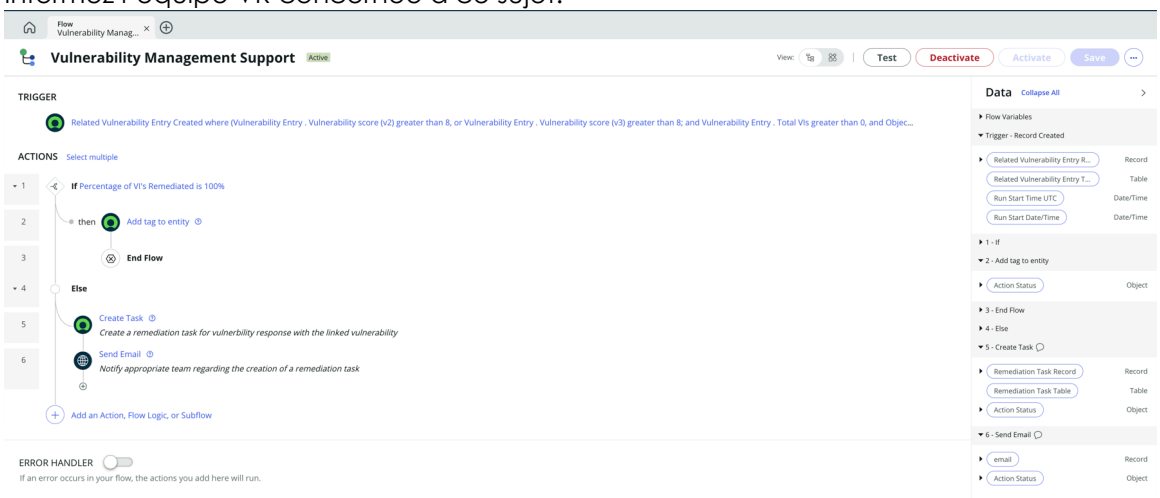
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Ajoutez une balise appelée Corrigé à l'observable.

6. **Sinon, enrichissez les données observables avec les options disponibles :**

a. Créez une tâche de rattrapage pour VR.

b. Informez l'équipe VR concernée à ce sujet.



Suivi des vulnérabilités zero-day

Apprenez à analyser les flux RSS entrant dans le système.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (afficher)

Pourquoi et quand exécuter cette tâche

Chaque fois qu'un nouveau flux RSS est créé dans le système, et qu'il y a une mention de « Zero Day » dans le titre ou la description.

Procédure

1. Accédez à la **Tout** > **Threat Intelligence Security Center** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez **le lien de suivi de vulnérabilité zero-day** pour afficher les détails de la règle respective dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

```
RSS Feed Created where (Title contains zero day, or Description
 contains zero day, or Title contains zero_day, or Description
 contains zero_day, or Title contains zero-day, or Description contains
 zero-day)
```

5. **Si l'observable est une adresse IPv4 ou IPv6 et qu'il se trouve dans une plage CIDR autorisée, alors :**

a. Créez un ticket pour l'équipe TISC ainsi qu'une tâche de rattrapage pour l'équipe VR.

b. Notifier les équipes TISC et VR concernées.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables de flux automatisés

Les tables suivantes vous aident à comprendre les tables de relations entre les entités et les tables d'enrichissement utilisées dans les flux automatisés.

Tables de relations entre les entités

Table	Entité
Observable d'indicateur connexe	sn_sec_tisc_m2m_indicator_observable
Indicateur connexe	sn_sec_tisc_m2m_indicator
Observable connexe	sn_sec_tisc_m2m_observable
Relation objet-objet	sn_sec_tisc_m2m_object
Objet d'indicateur connexe	sn_sec_tisc_m2m_object_indicator
Relation objet-observable	sn_sec_tisc_m2m_object_observable

Table d'enrichissement

Table	Entité
Résultats de la recherche de menace	sn_sec_tisc_lookup_result
Perceptions	sn_sec_tisc_sighting
Résultat de l'enrichissement de l'observable	sn_sec_tisc_observable_enrichment_result

Utilisation des importations de données

L'importation de données vous permet d'afficher tous les enregistrements en cours de traitement pour la tâche d'importation et répertorie également les tâches d'importation en attente d'approbation.

Affichage de toutes les importations

Utilisez cette section pour afficher tous les enregistrements importés qui sont affichés dans la vue de liste pour tous les utilisateurs.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Importations**.
2. Sélectionner **Importations de données** > **Toutes les importations**
   Cette page affiche tous les enregistrements en cours de traitement pour la tâche d'importation.
3. Ouvrez n'importe quel enregistrement pour afficher l'état du processus d'importation.

> **Remarque :** Vous pouvez également cliquer sur **Nouvelle importation** pour créer un enregistrement d'importation. Après avoir cliqué sur ce bouton, l'application vous dirige vers la page **Import Intelligence** . Pour plus d'informations sur la création de nouveaux enregistrements, consultez Importer Threat Intelligence la section et poursuivez avec le type d'importation respectif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage de mes importations

Utilisez cette section pour afficher les enregistrements d'importation créés par l'utilisateur connecté.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Importations**.
2. Sélectionner **Importations de données** > **Mes importations**
   Cette page affiche tous les enregistrements, ces enregistrements d'importation qui sont catégorisés pour un traitement ultérieur de la tâche d'importation.
3. Ouvrez n'importe quel enregistrement pour afficher l'état du processus d'importation.

   Remarque : Vous pouvez également cliquer sur **Nouvelle importation** pour créer un enregistrement d'importation. Après avoir cliqué sur ce bouton, l'application vous dirige vers la page **Import Intelligence** . Pour plus d'informations sur la création de nouveaux enregistrements, consultez Importer Threat Intelligence la section et poursuivez avec le type d'importation respectif.

4. Affichez le résumé des enregistrements d'importation.

   Remarque : Si l'une des tâches d'importation n'est pas soumise, vous pouvez **soumettre** les enregistrements pour traitement ultérieur et l'envoyer pour approbation. Si l'approbation n'est pas requise pour cette tâche d'importation particulière, ces enregistrements sont automatiquement traités.

Affichage de mes approbations

Utilisez cette section pour examiner et approuver les enregistrements de tâches d'importation.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Importations**.
2. Sélectionner **Importations de données** > **Mes approbations**
   Cette page affiche tous les enregistrements d'importation qui sont en attente d'approbation par l'utilisateur connecté.
3. Ouvrez n'importe quel enregistrement pour approuver ou rejeter l'enregistrement d'importation.
4. Cliquez sur **Approuver** pour approuver l'enregistrement de tâche d'importation.
   La boîte de dialogue **Approuver** importation s'affiche et affiche un message de confirmation indiquant s'il faut approuver ou non les importations sélectionnées.

   Remarque : Une notification par e-mail est envoyée au(x) utilisateur(s) respectif(s) pour indiquer que la tâche d'importation qui était en cours de traitement est maintenant approuvée. Pour en savoir plus sur les règles d'approbation, reportez-vous à Définition des règles d'approbation des importations de données.

5. Sélectionnez **Approuver** dans la boîte de dialogue.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une notification par e-mail est envoyée à l'utilisateur qui a créé la tâche d'importation et la tâche d'importation en cours de traitement est maintenant approuvée.

6. Cliquez sur **Rejeter** pour rejeter un enregistrement.

Remarque :

- Vous pouvez examiner et soumettre à nouveau la tâche d'importation rejetée. Assurez-vous d'ajouter des commentaires pour le rejet.
- Une notification par e-mail est envoyée à l'utilisateur qui a créé la tâche d'importation lorsque la tâche d'importation en cours est rejetée.
- Une notification par e-mail est envoyée aux approbateurs pour demander l'approbation.

Importer Threat Intelligence

Utilisez cette fonctionnalité pour ajouter ou importer manuellement des données de Threat Intelligence dans le référentiel.

Les formats d'importation suivants sont pris en charge dans le processus d'importation des données d'intelligence :

1. Importer à partir du fichier structuré
2. Importer à partir du format standard
3. Importer à partir de texte brut
4. Importer à partir du fichier (non structuré)

Importer des données à l'aide d'un fichier structuré

Chargez les données structurées dans les formats de fichiers pris en charge tels que CSV, XLSX ou XLS.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
   La page Bibliothèque Intel de menaces s'affiche.
2. Cliquez sur **Import Intelligence**.
3. Cliquez sur **Importer à partir de la carte de fichier structuré** .

Important : Lors de l'importation des données de Threat Intelligence dans les formats de fichier pris en charge tels que TXT, CSV, STIX 2.x JSON, MISP JSON ou Fichier structuré, la taille du fichier est limitée à 5 Mo. La limite de caractères au texte brut est limitée à 10 000.

4. Renseignez les champs du formulaire.

Champ	Description
Choisir une option	Sélectionnez l'option requise dans la liste déroulante telle que Observables ou Indicateurs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ **Observables** : sélectionnez les données des observables à importer. **Remarque :** Sélectionnez cette option si vous importez des données observables. Ne modifiez pas non plus les en-têtes de colonne dans le fichier. Les champs obligatoires sont Value et Type, les autres sont facultatifs. Saisissez également la date/heure au format AAAA-MM-JJThh :mm :ssZ. ◦ **Indicateurs** : sélectionnez les données d'indicateurs à importer. **Remarque :** Sélectionnez cette option si vous importez des données d'indicateurs. Ne modifiez pas non plus les en-têtes de colonne dans le fichier. Les champs obligatoires pour les indicateurs sont Modèle, Type de modèle et Début de validité, les autres sont facultatifs. Saisissez également la date/heure au format AAAA-MM-JJThh :mm :ssZ.
Prévisualiser et télécharger le fichier d'exemple pour les indicateurs	Utilisez ce lien pour télécharger le fichier d'exemple à l'aide du lien Aperçu et charger les données structurées dans un format de fichier compatible tel que CSV, XLS ou XLSX. **Remarque :** Les en-têtes de colonnes doivent correspondre exactement aux en-têtes. Les champs Valeur et Type sont requis pour chaque observable dans le fichier. Les champs restants sont facultatifs où, comme Premier observé, le Dernier observé doit être en nombre et correspond à l'heure d'époque en millisecondes.
Charger un fichier	Cliquez sur ce lien pour charger les données de fichier au format de fichier de structure recommandé. **Remarque :** Vous ne pouvez charger qu'un seul fichier à la fois. Pour ajouter un nouveau fichier, vous devez supprimer le fichier existant et ajouter un nouveau fichier.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Définir des définitions	
TLP	Sélectionnez l'indicateur TLP (Traffic Light Protocol) dans la liste déroulante à appliquer aux enregistrements importés. TLP est dans TISC est étiqueté avec différentes couleurs pour garantir que les données sensibles sont partagées avec les utilisateurs prévus. ◦ CLAIR : L'information peut être partagée sans restriction. ◦ ROUGE ◦ AMBRE+STRICT ◦ AMBRE ◦ VERT
Fiabilité (0-100)	Définissez la valeur de confiance entre 0 et 100 pour les enregistrements importés.
Période d'expiration (jours)	Entrez la période d'expiration des enregistrements importés. **Remarque :** Il s'agit d'un champ obligatoire.
Balises	
Ajouter des balises	Utilisez les balises pour annoter ou marquer les enregistrements ingérés dans le système à partir de cette source. Staart en tapant le nom de la balise dans la barre **de recherche** pour choisir les balises disponibles dans le système ou entrez un nouveau nom de balise et cliquez sur **Ajouter** pour l'attribuer à la source.
Taxonomie	
Sélectionner une taxonomie	Sélectionnez la taxonomie pour les données importées. À l'aide de taxonomies, définissez des dictionnaires pouvant servir de taxonomies affectées aux enregistrements de connaissance des menaces. Par exemple, la nomenclature CAPEC. Pour plus d'informations, consultez Création de taxonomies. **Remarque :** Les options de valeur de taxonomie changent en fonction de la taxonomie sélectionnée.
Remplacer valeur source	Cochez cette case si vous souhaitez remplacer les valeurs source pour TLP, Fiabilité, Expiration, Balises et Taxonomies

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	par les valeurs configurées. Si vous ne cochez pas cette case, les valeurs configurées sont appliquées si elles ne sont pas vides.

5. Cliquez sur **Suivant**.
6. Examinez les données avant de les soumettre pour traitement.

   Remarque : L'examen des enregistrements importés n'est pas pris en charge pour l'option STIX.

   Après avoir cliqué sur **Suivant**, vous pouvez voir le résumé de toutes les informations que l'utilisateur a fournies dans la section ci-dessus, et la section ci-dessous vous fournit tous les enregistrements qui doivent être importés.

   L'utilisateur peut effectuer n'importe quel type d'activités et les utilisateurs multiples peuvent collaborer à l'aide de la section de commentaire qui est disponible dans le menu contextuel de droite. La liste des enregistrements importés est restituée une fois que l'intégralité du fichier ou du texte brut est traitée. Le traitement de l'importation de fichiers volumineux prendra plus de temps et, pendant le traitement, vous pouvez également vérifier l'état, examiner et soumettre à partir de la page d'enregistrement d'importation.

   Remarque : Tous les enregistrements qui échouent aux validations sont ignorés du processus d'importation et ne sont pas affichés sur la page Révision et soumission pour un traitement ultérieur.

7. Cliquez sur **Mettre à jour le type** et sélectionnez le type pour mettre à jour n'importe quel type d'enregistrements importés.
8. Cliquez sur **Supprimer** pour supprimer n'importe quel type des enregistrements importés.
9. Cliquez sur **Envoyer**.

   Remarque : Une fois que vous avez soumis l'enregistrement d'importation, l'utilisateur est dirigé vers l'approbateur pour approuver l'enregistrement d'importation correspondant en fonction des règles d'approbation configurées. Si l'utilisateur actuel qui crée l'enregistrement n'a pas besoin du processus d'approbation, l'enregistrement passe par le processus d'approbation automatique ; la tâche d'importation est approuvée automatiquement lors de la soumission de la demande.

10. Cliquez sur **Afficher l'état** pour afficher l'état de l'enregistrement d'importation ou cliquez sur **Terminé**.
    L'enregistrement affiche l'état traité une fois les données importées pour traitement.
11. Cliquez sur **Annuler** pour annuler le processus d'importation.
12. Cliquez sur **Revenir** pour revenir à la page précédente et consulter l'enregistrement, si nécessaire.

Importer des données à l'aide du format standard

Chargez les données standard dans les formats de fichiers pris en charge tels que STIX 2.x JSON, MISP JSON.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
   La page Bibliothèque Intel de menaces s'affiche.
2. Cliquez sur **Import Intelligence**.
3. Cliquez sur **Importer à partir d'une carte de fichier standard** .

> **Important :** Lors de l'importation des données de Threat Intelligence dans les formats de fichier pris en charge tels que TXT, CSV, STIX 2.x JSON, MISP JSON ou Fichier structuré, la taille du fichier est limitée à 5 Mo. La limite de caractères au texte brut est limitée à 10 000.

4. Renseignez les champs du formulaire.

Champ	Description
Format de fichier	Sélectionnez l'option requise dans la liste déroulante, par exemple STIX 2.x JSON ou MISP JSON. ◦ **STIX 2.x JSON** : sélectionnez le format dans STIX 2.x JSON à importer. ◦ **MISP JSON** : sélectionnez le format au format MISP JSON à importer.
Charger un fichier	Cliquez sur ce lien pour charger les données au format de fichier standard.
Définir des définitions	
TLP	Sélectionnez l'indicateur TLP dans la liste déroulante à appliquer aux enregistrements importés.
Fiabilité (0-100)	Définissez la valeur de confiance.
Période d'expiration (jours)	Entrez la période d'expiration des enregistrements importés. **Remarque :** Il s'agit d'un champ obligatoire.
Ajouter des balises	Utilisez les balises pour annoter ou marquer les enregistrements ingérés dans le système à partir de cette source. Staart en tapant le nom de la balise dans la barre de recherche pour choisir les balises disponibles dans le système ou entrez un nouveau nom de balise et cliquez sur Ajouter pour l'attribuer à la source.
Taxonomie	
Sélectionner une taxonomie	Sélectionnez la taxonomie pour les données importées. À l'aide de taxonomies, définissez des dictionnaires pouvant servir de taxonomies affectées aux enregistrements de connaissance des

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	menaces. Par exemple, la nomenclature CAPEC. Pour plus d'informations, consultez Création de taxonomies.
Sélectionner valeurs de taxonomie	Indique les valeurs de taxonomie associées à la taxonomie.
Remplacer valeur source	Cochez cette case si vous souhaitez remplacer les valeurs source pour TLP, Fiabilité, Expiration, Balises et Taxonomies des valeurs configurées. Si vous ne cochez pas cette case, les valeurs par défaut sont appliquées.

5. Cliquez sur **Suivant**.
6. Examinez les données avant de les soumettre pour traitement.

   Remarque : L'examen des enregistrements importés n'est pas pris en charge pour l'option STIX.

   Après avoir cliqué sur **Suivant**, vous pouvez voir le résumé de toutes les informations que l'utilisateur a fournies dans la section ci-dessus, et la section ci-dessous vous fournit tous les enregistrements qui doivent être importés.

   L'utilisateur peut effectuer n'importe quel type d'activités et les utilisateurs multiples peuvent collaborer à l'aide de la section de commentaire qui est disponible dans le menu contextuel de droite.

   Remarque : Tous les enregistrements qui échouent aux validations sont ignorés du processus d'importation et ne sont pas affichés sur la page Révision et soumission pour un traitement ultérieur.

7. Cliquez sur **Mettre à jour le type** et sélectionnez le type pour mettre à jour n'importe quel type d'enregistrements importés.
8. Cliquez sur **Supprimer** pour supprimer n'importe quel type des enregistrements importés.
9. Cliquez sur **Envoyer**.

   Remarque :

   Une fois que vous avez soumis l'enregistrement d'importation, l'utilisateur est dirigé vers l'approbateur pour approuver l'enregistrement d'importation correspondant en fonction des règles d'approbation configurées. Si l'utilisateur actuel qui crée l'enregistrement n'a pas besoin du processus d'approbation, l'enregistrement passe par le processus d'approbation automatique ; la tâche d'importation est approuvée automatiquement lors de la soumission de la demande.

10. Cliquez sur **Afficher l'état** pour afficher l'état de l'enregistrement ou cliquez sur **Terminé**. L'enregistrement affiche le statut traité une fois traité.
11. Cliquez sur **Annuler** pour annuler le processus d'importation.
12. Cliquez sur **Revenir** pour revenir à la page précédente et consulter l'enregistrement, si nécessaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer des données à l'aide de texte brut

Importez les données observables en copiant et collant du texte brut ou en saisissant du texte libre.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
   La page Bibliothèque Intel de menaces s'affiche.
2. Cliquez sur **Import Intelligence**.

> **Important :**
> - Tous les caractères de neutralisation seront nettoyés dans le cadre de l'analyse et de l'extraction des observables.
> - Pour cette option de texte collé, seuls l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP sont extraits et aucun autre type d'observable n'est extrait pour l'importation de données. Dans le cas de ce type d'observables tels que le registre, les types de répertoire, ceux-ci sont ignorés de l'importation.

3. Cliquez sur **Importer à partir d'une carte de texte brut** .

> **Important :** Lors de l'importation des données de Threat Intelligence au format texte brut, les caractères sont limités à 10 000. L'option Texte brut peut être utilisée comme solution de contournement pour extraire les observables du PDF.

4. Renseignez les champs du formulaire.

Champ	Description
Zone de texte Données brutes	Saisissez ou copiez-collez le texte brut ici dans cette zone de texte. **Remarque :** Vous ne pouvez saisir ou coller le texte brut que dans 10 000 caractères.
Définir des définitions	
TLP	Sélectionnez l'indicateur TLP dans la liste déroulante à appliquer aux enregistrements importés.
Fiabilité (0-100)	Définissez la valeur de confiance.
Période d'expiration (jours)	Entrez la période d'expiration des enregistrements importés. **Remarque :** Il s'agit d'un champ obligatoire.
Ajouter des balises	Utilisez les balises pour annoter ou marquer les enregistrements ingérés dans le

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	système à partir de cette source. Staart en tapant le nom de la balise dans la barre de recherche pour choisir les balises disponibles dans le système ou entrez un nouveau nom de balise et cliquez sur Ajouter pour l'attribuer à la source.
Taxonomie	
Sélectionner une taxonomie	Sélectionnez la taxonomie pour les données importées. À l'aide de taxonomies, définissez des dictionnaires pouvant servir de taxonomies affectées aux enregistrements de connaissance des menaces. Par exemple, la nomenclature CAPEC. Pour plus d'informations, consultez Création de taxonomies.

5. Cliquez sur **Suivant**.
6. Examinez les données avant de les soumettre pour traitement.

   Après avoir cliqué sur **Suivant**, vous pouvez voir le résumé de toutes les informations que l'utilisateur a fournies dans la section ci-dessus, et la section ci-dessous vous fournit tous les enregistrements qui doivent être importés.

   L'utilisateur peut effectuer n'importe quel type d'activités et les utilisateurs multiples peuvent collaborer à l'aide de la section de commentaire qui est disponible dans le menu contextuel de droite.

   Remarque : Tous les enregistrements qui échouent aux validations sont ignorés du processus d'importation et ne sont pas affichés sur la page Révision et soumission pour un traitement ultérieur.

7. Cliquez sur **Mettre à jour le type** et sélectionnez le type pour mettre à jour n'importe quel type d'enregistrements importés.
8. Cliquez sur **Supprimer** pour supprimer n'importe quel type des enregistrements importés.
9. Cliquez sur **Envoyer**.

   Remarque : Une fois que vous avez soumis l'enregistrement d'importation, l'utilisateur est dirigé vers l'approbateur pour approuver l'enregistrement d'importation correspondant en fonction des règles d'approbation configurées. Si l'utilisateur actuel qui crée l'enregistrement n'a pas besoin du processus d'approbation, l'enregistrement passe par le processus d'approbation automatique ; la tâche d'importation est approuvée automatiquement lors de la soumission de la demande.

10. Cliquez sur **Afficher l'état** pour afficher l'état de l'enregistrement ou cliquez sur **Terminé**. L'enregistrement affiche le statut traité une fois traité.
11. Cliquez sur **Annuler** pour annuler le processus d'importation.
12. Cliquez sur **Revenir** pour revenir à la page précédente et consulter l'enregistrement, si nécessaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer des données à l'aide d'un format de fichier non structuré

Chargez les données dans un format non structuré pris en charge à l'aide des formats de fichier tels que TXT, CSV, JSON, XLS, XLSX.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
   La page Bibliothèque Intel de menaces s'affiche.
2. Cliquez sur **Import Intelligence**.

Important :

- Tous les caractères de neutralisation seront nettoyés dans le cadre de l'analyse et de l'extraction des observables.
- Pour cette option de format de fichier non structuré, seuls l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP sont extraits et aucun autre type d'observable n'est extrait pour l'importation de données. Dans le cas de ce type d'observables tels que le registre, les types de répertoire, ceux-ci sont ignorés de l'importation.

3. Cliquez sur **Importer à partir d'une carte de fichier (non structurée).**

Remarque : Lors de l'importation des données de Threat Intelligence dans les formats de fichier pris en charge tels que TXT, CSV, STIX 2.x JSON, MISP JSON ou Fichier structuré, la taille du fichier est limitée à 5 Mo.

4. Renseignez les champs du formulaire.

Champ	Description
Charger un fichier	Cliquez sur ce lien pour charger les données au format de fichier standard.
Définir des définitions	
TLP	Sélectionnez l'indicateur TLP dans la liste déroulante à appliquer aux enregistrements importés.
Fiabilité (0-100)	Définissez la valeur de confiance.
Période d'expiration (jours)	Entrez la période d'expiration des observables associés. **Remarque :** Il s'agit d'un champ obligatoire.
Ajouter des balises	Utilisez les balises pour annoter ou marquer les enregistrements ingérés dans le système à partir de cette source. Staart en tapant le nom de la balise dans la barre de recherche pour choisir les balises disponibles dans le système ou entrez

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	un nouveau nom de balise et cliquez sur Ajouter pour l'attribuer à la source.
Taxonomie	
Sélectionner une taxonomie	Sélectionnez la taxonomie pour les données importées. À l'aide de taxonomies, définissez des dictionnaires pouvant servir de taxonomies affectées aux enregistrements de connaissance des menaces. Par exemple, la nomenclature CAPEC. Pour plus d'informations, consultez Création de taxonomies.

5. Examinez les données avant de les soumettre pour traitement.

   Après avoir cliqué sur **Suivant**, vous pouvez voir le résumé de toutes les informations que l'utilisateur a fournies dans la section ci-dessus, et la section ci-dessous vous fournit tous les enregistrements qui doivent être importés.

   L'utilisateur peut effectuer n'importe quel type d'activités et les utilisateurs multiples peuvent collaborer à l'aide de la section de commentaire qui est disponible dans le menu contextuel de droite.

   > **Remarque :** Les formats pris en charge pour importer les données sont TXT, CSV, JSON, XLS et tous les enregistrements qui échouent aux validations sont ignorés du processus d'importation et ne sont pas affichés sur la page Révision et soumission pour traitement.

6. Cliquez sur **Mettre à jour le type** et sélectionnez le type pour mettre à jour n'importe quel type d'enregistrements importés.
7. Cliquez sur **Supprimer** pour supprimer n'importe quel type des enregistrements importés.
8. Cliquez sur **Envoyer**.

   > **Remarque :** Une fois que vous avez soumis l'enregistrement d'importation, l'utilisateur est dirigé vers l'approbateur pour approuver l'enregistrement d'importation correspondant en fonction des règles d'approbation configurées. Si l'utilisateur actuel qui crée l'enregistrement n'a pas besoin du processus d'approbation, l'enregistrement passe par le processus d'approbation automatique ; la tâche d'importation est approuvée automatiquement lors de la soumission de la demande.

9. Cliquez sur **Afficher l'état** pour afficher l'état de l'enregistrement ou cliquez sur **Terminé**. L'enregistrement affiche le statut traité une fois la soumission réussie.
10. Cliquez sur **Annuler** pour annuler le processus d'importation.
11. Cliquez sur **Revenir** pour revenir à la page précédente et consulter l'enregistrement, si nécessaire.

Console d'analyste de menaces

La page Console de l'analyste de menaces se compose des tickets et des tâches de ticket placés sous la supervision des analystes de menaces et de leur équipe.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez la **fonctionnalité Gestion des tickets** pour créer et suivre les enquêtes et les activités d'analyse des menaces.

Au cours des enquêtes sur les menaces, les analystes collectent les données à partir d'enregistrements de renseignement internes tels que les observables, les acteurs de menace, les campagnes, etc.

Vue d'ensemble de la console

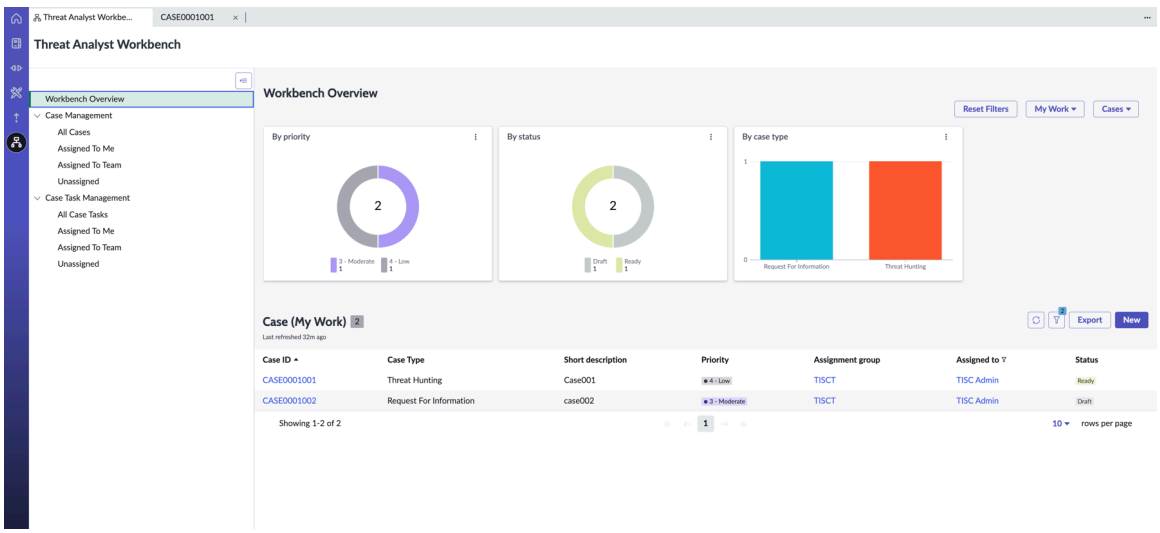
La page Vue d'ensemble de la console comprend les tâches de tickets et les tickets qui se trouvent sous les analystes de menaces et leur équipe.

La vue d'ensemble répertorie tous les tickets ouverts et leur état, ce qui aide les analystes à gérer leur charge de travail et à classer leurs enquêtes par ordre de priorité.

Rôle requis : sn_sec_tisc.analyst, sn_sec_tisc.admin

Une fois le ticket créé, les analystes affecteront les tâches du ticket à d'autres analystes ou équipes pour une enquête plus approfondie, et collaboreront également avec eux pour partager des informations et des aperçus.

Sous chaque filtre, différents widgets sont présents, regroupés par priorité, statut et type de ticket, qui se trouvent dans les files d'attente des analystes de menaces et dans la file d'attente de l'équipe d'analystes de menaces.



Lorsque des filtres sont appliqués sur les widgets, la moitié inférieure de la page de vue d'ensemble est renseignée avec les tickets correspondants ou les tâches de ticket présentés sous forme d'éléments de liste. Pour supprimer les filtres appliqués, cliquez sur **Réinitialiser les filtres** pour rétablir la vue d'origine.

À l'aide de cette page, les analystes de menaces et les administrateurs peuvent afficher leur travail, le travail de leurs équipes et tout travail non affecté. Vous pouvez accéder à la liste déroulante. Les options disponibles sont les suivantes :

- Mes tâches : sélectionnez cette option pour afficher les tâches qui vous sont affectées.
- Travail de mon équipe : sélectionnez cette option pour afficher le travail de votre équipe affecté à tous les groupes dont vous faites partie.
- Travail non affecté : sélectionnez cette option pour afficher le ticket ou la tâche de ticket qui n'est pas affecté. Pour affecter le ticket ou la tâche de ticket, vous devez accéder à la vue de formulaire et affecter le ou les utilisateurs ou groupes d'utilisateurs au ticket et aux tâches de ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez également afficher les tickets et les tâches de ticket directement à partir de la vue d'ensemble de la console qui vous sont affectés. Par défaut, la vue des tickets s'affiche, vous pouvez utiliser la liste déroulante et sélectionner les tâches de tickets si vous souhaitez afficher les tâches de tickets par priorité et statut.

Création de tickets à l'aide de Threat Analyst Workbench

Les tickets sont utilisés pour suivre les informations relatives à une campagne ou à un acteur de menace menaçant votre organisation. Une fois le ticket créé, vous pouvez ajouter des artefacts qui vous permettent d'examiner et d'analyser toutes les informations connexes à partir d'un ticket ou d'une tâche de ticket unique.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst, sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs comme il convient.

Créer un nouveau ticket

Champ	Description
ID du ticket	Un identificateur unique pour le ticket. Il s'agit d'un ID généré par le système.
Description brève	Résumé de la demande ou du problème faisant l'objet de l'examen ou brève description.
Description	Une description détaillée comprenant toute information pertinente sur le cas, comme le contexte, l'analyse requise et les résultats attendus.
Type de ticket	Sélectionnez le type de ticket faisant l'objet de l'enquête. Les options possibles pour l'enquête sont les suivantes : ◦ Chasse aux menaces ◦ Demande d'informations ◦ Ticket de gestion de la vulnérabilité ◦ Ticket de conformité ◦ Ticket de réponse aux incidents ◦ Ticket de collaboration ◦ Autres
Priorité	Une évaluation de la gravité de la demande ou du problème.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Groupe d'affectation	Groupe affecté et responsable du traitement du ticket.
Statut	L'état actuel du ticket.
Affecté à	L'analyste chargé de travailler sur un ticket.
Date d'échéance	Date et heure auxquelles la tâche doit être terminée ou fermée.
Contributeurs	Liste des délégataires déployés à partir des tâches et pouvant être ajoutés par-dessus.
TLP	Valeur unique qui indique le paramètre de sensibilité des données par TLP.
Liste de surveillance	Lorsqu'un utilisateur est ajouté à la liste de surveillance, il reçoit des notifications par e-mail sur les changements apportés à l'état et à la priorité.
Appliquer la restriction	Cochez cette case pour modifier les membres des groupes autorisés et des membres autorisés. Pour plus d'informations, consultez Restrictions appliquées pour le ou les tickets.

6. Renseignez les champs de la section Aperçus comme il convient.

Aperçus

Champ	Description
Notes	Toutes les notes supplémentaires relatives à l'enquête sur la menace.
Recommandations ou actions	Toutes les recommandations ou actions liées à l'enquête sur la menace.
Analyses et résultats	Saisissez l'analyse et les conclusions relatives à l'enquête sur la menace.
Synthèse de fermeture	Ajoutez le résumé de fermeture des résultats.

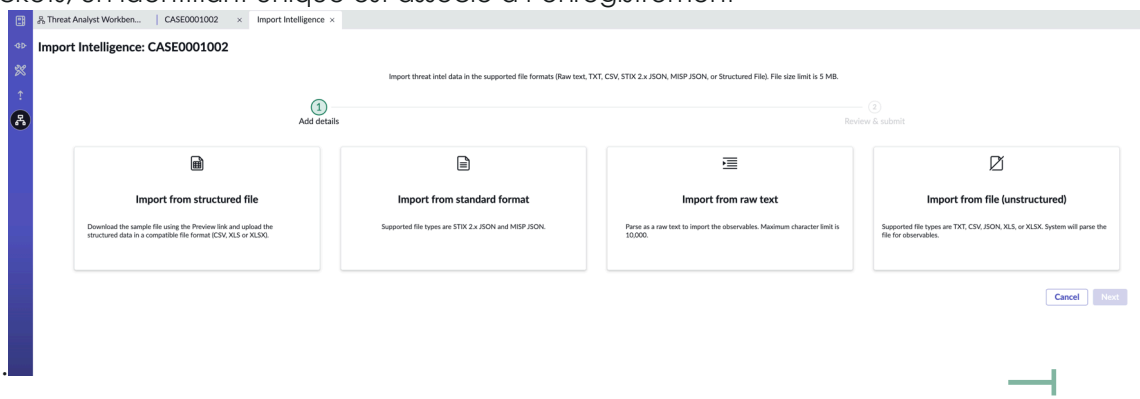
7. Cliquez sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois l'enregistrement enregistré, vous pouvez cliquer sur l'onglet **Importer des renseignements** pour importer les données de renseignements sur les menaces à l'aide de la fonctionnalité **Importer des renseignements** .

Remarque : Si vous importez et traitez des données à partir de Gestion des tickets, un identifiant unique est associé à l'enregistrement d'importation.



Restrictions appliquées pour le ou les tickets

Utilisez cette fonctionnalité pour restreindre un ticket et fournir une liste de groupes et d'utilisateurs qui peuvent y accéder.

Rôle requis :

- sn_sec_tisc_admin
- sn_sec_tisc.restriction_access_manager

Principaux éléments à prendre en compte

1. Restreignez un ticket et fournissez la liste des groupes/utilisateurs qui peuvent y accéder.
2. Activez le champ « Appliquer la restriction » présent dans la page du formulaire de ticket.
3. Modifiez les membres des groupes autorisés et des membres autorisés.
4. Une fois qu'un ticket est marqué comme restreint, seuls les membres des groupes autorisés, les membres de la liste des utilisateurs autorisés et les utilisateurs disposant du rôle sn_sec-tisc.admin peuvent accéder à ce ticket.
5. Accordez l'accès au rôle sn_sec_tisc.restriction_access_manager qui est requis pour lire/écrire le champ Appliquer la restriction. Si vous êtes analyste et que vous n'avez pas ce rôle, vous ne pouvez pas voir l'option Appliquer la restriction pour le ou les tickets ou les tâches de ticket.
6. L'analyste assigned_to existant et l'analyste qui l'a marqué comme restreint perdront également l'accès s'ils ne disposent pas de l'autorisation nécessaire.
7. La restriction des tickets au sein de l'équipe CTI est mise en œuvre au cas par cas. Les membres autorisés peuvent accéder aux tickets restreints s'ils figurent sur la liste des tickets autorisés. Le fait de les placer dans l'une des listes de tickets autorisés ne signifie pas qu'ils peuvent accéder à tous les autres tickets restreints.
8. Si le ticket est marqué comme restreint et que les membres autorisés ou le groupe autorisé sont laissés vides, seul sn_sec_tisc.admin peut accéder à ces tickets restreints.
9. Seuls les groupes CTI sont autorisés dans le champ **Groupe autorisé** . Un utilisateur disposant du rôle sn_sec_tisc.analyste est autorisé à figurer dans la liste **des membres autorisés** .

Remarque : Une note de travail est publiée si un ticket est marqué comme restreint.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles d'accès pour les tickets et les tâches de ticket

Autorisez les contrôles d'accès spécifiques à un ticket ou à une tâche de ticket.

Contrôle d'accès	Description
Accès en lecture	Les utilisateurs externes ajoutés ici auront accès au formulaire de ticket, mais ne pourront modifier aucun champ du ticket ni effectuer aucune action.
Accès privilégié	Les utilisateurs externes ajoutés ici auront accès à la modification de tous les champs du formulaire de ticket, mais ne seront pas autorisés à exécuter des orchestrations.

Accès des utilisateurs externes ou tâches de ticket

Les contrôles d'accès des utilisateurs externes sont nécessaires pour contrôler l'accès au sein d'un ticket.

Tâches de tickets affectées à des utilisateurs externes

1. Il est recommandé que l'utilisateur ait accès à l'espace de travail TISC et qu'il affiche uniquement les modules Tâches de ticket.
2. L'utilisateur externe peut uniquement voir les tâches de ticket affectées à cet utilisateur spécifique ou au(x) groupe(s) auquel l'utilisateur appartient.
3. L'utilisateur externe doit être en mesure de réaffecter la tâche au sein du groupe auquel il appartient.

Remarque : L'utilisateur externe est tout utilisateur qui n'appartient pas à l'équipe CTI.

Par défaut, la section de contrôle d'accès de l'utilisateur externe n'est pas visible et l'utilisateur a besoin d'un rôle supplémentaire. En outre, la section de contrôle d'accès de l'utilisateur externe ne doit pas être visible par les utilisateurs externes qui disposent d'un accès en lecture ou privilégié dans un ticket.

Remarque : Les utilisateurs externes accèdent à l'espace de travail TISC et ceux qui ont la visibilité sur les modules Ticket et Tâches de ticket. L'utilisateur ne verra que les tickets auxquels il a accès (en lecture ou en mode privilégié).

Rôles à affecter Accès utilisateur externe

Rôle	Description
sn_sec_tisc.special_access_read_manager	• L'utilisateur disposant de ce rôle sera en mesure de voir la section. • Sera en mesure de modifier le champ d'accès en lecture. • Le rôle est affecté par défaut à l'administrateur Threat Intelligence et peut être affecté à d'autres utilisateurs de l'équipe CTI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles à affecter Accès utilisateur externe (suite)

Rôle	Description
sn_sec_tisc.special_access_write_manager	• L'utilisateur disposant de ce rôle sera en mesure de voir la section. • Sera en mesure de modifier le champ Accès privilégié. • Le rôle est affecté par défaut à l'administrateur Threat Intelligence et peut être affecté à d'autres utilisateurs de l'équipe CTI.

Associer la technique MITRE

Associer une ou plusieurs techniques MITRE à un ticket.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez n'importe quel ticket.
5. Cliquez sur le bouton **Associer la technique MITRE** .
6. Cliquez sur **Ajouter une matrice** pour associer la technique MITRE.
   La boîte **de dialogue Associer la technique MITRE au ticket** s'affiche.
7. Sélectionnez la **matrice**.
   Toutes les matrices activées s'affichent pour vous permettre de sélectionner la matrice.
8. Sélectionnez la tactique dans les listes déroulantes.
   Toutes les tactiques associées à une matrice seront affichées.

   Remarque : Si vous souhaitez ajouter d'autres tactiques, cliquez sur **Ajouter une tactique**. Les tactiques précédemment sélectionnées ne s'afficheront plus dans la liste déroulante si vous ajoutez une nouvelle tactique.

9. Sélectionnez la **technique**.
   Toutes les techniques associées à la tactique sélectionnée seront affichées. Si vous ajoutez d'autres tactiques, vous pouvez sélectionner les techniques associées à ces tactiques sélectionnées.
10. Cliquez sur **Enregistrer**.
    Si vous souhaitez supprimer l'ensemble des données associées à la matrice, puis cliquez sur **Supprimer la matrice**, cette action ne supprimera que les données de matrice associées, mais la matrice restera dans le référentiel MITRE ATT&CK.

    L'enregistrement des données matricielles associé s'affiche sous la section Carte MITRE ATT&CK. Dans la vue de la carte :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez passer d'une matrice à l'autre à partir de la liste déroulante Matrice.

a. La première ligne de la vue de la carte affiche toutes les tactiques associées à la matrice sélectionnée actuelle.

b. Chaque carte tactique affiche le nom de la tactique et le nombre de techniques de cette tactique mappées à l'enregistrement de ticket actuel.

c. Toutes les techniques associées à ce cas sont affichées verticalement sous chaque tactique. Vous pouvez cliquer sur n'importe quelle technique pour afficher la vue du formulaire de technique.

11. Cliquez sur **Afficher l'ID** pour afficher les ID de toutes les techniques associées.

Remarque : Chaque carte de technique affiche le nom de la technique et l'ID de la technique uniquement lorsque **l'option Afficher l'ID** est activée.

12. Cliquez sur **Actualiser** pour actualiser la vue de la carte.
Vous pouvez afficher l'horodatage de la dernière actualisation de la matrice sélectionnée.

Remarque : Cliquez sur l'icône contextuelle pour afficher la carte de matrice associée dans un nouvel onglet.

Créer une tâche de ticket à l'aide de la console d'analyste de menaces

Créez des tâches de ticket à associer avec des tickets.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst, sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Gestion des tâches de ticket** > **Toutes les tâches des tickets**.
Toutes les tâches de ticket sont affichées.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs comme il convient.

Créer une nouvelle tâche de ticket

Champ	Description
ID de tâche	Un identificateur unique pour la tâche de ticket. Il s'agit d'un ID généré par le système.
Description brève	Résumé de la demande ou du problème faisant l'objet de l'examen ou brève description.
Description	Une description détaillée comprenant toute information pertinente sur la tâche de ticket (par exemple, le contexte, l'analyse requise et les résultats attendus).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID de ticket parent	Sélectionnez l'ID du ticket parent dans la recherche.
Priorité	Une évaluation de la gravité de la demande ou du problème.
Groupe d'affectation	Groupe affecté et responsable de la tâche de ticket.
Statut	L'état actuel de la tâche de ticket.
Affecté à	L'analyste chargé de travailler sur une tâche de ticket.
Date d'échéance	Date et heure auxquelles la tâche de ticket doit être terminée ou fermée.
TLP	Valeur unique qui indique le paramètre de sensibilité des données par TLP.
Appliquer la restriction	En tant que sn_sec_tisc_admin, cochez cette case pour modifier les membres du groupe autorisé et des membres autorisés. Pour plus d'informations, consultez Restrictions appliquées pour le ou les tickets.

6. Renseignez les champs de la section Aperçus comme il convient.

Aperçus

Champ	Description
Notes	Toutes les notes supplémentaires relatives à l'enquête sur la menace.
Fermeture	Ajoutez le résumé de fermeture des résultats.

7. Cliquez sur **Enregistrer**.
   Votre tâche de ticket sera associée à votre ticket.

Remarque : Après avoir enregistré la tâche de ticket, vous pouvez lui ajouter des balises et des taxonomies. Pour plus d'informations, consultez Création de taxonomies.

Ajouter des artefacts au(x) ticket(s) ou tâche(s) de ticket

Une fois que vous avez créé un ticket, vous pouvez y ajouter des artefacts, tels que des incidents de sécurité, des CI et des indicateurs de compromission. Ces artefacts servent d'indices dans la résolution de l'affaire.

Avant de commencer

Rôle requis : administrateur

Remarque : Les artefacts ne sont disponibles que pour les tickets existants. Pour les observables et les indicateurs, les artefacts peuvent également être ajoutés ou associés à un ticket à partir de la tâche d'importation à l'aide du bouton Import Intelligence. Pour plus d'informations sur l'importation, consultez Importer Threat Intelligence

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez un ticket ou une tâche de ticket.
5. Accédez à l'onglet **Artefacts** .
   Les artefacts associés s'affichent sous forme de listes connexes pour ce ticket ou cette tâche de ticket spécifique.
6. Lier ou dissocier les enregistrements du ticket ou de la tâche de ticket.

Remarque : Pour plus d'informations, voir Lier les enregistrements connexes aux renseignements sur la menace

La table suivante répertorie les listes connexes des artefacts associés au ou aux tickets ou aux tâches de ticket :

Enregistrements connexes

Liste connexe	Description
Techniques MITRE	Répertoriez les techniques MITRE associées au ou aux tickets.
Observable	Liste des observables associés à ce ticket ou tâche de ticket.
Indicateurs	Liste des indicateurs associés à ce ticket ou tâche de ticket.
Schémas d'attaque	Liste des modèles d'attaque associés à ce ticket ou tâche de ticket.
Campagnes	Répertoriez les campagnes associées à ces tickets ou tâches de ticket.
Déroulement des actions	Répertoriez le plan d'actions associé à ce ticket ou tâche de ticket.
Composants de données	Liste des composants de données associés à ce ticket ou tâche de ticket.
Regroupements des menaces	Répertorier les regroupements de menaces associés à ces tickets ou tâches de ticket.
Identités	Répertoriez les identités associées à ce ticket ou tâche de ticket.
Infrastructure	Répertoriez l'infrastructure telle que les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées associées à ces tickets ou tâches de ticket.
Ensembles d'intrusion	Répertoriez les ensembles d'intrusion tels qu'un ensemble de comportements et de ressources antagonistes avec des propriétés communes associées à ce ticket ou à ces tâches de ticket.
Emplacements	Répertorier les enregistrements d'emplacements associés à ce ticket ou tâche de ticket.
Programme malveillant	Répertorier les enregistrements sources de programmes malveillants associés à ces tickets ou tâches de ticket.
Définitions de marquage	Répertoriez les enregistrements de définitions de marquage associés à ce ticket ou à cette tâche de ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Description
Notes de menace	Répertoriez les enregistrements de définitions de marquage associés à ce ticket ou à cette tâche de ticket.
Données observées	Répertoriez les données observées associées à ce ticket ou tâche de ticket.
Opinions sur la menace	Répertoriez les opinions sur la menace associées à ces tickets ou tâches de ticket.
Rapports de menace	Répertoriez les rapports de menace associés à ces tickets ou tâches de ticket.
Perceptions	Liste des perceptions associées à ce ticket ou tâche de ticket.
Acteurs de menace	Répertoriez les acteurs de menace associés à ces tickets ou tâches de ticket.
Outils	Répertoriez les outils associés à ces tickets ou tâches de ticket.
Vulnérabilités	Si l'observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante et qui sont associées à ces tickets ou tâches de ticket.
Tickets connexes	Répertorie les tickets connexes.
Tâches du ticket connexe	Répertorie les tâches de tickets connexes.
Incidents de sécurité	Répertoriez les incidents de sécurité associés à ces tickets ou tâches de ticket.
Éléments de configuration affectés	Répertorier les éléments de configuration affectés associés à ces tickets ou tâches de ticket.
Services affectés	Répertorier les services affectés associés à ces tickets ou tâches de ticket.
Actifs affectés	Répertoriez les actifs affectés associés à ces tickets ou tâches de ticket.
Entrées de vulnérabilité	Répertoriez les entrées de vulnérabilité associées à ce ticket ou tâche de ticket.

Traduction automatique

Exécuter des actions d'enrichissement dans un ticket

Utilisez cette section pour comprendre comment les actions d'enrichissement sont effectuées sur le ou les tickets.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

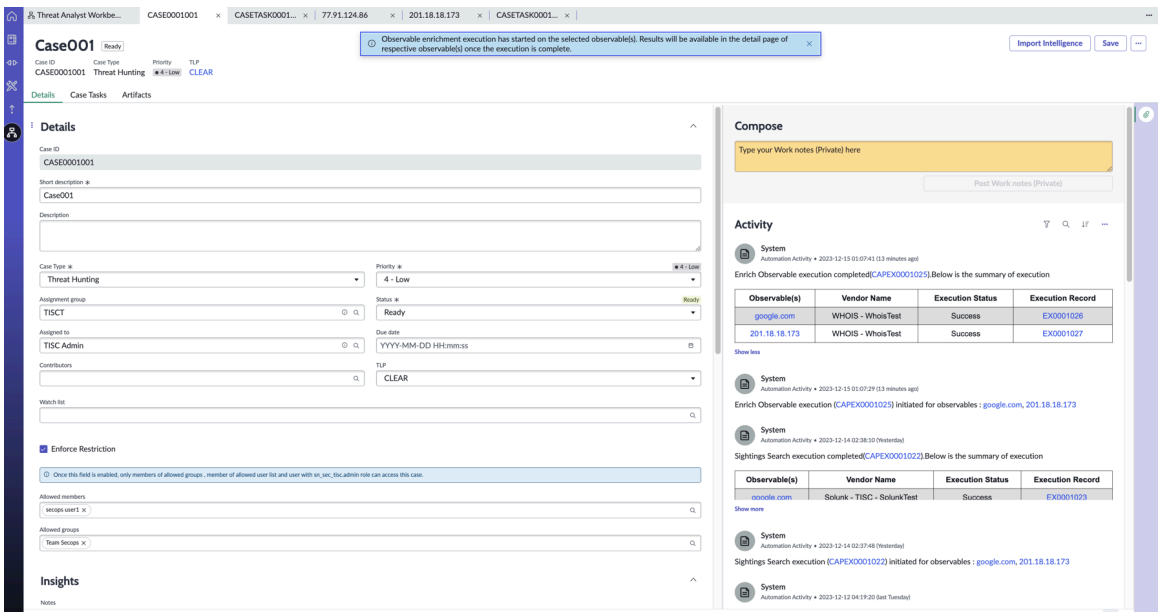
Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez un ticket ou une tâche de ticket.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Accédez à l'onglet **Artefacts** .
6. Sélectionnez la liste connexe Observables.
7. Sélectionnez un ou plusieurs observables.
8. Cliquez sur une action d'enrichissement dans la liste déroulante.
9. Sélectionnez la ou les implémentations disponibles.
10. Cliquez sur **Envoyer**.
    Par exemple, Exécuter une recherche de menace. L'action d'enrichissement sélectionnée sera exécutée et un message dinformation s'affichera indiquant que l'exécution de l'enrichissement de l'observable a démarré sur le ou les observables sélectionnés. Les résultats seront disponibles dans la page détaillée du ou des observables respectifs une fois l'exécution terminée.

Remarque : Une fois l'exécution initiée ou terminée, une note de travail est publiée dans le flux d'activité de la vue de formulaire.



Afficher les rapports de tickets

Utilisez la fonctionnalité Rapports de tickets pour générer des rapports relatifs aux tickets. Ces rapports comprennent un rapport post-enquête ou un rapport de synthèse.

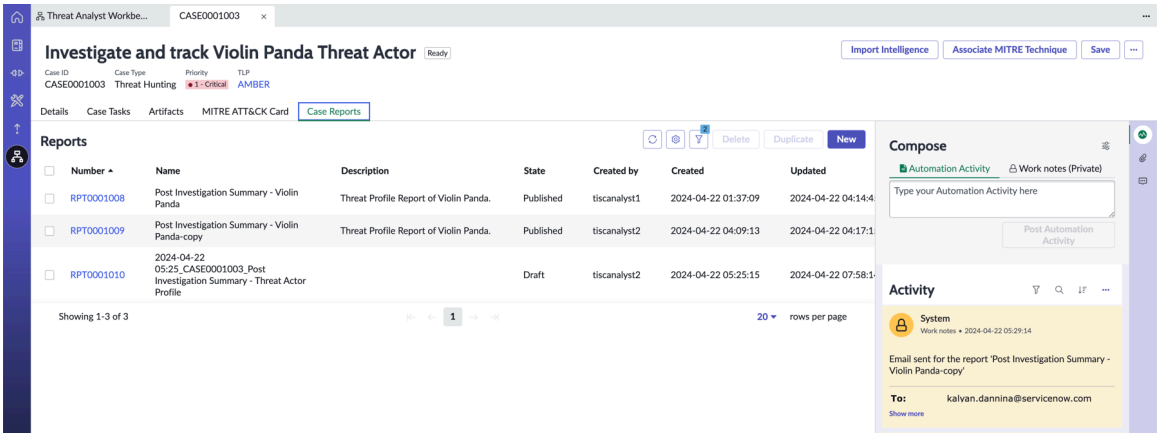
Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

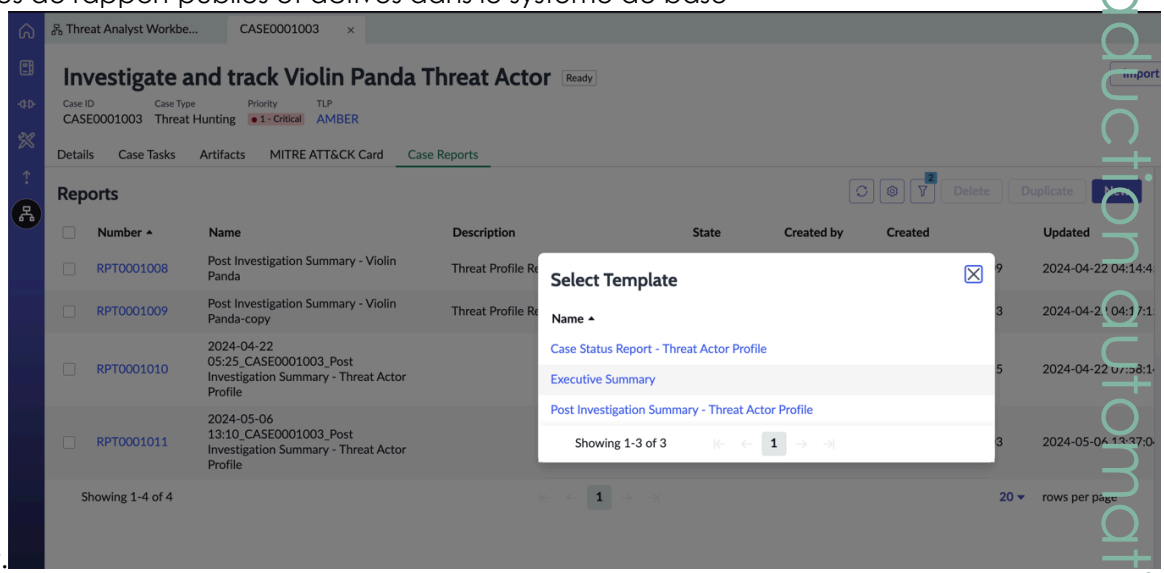
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez n'importe quel ticket.
5. Accédez à **Rapports de tickets**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Vous pouvez supprimer les rapports de la liste, créer une copie en double des rapports existants et personnaliser votre propre rapport.

6. Cliquez sur **Nouveau**.
   Les modèles de rapport publiés et activés dans le système de base s'affichent.



7. Sélectionnez le modèle de rapport souhaité.
   Le modèle de rapport sélectionné pour le type de rapport est généré. De plus, ici, une fois le rapport publié, cela signifie qu'un plus grand groupe d'utilisateurs peut le consulter, mais si le rapport est à l'état de brouillon, ce rapport est masqué aux utilisateurs. En tant qu'analyste, vous ne pouvez afficher que les rapports publiés, mais pas les rapports à l'état brouillon.

Remarque :

- Si vous souhaitez ajouter d'autres champs, sélectionnez les champs et ajoutez-les directement dans votre rapport de ticket.
- Si vous souhaitez ajouter une liste connexe, par exemple une liste d'observables, sélectionnez Observables. Tous les observables associés à ce cas particulier sont répertoriés, sélectionnez un ou plusieurs observables et cliquez sur **Ajouter**. Vous pouvez également filtrer l'observable requis et l'ajouter à votre ticket.

8. Cliquez sur **Enregistrer le contenu** pour enregistrer le contenu de votre rapport.
9. Cliquez sur **Aperçu** pour prévisualiser le rapport.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez faire ce qui suit :

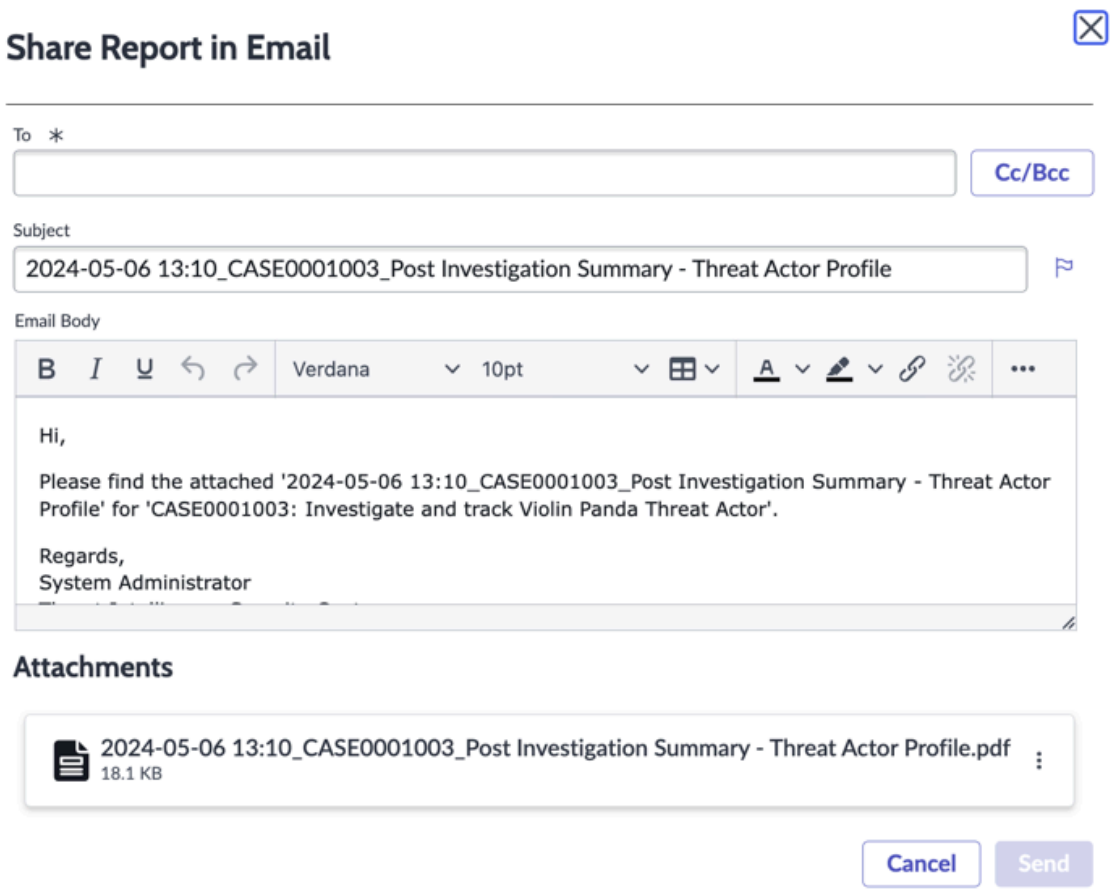
- **Agrandissez** la fenêtre de rapport.
- **Téléchargez** le rapport à l'aide de l'icône **Télécharger** .
- Affichez le rapport dans un nouvel onglet en cas de hauteur ou de taille du rapport afin d'avoir une meilleure expérience de visualisation.
- **Modifiez** le nom du rapport et la description du rapport.
- **Publiez** le rapport.

10. Cliquez sur le bouton **Modifier le contenu** pour republier le rapport.

Remarque : Un message d'avertissement s'affiche pour vous permettre de partager le rapport :

Vous devez republier le rapport après avoir apporté des modifications pour pouvoir télécharger ou partager le rapport. Voulez-vous quand même continuer la modification ?

11. Cliquez sur **Modifier**.
Si vous souhaitez modifier le rapport, vous pouvez continuer à modifier le rapport comme expliqué ou vous pouvez publier le rapport. Une fois publié, le rapport sera en lecture seule.
12. Cliquez sur **Partager le rapport par e-mail** pour partager le rapport.
Lors du partage du rapport, le rapport PDF généré est joint en tant que pièce jointe à l'e-



mail.

13. Ajoutez les champs d'e-mail requis, tels que À (personne à qui vous souhaitez partager le rapport), Cc et Cci

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

14. Marquez l'e-mail comme important, si nécessaire.
15. Cliquez sur **Envoyer**.
    Le rapport sera partagé avec un groupe plus large d'utilisateurs.

Télécharger les pièces jointes du fichier sécurisé

Utilisez cette section pour comprendre comment charger les pièces jointes de fichier sécurisé dans le ou les tickets.

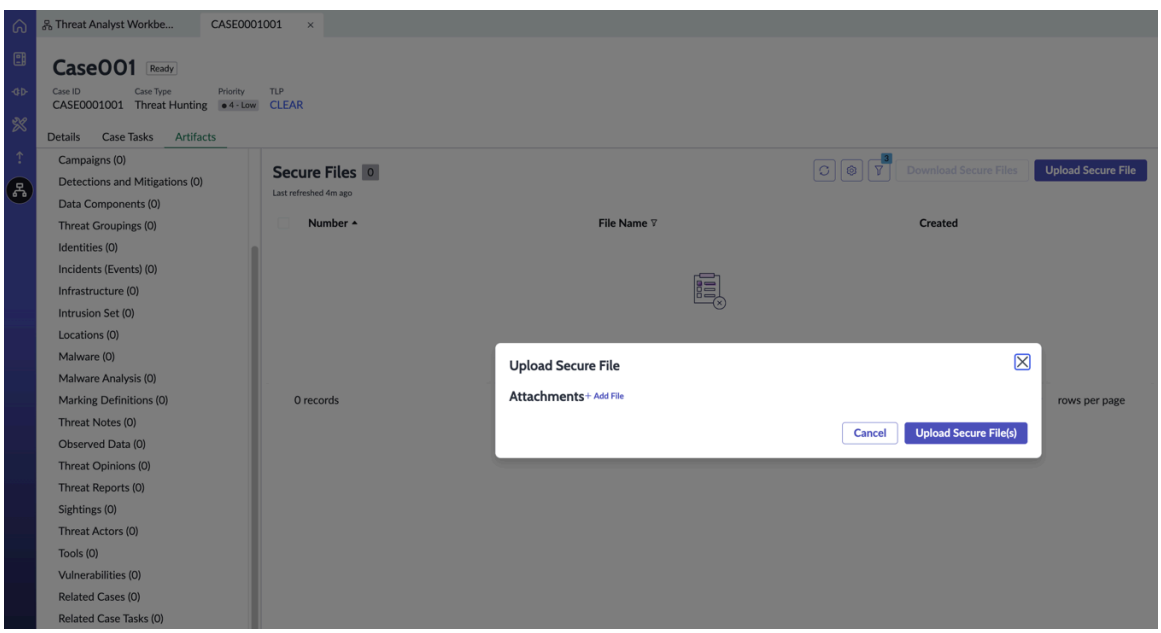
Avant de commencer

Rôle requis : sn_sec_tisc_secure_file_access, sn_sec_tiscadmin

Remarque : Les listes connexes de fichiers sécurisés ne s'affichent que lorsque vous disposez du rôle d'utilisateur sn_sec_tisc.secure_file_access.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez n'importe quel ticket.
5. Accéder à **Artifacts** > **Fichiers sécurisés** listes connexes.
6. Cliquez sur le bouton **Télécharger le fichier sécurisé** .
7. Cliquez sur **Ajouter un fichier** pour ajouter les pièces jointes.
8. Sélectionnez les fichiers et cliquez sur le bouton **Télécharger le(s) fichier(s) sécurisé(s).**
   Les pièces jointes sont téléchargées.



9. Cliquez sur **Télécharger des fichiers sécurisés** pour télécharger les pièces jointes.
   Les pièces jointes sont disponibles au format zip.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Vous pouvez également télécharger le fichier en accédant à la page des détails de l'enregistrement de fichier sécurisé.

Remarque :

- Toutes les pièces jointes sécurisées sont chiffrées et stockées dans le système à l'aide de Key Management Framework (KMF). Pour plus d'informations, consultez Chiffrement des pièces jointes .
- Si les utilisateurs ont un abonnement au *ServiceNow Hub d'intégration* **programme d'installation du pack professionnel**, les fichiers sécurisés sont compressés au format ZIP, puis cryptés et stockés

Centre de sécurité des renseignements sur les menaces Bibliothèque

Une bibliothèque de menaces est définie comme un groupe d'objets et d'entités organisés qui fournissent aux organisations des informations structurées et non structurées sur les menaces de sécurité.

Les informations sur les menaces sont disponibles sous forme de flux. Les flux vous fournissent des données précieuses sur les menaces provenant de sources telles que STIX, MISP, etc., qui répertorient les entités de renseignements sur les menaces.

La bibliothèque Threat Intelligence Security Center explique comment parcourir les données, en effectuant des recherches de base et avancées, et en filtrant des règles, invoquer l'assistant d'importation, ajouter manuellement des enregistrements Threat Intelligence, prendre les mesures nécessaires telles que l'ajout à la liste d'autorisation, la liste de refus et la liste de surveillance.

La vue détaillée fournit des aperçus aux enregistrements Intelligence et, à partir des vues de listes, vous pouvez effectuer des actions rapides sur un ou plusieurs enregistrements.

Présentation du modèle de données

Le modèle de données et l'architecture du module Centre de sécurité des renseignements sur les menaces sont conçus pour prendre en charge les options de la plateforme de renseignements sur les menaces et différentes vues de sécurité qui fournissent des données détaillées aux analystes des menaces.

Le modèle de données contient les structures de données qui sont représentées en tant qu'objets dans le référentiel Threat Intelligence.

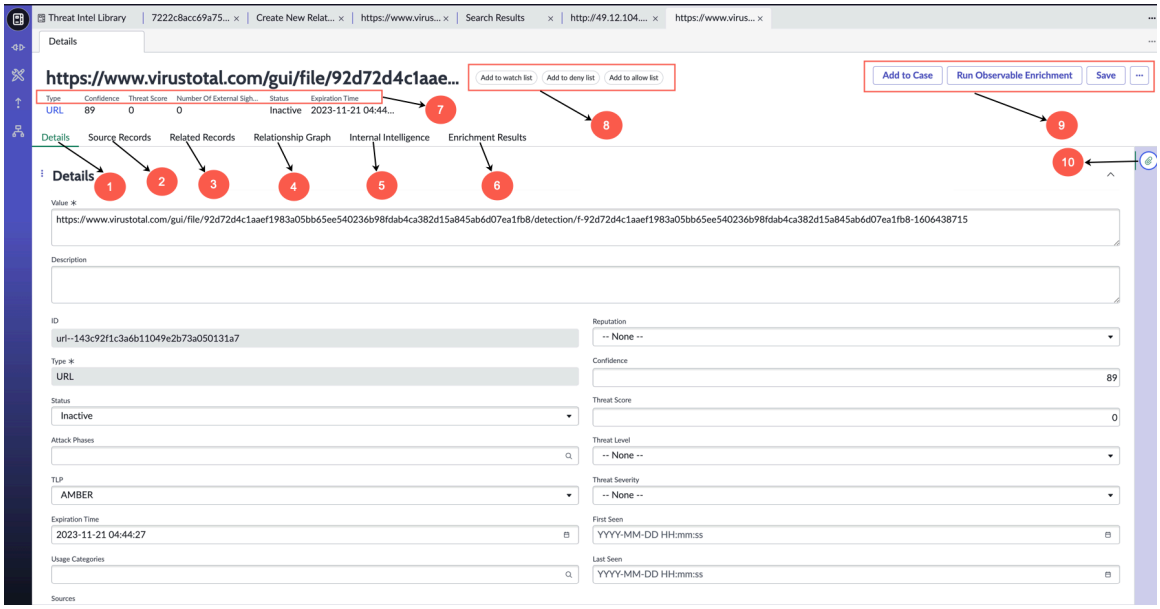
TISC Vue du formulaire Objets de bibliothèque

La Centre de sécurité des renseignements sur les menaces page d'accueil des objets comporte les fonctionnalités suivantes.

Utilisez ou accédez aux sections suivantes pour en savoir plus sur chaque SDO en détail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



TISC Vue du formulaire des objets de bibliothèque

Ordre	Menu/Onglet	Description
1	Onglet **Détails**	Utilisez cette section pour afficher ou modifier les SDO dans la vue de formulaire.
2	**Onglet Enregistrements sources**	Les enregistrements sources contribuent à un enregistrement agrégé tel qu'affiché dans la vue de formulaire. Ces enregistrements sources sont créés automatiquement à partir de flux ou créés manuellement par l'utilisateur.
3	Onglet **Enregistrements connexes**	Répertorie tous les enregistrements connexes associés au SDO.
4	**Onglet Graphe des relations**	Représentation visuelle des objets connexes.
5	**Onglet Intelligence interne**	Répertorie les enregistrements d'intelligence interne des objets associés.
6	**Onglet Résultats de l'enrichissement**	Répertorie les intégrations d'enrichissement associées aux objets.
7	**Bannière de formulaire**	Il s'agit d'une section en lecture seule, qui contient les champs clés tels que le type, la confiance, le score de menace, le nombre de

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

TISC Vue du formulaire des objets de bibliothèque (suite)

Ordre	Menu/Onglet	Description
		perceptions, l'état et le délai d'expiration.
8	**Actions d'interface utilisateur de la bannière de formulaire**	Il s'agit des listes de contrôle de sécurité sur lesquelles vous pouvez cliquer si vous devez les ajouter à la liste d'autorisation, les supprimer de la liste d'autorisation (liste de refus) ou les ajouter à la liste de surveillance en fonction des observables. Cliquez pour : • Ajouter à la liste de surveillance • Ajouter à la liste de refus • Ajouter à la liste d'autorisation **Remarque :** Les actions de formulaire ne s'appliquent qu'aux observables.
9	**Actions d'interface utilisateur du formulaire**	Les actions d'interface utilisateur de formulaire disponibles sont : 1. **Ajouter au ticket** : ajoutez les objets au ticket. 2. **Exécuter l'enrichissement de l'observable** : exécutez les enrichissements sur les objets sélectionnés. 3. **Enregistrer** : sauvegarder l'enregistrement. 4. **Supprimer** : supprimer l'enregistrement.
10	**Menu contextuel de droite**	Permet d'accéder facilement aux contrôles rapides tels que les pièces jointes, les notes, etc., en fonction des tâches associées à cet objet. Cette option est disponible dans les deux onglets restants pour que l'analyste des menaces puisse y accéder en tout temps.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

TISC Vue du formulaire des objets de bibliothèque (suite)

Ordre	Menu/Onglet	Description
		Le menu contextuel permet d'accéder facilement à : 1. **Pièces jointes** : joignez n'importe quel fichier lié aux objets. **Remarque :** Chaque fois que vous créez un observable, des indicateurs ou des objets ou que vous affichez les objets existants, le volet **Pièces jointes** est par défaut affiché sur la vue de formulaire respective. Vous pouvez cliquer sur l'icône **Pièces jointes** dans le menu contextuel de droite ou accéder à **Préférences** > **Espaces de travail** et désactivez **l'option Afficher la barre latérale**. Pour plus d'informations, consultez Configurer les préférences de l'espace de travail Next Experience . 2. **Aperçus** : ajoutez toute information supplémentaire relative aux observables ou indicateurs associés à cet objet.
N/A	**Rechercher dans le navigateur**	Utilisez cette fonction de recherche pour rechercher divers objets dans la bibliothèque Threat Intelligence (TI). Par exemple, vous pouvez rechercher tous les enregistrements d'observables dans le module de bibliothèque TI.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

TISC Vue du formulaire des objets de bibliothèque (suite)

Ordre	Menu/Onglet	Description
N/A	**Rechercher dans la bibliothèque Threat Intelligence**	Utilisez cette fonction de recherche pour rechercher les enregistrements sources dans plusieurs sources en fonction de vos critères de recherche. Les résultats seront affichés dans un onglet **Résultats de recherche** distinct. Par exemple, pour une adresse IP 104.227.137.35, si vous devez rechercher les enregistrements, en entrant 104.*, la recherche réduira les enregistrements et affichera les enregistrements qui contiennent l'adresse IP commençant par 104 dans l'onglet **Résultats de recherche** distinct. • Vous pouvez également modifier les mots-clés de recherche existants dans les critères de recherche sur la même page de résultats de recherche sans revenir à la page de la bibliothèque de menaces. • De même, vous pouvez également effectuer une recherche en fonction du nom et de la description d'un enregistrement particulier. • Une fois les enregistrements filtrés et répertoriés, vous pouvez cliquer sur la vue de liste qui vous amènera à l'enregistrement respectif dans un nouvel onglet.

Référentiel de la bibliothèque TISC

Le référentiel IoC contient des objets STIX, chacun de ces objets contient une information spécifique.

Observables

Les observables représentent des propriétés avec état (telles que le hachage MD5 d'un fichier ou la valeur d'une clé de Registre) ou des événements mesurables (tels que la

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

création d'une clé de registre ou la suppression d'un fichier) qui sont pertinents pour le fonctionnement des ordinateurs et des réseaux.

Voici les types d'observables disponibles dans l'application :

- Artifact
- Numéro AS
- Répertoire
- Nom du domaine
- Adresses e-mail
- E-mail
- Objet de l'e-mail
- Fichier
- Adresse IPv4
- CIDR IPv4
- Adresse IPv6
- CIDR IPv6
- Adresse MAC
- Hachage MD5
- Nom Mutex
- Réseau
- Autre observable
- Processus
- Hachage SHA1
- Hachage SHA256
- Hachage SHA512
- Logiciel
- URL
- Compte d'utilisateur
- Clé de registre Windows
- Certificat X.509

Traduction automatique

Définir un observable

Les observables peuvent être récupérés à partir de l'ingestion de flux planifiée ou de l'assistant d'importation. Toutefois, vous pouvez créer des observables selon vos besoins.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **Observables** > **Tous les observables**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez le **type d'observable**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le formulaire Créer un nouvel enregistrement d'observable s'affiche.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

4. Renseignez les champs du formulaire.

Remarque : Chaque fois que vous créez un observable ou que vous affichez les observables existants, le volet **Pièces jointes** est par défaut affiché dans la vue de formulaire. Vous pouvez cliquer sur l'icône Pièces jointes dans le menu contextuel de droite ou accéder à **Préférences** > **Espaces de travail** et désactivez **l'option Afficher la barre latérale**. Pour plus d'informations, consultez Configurer les préférences de l'espace de travail Next Experience .

Section Détails

Champ	Description
Valeur	Valeur (par exemple, adresse IP ou hachage) associée à l'observable.
Description	Description de l'enregistrement de l'observable.
Auteur	Saisissez le nom.
Type	Type de classification de l'observable tel qu'une adresse IP, un nom de domaine, un artefact, un répertoire, un fichier ou un hachage. Par défaut, cette option s'affiche lorsque vous sélectionnez le nouvel enregistrement.
Statut	État actif ou inactif de l'observable.
Phases d'attaque	Représente la phase d'attaque dans une kill chain telle que LM, MITRE ATT&CK.
TLP	Valeur unique qui indique le paramètre de sensibilité des données par TLP.
Réputation	Spécifie la réputation malveillante de l'observable.
Statut	Saisissez l'état de l'observable s'il est actif ou inactif.
Score de menace	Indique le score de menace pour cet observable.
Délai d'expiration	Spécifie le délai d'expiration de l'enregistrement de l'observable.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Fiabilité	Entrez la confiance pour cet enregistrement d'observable.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La propriété de confiance identifie la confiance que le créateur a dans l'exactitude de ses données. La valeur de confiance DOIT être un nombre compris entre 0 et 100.
Empêcher les mises à jour système	Définir ce marqueur sur vrai empêchera le système de remplacer les valeurs des champs de l'enregistrement.
Est un faux positif	Marqueur booléen qui indique si l'observable est identifié comme faux positif.

Attributs

Champ	Description
Résolution à	Spécifie une liste de références à une ou plusieurs adresses IP ou noms de domaine auxquels le nom de domaine est résolu.
Est FQDN	Un nom de domaine complet (FQDN) est l'adresse complète d'un hôte Internet ou d'un ordinateur. Il fournit son emplacement exact dans le système de noms de domaine (DNS) en spécifiant le nom d'hôte, le nom de domaine et le domaine de premier niveau (TLD).

Informations supplémentaires

Champ	Description
Niveau de menace	Indique le niveau de menace de l'enregistrement de l'observable.
Premier vu	Heure à laquelle cet enregistrement observable a été vu pour la première fois en train d'effectuer des activités malveillantes.
Gravité de la menace	Indique la gravité de la menace pour l'enregistrement de l'observable.
Dernier observé	Heure à laquelle cet enregistrement observable a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Catégories d'utilisation	Catégories sous lesquelles appartient l'observable, telles que le botnet ou le phishing.
Phases d'attaque	Représente la phase d'attaque dans une kill chain telle que LM, MITRE ATT&CK.
Contexte supplémentaire	Ajoutez un contexte supplémentaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sources	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.

Important : Score rapporté de la source : ce champ contient la valeur agrégée des scores de menace signalés par les sources à partir desquelles l'observable est ingéré. Pour afficher ce champ sur le formulaire d'enregistrement d'observable, vous devez l'ajouter manuellement, car il n'est pas disponible par défaut.

Attributs

Champ	Description
Résolution à	Spécifie une liste de références à une ou plusieurs adresses IP ou noms de domaine auxquels le nom de domaine est résolu.
Est FQDN	Un nom de domaine complet (FQDN) est l'adresse complète d'un hôte Internet ou d'un ordinateur. Il fournit son emplacement exact dans le système de noms de domaine (DNS) en spécifiant le nom d'hôte, le nom de domaine et le domaine de premier niveau (TLD).

Remarque : Les attributs FQDNRésolus dans et Est ne sont applicables qu'au type **Nom de domaine** des observables.

Attributs de type d'observable

Nom d'attribut	Types d'attributs
Artifact	◦ Clé de déchiffrement ◦ Algorithme de chiffrement ◦ Hachage MD5 ◦ Type MIME ◦ Hachage SHA1 ◦ Hachage SHA256 ◦ Hachage SHA512 ◦ URL
Numéro AS	◦ Nom ◦ RIR
Répertoire	◦ Heure de création du répertoire ◦ Heure du dernier accès au répertoire ◦ Heure de la dernière modification du répertoire ◦ Chemin d'accès codé

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom d'attribut	Types d'attributs
Nom du domaine	◦ Est FQDN ◦ Résolution à
Adresses e-mail	◦ Nom d'affichage ◦ Corps de l'e-mail ◦ Destinataires d'e-mail Bcc ◦ Destinataires d'e-mail Cc ◦ Destinataires d'e-mail à ◦ Expéditeur d'e-mail ◦ Objet de l'e-mail ◦ Date d'envoi
Fichier	◦ Informations supplémentaires ◦ Nom de fichier codé ◦ Heure de création du fichier ◦ Heure du dernier accès au fichier ◦ Heure de la dernière modification du fichier ◦ Nom du fichier Nombre magique ◦ Hachage MD5 ◦ Type MIME ◦ Hachage SHA1 ◦ Hachage SHA256 ◦ Hachage SHA512
Adresse IPv4	◦ Numéro AS ◦ Adresse MAC
CIDR IPv4	◦ Numéro AS ◦ Adresse MAC
Adresse IPv6	◦ Numéro AS ◦ Adresse MAC
CIDR IPv6	◦ Numéro AS ◦ Adresse MAC
Réseau	◦ Octets de destination ◦ Nombre de paquets de destination ◦ Port de destination ◦ Heure de fin ◦ Longueur de corps de message HTTP

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom d'attribut	Types d'attributs
	◦ En-tête de demande HTTP ◦ Méthode de demande HTTP ◦ Valeur de demande HTTP ◦ Version de demande HTTP ◦ Octet de code ICMP ◦ Octet de type ICMP ◦ Le réseau est-il actif ? ◦ L'embase bloque-t-elle ? ◦ L'embase est-elle à l'écoute ? ◦ Protocoles réseau ◦ Famille d'adresses d'embases ◦ Descripteur d'embase ◦ Traitement d'embase ◦ Options d'embase ◦ Type d'embase Nombre d'octets source ◦ Nombre de paquets source ◦ Port source ◦ Heure de début ◦ Marqueurs de destination TCP ◦ Marqueurs source TCP
Processus	◦ ASLR activée ◦ Ligne de commande ◦ Répertoire de travail actuel (CWD) ◦ DEP activée ◦ Variables environnementales ◦ Est masqué ◦ SID du propriétaire ◦ ID de processus ◦ Priorité ◦ Heure de création de processus ◦ Descriptions des services ◦ Nom d'affichage du service ◦ Nom du groupe de services ◦ Nom de service ◦ Type de démarrage de service ◦ État de service Type de service ◦ Information sur le démarrage

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom d'attribut	Types d'attributs
	◦ Niveau d'intégrité Windows ◦ Titre de la fenêtre
Logiciel	◦ Common Platform Enumeration (CPE) ◦ Langues prises en charge ◦ Identification logicielle (SWID) ◦ Version du fournisseur
Compte d'utilisateur	◦ Heure de création du compte ◦ Délai d'expiration du compte ◦ Connexion au compte ◦ Type de compte ◦ Informations supplémentaires ◦ Peut escalader les privilèges ◦ Heure de la dernière modification des informations d'identification ◦ Nom d'affichage ◦ Heure de la première connexion ◦ Le compte est-il désactivé ? ◦ Est doté de privilèges ◦ Est un compte de service ◦ Heure de la dernière connexion ◦ ID d'utilisateur
Clé de registre Windows	◦ Clé modifiée ◦ Valeur d'enregistrement de l'heure ◦ Nombre de sous-clés
Certificat X.509	◦ Informations supplémentaires ◦ Identificateur de clé d'autorité ◦ Contraintes de base ◦ Politiques de certificat ◦ Points de distribution CRL ◦ Utilisation de clé étendue ◦ Empêcher toute politique ◦ Émetteur ◦ Nom alternatif de l'émetteur ◦ Est signé automatiquement ◦ Utilisation de la clé ◦ Contraintes de nom

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom d'attribut	Types d'attributs
	◦ Contraintes de politique ◦ Mappages de stratégies ◦ Date de début de validité de l'utilisation de clé privée ◦ Date de fin de validité de l'utilisation de clé privée ◦ Algorithme de signature ◦ Objet ◦ Nom alternatif du sujet ◦ Attributs du répertoire d'objet ◦ Identificateur de clé d'objet ◦ Algorithme de clé publique d'objet ◦ Exposant de clé publique d'objet ◦ Module de clé publique d'objet ◦ Date de début de validité ◦ Fin de validité ◦ Version

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour un enregistrement d'observable.

5. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
6. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à un observable.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner taxonomie	Sélectionnez la taxonomie associée à un observable.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à un observable.

Enregistrements sources

Champ	Description
Les détails des enregistrements sources d'un observable sont affichés, le cas échéant.	

Que faire ensuite

La table suivante répertorie les enregistrements connexes associés aux observables :

Enregistrements connexes

Liste connexe	Description
Observable	Liste des observables associés à cet observable. **Remarque :** Cette section contient également les relations potentielles entre deux observables. Pour plus d'informations, consultez Confirmer la relation potentielle observable-observableet consultez Définir des relations observable-observable les relations confirmées entre les deux observables.
Indicateurs	Liste des indicateurs associés à cet observable.
Schémas d'attaque	Liste des modèles d'attaque associés à cet observable.
Campagnes	Répertorier les campagnes associées à cet observable.
Infrastructure	Répertoriez l'infrastructure telle que les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées associées à cet observable.
Ensembles d'intrusion	Répertoriez les ensembles d'intrusion tels qu'un ensemble de comportements antagonistes et de ressources avec des propriétés communes associées à cet observable.
Programme malveillant	Répertorier les enregistrements sources de programme malveillant associés à cet observable.
Acteurs de menace	Répertorier les acteurs de menace associés à cet observable.
Événements de menace	Répertorier les événements de menace associés à cet observable.
Vulnérabilités	Si l'observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante et qui sont associées à cet observable.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. En outre, dans la section **Enregistrements connexes** , vous pouvez confirmer les relations entre deux observables à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire **Observables** . Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
3. Vous pouvez ajouter des observables aux tickets. Pour plus d'informations, consultez Ajouter au ticket.
4. Vous pouvez également exécuter des actions d'enrichissement des observables. Pour plus d'informations, consultez Exécuter des actions d'enrichissement dans un ticket.

Enregistrements sources des observables

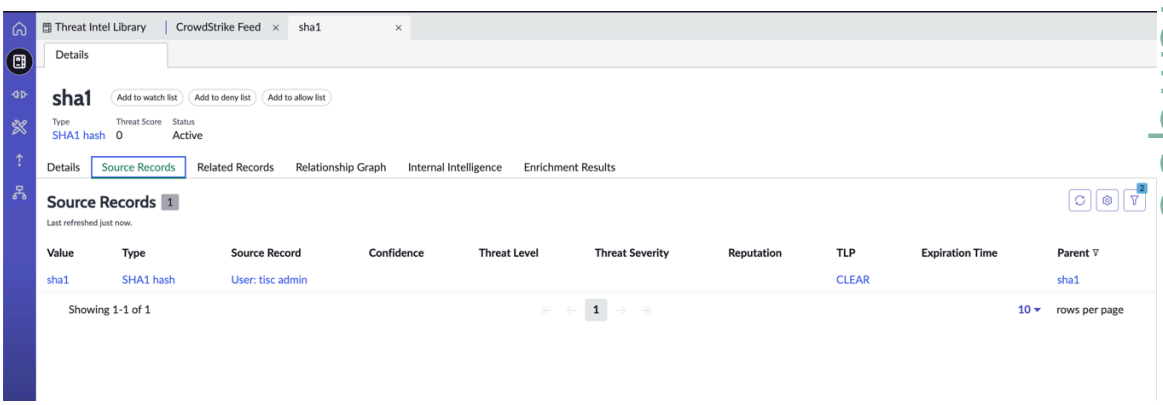
Les enregistrements sources contribuent à un enregistrement agrégé tel qu'affiché dans la vue de formulaire. Ces enregistrements sources sont créés automatiquement à partir de flux ou créés manuellement par l'utilisateur.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Sélectionnez un ou plusieurs observables.
5. Accédez aux **enregistrements sources**.
   Les enregistrements sources d'un enregistrement agrégé s'affichent.



6. Affichez les enregistrements.

Lier les enregistrements connexes aux renseignements sur la menace

Liez les enregistrements connexes associés aux objets de connaissance de la menace correspondants.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **Observables** > **Tous les observables**.
2. Sélectionnez n'importe quel enregistrement d'observable comme exemple.
3. Accédez à la section **Enregistrements connexes** .
4. Sélectionnez un enregistrement connexe.
5. Cliquez sur **Lier**.
   La boîte de dialogue Lier les objets s'affiche.
6. Sélectionnez les objets de la liste et cliquez sur le bouton **Lier** .
   Les objets associés à un enregistrement observable seront liés et affichés dans la vue de liste Enregistrements connexes.
7. Cliquez sur **Enregistrer**.
   Cliquez sur le bouton **Dissocier** pour dissocier les objets

Extraire les données des observables

Extraire les données des enregistrements connexes des observables.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **Observables**.
   Les observables associés à l'objet sélectionné s'affichent.
4. Sélectionnez n'importe quel enregistrement d'observable.
   Si des CVE sont associées aux observables donnés, vous pouvez extraire automatiquement leurs données associées à la vulnérabilité à l'aide du bouton fourni, et ces enregistrements associés s'affichent dans la section Contexte métier des vulnérabilités.
5. Accéder à **Intelligence interne** > **Entrées vulnérables**.
   Les enregistrements CVE associés pour les observables s'affichent.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

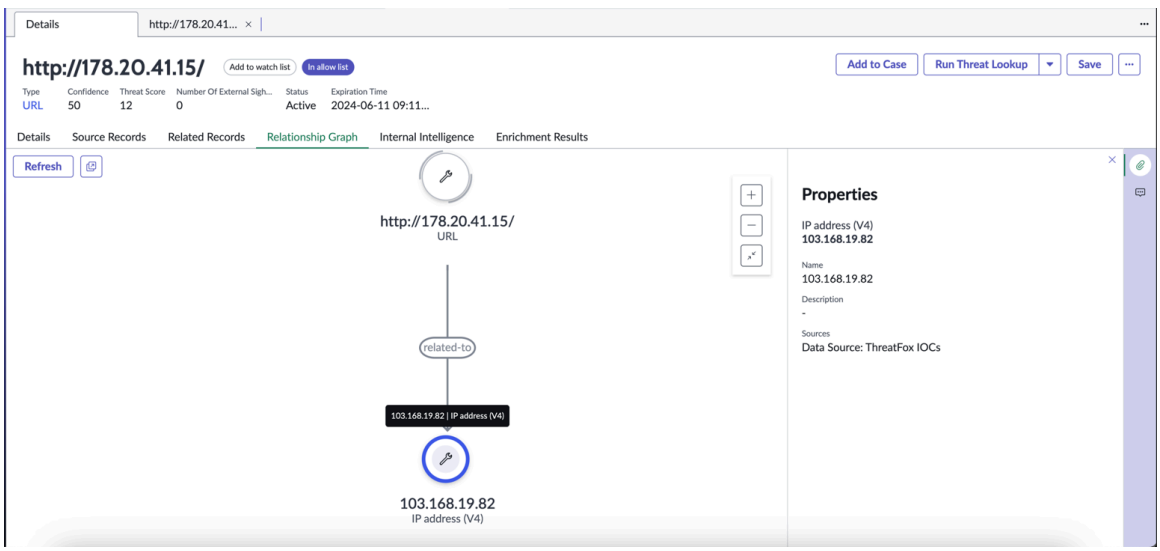
6. Sélectionnez n'importe quel CVE et cliquez sur le bouton **Extraire les données associées à la vulnérabilité** .

Remarque :

- Un message d'information affiche indiquant que cet objet de vulnérabilité spécifique n'a aucune entrée vulnérable qui lui est associée. Vous devez associer le ou les objets aux entrées vulnérables pour extraire les données. Pour plus d'informations, Extraire les données de vulnérabilité reportez-vous à la section Comment lier les enregistrements et effectuer la tâche planifiée pour extraire les données. et pour plus d'informations sur les travaux planifiés, consultez Travaux planifiés .
- Ce bouton déclenche une tâche planifiée en arrière-plan, et les détails de lancement et d'exécution de la tâche sont affichés dans la section Flux d'activité. Par exemple, lorsque le travail est déclenché, le flux d'activité affiche une activité qui a commencé à extraire les données associées aux entrées vulnérables. La tâche planifiée en arrière-plan vérifie en permanence tous les observables ayant une entrée vulnérable associée à l'observable et s'exécute automatiquement, et cette tâche planifiée s'exécute toutes les heures. Si les enregistrements ne sont pas récupérés, vous pouvez les lier manuellement et récupérer les données.

Afficher les détails dans le visualiseur

À l'aide du visualiseur, vous pouvez afficher les relations entre les objets, les observables et les indicateurs, ce qui vous fournit un contexte pour approfondir l'enquête. Le visualiseur utilise des couleurs et des icônes pour illustrer diverses informations sur les objets.



Vous pouvez faire ce qui suit :

- Effectuez un zoom avant sur n'importe quel objet, adaptez-le à l'écran, faites glisser les nœuds ou épinglez-les pour vous concentrer sur une relation particulière.
- Cliquez sur n'importe quel objet pour ouvrir le volet de détails. Dans le volet de détails, vous pouvez obtenir plus d'informations associées à l'objet. Vous pouvez afficher les propriétés du nœud telles que Objet, Nom de l'objet, Description et Sources. Par défaut, la section des détails de chaque nœud du graphique n'est pas affichée et vous devez cliquer sur chaque nœud du graphique pour afficher les détails du nœud sélectionné.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le visualiseur est disponible pour tous les objets de domaine STIX (SDO), à l'exception des objets Rapport et Données observées. Cliquez sur le bouton Actualiser pour actualiser le visualiseur.

- Vous pouvez également cliquer sur l'icône contextuelle pour afficher le graphique dans une fenêtre beaucoup plus grande.

Utilisation des enregistrements de l'intelligence interne

Utilisez cette fonctionnalité pour utiliser les données de renseignement internes collectées à partir du système de gestion de base de données de configuration (CMDB) dans Centre de sécurité des renseignements sur les menaces.

Afficher les enregistrements Intelligence interne

Affichez les enregistrements d'intelligence interne collectés à partir de CMDB, Security Incident Response (SIR) et Vulnerability Response (VR).

Avant de commencer

La section Intelligence interne fournit le contexte d'autres applications de la plateforme, telles que SIR, VR et CMDB, afin de fournir aux analystes une perspective plus large de la menace.

Rôle requis : sn_sec_tisc.analyst

Remarque : L'onglet Intelligence interne n'est visible que pour les observables et les objets de vulnérabilité.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **Observables** > **Tous les observables**.
2. Sélectionnez n'importe quel enregistrement d'observable(s).
3. Accédez à l'onglet **Intelligence interne** .
   La section Intelligence interne comprend trois sous-sections telles que Security Incident Response, Business Context et Vulnerability Response.

   Remarque : Vous devez avoir installé les applications respectives sur votre instance pour que ces sections soient répertoriées dans l'onglet **Intelligence interne** .

   a. **Réponse aux incidents de sécurité** : affiche tous les incidents liés aux observables et aux éléments de vulnérabilité associés.

      Remarque : La valeur Observable(s) doit correspondre entre l'incident SIR et également dans le TISC uniquement, alors les observables ou indicateurs associés sont répertoriés dans la section Réponse aux incidents de sécurité. Vous pouvez également lier et dissocier les enregistrements en effectuant une recherche dans les enregistrements dans les systèmes sources. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.

      - Sélectionnez n'importe quel enregistrement pour parcourir et afficher les détails dans le système source. Par exemple, Observables associés dans Réponse aux incidents de sécurité pour extraire les enregistrements observables associés.
      - Dans le cadre de la version actuelle, vous trouverez ci-dessous les données de renseignement que vous pouvez extraire des enregistrements sources (SIR) :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Observables associés
- Éléments de vulnérabilité

b. **Contexte professionnel** : affiche les utilisateurs affectés et tous les autres éléments de configuration. Dans le cadre de la version actuelle, vous trouverez ci-dessous les données d'intelligence que vous pouvez extraire des enregistrements sources (contexte métier) :

- Éléments de configuration
- Services affectés
- Actifs affectés

c. **Vulnerability Response** : affiche les données d'intelligence sur les vulnérabilités.

Entrées de vulnérabilité : cette option correspond aux vulnérabilités et extrait les enregistrements connexes.

Exécuter des actions d'enrichissement à partir d'un observable

Utilisez cette section pour comprendre comment les actions d'enrichissement sont effectuées sur les observables et autres objets.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Cliquez sur les actions d'enrichissement à partir du bouton fractionner.
5. Sélectionnez la ou les implémentations disponibles.
6. Cliquez sur **Envoyer**.
   Par exemple, Exécuter une recherche de menace. L'action d'enrichissement sélectionnée sera exécutée et un message dinformation s'affichera indiquant que l'exécution de l'enrichissement de l'observable a démarré sur le ou les observables sélectionnés. Les résultats seront disponibles dans la page détaillée du ou des observables respectifs une fois l'exécution terminée.

> **Remarque :** Une fois l'exécution initiée ou terminée, une note de travail est publiée dans le flux d'activité de la vue de formulaire.

Ajouter au ticket

Ajoutez des observables, des indicateurs ou d'autres objets au ticket.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Voici la procédure qui montre comment ajouter un ticket à un enregistrement d'observable.

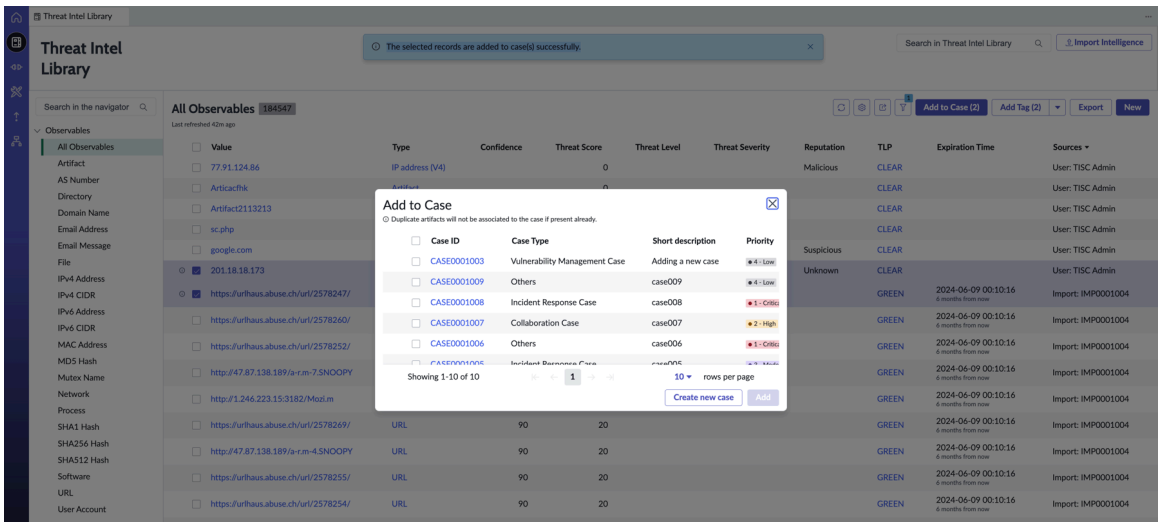
Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **Observables** > **Tous les observables**.
2. Sélectionnez le ou les observables.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **le bouton Ajouter au ticket** .
   Cela affiche uniquement les tickets pour lesquels l'enregistrement n'est pas déjà associé.



4. Vérifiez si vous souhaitez ajouter l'enregistrement aux tickets existants et, si tel est le cas, sélectionnez le ticket de sortie. Sinon, cliquez sur **Créer un ticket**.
   Créez un nouveau ticket en saisissant les informations suivantes.

Créer un nouveau ticket

Champ	Description
ID du ticket	Un identificateur unique pour le ticket. Il s'agit d'un ID généré par le système.
Description brève	Résumé de la demande ou du problème faisant l'objet de l'examen ou brève description.
Type de ticket	Sélectionnez le type de ticket faisant l'objet de l'enquête. Les options possibles pour l'enquête sont les suivantes : ◦ Chasse aux menaces ◦ Demande d'informations ◦ Ticket de gestion de la vulnérabilité ◦ Ticket de conformité ◦ Ticket de réponse aux incidents ◦ Ticket de collaboration ◦ Autres
Priorité	Une évaluation de la gravité de la demande ou du problème.
Groupe d'affectation	Groupe affecté et responsable du traitement du ticket.
Affecté à	L'analyste chargé de travailler sur un ticket.

5. Cliquez sur **Créer** si vous créez un nouveau ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le nouveau ticket est ajouté à la liste de tickets existante.

6. Sélectionnez le ou les tickets nouvellement ajoutés.
7. Cliquez sur **Ajouter**.
   Un message dinformation s'affiche indiquant que les enregistrements sélectionnés ont été ajoutés au ou aux tickets.

Exécuter les opérations d'enrichissement dans TISC

Le tableau suivant ci-dessous décrit les interactions impliquées dans l'exécution de différentes opérations d'enrichissement à partir de TISC.

Écrans du modal TISC

Option	Interactions avec les cadres de travail UX	Intégrations prises en charge
Exécuter une recherche de menace	À l'écran 1 – Sélectionnez la ou les implémentations et soumettez-les. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Exécuter une recherche de menace.	• Virus Total • Intelligence du faucon Crowd Strike
Exécuter la recherche de perception	Écran 1 – Sélectionner les implémentations et Écran 2 – Les entrées communes sont applicables. La recherche de perception utilise la date et la fréquence comme entrées communes à plusieurs implémentations de Splunk et d'autres intégrations.	• Recherche élastique • Observation Splunk
Exécuter l'enrichissement de l'élément observable	Écran 1 uniquement – Sélectionner les implémentations. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Exécuter l'enrichissement des observables.	• LE WHOIS • Shodan

Exécuter une recherche de menace

Sélectionnez une ou plusieurs implémentations, selon le cas, pour exécuter la recherche de menace sur les observables.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

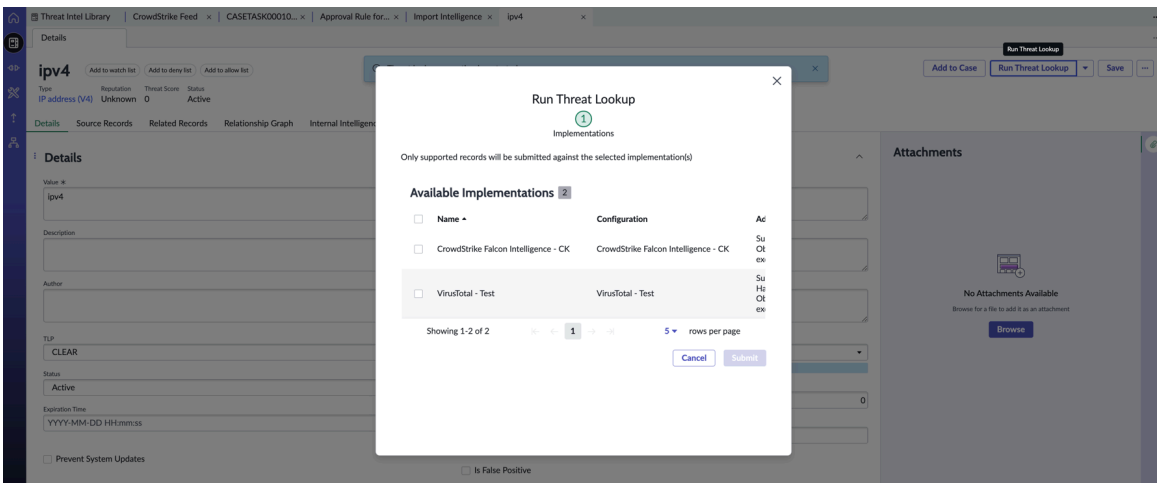
Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n'importe quel enregistrement d'observable.
5. Cliquez sur **Exécuter la recherche de menace**.
   L'écran modal Exécuter une recherche de menace **Sélectionner des implémentations** s'affiche.

   Remarque : Exécuter la recherche de menace effectue des recherches de renseignements sur les menaces pour déterminer si les observables sont associés à des menaces connues.

6. Sélectionnez la ou les implémentations requises dans la liste.



7. Cliquez sur **Envoyer**.
   L'action d'enrichissement sélectionnée sera exécutée et un message dinformation s'affichera indiquant que l'exécution de la recherche de menaces a commencé.

   Remarque :

   - Une fois l'exécution initiée ou terminée, une note de travail est publiée dans le flux d'activité de la vue de formulaire.
   - Les résultats d'enrichissement transmis à partir de l'espace de travail SIR se trouvent dans l'onglet **Résultats de l'enrichissement** de la page de détails des observables correspondants dans l'espace de travail TISC.
   - Les résultats d'enrichissement transmis par push depuis l'espace de travail SIR peuvent être identifiés à l'aide du champ **Source** de la table des résultats d'enrichissement.

Exécuter la recherche de perception

Effectuez l'intégration connexe Exécuter la recherche de perception.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

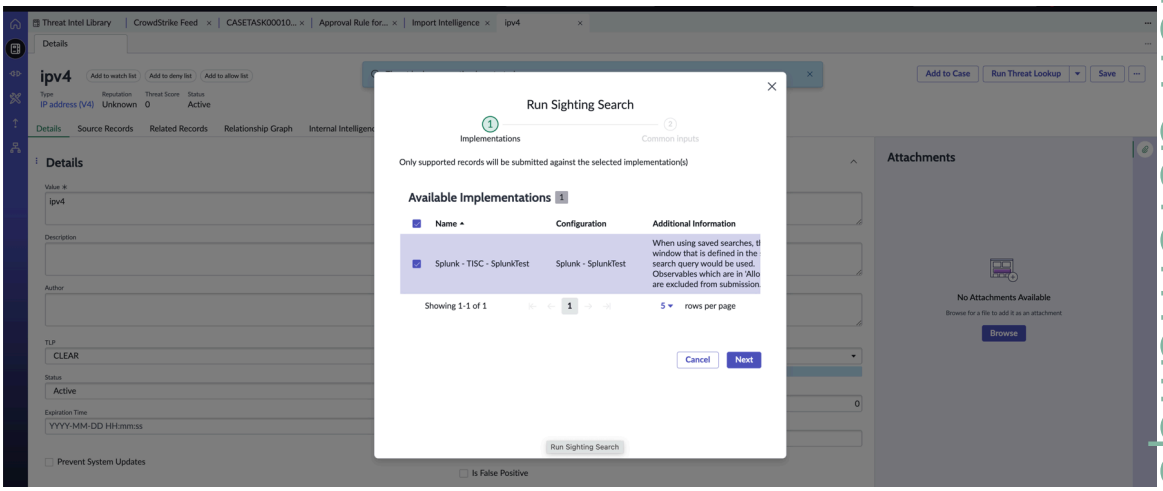
Pour effectuer cette action, sélectionnez l'implémentation et ajoutez des entrées de temps d'exécution communes qui s'appliquent à toutes les implémentations sélectionnées, le cas échéant.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n'importe quel enregistrement d'observable.
5. Cliquez sur **Exécuter la recherche de perception**.
   L'écran modal Exécuter la recherche de perception **Sélectionner les implémentations** s'affiche.

   Remarque : Exécuter la recherche de perception effectue des recherches de renseignements sur les menaces pour déterminer si les observables sont associés à des menaces connues.

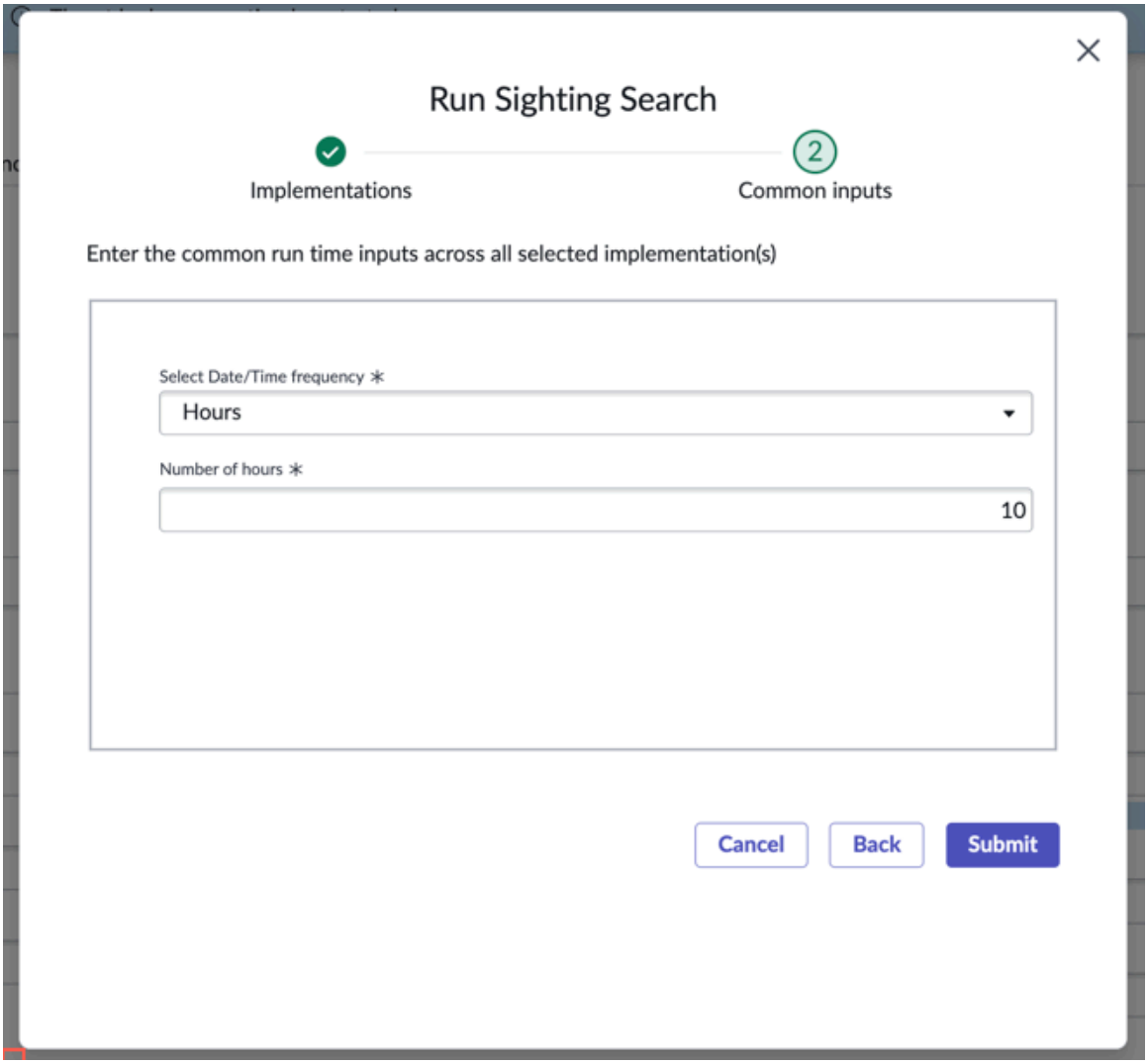
6. Sélectionnez la ou les implémentations requises dans la liste.



7. Cliquez sur **Suivant**.
8. Sélectionnez la valeur d'entrée de temps d'exécution courante, telle que Sélectionner la date/heure, la fréquence et le Nombre d'heures.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Cliquez sur **Envoyer**.
   L'action d'enrichissement sélectionnée sera exécutée et un message d'information s'affichera indiquant que l'exécution de l'exécution de la recherche de perception a commencé.

Remarque :

- Une fois l'exécution initiée ou terminée, une note de travail est publiée dans le flux d'activité de la vue de formulaire.
- Les résultats d'enrichissement transmis à partir de l'espace de travail SIR se trouvent dans l'onglet **Résultats de l'enrichissement** de la page de détails des observables correspondants dans l'espace de travail TISC.
- Les résultats d'enrichissement transmis par push depuis l'espace de travail SIR peuvent être identifiés à l'aide du champ **Source** de la table des résultats d'enrichissement.

Exécuter l'enrichissement de l'élément observable

Sélectionnez une ou plusieurs implémentations, selon le cas, pour exécuter la recherche de menace sur les observables.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Traduction automatique

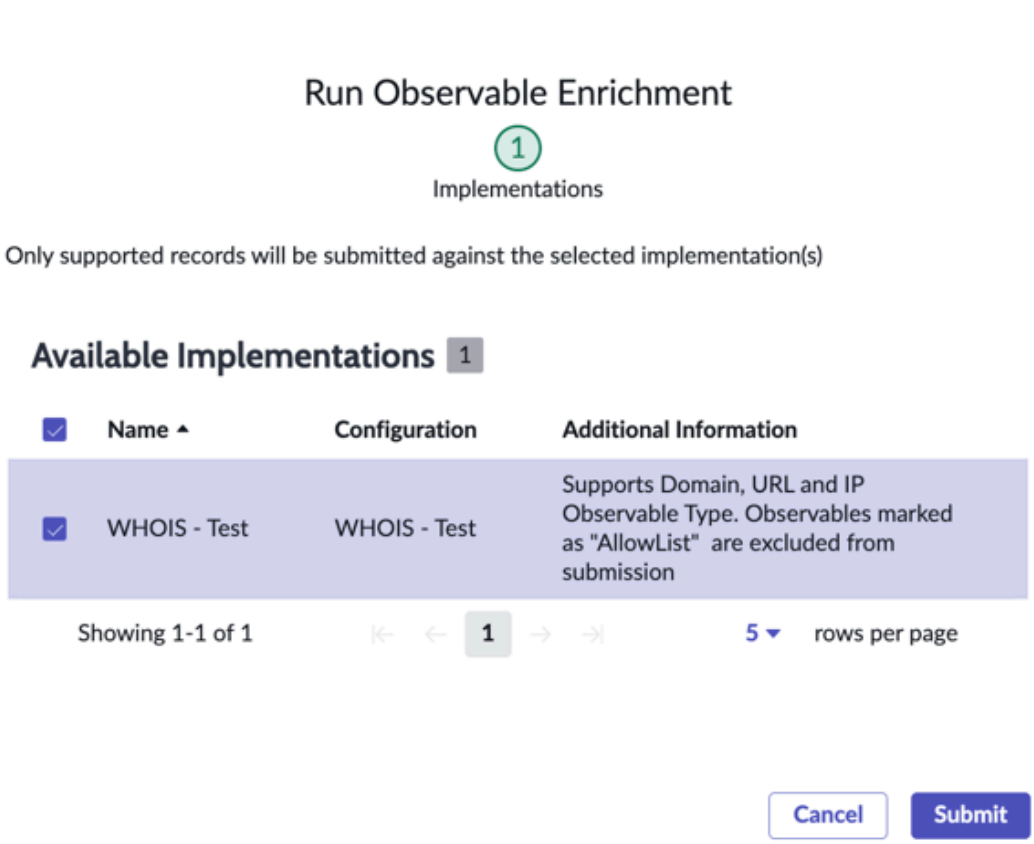
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Console de l'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n'importe quel enregistrement d'observable.
5. Cliquez sur **Exécuter l'enrichissement des observables**.
   L'écran modal Exécuter l'enrichissement de l'observable **Sélectionner les implémentations** s'affiche.

   Remarque : Seuls les enregistrements pris en charge seront soumis sur la ou les implémentations sélectionnées

6. Sélectionnez la ou les implémentations requises (par exemple, WHOIS) dans la liste.



7. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'action d'enrichissement sélectionnée sera exécutée et un message dinformation s'affichera indiquant que l'exécution de la recherche de menaces a commencé.

Remarque :

- Une fois l'exécution initiée ou terminée, une note de travail est publiée dans le flux d'activité de la vue de formulaire.
- Les résultats d'enrichissement transmis à partir de l'espace de travail SIR se trouvent dans l'onglet **Résultats de l'enrichissement** de la page de détails des observables correspondants dans l'espace de travail TISC.
- Les résultats d'enrichissement transmis par push depuis l'espace de travail SIR peuvent être identifiés à l'aide du champ **Source** de la table des résultats d'enrichissement.

Afficher les résultats de l'enrichissement

Affichez les résultats d'enrichissement des observables, des indicateurs et de divers objets.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **Observables** > **Tous les observables**.
2. Sélectionnez n'importe quel enregistrement d'observable(s).
3. Accédez à **l'onglet Résultats de l'enrichissement** .
   Les résultats de l'enrichissement affichent les résultats de l'enrichissement des intégrations TISC.

Nom d'enrichissement	Description
Résultats de la recherche de menace	Répertorie tous les résultats de la recherche de menaces associée à un observable.
Perceptions	Répertorie toutes les observations associées à un observable.
Résultats de l'enrichissement de l'observable	Répertorie tous les résultats d'enrichissement observable associés à un observable.

Indicateurs

Les indicateurs sont des artefacts observés sur un réseau ou un système d'exploitation qui sont susceptibles d'indiquer une intrusion. Les IoC typiques sont les signatures de virus et les adresses IP, les hachages MD5 de fichiers ou d'URL de logiciels malveillants ou les noms de domaine.

Définir un indicateur

Définissez un indicateur.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **Indicateurs**.
2. Sélectionnez **Indicateur**.
3. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

4. Renseignez les champs du formulaire.

Section Détails

Champ	Description
ID	ID unique de l'indicateur.
Description	Description de l'indicateur.
Nom	Nom de l'indicateur.
Modèle	Le modèle de détection de cet indicateur peut être exprimé sous la forme d'un modèle STIX.
Type de modèle	Langage du modèle utilisé dans cet indicateur.
Version du modèle	Version de la langue du modèle utilisée pour les données dans la propriété de modèle qui doit correspondre au type de données de modèle incluses dans la propriété de modèle.
Date de début de validité	Moment à partir duquel cet indicateur est considéré comme un indicateur valide des comportements auxquels il est associé ou qu'il représente.
Fin de validité	Délai après lequel cet indicateur ne doit plus être considéré comme un indicateur valide des comportements auxquels il est lié ou qu'il représente.
Classification IOC	La classification CIO des indicateurs.
Types des indicateurs	Indique les différentes catégories de l'indicateur.
Statut	Indique l'état des indicateurs.
Plateformes	Définit les plateformes auxquelles cet indicateur s'applique.
TLP	Valeur unique qui indique le paramètre de sensibilité des données par TLP.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Phases d'attaque	Représente la phase d'attaque dans une kill chain telle que LM, MITRE ATT&CK.
Fiabilité	Saisissez la confiance de cet enregistrement d'indicateur. La propriété de confiance identifie la confiance que le créateur a dans l'exactitude de ses données. La valeur de confiance DOIT être un nombre compris entre 0 et 100.
Niveau de menace	Indique le niveau de menace de l'enregistrement de l'indicateur.
Délai d'expiration	Spécifie le délai d'expiration de l'enregistrement de l'indicateur.
Gravité de la menace	Indique la gravité de la menace de l'enregistrement de l'indicateur.
Catégories d'utilisation	Catégories sous lesquelles appartient l'observable, telles que le botnet ou le phishing.
Premier vu	Heure à laquelle cet enregistrement d'indicateur a été vu pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cet enregistrement d'indicateur a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez toutes les remarques supplémentaires pour un indicateur.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet indicateur.
Version de spéc.	Version de la spécification STIX utilisée pour représenter l'indicateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Créé	Spécifie l'heure à laquelle l'indicateur est créé dans le système.
Mis à jour	Spécifie l'heure à laquelle l'indicateur est mis à jour dans le système.
Extensions	Indique les extensions de l'indicateur.
État du traitement	Représente l'état de traitement de cet indicateur.

5. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
6. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à un indicateur.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez la taxonomie associée à un indicateur.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à un indicateur.

Enregistrements sources

Champ	Description
Les détails des enregistrements sources d'un indicateur sont affichés, le cas échéant.	

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux indicateurs.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Liste connexe	Description
Références indicateurs	Liste des références externes qui décrivent cet indicateur.
Observables	Répertorie les enregistrements d'observables associés à cet indicateur.
Indicateurs	Répertorie les indicateurs associés à cet indicateur. **Remarque :** Cette section contient également les relations potentielles entre deux indicateurs. Pour plus d'informations, consultez Confirmer les relations éventuelles indicateur-indicateuret consultez Définir les relations indicateur-indicateur les relations confirmées entre les deux observables.
Éléments de configuration	Répertorie les éléments de configuration associés à cet indicateur.
Schémas d'attaque	Répertorie la source Schémas d'attaque qui décrivent les méthodes par lesquelles les adversaires tentent de compromettre les cibles associées à cet indicateur.
Campagnes	Répertorie la source de campagnes qui décrit un ensemble d'activités malveillantes ou d'attaques qui se produisent au fil du temps contre un ensemble spécifique de cibles associées à cet indicateur.
Détections et atténuations	Répertorie les détections et atténuations associées à cet indicateur.
Identités	Répertorie les identités associées à cet indicateur.
Infrastructure	Répertorie la source d'infrastructure qui décrit les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées destinés à soutenir un objectif d'une attaque et associés à cet indicateur.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources des adversaires ayant des propriétés communes associées à cet indicateur.
Emplacements	Répertorie les emplacements géographiques associés à l'objet.
Programme malveillant	Répertorie les enregistrements sources de programmes malveillants associés à cet indicateur.
Définitions de marquage	Liste les définitions de marquage associées à cet objet.
Perceptions	Répertorie les enregistrements de sources de perceptions associés à cet objet.
Acteurs de menace	Répertorie les changements associés à l'observable.
Événements de menace	Répertorie les observables associés qui ont été identifiés par la source de menace.
Outil	Répertorie l'outil associé à cet objet.
Vulnérabilités	Si l'observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. En outre, dans la section **Enregistrements connexes** , vous pouvez confirmer les relations entre deux observables à l'aide de la section **Relations potentielles** disponible dans la vue du formulaire **Indicateurs** . Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
3. Vous pouvez ajouter des indicateurs aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Schémas d'attaque

Les schémas d'attaque sont un type de tactiques, techniques et procédures (TTP) qui décrivent les méthodes par lesquelles les adversaires tentent de compromettre les cibles.

Les schémas d'attaque sont utilisés pour faciliter la catégorisation des attaques. Ils généralisent des attaques spécifiques aux modèles qu'ils suivent et fournissent des informations détaillées sur la façon dont les attaques sont exécutées.

Par exemple, le spear phishing est un type d'attaque courant qui consiste pour un attaquant à envoyer un e-mail soigneusement conçu à une partie dans le but de l'inciter à cliquer sur un lien ou à ouvrir une pièce jointe pour diffuser un logiciel malveillant. Les schémas d'attaque sont plus spécifiques, comme le spear phishing par un acteur de menace particulier (par exemple, le fait que la cible a gagné un concours) peuvent également être des schémas d'attaque.

Définir un modèle d'attaque

Définissez un modèle d'attaque pour aider les analystes de menaces à classer les attaques.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **Modèle d'attaque**.
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails du modèle d'attaque

Champ	Description
ID	ID unique d'un modèle d'attaque.
Nom	Entrez un nom pour ce modèle d'attaque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Entrez la description d'un modèle d'attaque.
Alias	Noms alternatifs permettant d'identifier ce modèle d'attaque.
Phase d'attaque	Représente la phase d'attaque dans une kill chain telle que LM, MITRE ATT&CK.
Autorisations requises	Sélectionnez les autorisations requises pour ce modèle d'attaque.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez la confiance pour ce mode de schéma d'attaque. La propriété de confiance identifie la confiance que le créateur a dans l'exactitude de ses données. La valeur de confiance DOIT être un nombre compris entre 0 et 100.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Empêcher les mises à jour système	Définir ce marqueur sur vrai empêchera le système de remplacer les valeurs des champs de l'enregistrement.

Important : Après la création d'un enregistrement d'objet, la case à cocher **Empêcher les mises à jour système** s'affiche.

Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Aperçus

Champ	Description
Notes	Ajoutez toutes les notes supplémentaires pour un modèle d'attaque.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet, le modèle d'attaque. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Créé	Spécifie l'heure à laquelle l'enregistrement est créé dans le système.
Mis à jour	Spécifie l'heure à laquelle l'enregistrement est modifié dans le système.
Extensions	Indique les extensions du schéma d'attaque.
État du traitement	Représente l'état de traitement de cet objet, modèle d'attaque.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à un observable.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à un modèle d'attaque.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à un modèle d'attaque.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au modèle d'attaque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Campagne

Une campagne est définie comme un regroupement de comportements antagonistes qui décrivent un ensemble d'activités malveillantes ou d'attaques, parfois appelées vagues, qui se produisent sur une période de temps contre un ensemble spécifique de cibles.

Définir la campagne

Définissez une campagne pour regrouper les comportements antagonistes.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **l'objet Campaign** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue Campagne

Champ	Description
ID	ID unique d'un comportement antagoniste.
Nom	Entrez un nom pour un comportement antagoniste.
Description	Saisissez une description pour cette campagne.
Objectif	L'objectif principal, l'objectif, le résultat souhaité ou l'effet escompté de la campagne. Ce que l'auteur de la menace ou l'ensemble d'intrusion espère accomplir avec cette campagne.
Alias	Noms alternatifs à identifier pour cette campagne.
TLP	Le protocole TLP (Traffic Light Protocol) indique les informations sensibles partagées avec le bon public. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité pour ce modèle d'attaque.
Fiabilité	Saisissez la confiance pour cette campagne.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour une campagne.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cette campagne.
Premier vu	Heure à laquelle cet objet a été vu pour la première fois en train d'effectuer un comportement antagoniste.
Dernier observé	Heure à laquelle cet objet a été vu pour la dernière fois en train d'effectuer un comportement antagoniste.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
État du traitement	Représente l'état de traitement de cet objet, campagne.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.

Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à une campagne.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à une campagne.
Ajouter valeurs de taxonomie	Ajouter des valeurs de taxonomie associées à la campagne.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la campagne.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensemble d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Déroulement de l'action

Un plan d'action est une action entreprise soit pour empêcher une attaque, soit pour répondre à une attaque en cours.

Le plan d'action décrit les réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu). Il peut également décrire des actions de niveau supérieur telles que la formation des employés ou des changements de politique.

Par exemple, un plan d'action pour atténuer une vulnérabilité pourrait consister à appliquer le correctif qui la corrige.

Définir le plan d'action

Définissez un plan d'action pour prévenir une attaque ou pour répondre à une attaque en cours.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **Déroulement de l'objet Action** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Déroulement de la vue des détails de l'action

Champ	Description
ID	ID unique d'un plan d'action pour prévenir une attaque.
Nom	Entrez un nom descriptif pour ce plan d'action.
Description	Description qui fournit plus de détails et de contexte sur le plan d'action, y compris potentiellement son objectif et ses caractéristiques clés.
Action	Pour capturer des plans d'action structurés ou automatisés.
TLP	Le protocole TLP (Traffic Light Protocol) indique les informations sensibles partagées avec le bon public. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité pour ce modèle d'attaque.
Fiabilité	Entrez la confiance pour ce plan d'action.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour un plan d'action.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.

Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à un observable.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner taxonomie	Sélectionnez une taxonomie associée à un modèle d'attaque.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à un modèle d'attaque.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au plan d'action.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Identité

Les identités représentent des individus, des organisations ou des groupes réels, ainsi que des classes d'individus, de systèmes ou de groupes. Les identités s'appliquent pour STIX 2.x.

Un SDO d'identité peut capturer des informations d'identification de base, des informations de contact et les secteurs auxquels l'identité appartient. L'identité représente les cibles des attaques, les sources d'information, les créateurs d'objets et les identités des acteurs de menace.

Définir les identités

Définissez les identités qui représentent des individus, des organisations ou des groupes réels.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **Objet d'identité** .
4. Cliquez sur **Nouveau**.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails d'identité

Champ	Description
ID	ID unique d'une identité.
Nom	Entrez un nom descriptif pour cette identité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Lorsqu'il s'agit d'une entité spécifique (un individu ou une organisation), cette propriété doit contenir le nom canonique de l'entité spécifique.
Description	Description qui fournit plus de détails et de contexte sur le plan d'action, y compris potentiellement son objectif et ses caractéristiques clés.
Rôles	Liste des rôles que cette identité remplit.
Classe d'identité	Type d'entité que cette identité décrit. Par exemple, personne ou organisation.
Secteurs	Liste des secteurs d'activité auxquels cette identité appartient.
Informations de contact	Les informations de contact, telles que l'adresse e-mail et le numéro de téléphone, pour cette identité.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Saisissez la confiance pour cette identité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour l'identité.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire lié à cette identité.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'identité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à l'identité.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à l'identité.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'identité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Infrastructure

Le SDO d'infrastructure représente un type de tactiques, de techniques et de procédures (TTP). Ils décrivent les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées destinés à soutenir un objectif d'une attaque. L'infrastructure s'applique pour STIX 2.x.

Les éléments d'une attaque sont représentés par d'autres SDO ou SCO. Toutefois, le SDO d'infrastructure représente un groupe nommé de données qui constitue l'infrastructure.

Des exemples d'infrastructure incluent les serveurs C2 utilisés dans une attaque, un appareil ou un serveur faisant partie d'une défense, ou les serveurs de base de données ciblés par une attaque.

Définir l'infrastructure

Définissez une infrastructure qui regroupe les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées destinés à soutenir un objectif d'une attaque.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à l'objet **Infrastructure** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue Détails de l'infrastructure

Champ	Description
ID	ID unique d'un plan d'action pour prévenir une attaque.
Nom	Entrez un nom descriptif pour ce plan d'action. Lorsqu'il s'agit d'une entité spécifique (un individu ou une organisation), cette propriété doit contenir le nom canonique de l'entité spécifique.
Description	Description qui fournit plus de détails et de contexte sur l'infrastructure, y compris potentiellement son objectif, la façon dont elle est utilisée, son lien avec d'autres activités de renseignement capturées

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	dans des objets connexes et ses principales caractéristiques.
Types d'infrastructure	Décrit la catégorisation de l'infrastructure.
Alias	Noms alternatifs permettant d'identifier cette infrastructure.
Phases d'attaque	Représente la phase d'attaque dans une kill chain telle que LM, MITRE ATT&CK.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Premier vu	Heure à laquelle cette infrastructure a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette infrastructure a été vue pour la dernière fois en train d'effectuer des activités malveillantes.
Fiabilité	Entrez la confiance pour ce plan d'action.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cette infrastructure.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cette infrastructure.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.
Mis à jour	Spécifie le moment auquel l'enregistrement est modifié dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'infrastructure.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette infrastructure.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette infrastructure.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'identité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Ensemble d'intrusion

Un ensemble d'intrusions est un ensemble groupé de comportements et de ressources antagonistes ayant des propriétés communes. Un ensemble d'intrusions implique généralement une seule organisation. L'ensemble d'intrusions s'applique à STIX 2.x.

Un ensemble d'intrusions peut capturer plusieurs campagnes ou autres activités. Ces activités partagent des attributs indiquant un acteur de menace connu ou inconnu.

Une nouvelle activité peut être attribuée à un ensemble d'intrusions, même si les auteurs de menace à l'origine de l'attaque ne sont pas connus. Les auteurs de menace peuvent passer de la prise en charge d'un ensemble d'intrusion à la prise en charge d'un autre, ou ils peuvent prendre en charge plusieurs ensembles d'intrusion.

Un ensemble d'intrusion est l'ensemble de l'attaque et peut être utilisé sur une longue période dans plusieurs campagnes pour atteindre des objectifs potentiellement multiples.

Définir l'ensemble d'intrusion

Définissez un ensemble d'intrusions, c'est-à-dire un ensemble groupé de comportements et de ressources antagonistes ayant des propriétés communes.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **Ensemble d'intrusions**.
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue des détails de l'ensemble d'intrusions

Champ	Description
ID	ID unique d'un ensemble d'intrusions.
Nom	Entrez un nom descriptif pour cet ensemble d'intrusions. Lorsqu'il s'agit d'une entité spécifique (un individu ou une organisation), cette propriété doit contenir le nom canonique de l'entité spécifique.
Description	Description qui fournit plus de détails et de contexte sur l'ensemble d'intrusions, incluant éventuellement son objectif et ses caractéristiques clés.
Alias	Noms alternatifs permettant d'identifier cet ensemble d'intrusions.
Objectifs	Les objectifs de haut niveau de cet ensemble d'intrusion, à savoir ce qu'ils essaient de faire. Par exemple, ils peuvent être motivés par un gain personnel, mais leur objectif est de voler des numéros de carte de crédit. Pour ce faire, ils peuvent exécuter des campagnes spécifiques qui ont des objectifs détaillés, comme compromettre les systèmes de point de vente d'un grand détaillant.
Premier vu	Heure à laquelle cet ensemble d'intrusion a été observé pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cet ensemble d'intrusion a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Motivation principale	La raison, la motivation ou l'objectif principal derrière cet ensemble d'intrusion. La motivation est la raison pour laquelle l'ensemble d'intrusion souhaite atteindre l'objectif (ce qu'il essaie d'atteindre).
Motivations secondaires	Les raisons, motivations ou objectifs secondaires de cet ensemble d'intrusion. Ces motivations peuvent exister en tant que cause égale ou presque égale à la motivation première. Cependant, cela ne remplace pas ou n'amplifie pas nécessairement la motivation principale, mais cela peut indiquer un contexte supplémentaire. La position dans la liste n'a aucune signification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Niveau de ressource	Cette propriété spécifie le niveau organisationnel auquel cet ensemble d'intrusion fonctionne généralement, qui à son tour détermine les ressources disponibles pour cet ensemble d'intrusion en vue d'une utilisation dans une attaque.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez la confiance pour cet ensemble d'intrusions.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet ensemble d'intrusions.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cet ensemble d'intrusions.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Créé	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.
Mis à jour	Spécifie le moment auquel l'enregistrement est modifié dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.

Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'ensemble d'intrusion.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cet ensemble d'intrusions.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à cet ensemble d'intrusions.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au jeu d'intrusion.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Emplacement

Un emplacement représente un emplacement géographique. Les emplacements sont principalement utilisés pour donner un contexte à d'autres SDO. Les emplacements s'appliquent à STIX 2.x.

L'emplacement peut contenir tout ou partie des éléments suivants : région (Amérique du Nord), adresse municipale (New York, États-Unis), latitude et longitude.

Le SDO d'emplacement peut se rapporter à un ensemble d'identité ou d'intrusion pour indiquer que l'ensemble d'identité ou d'intrusion se trouve à cet emplacement. Il peut également s'agir d'un logiciel malveillant ou d'un modèle d'attaque pour indiquer que la victime cible se trouve dans un endroit particulier.

Par exemple, un emplacement pourrait être utilisé dans une relation pour décrire que l'ensemble d'intrusion Bourgeois Swallow est originaire d'Europe de l'Est.

Au moins une des propriétés ou ensembles de propriétés suivants doit être fourni :

- région
- pays
- Latitude et longitude

Définir l'emplacement

Définissez un emplacement géographique pour fournir plus de contexte aux autres SDO.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **l'objet Emplacement** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire

Vue des détails d'identité

Champ	Description
ID	ID unique de l'emplacement.
Nom	Entrez un nom descriptif pour identifier l'emplacement.
Description	Description qui fournit plus de détails et de contexte sur l'ensemble d'intrusions,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	incluant éventuellement son objectif et ses caractéristiques clés.
Latitude	Latitude de l'emplacement en degrés décimaux. Les nombres positifs décrivent les latitudes au nord de l'équateur et les nombres négatifs décrivent les latitudes au sud de l'équateur. La valeur de cette propriété doit être comprise entre -90,0 et 90,0 respectivement.
Longitude	Longitude de l'emplacement en degrés décimaux. Les nombres positifs décrivent les longitudes à l'est du méridien d'origine et les nombres négatifs les longitudes à l'ouest du méridien d'origine. La valeur de cette propriété doit être comprise entre -180,0 et 180,0 inclus.
Précision	Définit la précision des coordonnées spécifiées par les propriétés de latitude et de longitude. Celle-ci est mesurée en mètres. L'emplacement réel peut être n'importe où jusqu'à des mètres de précision du point défini. Si cette propriété n'est pas présente, la précision n'est pas spécifiée. Si cette propriété est présente, les propriétés de latitude et de longitude doivent être présentes.
Région	Région dans laquelle se trouve cet emplacement.
Pays	Pays dans lequel se trouve cet emplacement.
Zone administrative	État, province ou autre zone administrative infranationale dans laquelle se trouve cet emplacement.
Ville	Ville dans laquelle se trouve cet emplacement.
Adresse (rue)	Adresse postale que cet emplacement décrit. Cette propriété comprend tous les aspects ou parties de l'adresse postale.
Code postal	Code postal dans lequel se trouve cet emplacement.
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des remarques supplémentaires pour cet emplacement.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet emplacement.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions pour cet emplacement.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.
Mis à jour	Spécifie le moment auquel l'enregistrement est modifié dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.

7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'emplacement.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cet emplacement.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cet emplacement.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'emplacement.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Programme malveillant

Un programme malveillant est un type de TTP qui représente un code malveillant. Il s'agit d'un programme qui est inséré secrètement dans un système. Les logiciels malveillants s'appliquent à STIX 2.x.

L'intention d'un programme malveillant est de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation (OS) de la victime.

Malware SDO caractérise, identifie et catégorise les instances et les familles de logiciels malveillants à partir de données dérivées de l'analyse. Ce SDO capture des informations détaillées sur le fonctionnement du logiciel malveillant et ce qu'il fait.

Définir les programmes malveillants

Définissez un programme malveillant qui représente un code malveillant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à l'objet Intel, menace **de programme malveillant** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails du programme malveillant

Champ	Description
ID	ID unique permettant d'identifier l'instance de programme malveillant.
Nom	Saisissez un nom pour identifier l'instance ou la famille de logiciels malveillants, tel que spécifié par le créateur du SDO. Pour une famille de logiciels malveillants, le nom doit être défini.
Description	Une description qui fournit plus de détails et de contexte sur l'instance ou la famille de logiciels malveillants, y compris potentiellement son but et ses caractéristiques clés.
Types de programmes malveillants	Indique les différentes catégories de logiciels malveillants.
Est la famille	Cochez cette case pour spécifier si l'objet représente une famille de programmes malveillants ou une instance de programme malveillant.
Alias	Noms alternatifs utilisés pour identifier ce programme malveillant ou famille de programmes malveillants.
Phases d'attaque	Représente la phase d'attaque dans une kill chain telle que LM, MITRE ATT&CK.
Premier vu	Heure à laquelle cette instance ou famille de logiciels malveillants a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette instance ou famille de programme malveillant a été vue pour

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	la dernière fois en train d'effectuer des activités malveillantes
Architectures de processus	Indique les architectures de processus pour ce programme malveillant.
Langues d'implémentation	Indique les langues d'implémentation de ce programme malveillant.
Options de logiciel malveillant	Les capacités que peut présenter une instance ou une famille de logiciels malveillants.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Saisissez la confiance de ce programme malveillant.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour l'enregistrement de programme malveillant.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cet enregistrement de programme malveillant.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, programme malveillant.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au programme malveillant.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée au programme malveillant.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées au programme malveillant.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au programme malveillant.

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Détections et atténuations	Répertorie les détections et atténuations associées à ce programme malveillant.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Analyse de programme malveillant	Répertorie les enregistrements d'analyse de programme malveillant associés à cet objet.
Programme malveillant	Répertorie les enregistrements de programmes malveillants associés à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Analyse de programme malveillant

Malware Analysis capture les métadonnées et les résultats d'un malware. L'analyse des logiciels malveillants s'applique à STIX 2.x.

L'analyse de programme malveillant comprend une analyse statique ou dynamique effectuée sur une instance ou une famille de logiciels malveillants.

Définir l'analyse de programme malveillant

Définissez une analyse de programme malveillant qui capture les métadonnées et les résultats d'une analyse statique ou dynamique particulière effectuée sur une instance ou une famille de programmes malveillants.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à l'objet **Analyse de programme malveillant** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails de l'analyse de programme malveillant

Champ	Description
ID	ID unique permettant d'identifier l'analyse de programme malveillant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Produit	Nom du moteur d'analyse ou du produit qui a été utilisé. Les noms de produits DEVRAIENT être tous en minuscules avec des mots séparés par un tiret « -« . Pour les cas où le nom d'un produit ne peut pas être spécifié, une valeur anonymisée doit être utilisée.
Version	Version du produit d'analyse qui a été utilisée pour effectuer l'analyse.
Ordinateur virtuel hôte	Description de l'environnement d'ordinateur virtuel utilisé pour héberger le système d'exploitation invité, le cas échéant, qui a été utilisé pour l'analyse dynamique de l'instance ou de la famille de programmes malveillants. Si cette valeur n'est pas incluse en conjonction avec la propriété operating_system_ref, cela signifie que l'analyse dynamique peut avoir été effectuée sur du système d'exploitation nu (c'est-à-dire sans virtualisation) ou que les informations ont été rédigées. La valeur de cette propriété DOIT être l'identificateur d'un objet logiciel SCO.
Système d'exploitation	Système d'exploitation utilisé pour l'analyse dynamique de l'instance ou de la famille de logiciels malveillants. Cela s'applique aussi bien aux systèmes d'exploitation virtualisés qu'à ceux fonctionnant sur du bare metal. La valeur de cette propriété DOIT être l'identificateur d'un objet logiciel SCO.
Version de configuration	Noms alternatifs utilisés pour identifier ce programme malveillant ou famille de programmes malveillants.
Modules	Les modules d'analyse spécifiques qui ont été utilisés et configurés dans le produit au cours de cette exécution d'analyse.
Version du moteur d'analyse	Version du moteur ou du produit d'analyse (y compris les moteurs antivirus) qui a été utilisée pour effectuer l'analyse.
Version de la définition de l'analyse	Version des définitions d'analyse utilisée par l'outil d'analyse, y compris les outils audiovisuels.
Analyse démarrée	La date et l'heure auxquelles l'analyse de programme malveillant a été lancée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Analyse terminée	Date et heure auxquelles l'analyse de programme malveillant a été terminée.
Résultat	Le résultat de la classification tel que déterminé par le processus d'analyse du scanner ou de l'outil.
Nom des résultats	Le résultat de classification ou le nom affecté à l'instance de programme malveillant par l'outil de scanner.
Soumis	Date et heure auxquelles le programme malveillant a été soumis pour la première fois à l'analyse ou à l'analyse. Cette valeur reste constante tant que la date de numérisation peut changer. Par exemple, lorsqu'un logiciel malveillant a été soumis à un outil d'analyse de virus.
Observable analysé	Sélectionnez l'observable qui a été analysé.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez la confiance pour cette analyse de programme malveillant.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour l'enregistrement de famille de programmes malveillants.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cet enregistrement de programme malveillant.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, programme malveillant.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au programme malveillant.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée au programme malveillant.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées au programme malveillant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au programme malveillant.

Enregistrements relatifs

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Programme malveillant	Répertorie les enregistrements de programmes malveillants associés à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Perception d'objets

Les observations indiquent qu'un objet a été vu. Les objets peuvent être un logiciel malveillant, un outil, un acteur de menace, etc.

Les perceptions permettent de suivre qui et quoi est la cible, comment les attaques sont menées et de suivre les tendances du comportement d'attaque.

L'objet de relation de perception contient des propriétés supplémentaires qui ne sont pas présentes dans les objets de relation génériques. Ces propriétés supplémentaires représentent des données spécifiques aux relations de perception.

Définir la perception d'objets

Définissez la perception d'objet qui décrit qu'un objet (programme malveillant, outil, acteur de menace, entre autres) a été vu.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **Objet de perception d'objet** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Choisir Entité&Valeur

Champ	Description
Entité	Sélectionnez l'enregistrement de perception d'objets d'entité. **Remarque :** Lors de toute création d'un nouvel enregistrement de perception d'objet, un enregistrement de relation associé est requis pour l'agrégation.
Perception de	Indique qu'une entité ou un indicateur particulier a été observé dans un environnement qui peut être une indication d'une menace potentielle. **Remarque :** Sélectionnez l'enregistrement associé à la perception qui est associé à l'objet sélectionné dans le champ Entité afin que les enregistrements connexes puissent maintenant être créés et regrouper les enregistrements de perception.

Vue des détails de perception d'objets

Champ	Description
ID	ID unique d'un plan d'action pour prévenir une attaque.
Description	Une description qui fournit plus de détails et de contexte sur l'observation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Premier vu	Début de la fenêtre horaire pendant laquelle le SDO a référencé par lequel la propriété a été aperçue.
Dernier observé	Fin de la fenêtre de temps pendant laquelle le SDO a référencé par lequel la propriété a été vue.
Nombre	S'il est présent, il doit s'agir d'un nombre entier compris entre 0 et 999 999 999 inclus qui représente le nombre de fois où le SDO est référencé par lequel la propriété a été aperçue.
Est une synthèse	Indique si l'observation doit être considérée comme les données récapitulatives. Les données récapitulatives sont une agrégation des rapports d'observations précédents et ne doivent pas être considérées comme des données de source primaire.
Est interne	Indique si la perception est interne.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez la confiance pour ce plan d'action.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet ensemble d'intrusions.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'identité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette infrastructure.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette infrastructure.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la perception d'objets.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Objets	Répertorie les objets associés aux observations.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Données observées

Les données observées transmettent des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX. Les données observées s'appliquent à STIX 2.x.

Les données observées capturent à la fois une observation unique d'une seule entité (fichier, connexion réseau) ainsi que l'agrégation de plusieurs observations d'une entité.

Vous pouvez utiliser les données observées seules (sans relations) pour transmettre des données brutes collectées à partir de n'importe quelle source. Les sources comprennent les rapports d'analyste, les bacs à sable et les outils de détection basés sur le réseau et l'hôte.

Par exemple, les données observées peuvent capturer des informations sur une adresse IP, une connexion réseau, un fichier ou une clé de registre. Les données observées ne sont pas une affirmation de renseignement, ce sont simplement des informations brutes sans aucun contexte pour ce qu'elles signifient.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir les données observées

Transmet des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **l'objet de données observées** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails des données observées

Champ	Description
ID	ID unique permettant d'identifier les données observées.
Premier observé	Heure à laquelle les données ont été vues initialement.
Derniers observés	La dernière fois que les données ont été vues.
Nombre observé	Le nombre de fois où chaque objet cyber-observable a été vu. La valeur doit être un entier compris entre 1 et 999 999 999.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Saisissez le score de confiance pour les données observées
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour ces données observées.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ces données observées.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées aux données observées.
Ajouter des balises	Ajouter de nouvelles balises.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ces données observées.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à ces données observées.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux données observées.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Acteur de menace

Les auteurs de menace sont des individus, des groupes ou des organisations qui agissent avec des intentions malveillantes. Les acteurs de menace postulent pour STIX 2.x.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un acteur de menace n'est pas un ensemble d'intrusion, mais il peut soutenir ou être affilié à divers ensembles d'intrusion, groupes ou organisations au fil du temps.

Les acteurs de menace utilisent leurs ressources, ainsi que les ressources d'un ensemble d'intrusions, pour mener des attaques et mener des campagnes contre des cibles.

Vous pouvez identifier les acteurs de menace en fonction de leurs motivations, de leurs capacités, de leurs objectifs, de leur niveau de sophistication, de leurs activités passées, des ressources auxquelles ils ont accès et de leur rôle au sein de l'organisation.

Définir un acteur de menace

Définissez les acteurs de menace comme étant des individus, des groupes ou des organisations qui agissent avec des intentions malveillantes.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à l'objet **Acteur de menace** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails de l'acteur de menace

Champ	Description
ID	ID unique d'un plan d'action pour prévenir une attaque.
Nom	Entrez un nom descriptif pour identifier l'emplacement.
Description	Description qui fournit plus de détails et de contexte sur l'ensemble d'intrusions, incluant éventuellement son objectif et ses caractéristiques clés.
Alias	Une liste d'autres noms permettant d'identifier cet acteur de menace.
Objectifs	Les objectifs de haut niveau de cet acteur de la menace, c'est-à-dire ce qu'il essaie de faire. Par exemple, ils peuvent être motivés par un gain personnel, mais leur objectif est de voler des numéros de carte de crédit.
Types d'acteurs de menace	Le(s) type(s) de cet acteur de menace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Rôles d'acteur de menace	Les différents rôles d'acteur de menace pour cet objet.
Premier vu	L'heure à laquelle cet acteur de menace a été vu pour la première fois. Cette propriété est une propriété récapitulative des données provenant des observations et d'autres données qui peuvent ou non être disponibles dans STIX. Si de nouvelles observations sont reçues qui sont antérieures au premier horodatage vu, l'objet peut être mis à jour pour tenir compte des nouvelles données.
Dernier observé	Heure à laquelle cet acteur de menace a été vu pour la dernière fois.
Motivation principale	La raison, la motivation ou l'objectif principal de cet acteur de menace. La motivation est la raison pour laquelle l'auteur de menace souhaite atteindre l'objectif (ce qu'il essaie d'atteindre). Par exemple, un acteur de menace dont l'objectif est de perturber le secteur financier d'un pays peut être motivé par une haine idéologique du capitalisme.
Sophistication	Les compétences, les connaissances spécifiques, la formation spéciale ou l'expertise qu'un auteur de menace doit posséder pour effectuer l'attaque.
Motivations secondaires	Cette propriété indique les raisons, motivations ou objectifs secondaires qui sous-tendent cet acteur de menace. Ces motivations peuvent exister en tant que cause égale ou presque égale à la motivation première. Cependant, cela ne remplace pas ou n'amplifie pas nécessairement la motivation principale, mais cela peut indiquer un contexte supplémentaire. La position dans la liste n'a aucune signification.
Niveau de ressource	Le niveau organisationnel auquel cet acteur de menace travaille généralement, qui à son tour détermine les ressources dont il dispose pour une utilisation dans une attaque. Cet attribut est lié à la propriété de sophistication : un niveau de ressource spécifique implique que l'acteur de menace a accès à au moins un niveau de sophistication spécifique.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet acteur de menace.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.

Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'acteur de menace.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cet acteur de menace.
Ajouter valeurs de taxonomie	Ajouter les valeurs de taxonomie associées à cet acteur de menace.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'acteur de menace.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Liste des emplacements associés à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Événement de menace

Événement ou situation susceptible d'entraîner des conséquences ou un impact indésirables.

L'attaque d'un site Web par un pirate informatique constitue un événement menaçant. Si les pirates parviennent à endommager un site Web ou à voler des informations, cela sera défini comme un événement menaçant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir l'événement de menace

Définissez un événement de menace lorsqu'un événement entraîne l'accès non autorisé à des informations non publiques et l'acquisition de celles-ci, ou la perturbation ou l'utilisation abusive d'un système d'information.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **l'objet Événement de menace** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails de l'acteur de menace

Champ	Description
ID	ID unique d'un plan d'action pour prévenir un événement de menace.
Nom	Entrez un nom descriptif pour identifier l'événement de menace.
Description	Description qui fournit plus de détails et de contexte sur l'événement de menace, incluant potentiellement son objectif et ses caractéristiques clés.
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet acteur de menace.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

Traduction automatique

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.

Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'événement de menace.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cet événement de menace.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cet événement de menace.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'événement de menace.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Regroupement des menaces

Un objet Regroupements de menaces déclare explicitement que les objets STIX référencés ont un contexte partagé. Le regroupement des menaces s'applique à STIX 2.x.

Un objet Regroupements de menaces représente un ensemble de données qui, si elles sont suffisamment analysées, arrivent à maturité pour transmettre un rapport d'incident ou de menace en tant qu'objet de rapport STIX. Par exemple, un regroupement peut être utilisé pour caractériser une enquête en cours sur un événement ou un incident de sécurité.

Un objet Groupes de menaces peut également être utilisé pour affirmer que les objets STIX référencés sont liés à un processus d'analyse en cours. Par exemple, un analyste des menaces peut collaborer avec d'autres membres de sa communauté de confiance pour examiner une série de campagnes et d'indicateurs.

Le SDO de regroupement de menaces contient une liste de références aux SDO, SCO et SRO, ainsi qu'une déclaration explicite du contexte partagé par le contenu, une description textuelle et le nom du groupement.

Définir le regroupement des menaces

Définissez les regroupements de menaces comme des objets qui ont un contexte partagé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure
1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **l'objet Regroupement de menaces** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails de regroupement de menaces

Champ	Description
ID	ID unique d'un plan d'action pour empêcher qu'une attaque de type Groupe de menaces ne se produise.
Nom	Entrez un nom descriptif pour identifier le groupe de menaces.
Description	Description qui fournit plus de détails et de contexte sur l'événement de menace, incluant potentiellement son objectif et ses caractéristiques clés.
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour ce regroupement de menaces.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au regroupement de menaces.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ce regroupement de menaces.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à ce regroupement de menaces.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au regroupement de menaces.

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Note de menace

Une note de menace transmet un texte informatif pour fournir une analyse supplémentaire qui n'est pas contenue dans les objets STIX, les objets de définition de marquage ou les objets de contenu linguistique auxquels la note se rapporte. Les notes de menace s'appliquent à STIX 2.x.

Par exemple, un analyste peut ajouter une note à un objet Campaign créé par une autre organisation. La note peut indiquer qu'ils ont vu des messages liés à cette campagne sur un forum de hackers.

Les notes sont généralement créées par des analystes humains et sont composées de texte orienté humain, elles contiennent une propriété supplémentaire pour capturer l'auteur qui a créé la note.

Définir une note de menace

Définissez les notes de menace qui transmettent des informations pour fournir un contexte ou une analyse supplémentaire qui n'est pas disponible dans les objets existants.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **la note de menace**.
4. Cliquez sur **Nouveau**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails de la note de menace

Champ	Description
ID	ID unique d'une note de menace.
Abstrait	Spécifiez un bref résumé du contenu de la note.
Contenu	Spécifie le contenu de la note.
Auteurs	Spécifie le nom de l'auteur (par exemple, un analyste).
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cette note de menace.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au regroupement de menaces.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ce regroupement de menaces.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à ce regroupement de menaces.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la note de menace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Opinion sur la menace

Une opinion est une évaluation de l'exactitude des informations contenues dans un objet STIX produit par une entité différente. Les avis sur les menaces s'appliquent pour STIX 2.x.

La propriété opinion capture le niveau d'accord ou de désaccord à l'aide d'une échelle fixe. L'échelle fixe prend également en charge un mappage numérique pour permettre des opérations statistiques cohérentes entre les opinions.

Par exemple, un analyste d'une organisation consommatrice peut dire qu'il est « fortement en désaccord » avec un objet de campagne et expliquer pourquoi.

Les opinions sont subjectives et le cahier des charges n'aborde pas la meilleure façon de les interpréter.

Les analystes humains créent des opinions et sont composés de texte orienté vers l'humain, ils contiennent une propriété supplémentaire pour capturer l'auteur qui a créé l'opinion.

Définir l'opinion sur la menace

Définissez les opinions sur les menaces comme une évaluation de l'exactitude des informations contenues dans un objet STIX.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à l'objet Opinion sur les **menaces** .
4. Cliquez sur **Nouveau**.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Renseignez les champs du formulaire.

Vue des détails de l'opinion sur la menace

Champ	Description
ID	ID unique d'une opinion sur les menaces.
Avis	L'avis du producteur sur l'objet STIX.
Explication	Spécifie le contenu de l'opinion.
Auteurs	Spécifie le nom de l'auteur (par exemple, un analyste).
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez la confiance pour ce plan d'action.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet avis sur la menace.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet avis sur la menace.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.
Mis à jour	Spécifie le moment auquel l'enregistrement est modifié dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'opinion sur les menaces.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette opinion sur la menace.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette opinion sur la menace.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'opinion sur la menace.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
	propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Rapport de menace

Les rapports de menace sont des collections de renseignements sur les menaces axées sur un ou plusieurs sujets. Les rapports de menace s'appliquent pour STIX 2.x.

Les rapports de menace comprennent une description d'un acteur de menace, d'un programme malveillant, d'une technique d'attaque, y compris le contexte et des détails connexes. Ils sont utilisés pour regrouper les renseignements sur les menaces connexes afin qu'ils puissent être publiés sous la forme d'une histoire complète sur les cybermenaces.

Le SDO de rapport de menace contient une liste de références aux objets STIX ainsi qu'une description textuelle et le nom du rapport.

Définir le rapport de menace

Définissez des rapports de menace qui décrivent un acteur de menace, un programme malveillant ou une technique d'attaque, y compris le contexte et les détails connexes.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à l'objet **Rapport de menace** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue des détails du rapport de menace

Champ	Description
ID	Spécifiez un nom pour identifier le rapport de menace.
Nom	Spécifiez un bref résumé du contenu de la note.
Description	Une description qui fournit des informations et un contexte supplémentaires sur le rapport.
Types de rapports	Spécifie le nom de l'auteur (par exemple, un analyste).
Publié	Date à laquelle ce rapport a été officiellement publié par l'auteur du rapport.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cette note de menace.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au regroupement de menaces.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ce regroupement de menaces.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à ce regroupement de menaces.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux rapports de menace.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.
Regroupements des menaces	Répertorie les regroupements de menaces associés à cet objet.
Rapports de menace	Répertorie les rapports de menace associés à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Outil

Les outils sont des logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques. Les outils s'appliquent à STIX 2.x.

Les outils vous permettent de savoir comment et quand les auteurs de menace les utilisent pour exécuter des campagnes. Contrairement aux logiciels malveillants, ces outils ou progiciels se trouvent souvent sur un système et ont des objectifs légitimes pour les utilisateurs avancés, les administrateurs, les administrateurs réseau ou même les utilisateurs normaux.

Par exemple, les outils d'accès à distance (RDP) et les outils d'analyse du réseau (Nmap) sont des outils qu'un auteur de menace utilise lors d'une attaque.

Définir des outils

Définissez les outils comme des logiciels légitimes utilisés pour effectuer des attaques.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **l'objet Outil** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue des détails d'outils

Champ	Description
ID	ID unique permettant d'identifier un outil.
Nom	Saisissez un nom descriptif pour identifier l'outil.
Description	Une description qui fournit plus de détails et de contexte sur l'outil, y compris éventuellement son objectif et ses caractéristiques clés.
Types d'outil	Le ou les types d'outils décrits.
Alias	Noms alternatifs utilisés pour identifier cet outil.
Version de l'outil	L'identificateur de version associé à l'outil.
Phases d'attaque	Représente la phase d'attaque dans une kill chain telle que LM, MITRE ATT&CK.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet outil.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet outil.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au regroupement de menaces.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ce regroupement de menaces.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à ce regroupement de menaces.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux outils.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Détections et atténuations	Répertorie les détections et atténuations associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Vulnérabilité

Une vulnérabilité est une faiblesse ou un défaut d'un composant logiciel ou matériel que les attaquants exploitent. Les vulnérabilités s'appliquent à STIX 2.x.

La faiblesse ou le défaut réside dans les exigences, les conceptions ou les implémentations du code que l'on trouve dans un composant logiciel ou matériel. Cette faiblesse est directement exploitée pour avoir un impact négatif sur la confidentialité, l'intégrité ou la disponibilité de ce système.

CVE est une liste des vulnérabilités et des expositions liées à la sécurité de l'information qui fournit des noms communs pour les problèmes connus du public [CVE].

Par exemple, si un programme malveillant exploite CVE-2015-12345, un objet malveillant peut être lié à un objet de vulnérabilité qui fait référence à CVE-2015-12345.

Définir la vulnérabilité

Définissez la vulnérabilité comme une faiblesse ou un défaut dans un composant logiciel ou matériel que les attaquants exploitent.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **Objet de vulnérabilité** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue des détails des vulnérabilités

Champ	Description
ID	ID unique permettant d'identifier une vulnérabilité.
Nom	Un nom utilisé pour identifier la vulnérabilité.
Description	Une description qui fournit plus de détails et de contexte sur la vulnérabilité, y compris potentiellement son objectif et ses caractéristiques clés.
Gravité	Indique le degré normalisé de gravité de cette vulnérabilité
CVSS3.0	Indique le CVSS v3 pour cette vulnérabilité.
CVSS2.0	Indique le CVSS v2 pour cette vulnérabilité.
État d'exploitation	Indique l'état de l'exploit associé à cette vulnérabilité
Publié	Indique quand la vulnérabilité est publiée.
Dernière modification de l'enregistrement	Indique la date de la dernière modification de l'enregistrement.
Logiciel affecté	Répertorie les logiciels affectés associés à la vulnérabilité.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cette vulnérabilité.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cette vulnérabilité.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à la vulnérabilité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette vulnérabilité.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette vulnérabilité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la vulnérabilité.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Détections et atténuations	Répertorie les détections et atténuations associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut d'un logiciel ou d'un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Extraire les données de vulnérabilité

Extrayez les données associées à la vulnérabilité telles que les éléments de configuration, les entrées vulnérables et le contexte commercial.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à **Objet de vulnérabilité** .
   Les vulnérabilités associées à cet objet sont affichées.
4. Sélectionnez l'enregistrement de vulnérabilité correspondant.
   Si des CVE lui sont associés, vous pouvez extraire automatiquement ses données associées à une vulnérabilité à l'aide du bouton fourni, et ces enregistrements associés s'affichent dans la section Contexte métier des vulnérabilités.
5. Accéder à **Intelligence interne** > **Entrées vulnérables**.
   Les enregistrements CVE associés s'affichent.
6. Sélectionnez n'importe quel CVE et cliquez sur le bouton **Extraire les données associées à la vulnérabilité** .

Remarque :

- Ce lien associera automatiquement les enregistrements et extraira ce contexte professionnel particulier des enregistrements.
- Si aucun enregistrement n'est associé, un message dinformation s'affiche indiquant que cet objet de vulnérabilité spécifique n'a aucune entrée vulnérable qui lui est associée. Vous devez associer manuellement le ou les objets aux entrées vulnérables pour extraire les données.
- Ce bouton déclenche une tâche planifiée en arrière-plan, et les détails de lancement et d'exécution de la tâche sont affichés dans la section **Flux d'activité** . Par exemple, lorsque le travail est déclenché, le flux d'activité affiche une activité qui a commencé à extraire les données associées aux entrées vulnérables. Pour plus d'informations sur la façon dont les travaux planifiés sont exécutés pour extraire les données, consultez Travaux planifiés .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Lier** pour lier manuellement les objets.
8. Sélectionnez les enregistrements à lier et extrayez les données associées à la vulnérabilité à l'aide du bouton **Extraire les données associées** à la vulnérabilité.
   Une fois que vous aurez cliqué sur ce bouton, le travail en arrière-plan sera déclenché et les données seront automatiquement extraites dans leur section respective. Un message affiche que la tâche d'extraction des données associées aux entrées vulnérables a commencé. Vous pouvez suivre l'état dans le flux d'activité et actualiser la liste une fois la tâche terminée pour vérifier les résultats. Par exemple, si les données sont liées aux éléments de configuration, vérifiez les résultats dans la section Éléments de configuration. Pour plus d'informations sur l'ajout de CVE, consultez Ajouter des CVE à des entrées tierces .

   Remarque : De même, vous pouvez extraire les données d'enregistrements des observables. Pour plus d'informations, consultez Extraire les données de vulnérabilité.

Définition de marquage

L'objet marking-definition représente un marquage spécifique. Les marquages de données représentent généralement les besoins de traitement ou de partage des données.

Définir la définition de marquage

Définissez des définitions de marquage pour gérer et partager les exigences pour les données.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à l'objet **Définition de marquage** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails de la source de définition de marquage

Champ	Description
ID	ID unique permettant d'identifier une définition de marquage.
Nom	Nom utilisé pour identifier la définition de marquage.
Type de définition	La propriété type identifie le type d'objet. La propriété definition_type identifie le type de définition de marquage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Définition	La propriété de définition contient l'objet de marquage lui-même, par exemple TLP.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Saisissez le score de confiance pour cet objet. La propriété de confiance identifie la confiance que le créateur a dans l'exactitude de ses données. La valeur de confiance DOIT être un nombre compris entre 0 et 100.

Aperçus

Champ	Description
Notes	Ajoutez des remarques supplémentaires pour cette définition de marquage.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cette définition de marquage.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à la vulnérabilité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette vulnérabilité.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette vulnérabilité.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la vulnérabilité.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque associés à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Détections et atténuations	Répertorie les détections et atténuations associées à cet objet.
Identités	Liste les identités associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Indicateurs	Répertorie les indicateurs de compromission (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Analyse de programme malveillant	Répertorie l'analyse malveillante associée à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.
Regroupements des menaces	Répertorie les regroupements de menaces associés à cet objet.
Notes de menace	Répertorie les notes de menace associées à cet objet.
Opinions sur la menace	Répertorie les opinions sur la menace associées à cet objet.
Outils	Répertorie les outils associés à cet objet.
Vulnérabilités	Répertorie les vulnérabilités associées à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Composant de données

Les composants de données sont utilisés pour identifier des propriétés ou des valeurs spécifiques d'une source de données.

Définir le composant de données

Définir un composant de données pour identifier les propriétés ou les valeurs d'une source de données

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à l'objet **Composant de données** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails des composants de données

Champ	Description
ID	ID unique permettant d'identifier un composant de données.
Nom	Nom utilisé pour identifier le composant de données.
Description	Une description qui fournit plus de détails et de contexte sur la vulnérabilité, y

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	compris potentiellement son objectif et ses caractéristiques clés.
Source de données	Indique le degré normalisé de gravité de cette vulnérabilité
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Fiabilité	Indique le score de confiance pour cet objet. La confiance doit être comprise entre 0 et 100.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez toutes les notes supplémentaires pour ce composant de données.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce composant de données.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du composant de données.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.

Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à la vulnérabilité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette vulnérabilité.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette vulnérabilité.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au composant de données.

Enregistrements connexes

Champ	Description
Schémas d'attaque	Répertorie les schémas d'attaque associés à cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Sources de données

Les sources de données représentent les différents sujets/sujets d'informations qui peuvent être collectés par les capteurs/journaux. Les sources de données comprennent également des composants de données, qui identifient des propriétés/valeurs spécifiques d'une source de données.

Définir les sources de données

Définissez une source de données pour représenter les différents sujets ou rubriques d'information.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à l'objet **Sources de données** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objet pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire.

Vue des détails des vulnérabilités

Champ	Description
ID	ID unique permettant d'identifier la source de données.
Nom	Nom utilisé pour identifier la source de données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Description qui fournit plus de détails et de contexte sur la source de données, incluant éventuellement son objectif et ses caractéristiques clés.
Couches de collecte	Indique la description de l'endroit où la source de données peut être physiquement collectée, comme l'hôte, le réseau, le plan de contrôle du cloud, entre autres.
Plateformes	Indique que le système dans lequel un adversaire opère pourrait être un système d'exploitation ou une application.
Contributeurs	Indique les contributeurs de cette source de données.
TLP	TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cette source de données.

Informations supplémentaires

Champ	Description
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cette source de données.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Extensions	Indique les extensions du schéma d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, le plan d'action.
Créé	Spécifie la date et l'heure de création de l'objet dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après la création d'un enregistrement d'observable, la case à cocher **Empêcher les mises à jour système** s'affiche.
>
> Activez cette case à cocher pour empêcher toute mise à jour du système après la création des enregistrements d'observable, d'indicateur ou d'objets STIX.

Balises et taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à la source de données.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette source de données.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette source de données.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la source de données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui se réfèrent à des informations non STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes aux renseignements sur la menace.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir une relation entre deux objets quelconques, utilisez le lien **Relations potentielles** de la **bibliothèque Intel de menaces** pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue du formulaire Objets pour confirmer les relations entre deux objets à l'aide de la section **Relations potentielles** disponible dans la vue de formulaire. Pour plus d'informations, Confirmer les relations éventuelles à partir des enregistrements connexesconsultez .
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Définir des flux RSS

Un flux de renseignements sur les menaces est un flux de données continu en temps réel qui recueille des informations relatives aux cyberrisques ou aux menaces. Les flux RSS offrent un moyen facile de rester à jour avec vos sites Web préférés, tels que les blogs ou les dernières nouvelles en matière de cybersécurité.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accédez à l'objet **Flux RSS** .

   Remarque : Les flux ingérés peuvent être parcourus à l'aide de cette section, mais vous ne pouvez pas créer de nouveaux enregistrements.

4. Sur le formulaire, les champs suivants sont renseignés automatiquement.

Vue des détails de Flux RSS

Champ	Description
Titre	Titre du flux RSS.
Description	Une description qui fournit plus de détails et de contexte sur les flux RSS, y compris

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	potentiellement leur objectif et leurs caractéristiques clés.
Lien	Indique le lien ajouté aux flux RSS.
Source	Spécifie la source du flux RSS à partir de laquelle cet enregistrement d'objet est créé.
Date de publication	Indique quand le flux RSS est publié.
Auteur	Indique l'auteur du flux RSS.

5. Cliquez sur **Enregistrer**.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour ce flux.

Informations supplémentaires

Champ	Description
URL du média	Indique l'URL du média.
Commentaires de commentaires	Tout commentaire supplémentaire sur le commentaire.

Objets de relations

Utilisez les objets de relations pour lier deux observables ou un observable et SDO pour expliquer comment ils sont liés l'un à l'autre.

Les objets de relation STIX (SRO) représentent les types de relations entre divers objets STIX. Les objets de relation suivants sont disponibles :

- **Relation observable-observable** : cet objet définit les relations entre observables.
- **Relation objet-objet** : cet objet définit les relations entre les SDO, à l'exception de l'objet indicateur. Un exemple de relation définie objet-objet est qu'un modèle d'attaque délivre un programme malveillant.
- **Relation objet-observable** : cet objet définit les relations entre les SDO et l'objet observable (SCO). Un exemple de relation définie objet-observable est qu'une infrastructure est constituée d'objets cyber-observables qui fournissent des informations sur une attaque potentielle.
- **Relation objet-indicateur** : cet objet définit les relations entre les SDO et l'objet indicateur.
- **Relations indicateur-indicateur** : cet objet définit les relations entre les objets d'indicateur.
- **Relation indicateur-observable** : cet objet définit les relations entre l'objet indicateur et d'autres SDO. Un exemple de relation objet - indicateur est qu'un indicateur détecte des preuves d'une campagne.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Relations d'objet

Objet de relation	Source de l'exemple	Exemple de cible	Exemple de description
Relations observable-observable	Adresse IP, nom de domaine		Cette relation décrit entre les observables.
Relations objet-objet	Modèle d'attaque	Programme malveillant	Cette relation décrit que ce modèle d'attaque est utilisé pour diffuser cette instance (ou famille) de programme malveillant.
Relations objet-observable			Cette relation décrit entre les objets et les observables.
Relations objet-indicateur	Indicateur	Modèle d'attaque, Campagne, Infrastructure, Ensemble d'intrusions, Programme malveillant, Acteur de menace, Outil	Cette relation décrit le fait que l'indicateur peut détecter des preuves du modèle d'attaque, de la campagne, de l'infrastructure, de l'ensemble d'intrusions, du programme malveillant, de l'acteur de menace ou de l'outil associé. Il se peut que la preuve ne soit pas directe. Par exemple, l'indicateur peut détecter des preuves secondaires de la campagne, telles que des programmes malveillants couramment utilisés par cette campagne particulière.
Indicateur : relations indicateur	Infrastructure	Données observées	Cette relation décrit que l'indicateur est créé en fonction des informations provenant d'un objet de données observé. Un exemple de relation définie objet-observable est qu'une infrastructure

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Relations d'objet (suite)

Objet de relation	Source de l'exemple	Exemple de cible	Exemple de description
			est constituée d'objets cyber-observables qui fournissent des informations sur une attaque potentielle.
Indicateur : Observable			Cette relation décrit entre les indicateurs et les observables.

Définir des relations observable-observable

Définir des relations entre les observables.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Observable-Observable**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Observable source	Sélectionnez et définissez l'objet source.
Observable cible	Sélectionnez et définissez l'objet cible.
Type de relation	Une description qui fournit plus de détails et de contexte sur le type de relation. Les options disponibles sont les suivantes : Définissez le sens de la relation, qu'il soit direct ou inverse. ◦ Inverse : il s'agit du type de relation entre l'observable et l'objet. ◦ Direct : il s'agit du type de relation entre l'objet et l'observable.
Base de corrélation	Nom de la règle de corrélation sur la base de laquelle le système a identifié comme enregistrements connexes de cet observable. Cette règle est renseignée automatiquement.

6. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir des relations objet-objet

Définissez les relations entre les SDO, à l'exception de l'objet d'indicateur.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **Relations** > **objet-objet**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Objet source	Sélectionnez et définissez l'objet source.
Type de l'objet source	Définit le type d'objet source.
Objet cible	Sélectionnez et définissez l'objet cible.
Type de l'objet cible	Définit le type d'objet cible.
Type de relation	Une description qui fournit plus de détails et de contexte sur le type de relation. Définissez le sens de la relation, qu'il soit direct ou inverse. ◦ Inverse : il s'agit du type de relation entre l'observable et l'objet. ◦ Direct : il s'agit du type de relation entre l'objet et l'observable.
Heure de début	Spécifie le moment auquel la relation est créée.
Heure de fin	Spécifie le moment où la relation est interrompue ou supprimée.
Description	Une brève description des relations d'objet.

6. Cliquez sur **Envoyer**.

Définir des relations objet-observable

Définissez les relations entre les SDO et l'objet observable (SCO).

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Accéder à **Relations** > **Objet-Observable**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Observable	Sélectionnez et définissez l'observable.
Objet	Sélectionnez et définissez l'objet.
Type de relation	Une description qui fournit plus de détails et de contexte sur le type de relation. Définissez le sens de la relation, qu'il soit direct ou inverse. ◦ Inverse : il s'agit du type de relation entre l'observable et l'objet. ◦ Direct : il s'agit du type de relation entre l'objet et l'observable.
Heure de début	Spécifie le moment auquel la relation est créée.
Heure de fin	Spécifie le moment où la relation est interrompue ou supprimée.
Description	Une brève description des relations d'objet.

6. Cliquez sur **Envoyer**.

Définir des relations objet-indicateur

Définissez les relations entre l'objet de l'indicateur et d'autres SDO.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Objet-Indicateur**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Indicateur	Sélectionnez et définissez l'indicateur.
Objet	Sélectionnez et définissez l'objet.
Type de relation	Une description qui fournit plus de détails et de contexte sur le type de relation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Définissez le sens de la relation, qu'il soit direct ou inverse. ◦ Inverse : il s'agit du type de relation entre l'observable et l'objet. ◦ Direct : il s'agit du type de relation entre l'objet et l'observable.
Heure de début	Spécifie le moment auquel la relation est créée.
Heure de fin	Spécifie le moment où la relation est interrompue ou supprimée.
Description	Une brève description des relations d'objet.

6. Cliquez sur **Envoyer**.

Définir les relations indicateur-indicateur

Définir les relations entre l'objet indicateur et d'autres Utilisez les objets de relations pour lier deux observables ou un observable et SDO pour expliquer comment ils sont liés l'un à l'autre.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Indicateur : indicateur**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Description	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Domaine	Définit le champ d'application de l'enregistrement d'objet. La valeur de ce champ est renseignée automatiquement.
Indicateur cible	Sélectionnez et définissez l'objet d'indicateur cible.
Type de relation	Une description qui fournit plus de détails et de contexte sur le type de relation. Définissez le sens de la relation, qu'il soit direct ou inverse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Inverse : il s'agit du type de relation entre l'observable et l'objet. ◦ Direct : il s'agit du type de relation entre l'objet et l'observable.
Indicateur source	Sélectionnez et définissez l'indicateur d'objet source.

6. Cliquez sur **Envoyer**.

Définir des relations indicateur-observable

Définissez les relations entre l'objet de l'indicateur et d'autres SDO.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Indicateur : Observable**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs dans le formulaire comme il vous convient.

Champ	Description
Observable	Sélectionnez et définissez l'observable.
Indicateur	Sélectionnez et définissez l'objet d'indicateur.

6. Cliquez sur **Envoyer**.

Relations éventuelles

L'application utilise la corrélation automatisée pour établir des relations potentiellement possibles entre deux SDO, deux observables ou un observable et SDO.

1. Sélectionnez un ou plusieurs enregistrements potentiellement connexes et appliquez cette action à l'interface utilisateur, ce qui changera davantage les enregistrements en relations confirmées et visibles dans la section Enregistrements connexes.
2. Toutes les corrélations confirmées ingérées ou créées manuellement par un analyste remplaceront les relations potentielles créées par corrélation automatique.

Confirmer la relation potentielle observable-observable

Utilisez cette section pour confirmer les relations entre les observables.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **Relations éventuelles** > **Observable-Observable**.
4. Sélectionnez l'enregistrement du ou des observables.
5. Cliquez sur **Confirmer la relation**.
   Idéalement, un enregistrement de relation potentielle est créé, qui est identifié en fonction de ses règles de corrélation. Une fois que vous avez confirmé la relation, l'enregistrement des observables est déplacé vers la section Relations, ce qui signifie que la relation entre les observables et les observables est confirmée. L'enregistrement affiche une relation confirmée uniquement lorsque les règles de corrélation sont mises en correspondance. Par exemple, une relation potentielle peut être créée lorsque deux observables de type URL ont le même nom de domaine.

   Vous pouvez également créer un nouvel enregistrement d'observables en liant les observables à partir de la liste des observables et confirmer les relations à partir de l'onglet Enregistrements connexes de chaque observable.

   a. Ouvrez n'importe quel enregistrement d'observable.

   b. Accédez à l'onglet **Enregistrements connexes** .

   c. Cliquez sur le bouton **Lien** .

   d. Sélectionnez un ou plusieurs observables.

   e. Cliquez sur **Lier**.
      Cela créera une nouvelle relation entre l'enregistrement observable sélectionné et les observables nouvellement liés.

6. Cliquez sur **Supprimer** pour supprimer les relations.

Confirmer les relations éventuelles objet-objet

Définissez les relations potentielles entre les objets.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **Relations éventuelles** > **objet-objet**.
4. Sélectionnez l'enregistrement de l'observable.
5. Cliquez sur **Confirmer la relation**.
   Idéalement, un enregistrement de relation potentielle est créé, qui est identifié en fonction de ses règles de corrélation. Une fois que vous avez confirmé la relation de cette section, l'enregistrement des observables est déplacé vers la section Relations, ce qui signifie que la relation entre les observables et les observables est confirmée. L'enregistrement affiche une relation confirmée uniquement lorsque les règles de corrélation sont mises

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

en correspondance. Par exemple, une relation potentielle peut être créée lorsque deux observables de type URL ont le même nom de domaine.

Vous pouvez également créer un nouvel enregistrement d'observables en liant les observables à partir de la liste des observables et confirmer les relations à partir de l'onglet Enregistrements connexes de chaque observable.

a. Ouvrez n'importe quel enregistrement d'observable.

b. Accédez à l'onglet **Enregistrements connexes** .

c. Cliquez sur le bouton **Lien** .

d. Sélectionnez un ou plusieurs observables.

e. Cliquez sur **Lier**.
Cela créera une nouvelle relation entre l'enregistrement observable sélectionné et les observables nouvellement liés.

6. Cliquez sur **Supprimer** pour supprimer les relations.

Confirmer les relations éventuelles indicateur-indicateur

Définissez les relations potentielles entre les objets.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.
2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.
3. Accéder à **Relations éventuelles** > **indicateur-indicateur**.
4. Sélectionnez l'enregistrement de l'observable.
5. Cliquez sur **Confirmer la relation**.
Idéalement, un enregistrement de relation potentielle est confirmé en fonction des règles de corrélation automatisées. Une fois que vous avez confirmé la relation, l'enregistrement des observables est déplacé vers la section Relations, ce qui signifie que la relation entre les observables et les observables est confirmée.

L'enregistrement affiche une relation confirmée uniquement lorsque les règles de corrélation sont mises en correspondance. Par exemple, une relation potentielle est confirmée lorsque deux observables de type URL ont le même nom de domaine.

Vous pouvez également créer un nouvel enregistrement d'observables en liant les observables à partir de la liste des observables et confirmer les relations à partir de l'onglet Enregistrements connexes de chaque observable.

a. Ouvrez n'importe quel enregistrement d'observable.

b. Accédez à l'onglet **Enregistrements connexes** .

c. Cliquez sur le bouton **Lien** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Sélectionnez un ou plusieurs observables.

e. Cliquez sur **Lier**.
Cela créera une nouvelle relation entre l'enregistrement observable sélectionné et les observables nouvellement liés.

6. Cliquez sur **Supprimer** pour supprimer les relations.

Confirmer les relations éventuelles à partir des enregistrements connexes

Confirmez les relations entre les deux SDO.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Threat Intelligence Security Center**.

2. Cliquez sur l'icône **Bibliothèque Intel de menaces** dans l'espace de travail.

3. Accédez à la section **Enregistrements connexes** .

4. Développer les relations potentielles.

5. Ouvrez un enregistrement tel que des observables, des indicateurs ou tout autre objet que vous souhaitez pour confirmer les relations entre deux SDO.

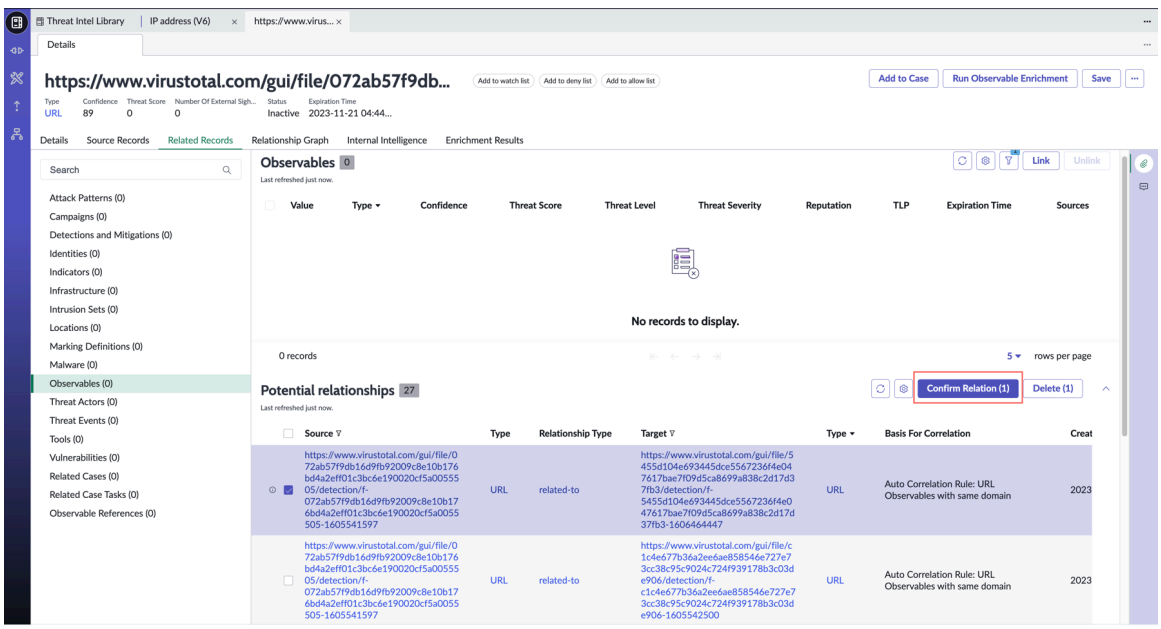
6. Par exemple, sélectionnez ici **Observables** dans le volet de navigation de gauche.

7. Sélectionnez les enregistrements **observable** dans la liste.

> **Remarque :** La section de liste affiche tous les enregistrements observables liés de l'observable associé.

8. Cliquez sur le bouton **Confirmer les relations** pour confirmer les relations entre les objets.

> **Remarque :** Pour plus d'informations, reportez-vous aux sectionsObjets de relations et Relations éventuelles.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Cliquez sur **Supprimer** pour supprimer les observables associés.
   Pour plus d'informations sur la façon dont les relations potentielles et les relations sont établies entre les ODS, voir Relations éventuelles et Objets de relations.

Corrélation automatisée

La corrélation automatisée vous aide à identifier les relations entre les observables, les indicateurs et les objets.

Avec le processus de corrélation, l'application établira automatiquement la corrélation entre les enregistrements de renseignements sur les menaces en fonction des règles prédéfinies. Selon le type de règle appliqué, la relation peut être une relation confirmée ou une relation potentielle. Si les relations entre les objets sont confirmées, ces objets s'affichent automatiquement dans la vue de détails de cet objet dans la section **Enregistrements connexes** .

Ce qui suit décrit les relations et les relations potentielles :

- **Relations** : utilisez les objets de relations pour lier deux observables ou un observable et SDO pour expliquer comment ils sont liés l'un à l'autre.
- **Relations potentielles** : utilisez les relations potentielles pour établir des relations potentiellement possibles entre deux SDO, deux observables ou un observable et SDO à l'aide de la corrélation automatisée.

Voici les règles de corrélation prédéfinies mises en service dans le système de base :

Règles de corrélation

Nom de la règle	Description de la règle	Définition de règle	Action de règle
Observables avec le même hachage de fichier	La règle compare les valeurs de hachage des observables (du même type) et identifie s'ils partagent le même hachage.	La règle compare les valeurs de hachage (du même type) des indicateurs et identifie s'ils partagent le même hachage.	Crée une relation
Observables d'URL avec le même domaine	La règle examine les points communs dans la structure des URL pour identifier si elles partagent le même domaine de base.	La règle examine les points communs dans la structure des URL : identifie si elles partagent le même domaine de base et ont une structure de sous-répertoire similaire.	Crée une relation potentielle
Observable trouvé en tant que sources dans l'objet de réseau	La règle fait correspondre la valeur de l'attribut de source du réseau avec les observables IPV4, IPV6 ou de nom de domaine dans le système et établit	La règle fait correspondre la valeur de l'attribut Source avec les observables IPV4, IPV6 ou de nom de domaine dans le système et établit	Crée une relation

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles de corrélation (suite)

Nom de la règle	Description de la règle	Définition de règle	Action de règle
	des liens en tant que source du trafic.	des liens en tant que Source du trafic.	
Observable trouvé comme destination dans l'objet de réseau	La règle fait correspondre la valeur de l'attribut de destination du réseau avec les observables IPV4, IPV6 ou de nom de domaine dans le système et établit un lien en tant que destination du trafic.	La règle fait correspondre la valeur de l'attribut Source avec des observables IPV4, IPV6 ou de nom de domaine dans le système et établit des liens en tant que destination du trafic.	Crée une relation
Relier les observables en fonction de la communication	Sur la base des objets réseau, la règle identifie tous les observables (IPV4, IPV6 et nom de domaine) qui ont communiqué avec la même destination (IPV4, IPV6 ou nom de domaine) et établit une relation entre ces observables. En outre, les observables associés (IPV4, IPV6 et nom de domaine) s'ils sont associés au même objet réseau que la source communiquant avec la destination.	Sur le châssis des objets réseau, la règle identifie tous les indicateurs qui ont communiqué avec la même destination (IPV4, IPV6, mac-addr ou domain-name) et établit une relation entre ces indicateurs comme étant connectés à la même infrastructure C2.	Crée une relation
Observables du domaine racine associés aux sous-domaines	La règle lie un domaine racine à des sous-domaines et vice versa pour le type de domaine des observables.	La règle relie un domaine racine à des sous-domaines.	Crée une relation
Domaines associés aux adresses IP en fonction des résolutions DNS	À l'aide des attributs domain-ipv4 ou domain-ipv6 des observables de domaine, la règle établit les relations entre les domaines et les adresses IP.	Utilisez les attributs domain-ipv4 ou domain-ipv6, La règle identifie tous les domaines ou sous-domaines qui se résolvent à la même adresse IP et établit des relations entre les	Crée une relation

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles de corrélation (suite)

Nom de la règle	Description de la règle	Définition de règle	Action de règle
		indicateurs, indiquant leur connexion à la même infrastructure C2.	
Domaines correspondants avec des certificats SSL	La règle analyse les informations du certificat SSL associées aux observables du domaine et établit une relation entre eux.	La règle analyse les informations du certificat SSL associées aux indicateurs et identifie que les deux certificats sont émis par la même autorité de certification et partagent la même date d'expiration, et établit des relations entre les indicateurs, indiquant leur connexion à la même infrastructure C2 ou à la même campagne de menaces.	Crée une relation
Relier des entités basées sur des observables communs	La règle compare si le même observable est lié à deux entités différentes et les relie l'un à l'autre.	La règle compare si le même observable est lié à deux entités différentes et les identifie comme liées l'une à l'autre.	Crée une relation potentielle
Relier les indicateurs en fonction des observables communs	La règle compare si le même observable est lié à deux indicateurs différents et les relie l'un à l'autre.	La règle compare si le même observable est lié à deux indicateurs différents et les identifie comme liés l'un à l'autre.	Crée une relation potentielle
Associer des indicateurs à des objets basés sur des observables communs	La règle compare si le même observable est lié à des indicateurs et à des objets et les relie les uns aux autres.	La règle compare si le même observable est lié à deux indicateurs et objets différents et les identifie comme étant liés l'un à l'autre.	Crée une relation potentielle

MITRE-ATT&CK™ Dépôt

Le MITRE-ATT&CK référentiel est disponible sous Intelligence Library où les données des sources MITRE sont ingérées.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les données MITRE qui arrivent au référentiel sont stockées dans un référentiel MITRE distinct des données de la bibliothèque Intel de menaces, où les données MITRE ne sont pas déployées pour le flux d'agrégation ou de déduplication et sont indépendantes.

Les sources de données disponibles dans l'application sont les suivantes :

1. MITRE : entreprise ATT&CK
2. MITRE - Mobile ATT&CK
3. MITRE - ICS ATT&CK

Les données de ces sources sont stockées dans un référentiel MITRE distinct sous TI library dans le système de base. Au cas où, si vous souhaitez créer une nouvelle source MITRE, configurez une source personnalisée. Pour plus d'informations, consultez et dans la vue de formulaire, cochez Afficher le flux personnalisé la case **Avancé** et sélectionnez le **processeur de rapport** en tant que : **MITRECollectionDataProcessor**.

Gérer les matrices

Gérez les matrices importées à partir des collections MITRE TAXII. Les matrices sont un ensemble de tactiques et de techniques. Vous pouvez afficher les matrices à examiner si vos collections sont disponibles dans le référentiel MITRE-ATT&CK.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Une fois que vous avez activé les sources de données de flux connexes MITRE ATT&CK qui sont disponibles dans le système de base, cliquez sur **Exécuter maintenant** pour exécuter les intégrations et extraire les informations connexes MITRE.
   Pour plus d'informations sur l'activation des intégrations
2. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **MITRE ATT&CK**.
   Les enregistrements connexes MITRE ATT&CK s'affichent. Par défaut, tous les enregistrements sont activés.

   Remarque : Vous pouvez activer uniquement les matrices qui sont pertinentes pour votre organisation.

3. Sélectionnez n'importe quel enregistrement de matrice et cliquez sur **Désactiver** si vous souhaitez désactiver un enregistrement spécifique.
4. Vous pouvez également créer un nouvel enregistrement de matrices en cliquant sur **Nouveau** pour créer manuellement les matrices MITRE ATT&CK.
5. Renseignez les champs de manière appropriée.

Créer une nouvelle atténuation MITRE : détails

Champ	Description
Nom	Entrez le nom de la matrice.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Actif	Cochez cette case pour activer l'enregistrement de matrice.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'ensemble d'intrusions, incluant éventuellement son objectif et ses caractéristiques clés.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour ce type d'objet.
Commentaires	Ajoutez tous les commentaires que vous pourriez avoir en plus.

Gérer les techniques

Gérez les techniques importées des collections MITRE TAXII. Les techniques contiennent différentes façons dont les attaquants se sont développés pour employer une tactique donnée. Vous pouvez examiner et désactiver les techniques qui ne sont pas pertinentes pour votre organisation. Dans STIX, les techniques sont connues sous le nom de schémas d'attaque.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Les techniques représentent la façon dont un adversaire atteint un objectif tactique en effectuant une action.

Procédure

1. Une fois que vous avez activé les sources de données de flux connexes MITRE ATT&CK qui sont disponibles dans le système de base, cliquez sur **Exécuter maintenant** pour exécuter les intégrations et extraire les informations connexes MITRE.
   Pour plus d'informations sur l'activation des intégrations
2. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **MITRE ATT&CK** > **Techniques**.
   Les enregistrements des techniques MITRE ATT&CK s'affichent. Par défaut, tous les enregistrements sont activés.
3. Sélectionnez n'importe quel enregistrement de technique et cliquez sur **Désactiver** si vous souhaitez désactiver un enregistrement spécifique.
4. Vous pouvez également créer de nouveaux enregistrements de techniques en cliquant sur **Nouveau** pour créer manuellement les techniques MITRE ATT&CK.
5. Renseignez les champs de manière appropriée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une nouvelle atténuation MITRE : détails

Champ	Description
ID	ID unique d'une technique.
Nom	Entrez le nom de la technique.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Plateformes	Ajoutez les plateformes requises.
Autorisations requises	Ajoutez les autorisations requises.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'ensemble d'intrusions, incluant éventuellement son objectif et ses caractéristiques clés.
Détection	Cette technique de détection est utilisée pour identifier l'accès ou l'activité non autorisée d'un adversaire sur les réseaux informatiques.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour ce type d'objet.
Commentaires	Ajoutez tous les commentaires que vous pourriez avoir en plus.

Gérer les atténuations

Gérez les atténuations importées à partir des collections MITRE TAXII. Les atténuations vous permettent d'empêcher un adversaire d'exécuter avec succès des techniques ou des sous-techniques contre votre organisation. Dans STIX, les mesures d'atténuation sont connues sous le nom de plan d'action.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Une fois que vous avez activé les sources de données de flux connexes MITRE ATT&CK qui sont disponibles dans le système de base, cliquez sur **Exécuter maintenant** pour exécuter les intégrations et extraire les informations connexes MITRE.
   Pour en savoir plus sur l'activation des intégrations.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **MITRE ATT&CK** > **Atténuations**.
   Cliquez sur une atténuation pour afficher toutes les informations associées.
3. Cliquez sur **Nouveau** pour créer manuellement les atténuations MITRE ATT&CK.
4. Renseignez les champs de manière appropriée.

Créer de nouveaux outils MITRE - Détails

Champ	Description
ID	ID unique d'un plan d'action pour prévenir une attaque.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Nom	Entrez un nom descriptif pour identifier l'objet.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Alias	Liste d'autres noms permettant d'identifier cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'objet, y compris éventuellement sa fonction et ses caractéristiques clés.
Contributeurs	Spécifie les contributeurs.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet objet.
Commentaires	Ajoutez des commentaires pour cet objet.

5. Cliquez sur **Enregistrer**.

Gérer les groupes

Gérez les groupes importés à partir des collections MITRE TAXII. Les groupes sont des ensembles d'activités d'intrusion connexes qui sont suivis par un nom commun dans la communauté de sécurité. Les analystes suivent les grappes d'activités à l'aide de divers termes tels que groupes de menaces, groupes d'activités, acteurs de menace, ensembles

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'intrusion et campagnes. Dans STIX, les groupes sont connus sous le nom d'ensembles d'intrusion.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **MITRE ATT&CK** > **Groupes**.
   Vous pouvez afficher les groupes répertoriés.
2. Cliquez sur **Nouveau** pour créer manuellement les groupes MITRE ATT&CK.
3. Renseignez les champs de manière appropriée.

Créer des groupes MITRE : détails

Champ	Description
ID	ID unique d'un plan d'action pour prévenir une attaque.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Nom	Entrez un nom descriptif pour identifier l'objet.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Alias	Liste d'autres noms permettant d'identifier cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'objet, y compris éventuellement sa fonction et ses caractéristiques clés.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet objet.
Commentaires	Ajoutez des commentaires pour cet objet.

4. Cliquez sur **Enregistrer**.
5. Pour voir comment ces objets sont liés, cliquez sur **Relations**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer les programmes malveillants

Gérez les informations sur les programmes malveillants que vous avez importées à partir des collections MITRE TAXII. Il s'agit d'un type de TTP qui représente un code malveillant.

Avant de commencer

Il s'agit d'un programme qui est inséré secrètement dans un système. L'intention d'un programme malveillant est de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation (OS) de la victime.

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **MITRE ATT&CK** > **Groupes**.
   Vous pouvez afficher les programmes malveillants répertoriés.
2. Cliquez sur un programme malveillant pour afficher toutes les informations associées.
3. Cliquez sur **Nouveau** pour créer manuellement le programme malveillant MITRE ATT&CK.
4. Renseignez les champs de manière appropriée.

Créer un nouveau programme malveillant MITRE : détails

Champ	Description
ID	ID unique d'un plan d'action pour prévenir une attaque.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Nom	Entrez un nom descriptif pour identifier l'objet.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Alias	Liste d'autres noms permettant d'identifier cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'objet, y compris éventuellement sa fonction et ses caractéristiques clés.
Contributeurs	Spécifie les contributeurs.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet objet.
Commentaires	Ajoutez des commentaires pour cet objet.

5. Cliquez sur **Enregistrer**.
6. Pour voir comment ces objets sont liés, cliquez sur **Relations**.

Gérer les outils

Gérez les informations sur les outils que vous avez importées à partir des collections MITRE TAXII. Les outils sont des logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Pourquoi et quand exécuter cette tâche
Les outils vous permettent de savoir comment et quand les auteurs de menace les utilisent pour exécuter des campagnes. Contrairement aux logiciels malveillants, ces outils ou progiciels se trouvent souvent sur un système et ont des objectifs légitimes pour les utilisateurs avancés, les administrateurs, les administrateurs réseau ou même les utilisateurs normaux.

Procédure
1. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **MITRE ATT&CK** > **Outils**.
   Vous pouvez afficher les outils répertoriés.
2. Cliquez sur un outil pour afficher toutes les informations associées.
3. Cliquez sur **Nouveau** pour créer manuellement les outils MITRE ATT&CK.
4. Renseignez les champs de manière appropriée.

Créer de nouveaux outils MITRE - Détails

Champ	Description
ID	ID unique d'un plan d'action pour prévenir une attaque.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Nom	Entrez un nom descriptif pour identifier l'objet.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Alias	Liste d'autres noms permettant d'identifier cet objet.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'objet, y compris éventuellement sa fonction et ses caractéristiques clés.
Contributeurs	Spécifie les contributeurs.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet objet.
Commentaires	Ajoutez des commentaires pour cet objet.

5. Cliquez sur **Enregistrer**.
6. Pour voir comment ces objets sont liés, cliquez sur **Relations**.

Gérer les relations MITRE

Gérez les informations sur les relations MITRE que vous avez importées à partir des collections MITRE TAXII.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Threat Intelligence Security Center** > **Bibliothèque Intel de menaces** > **MITRE ATT&CK** > **Relations**.
   Vous pouvez afficher les relations répertoriées.
2. Cliquez sur un objet source pour afficher toutes les informations associées.
3. Cliquez sur **Nouveau** pour créer manuellement les relations MITRE ATT&CK.
4. Renseignez les champs de manière appropriée.

Créer de nouveaux outils MITRE - Détails

Champ	Description
Objet MITRE source	Ajoutez l'objet MITRE source.
Objet MITRE cible	Ajoutez l'objet MITRE cible.
Type MITRE source	Entrez le type MITRE source.
Type MITRE cible	Entrez le type MITRE cible.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type de relation	Définissez les relations entre les objets. Une description qui fournit plus de détails et de contexte sur le type de relation. Les options disponibles sont les suivantes : Définissez le sens de la relation, qu'il soit direct ou inverse. ◦ Inverse : il s'agit du type de relation entre l'observable et l'objet. ◦ Direct : il s'agit du type de relation entre l'objet et l'observable.
Source	Sélectionnez et définissez l'objet source.
ID de la relation	Définissez l'ID de relation.

5. Cliquez sur **Enregistrer**.
6. Pour voir comment ces objets sont liés, cliquez sur **Relations**.

Gestion et conservation des données

Les données sont stockées et gérées dans l'instance TISC en fonction de la structure des objets de bibliothèque TIDC que les administrateurs peuvent afficher et configurer en fonction des besoins de leur organisation.

L'archivage et la restauration des données sont l'une des fonctionnalités clés pour protéger les enregistrements en vue de leur utilisation future. Les sections suivantes définissent et expliquent le processus d'archivage TISC et la conservation des enregistrements, car Threat Intelligence contient d'énormes volumes de données et d'enregistrements.

Processus d'archivage des données

Les données augmentent rapidement dans les tables avec l'adoption accrue de la plate-forme. Certaines tables sont incluses dans le système de base avec différentes stratégies de gestion des données, mais d'autres utilisateurs sont nécessaires pour les implémenter eux-mêmes.

Les utilisateurs peuvent gérer leurs données dans des tables de différentes manières :

- Supprimer les données
- Archiver les données

Remarque : Si les utilisateurs n'adoptent aucune des méthodes de gestion de leurs données, l'utilisation augmente au fil du temps et les données ont tendance à devenir beaucoup plus volumineuses, ce qui aura un impact important sur les performances de l'instance d'application ainsi que sur le stockage.

Règles d'archivage pour les observables

Les règles d'archivage pour les observables provisionnés dans le système de base sont répertoriées dans la section ci-dessous.

- E-mail
- Hachage SHA256

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Autre observable
- Hachage SHA512
- Lime
- Hachage SHA1
- Adresse courriel
- URL
- Numéro AS
- Objet de l'e-mail
- IPv4 CIDR
- Nom Mutex
- Artefact
- Compte d'utilisateur
- Clé de registre Windows
- Adresse IPv6
- Hachage MD5
- Adresse IPv4
- Répertoire
- Certificat X.509
- Règle d'archivage du flux RSS
- Importe les règles d'archivage
- Processus d'emplacement

Modifier les règles d'archivage pour les observables

Modifiez les règles d'archivage pour les observables et affichez également une estimation du nombre d'enregistrements affectés par la règle.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Les exemples de règles d'archivage sont inactifs par défaut.

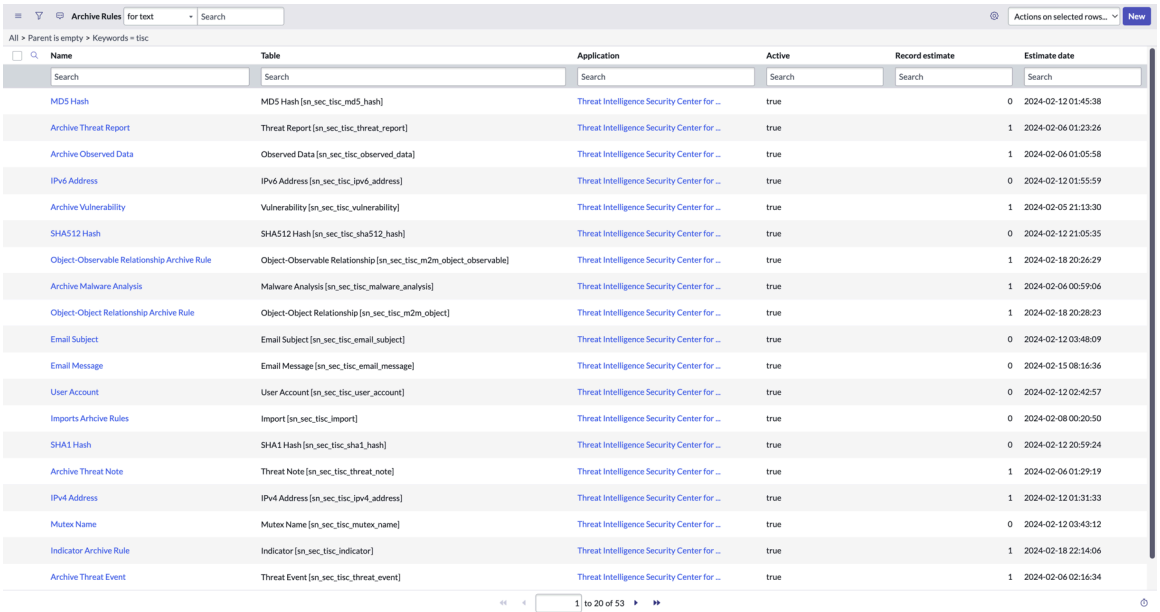
L'option Historiquement significatif et la condition doivent toujours être définies sur False pour les observables, les indicateurs, les enregistrements connexes et les objets. Si vous définissez cette option sur faux, vous pouvez archiver les enregistrements. Si cette option est définie sur vrai, cela signifie que vous ne pouvez pas archiver les enregistrements, quelle que soit la définition des règles.

Procédure

1. Accédez à la **Tout** > **Archivage système** > **Règles d'archivage**.
   La liste des règles d'archivage applicables à TISC s'affiche. Ces règles d'archivage sont différentes pour chaque type d'objet et s'appliquent indépendamment.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Sélectionnez une règle d'archivage.
   Par exemple, sélectionnez Enregistrement observable d'annuaire pour afficher la règle d'archivage du système de base.
3. Cliquez sur **Ajouter une condition de filtre**.
4. Sélectionnez **l'option Historiquement significatif** et définissez la condition sur **Faux**.
   Si vous définissez cette option sur faux, vous pouvez archiver les enregistrements. Si cette option est définie sur vrai, cela signifie que vous ne pouvez pas archiver les enregistrements, quelle que soit la définition des règles.
5. Dans cet exemple, définissez l'état de l'observable sur Inactif et le délai d'expiration est sur 2 ans.
   Cela signifie que l'enregistrement de l'observable peut être archivé lorsque l'état est inactif et que la période d'expiration de cet observable est définie sur 2 ans, de sorte que tout ce qui se trouve avant cette période à partir de la date actuelle sera archivé.

   Remarque : Chaque règle d'archivage est déclenchée toutes les heures, de sorte que tout changement apporté à la règle est modifié à partir du moment où sa tâche est planifiée. Si vous souhaitez exécuter la tâche explicitement et que vous ne souhaitez pas attendre que la tâche soit planifiée, vous pouvez la modifier en conséquence. Suivez les étapes ci-dessous.

6. Accédez à la **Liens connexes** > **Recalculer l'estimation**.

   L'estimation d'enregistrement a été recalculée et mise à jour avec la valeur estimée.

   Remarque : Si votre valeur d'estimation d'enregistrement est 0, les enregistrements ne sont pas archivés. Si la valeur d'estimation d'enregistrement est 1, l'application identifie cette valeur et cet enregistrement est archivé.

7. Sélectionnez **Exécuter l'archivage maintenant**.
8. Accédez à la section **Exécution d'archivage** ci-dessous pour vérifier votre processus d'exécution d'archivage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous remarquerez que le nombre total d'enregistrements archivés n'est que d'un seul enregistrement, car votre valeur d'estimation d'enregistrement est également égale à un.

9. Accédez à la **Bibliothèque Intel de menaces** > **Observables**.
10. Recherchez l'enregistrement archivé.
    L'enregistrement doit avoir été archivé et n'affiche pas les résultats lorsque vous recherchez l'enregistrement.

Remarque :

- Dans le cadre des règles d'archivage TISC, toutes les sources et ses enregistrements connexes qui sont répertoriés dans le cadre des enregistrements connexes archivés seront également archivés avec l'enregistrement observable agrégé. Vous pouvez descendre dans la hiérarchie jusqu'à la section Journal d'archivage pour voir la liste des enregistrements archivés qui ont été exécutés automatiquement en arrière-plan et affichés sous cette section.
- Si vous souhaitez afficher l'enregistrement archivé, recherchez l'enregistrement dans cette table connexe. Simultanément, vous pouvez également vérifier votre enregistrement archivé en accédant à **Archivage système** > **Journal d'archive**. Le nombre d'enregistrements archivés s'affiche.

Règles d'archivage des objets

Les règles d'archivage pour les observables provisionnés dans le système de base sont répertoriées dans la section ci-dessous.

Les exemples de règles d'archivage sont inactifs par défaut.

L'option **Historiquement significatif** et la condition doivent toujours être définies sur **False** pour les observables, les indicateurs, les enregistrements connexes et les objets. Si vous définissez cette option sur faux, vous pouvez archiver les enregistrements. Si cette option est définie sur vrai, cela signifie que vous ne pouvez pas archiver les enregistrements, quelle que soit la définition des règles.

- Identité d'archivage
- Archiver le composant de données
- Archiver les programmes malveillants
- Archiver la perception d'objets
- Outil d'archivage
- Archiver l'événement de menace
- Archiver le modèle d'attaque
- Archiver le regroupement des menaces
- Vulnérabilité des archives
- Infrastructure d'archivage
- Archiver la note de menace
- Archiver le déroulement de l'action
- Archiver un acteur de menace
- Archiver le rapport de menace

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Archiver l'ensemble d'intrusion
- Archiver la campagne
- Archiver les données observées
- Archiver la définition de marquage
- Archiver l'opinion sur les menaces
- Archiver l'analyse de programme malveillant

Remarque : Pour archiver différents objets, suivez la procédure expliquée ici pour les règles Modifier les règles d'archivage pour les observablesd'archivage des observables.

Règles d'archivage des enregistrements connexes et des indicateurs

Les règles d'archivage pour les indicateurs et les enregistrements connexes qui sont provisionnés dans le système de base sont répertoriées dans la section ci-dessous.

Les exemples de règles d'archivage sont inactifs par défaut.

L'option **Historiquement significatif** et la condition doivent toujours être définies sur **False** pour les observables, les indicateurs, les enregistrements connexes et les objets. Si vous définissez cette option sur faux, vous pouvez archiver les enregistrements. Si cette option est définie sur vrai, cela signifie que vous ne pouvez pas archiver les enregistrements, quelle que soit la définition des règles.

- **Indicateur** : règle d'archivage de l'indicateur
- **Archivage des documents connexes** :
  - Règle d'archivage des observables connexes
  - Règle d'archivage de relation objet-objet
  - Règle d'archivage de relation objet-objet
  - Règle d'archivage de l'objet d'indicateur connexe
  - Règle d'archivage de l'indicateur connexe
  - Règle d'archivage observable d'indicateur connexe

Remarque : Pour archiver les indicateurs et les enregistrements associés, suivez la procédure expliquée ici pour les règles Modifier les règles d'archivage pour les observablesd'archivage des observables.

Règles d'archivage pour les enregistrements connexes

1. Pour les enregistrements connexes, les enregistrements sont archivés en fonction de l'objet ou de l'observable source et cible.
2. Le travail planifié **Mise à jour de la colonne archivée de la relation** est déclenché et s'exécute une fois par jour.
3. Une fois la tâche planifiée déclenchée et exécutée, les colonnes archivées source et archivée cible sont mises à jour en conséquence dans les enregistrements connexes.
4. Les règles d'archivage de relation, lorsqu'elles sont déclenchées lors de la prochaine exécution et identifient les enregistrements avec les colonnes archivées source et cible archivées, sont définies sur vrai et ces enregistrements sont archivés.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calendrier de la tâche d'archivage

Une fois que les règles d'archivage sont configurées et que des règles d'archivage sont actives, le travail d'archivage traite ces règles et archive les enregistrements.

La tâche planifiée d'archivage est configurée en tant que tâche de répétition d'une heure. Il appelle une classe qui transfère le thread à un thread d'arrière-plan appelé glide.db.archiver.

Afin d'éviter que le processus d'archivage ne consomme trop de ressources système, les propriétés d'archivage ci-dessous peuvent être utilisées pour contrôler le nombre d'enregistrements traités par la règle d'archivage à un intervalle.

En modifiant les propriétés d'archivage, la tâche d'archivage peut dépasser la durée de 1 heure et vous pouvez avoir plusieurs tâches d'archivage exécutées.

Propriétés des règles d'archivage

Ce qui suit décrit les propriétés de la règle d'archivage.

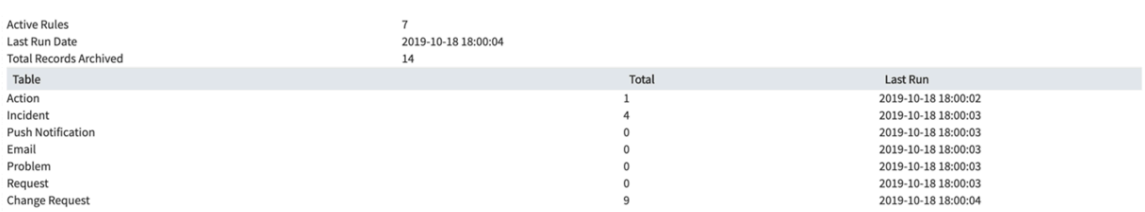
Nom	Description	Type	Valeur entière
glide.db.archive-.batch_size	Contrôle le nombre d'enregistrements qu'une règle d'archivage traite par traitement par traitement par lots.	Entier	1 000
glide.db.archive.sleep_time	Contrôle le temps de veille entre chaque exécution de tâche par lots de règle d'archivage, en secondes.	Entier	1
glide.db.archive-.max_itérations	Contrôle le nombre maximal de tâches par lots à exécuter dans un délai d'une heure.	Entier	10

Page de diagnostic des règles d'archivage

À l'aide de cette page, vous pouvez afficher les détails du nombre de règles d'archivage actives, du nombre total d'enregistrements qui ont été archivés et de la dernière exécution de la tâche d'archivage.

Lien permettant d'accéder à la page Diagnostic :

```
https://<your-instance>.service-now.com/ui_page.do?sys_id=71681edc9f3120007aaa207c7f4bcc2b
```



Active Rules	7
Last Run Date	2019-10-18 18:00:04
Total Records Archived	14

Table	Total	Last Run
Action	1	2019-10-18 18:00:02
Incident	4	2019-10-18 18:00:03
Push Notification	0	2019-10-18 18:00:03
Email	0	2019-10-18 18:00:03
Problem	0	2019-10-18 18:00:03
Request	0	2019-10-18 18:00:03
Change Request	9	2019-10-18 18:00:04

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure d'archivage

1. Chargez N enregistrements qui répondent aux critères de la règle d'archivage (où N est la propriété de taille de lot).
2. Insérer dans le tableau ar_*.
3. Supprimez l'enregistrement de la table d'origine.
4. Créez une entrée sys_archive_log.

Lorsqu'un enregistrement est archivé, une entrée est créée dans la table Journal d'archivage (sys_archive_log) et le code XML de l'enregistrement est enregistré en tant que charge utile.

Débogage

Quelques colonnes sont utiles pour le débogage : Exécution d'archivage, Archive, Restauré, ID et De la table.

1. **Exécution d'archivage** : cette opération vous donnera les détails de l'exécution d'archivage qui a archivé cet enregistrement.
2. **Archive** : règle d'archivage qui remplit la condition.
3. **Restauré** : ce champ est vide si l'enregistrement n'a pas été restauré. Si les enregistrements ont été restaurés, ce champ contient la date et l'heure de restauration de l'enregistrement.
4. **À partir de la table** : table à partir de laquelle l'enregistrement a été supprimé.

Important : La suppression d'une entrée de journal d'archivage vous empêche de restaurer les données des enregistrements archivés.

La présence d'une entrée dans le journal d'archivage est tout ce dont le système a besoin pour savoir que l'enregistrement a déjà été archivé (s'il a été restauré), en tout cas s'il a été ignoré, ce qui signifie que le moteur d'archivage ne réarchivera pas quelque chose qui a été restauré.

Les enregistrements connexes et les pièces jointes peuvent également être archivés, car dans la règle d'archivage, vous pouvez spécifier les enregistrements connexes que vous souhaitez archiver. Si vous restaurez l'enregistrement d'origine, les enregistrements connexes doivent également être restaurés (ceci n'est pas automatique, car les tables d'enregistrements connexes sont indépendantes après l'archivage).

Lancer une règle de destruction à partir d'un script

Créez une règle de destruction pour supprimer les enregistrements archivés et connexes après une durée spécifiée.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

- `new GlideArchiver().archiveDestroyByRule(xxxx) ; où xxxx est la sys_id de la règle de destruction.`
- Si vous devez modifier les propriétés de la règle de destruction qui s'exécutent sur vos données archivées, consultez Règle d'archivage et propriétés de la règle de destruction .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichez les règles de destruction pour les enregistrements archivés :

Procédure

1. Accédez à la **Tout** > **Archivage système** > **Archivage Règles de destruction**.
2. Sélectionnez n'importe quel enregistrement pour afficher la règle de destruction. En fonction de la période de durée d'archivage, les enregistrements sont automatiquement supprimés de l'application. Si vous souhaitez exécuter manuellement la règle de destruction, puis Exécuter la **destruction des archives maintenant** ou si vous souhaitez modifier la durée d'archivage par défaut, vous éditez ou modifiez le formulaire en conséquence.

Remarque : Pour chaque table, une règle de destruction individuelle s'applique.

Afficher les règles de destruction dans TISC

Affichez les règles de destruction qui sont mises en service dans le système de base.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Archivage système** > **Archivage Règles de destruction**. La liste des règles de destruction applicables pour TISC s'affiche. Ces règles de destruction sont différentes pour chaque type d'objet et s'appliquent indépendamment.
2. Consultez les règles de destruction applicables pour TISC.
3. Cliquez sur n'importe quelle règle pour afficher la période de durée d'archivage.



Limites de l'archivage des données

Il y a une limite à la taille d'une table d'archivage que vous pouvez créer pour stocker des données. La limite est basée sur la taille des données, et non sur le nombre d'enregistrements.

Si vous recevez une erreur indiquant qu'une table d'archivage n'a pas pu être créée, cela peut être lié à cette limitation de taille. Pour plus d'informations, reportez-vous à la section Limites de taille des tables d'archivage des données .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Surveillance des règles d'archivage

Cette section vous aide à suivre et à surveiller les règles d'archivage.

Description de la règle	Accédez à la	Sortie prévue
Threads d'archivage actifs	**Archivage système** > **État d'archivage**	• **Nom** : glde.db.archiver.xxxx où xxxx est le sysid de la règle d'archivage correspondante. • **Valeur** : démarrer avec actif ou inactif
Progression globale de l'archivage	**Archivage système** > **Règles d'archivage**	La colonne d'estimation indique le nombre d'enregistrements qui doivent encore être archivés. Mis à jour toutes les heures avant l'itération suivante.
Progression de l'archivage individuel	**Archivage système** > **Règles d'archivage**	• **Durée** : environ 45 minutes. • **Total primaire** : 30000 par exécution.

Ressources d'apprentissage

Cette section ci-dessous vous permet d'en savoir plus sur le processus d'archivage des données et les meilleures pratiques.

Références

Titre de référence	Liens de référence
Comment restaurer plusieurs enregistrements connexes archivés d'enregistrements archivés en mode batch.	KB0819650
Archivage des données : vue d'ensemble et FAQ	KB0785300
Archivage | Recherches Splunk	KB0782324
Pièces jointes orphelines Enregistrements de documents en raison de l'archivage	KB0647663
Archiver l'architecture des tâches, configuration des règles d'archivage, règles de destruction des archives	
Archivage multithread	KB0821186
Bonnes pratiques d'archivage	KB0999731
Archivage des données sur docs.servicenow.com	Administration de la Now Platform

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Références (suite)

Titre de référence	Liens de référence
Archiver la règle et détruire les propriétés de la règle sur docs.servicenow.com	Administration de la Now Platform
Archivage de l'enregistrement TOI	Archivage
Vidéos d'entraînement à la performance	KB0960168

Flux fonctionnel de traitement des données TISC

Threat Intelligence Security Center (TISC) fournit une solution qui automatise la collecte et le traitement des données, ce qui permet de réduire la charge de travail des analystes Threat Intelligence en évitant les étapes manuelles impliquées.

Le Centre de sécurité des renseignements sur les menaces (TISC) collecte des renseignements à l'aide de l'une des méthodes suivantes :

1. Ingestion à partir de sources de données préconfigurées et exécutées selon une planification.
2. Analystes Intelligence sur les menaces qui importent des données à l'aide de la fonctionnalité Import Intelligence.
3. Création manuelle d'enregistrements individuels au sein de l'application.

> **Remarque :** Les données collectées dans l'application sont traitées pour normaliser, dédupliquer et agréger les informations avant le chargement dans la bibliothèque Threat Intel.

Terminologie de base utilisée dans le traitement des données

1. Tables sources : les tables sources contiennent les données relatives aux entités qui sont extraites de plusieurs sources, puis les enregistrements sont créés par chaque source.
2. Enregistrements agrégés : les tables d'enregistrements agrégés contiennent les données relatives à une entité spécifique en agrégeant les données de tous les enregistrements sources d'une entité spécifique.

Flux de données TISC

1. En cas d'exécution réussie de l'intelligence d'importation/source de données, les enregistrements sont créés dans les tables source correspondantes.
2. Une fois que les données entrent dans la table source, elles passent par une logique de filtrage pour valider si l'enregistrement doit être filtré en fonction des **règles de filtrage entrant configurées**. (Considérons SourceRecord1 comme un enregistrement source pour notre explication).
3. Si l'enregistrement est filtré par l'une des règles de filtrage entrant configurées, l'enregistrement source correspondant (SourceRecord1) est marqué comme **filtré** et la règle qui a filtré l'enregistrement se trouve dans la règle de filtrage appliquée.
4. Supposons que l'enregistrement source (SourceRecord1) s'agrège en AggregateRecord1.
5. Si l'enregistrement n'est pas filtré, il est marqué pour la déduplication en définissant l'état du traitement sur Prêt pour la déduplication.
6. La logique de déduplication valide les éléments ci-dessous :

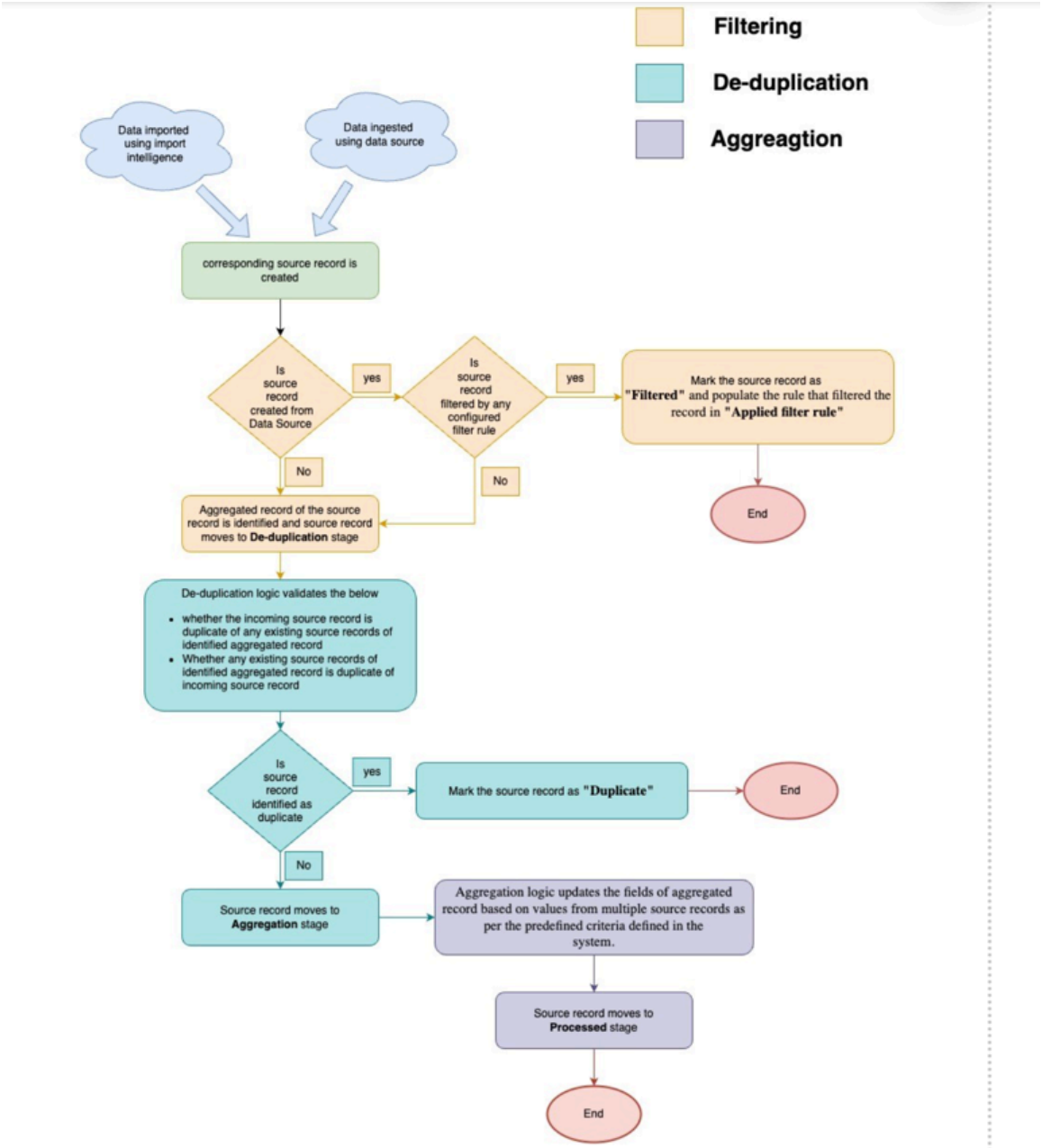
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

   a. Indique si l'enregistrement source entrant (SourceRecord1) est un doublon de tout enregistrement source existant pour AggregateRecord1.
   b. Tous les enregistrements sources existants pour AggregateRecord1 sont un doublon de l'enregistrement source entrant (SourceRecord1).
7. Chaque entité a des champs et des relations spécifiques sur la base desquels l'enregistrement source est validé pour la duplication.
8. Si l'enregistrement source entrant (SourceRecord1) est un doublon d'un enregistrement source existant de AggregateRecord1, l'enregistrement source entrant (SourceRecord1) est marqué comme Doublon.
9. Si l'un des enregistrements sources existants (Existing Source Record1) de AggregateRecord1 est identifié comme doublon de l'enregistrement source entrant (SourceRecord1), alors l'enregistrement source existant (Existing Source Record1) est marqué comme Doublon et l'enregistrement source entrant (SourceRecord1) est marqué pour l'agrégation en définissant l'état du traitement sur Prêt pour l'agrégation.
10. Dans le cadre de l'agrégation, les champs de l'enregistrement agrégé AggregateRecord1 sont mis à jour en fonction des valeurs provenant de plusieurs enregistrements sources qui sont regroupés selon les critères prédéfinis définis dans le système.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Data Loss Prevention Incident Response

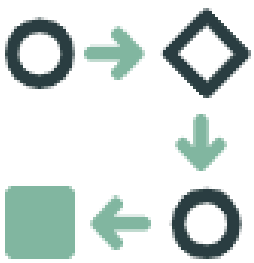
L'application Data Loss Prevention Incident Response (DLP IR) vous permet d'examiner et de gérer le workflow de rattrapage des incidents DLP provenant de plusieurs sources, telles que les points de terminaison, le réseau, la messagerie électronique et le cloud.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Data Loss Prevention Incident Response

Explorer	Installer et configurer	Administrer
		
En savoir plus sur la façon dont les analystes et les administrateurs utilisent DLP Incident Response	Installation et configuration de l'application DLP Incident Response	Tâches d'administration sur la gestion des incidents DLP sur la Now Platform
Utiliser	**Intégrer**	
		
Mettez à jour et gérez les incidents en tirant parti du portail de l'utilisateur final DLP, du portail des opérations DLP et du tableau de bord DLP.	Étendre les options DLP en s'intégrant à des applications tierces	

Traduction automatique

Explorer Data Loss Prevention Incident Response

Explorez Data Loss Prevention Incident Response l'application pour apprendre à gérer les informations sensibles de vos clients, telles que les données financières et propriétaires, les dossiers médicaux ou les numéros de sécurité sociale.

La perte de données se produit lorsque des informations confidentielles ou sensibles quittent le réseau de l'entreprise à la suite d'une communication non autorisée. Avec l'application DLP, vous pouvez identifier, répondre et protéger vos canaux de perte de données.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En utilisant l'application Data Loss Prevention Incident Response , votre organisation bénéficie des avantages clés suivants :

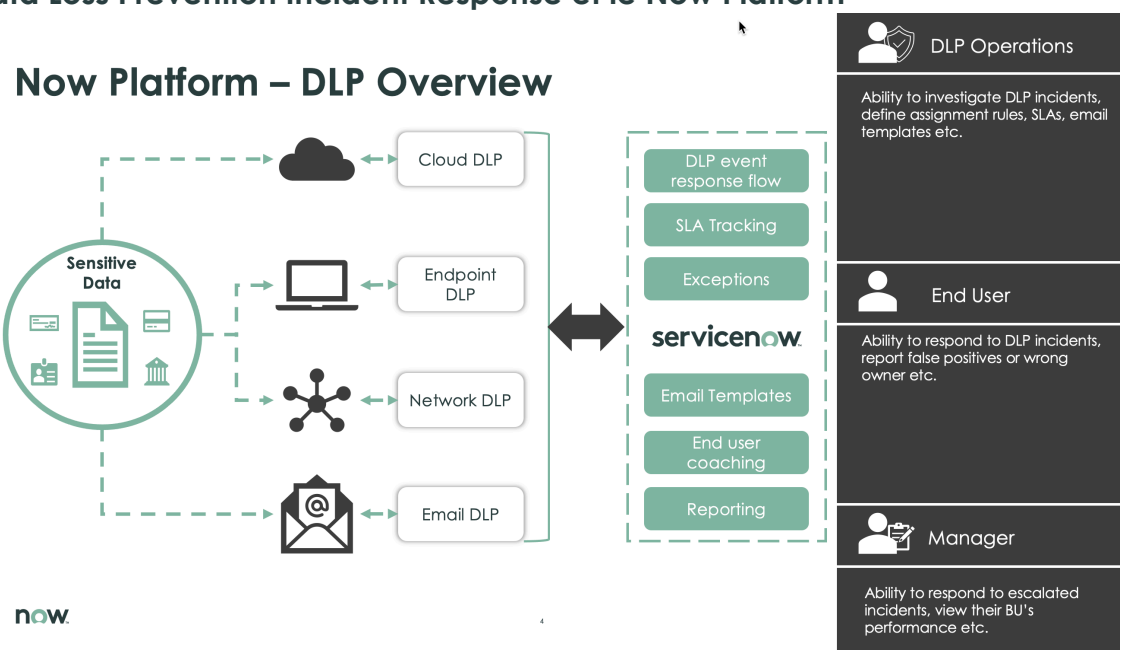
- Intégration à plusieurs solutions de prévention des pertes de données tierces pour obtenir une vue unifiée des incidents dans le Now Platform.
- Surveiller et affecter des incidents aux utilisateurs finaux afin de rationaliser la gestion des incidents DLP.
- Coachez vos employés à travers les modèles d'e-mails personnalisés et les notifications qui sont envoyés pour chaque incident, ainsi que sous la forme d'un résumé.
- Escaladez les incidents DLP en retard des utilisateurs finaux vers les gestionnaires.
- Affichez des rapports récapitulatifs des incidents ouverts par politique, gravité, principaux contrevenants, et ainsi de suite.
- Suivez les tendances des incidents DLP, les tendances des faux positifs et les tendances de rattrapage.

Utilisez cette section pour en savoir plus sur les fonctionnalités clés et les différents rôles impliqués dans le travail avec les incidents DLP.

Vue d'ensemble de la réponse aux incidents DLP

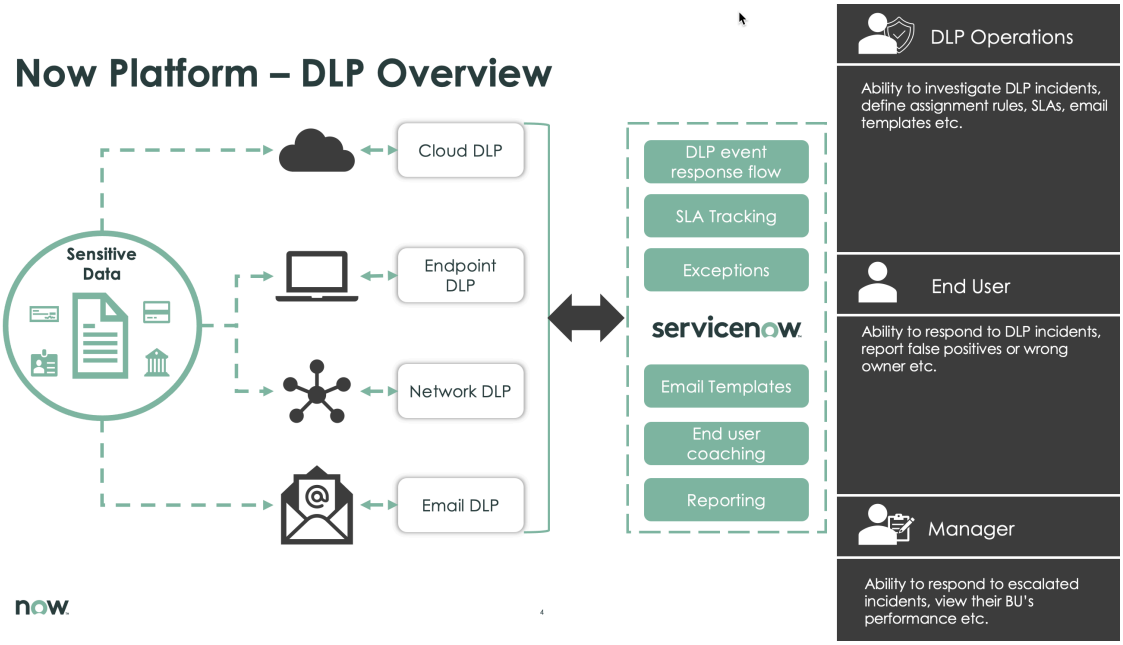
Découvrez comment utiliser l'application Now Platform et l'application Data Loss Prevention Incident Response (DLP IR). Gérez les informations sensibles de vos clients, telles que les données financières et propriétaires, les dossiers médicaux ou les numéros de sécurité sociale. Automatisez les workflows de rattrapage avec l'application DLP Incident Response.

Data Loss Prevention Incident Response et le Now Platform



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



1. Il s'agit d'une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP
2. Tâches de l'administrateur DLP : il s'agit d'une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP
3. Utilisation du portail de l'utilisateur final DLP : il s'agit d'une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP
4. Utilisation du portail des opérations DLP : il s'agit d'une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP
5. Utilisation du tableau de bord DLP : il s'agit d'une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP

L'application Data Loss Prevention Incident Response comprend les fonctionnalités suivantes :

- Espace de travail de l'utilisateur final où vos utilisateurs finaux ou employés peuvent examiner les incidents DLP affectés et y répondre.
- Espace de travail de gestionnaire où un gestionnaire peut examiner les incidents DLP escaladés et prendre des mesures appropriées.
- Espace de travail unifié où votre équipe des opérations DLP peut suivre les tendances des incidents ouverts, des principaux contrevenants et des incidents par source d'analyse, et peut afficher, modifier, affecter et fermer les incidents DLP sur plusieurs sources (points de terminaison, réseaux et e-mail).
- Contrôles administratifs qui définissent les modèles d'e-mail pour le coaching et la communication des utilisateurs finaux, règles d'affectation pour l'affectation automatique des incidents, règles d'escalade automatique et délégation pour la réponse aux incidents.

Introduction à Réponse aux incidents DLP

Vérifiez les informations suivantes avant de commencer à configurer votre Data Loss Prevention Incident Response application (DLP IR).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis Now Platform et DLP.	DLP Incident Response prend en charge les rôles suivants : • L'administrateur (admin) installe les applications à partir de et ServiceNow Store affecte l'administrateur DLP (sn_dlir.admin). • sn_dlir.admin • sn_dlir.analyste
Vérifiez que les ServiceNow applications principales qui sont requises pour prendre en charge l'application Data Loss Prevention Incident Response sont installées et activées.	Le Data Loss Prevention Incident Response module d'extension (com.snc.data_loss_incident) est requis pour prendre en charge le Data Loss Prevention Incident Response produit. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour garantir une installation fluide : • Prévention de la perte de données Réponse aux incidents (com.snc.data_loss_incident) • Security Support Common Pour plus d'informations sur la configuration de votre Now Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une application Security Operations ou Activer une application ServiceNow Store.
Séparation de domaine	Vérifiez la rubrique si vous avez l'intention de séparer les données, les processus et les Séparation de domaine et Réponse aux incidents DLP tâches administratives.

Installation et configuration DLP IR d'Incident Response

Téléchargez l'application Data Loss Prevention Incident Response (DLP IR) à partir de et ServiceNow Store installez-la sur votre instance.

Avant d'appeler les workflows pour l'intégration, installez et configurez l'application Data Loss Prevention Incident Response à partir de ServiceNow Store sur votre Now Platform instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installez et configurez l'application Réponse aux incidents DLP

Gérez les informations sensibles et automatisez les workflows de rattrapage à l'aide de l'application Data Loss Prevention Incident Response (DLP IR) de votre Now Platform instance.

Avant de commencer

Avant de pouvoir effectuer les étapes de configuration, vous devez télécharger l'application à ServiceNow Store partir du et l'installer sur votre instance.

Rôles requis : admin et sn_dlir.admin

Procédure

1. Suivez les instructions de téléchargement d'une application à partir de ServiceNow Store.
2. Une fois que vous avez téléchargé l'application **Réponse aux incidents DLP** et toutes ses applications dépendantes, naviguez vers **Tout** > **Administration DLP** > **Configuration par défaut** pour terminer le reste de la configuration de l'application.

Séparation de domaine et Réponse aux incidents DLP

Vous pouvez utiliser Séparation de domaine avec Réponse aux incidents DLP pour séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Standard

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Fonctionnement de Séparation de domaine avec DLP Incident Response

- Créez un utilisateur avec les rôles requis sn_dlir.admin et sn_dlir.analyst dans le domaine respectif.
- Effectuez les configurations de Réponse aux incidents DLP dans le domaine approprié.

Administration de Réponse aux incidents DLP

Vous pouvez configurer et affecter des règles, configurer des règles de date d'échéance, utiliser des modèles d'e-mail, configurer des actions de réponse de l'utilisateur final et bien plus encore pour gérer les Data Loss Prevention Incident Response incidents (DLP IR) sur le Now Platform.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'application Data Loss Prevention Incident Response vous permet d'effectuer les configurations suivantes.

Paramètres de configuration DLP par défaut

Définissez les paramètres de configuration par défaut pour Data Loss Prevention Incident Response les incidents (DLP IR) afin d'identifier et de configurer les préférences de notification d'incident et d'affectation d'incident pour vos utilisateurs finaux.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

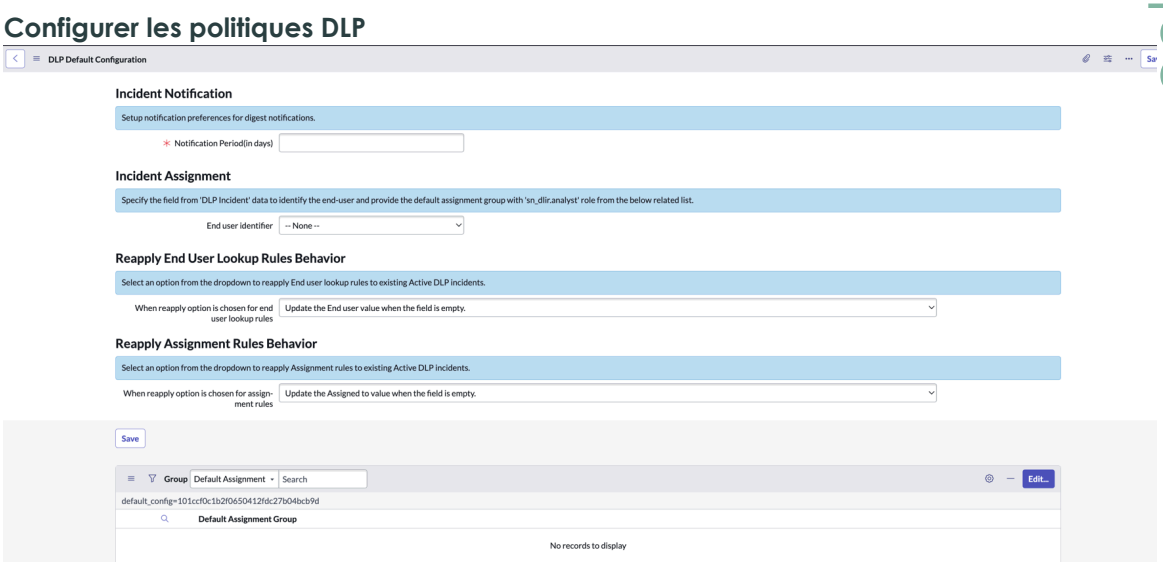
Ce module vous permet de définir les paramètres de configuration par défaut lorsque les règles d'affectation de base et les règles d'identificateur sont épuisées et ne peuvent pas correspondre à une condition ou à un utilisateur. Vous pouvez également définir et réappliquer des règles de recherche d'utilisateur final et des règles d'affectation aux incidents DLP actifs existants.

La notification d'incident de l'utilisateur final vous permet de spécifier la fréquence à laquelle les notifications par e-mail sont envoyées à vos utilisateurs finaux. Par exemple, vous pouvez configurer des préférences de notification pour accumuler les incidents et envoyer un résumé d'e-mail une fois par semaine. En affectant un incident, vous pouvez spécifier à quel groupe vous affectez initialement les incidents DLP. Vous pouvez également spécifier comment les utilisateurs finaux sont identifiés par l'équipe des opérations DLP.

Par exemple, supposons qu'un utilisateur ait stocké des informations de carte de crédit dans un fichier sur un réseau. Lorsque le produit tiers d'intégration DLP crée un incident pour violation de la politique en matière de données sensibles, les données d'incident ingérées par le Now Platform DLP contiennent des informations sur l'utilisateur final. Vous serez alors en mesure d'affecter l'incident à l'utilisateur final approprié.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Configuration par défaut**.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Renseignez les champs du formulaire.

Formulaire Configuration DLP par défaut

Nom de la configuration	Champ	Description
Notification d'incident de l'utilisateur final	Période de préavis (jours)	Définissez le nombre de jours après lequel une notification par e-mail doit être envoyée à l'utilisateur final. Le nombre de jours doit être compris entre 1 et 60 jours.
	Mettre à jour automatiquement l'état parent en fonction des incidents clonés/enfants	Option permettant de mettre à jour automatiquement l'incident de l'état parent en fonction des incidents clonés ou enfants.
Affectation d'incident	Identificateur de l'utilisateur final	Spécifiez le champ à utiliser à partir des données d'incident pour identifier l'utilisateur final. Les valeurs possibles sont les suivantes : ◦ **E-mail du propriétaire des données** ◦ **Destination** ◦ **Fichier créé par** ◦ **Fichier modifié par** ◦ **Propriétaire du fichier** ◦ **Nom d'utilisateur FTP** ◦ **Expéditeur**
Réappliquer le comportement des règles de recherche de l'utilisateur final	Quand l'option Nouv. demande choisie pour règles de rech. de l'utilisateur final	Option permettant de réappliquer des règles de recherche d'utilisateur final aux incidents DLP actifs existants. Vous pouvez sélectionner l'une des options suivantes pour présenter une nouvelle demande : ◦ **Mettre à jour la valeur Utilisateur final quand le champ est vide** : met à jour la valeur Utilisateur final des incidents DLP actifs existants si ce champ est vide. ◦ **Mettre à jour la valeur Utilisateur final** : met à jour la valeur Utilisateur final des incidents DLP actifs existants. ◦ **Mettez à jour les valeurs Utilisateur final et Affecté à lorsque les deux champs sont vides** : Met à jour les valeurs Utilisateur final et Affecté à des incidents DLP actifs existants si les deux champs sont vides.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la configuration	Champ	Description
		Remarque : Si cette option est sélectionnée, l'option **Mettre à jour la valeur Affecté à lorsque le champ est vide** est automatiquement désactivée dans la section Réappliquer le comportement des règles d'affectation, car elle s'applique aux deux. ◦ **Mettre à jour les valeurs Utilisateur final et Affecté à pour tous les incidents DLP actifs** : met à jour les valeurs Utilisateur final et Affecté à pour tous les incidents DLP actifs. **Remarque :** Si cette option est sélectionnée, l'option **Mettre à jour la valeur Affecté à pour tous les incidents DLP actifs** est automatiquement désactivée dans la section Comportement à réappliquer des règles d'affectation, car elle s'applique aux deux.
Réappliquer le comportement des règles d'affectation	Lorsque l'option de Nouvelle demande est choisie pour les règles d'affectation	Option permettant de réappliquer des règles d'affectation aux incidents DLP actifs existants. Vous pouvez sélectionner l'une des options suivantes pour présenter une nouvelle demande : ◦ **Mettez à jour la valeur Affecté à quand le champ est vide.** ◦ **Mettez à jour la valeur Affecté à pour tous les incidents DLP actifs.**

3. Sélectionnez le **groupe d'affectation par défaut** dans la section de liste connexe à laquelle tous les incidents DLP sont affectés.
   Cliquez sur **Modifier** pour ajouter le groupe d'utilisateurs. Lorsque vous cliquez sur **Modifier** dans la section de liste connexe et que vous sélectionnez un élément dans les colonnes **Collections** , puis que vous ajoutez ce délégataire sélectionné aux colonnes Groupe de la page **Modifier les membres** , puis que vous enregistrez la liste.

   Remarque : Vous ne pouvez afficher et sélectionner que les groupes qui ont été affectés au rôle sn_dlir.analyst à partir de la liste connexe. Vous ne pouvez sélectionner qu'un seul groupe.

4. Cliquez sur **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer des règles de recherche d'utilisateur final

Vous pouvez créer et configurer des règles de recherche d'utilisateur final et affecter les incidents DLP aux utilisateurs finaux respectifs en fonction de ces règles.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

L'administrateur DLP définit ces règles de recherche d'utilisateur final pour affecter automatiquement les utilisateurs finaux aux incidents DLP en utilisant uniquement le champ d'utilisateur final. La règle de recherche d'utilisateur final DLP vous permet d'affecter l'utilisateur final à des incidents DLP en fonction de l'identificateur d'utilisateur final, d'attributs personnalisés ou d'un script.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Règles de recherche d'utilisateur final DLP**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Règle de recherche d'utilisateur final DLP

Champ	Description
Nom	Nom de la règle de recherche de l'utilisateur final.
Actif	Option permettant d'indiquer si la règle de recherche de l'utilisateur final est active.
Ordre d'exécution	La priorité de la règle de recherche de l'utilisateur final. Ce champ indique l'ordre dans lequel les règles de recherche de l'utilisateur final sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle de recherche de l'utilisateur final associée au numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Description	Description unique de la règle de recherche d'utilisateur final.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour la règle de recherche de l'utilisateur final, sélectionnez l'un des champs d'incident.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

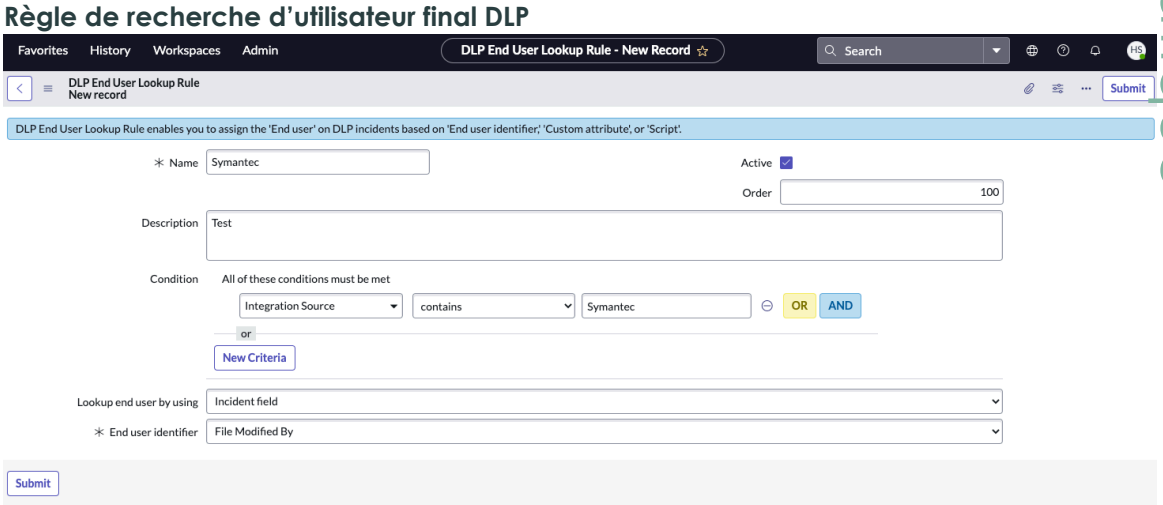
Champ	Description
	Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, vous pouvez définir les conditions de cette règle de recherche d'utilisateur final en sélectionnant la condition Source **d'intégration**, **contient**, **Symantec**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Rechercher un utilisateur final à l'aide de	Option permettant de rechercher un utilisateur final à l'aide du **champ Incident** ou **d'un script**.
Identificateur de l'utilisateur final	L'identificateur d'utilisateur final de l'incident DLP. Ce champ s'affiche lorsque le **champ Incident** est sélectionné dans le champ **Rechercher un utilisateur final à l'aide** du champ. Vous pouvez sélectionner un identificateur d'utilisateur final parmi les suivants : ◦ **E-mail du propriétaire des données** ◦ **Destination** ◦ **Fichier créé par** ◦ **Fichier modifié par** ◦ **Propriétaire du fichier** ◦ **Nom d'utilisateur FTP** ◦ **Expéditeur**

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Les identificateurs d'utilisateur final répertoriés ci-dessus peuvent être configurés à l'aide de la propriété système `sn_dlir.assignment.fields`. Pour plus d'informations, consultez Configurer les paramètres avancés. ◦ **Utilisateur personnalisé à partir de l'incident**
Attribut personnalisé	Option permettant de spécifier un attribut personnalisé à partir de l'incident qui fait référence à un utilisateur. Ce champ s'affiche uniquement lorsque **le a** est sélectionné dans le champ **Identificateur de l'utilisateur final** .
Script	Vous pouvez utiliser l'éditeur de script pour personnaliser et formater les valeurs de champ lors de la création de la règle de recherche de l'utilisateur final. Par exemple, vous pouvez utiliser le champ de l'adresse e-mail pour identifier l'utilisateur final.

Example
L'exemple suivant montre une règle de recherche d'utilisateur final portant le nom « Symantec ». Le créateur de conditions nécessite que la « source d'intégration » soit « Symantec ». **L'option Rechercher un utilisateur final à l'aide** de l'option est définie sur « Champ d'incident » et l'option **d'identificateur d'utilisateur final** est définie sur « Fichier modifié par ».

Règle de recherche d'utilisateur final DLP



4. Cliquez sur **Envoyer**.
   Vous pouvez également sélectionner une ou plusieurs règles de recherche d'utilisateur final et les réappliquer à tous les incidents DLP existants.
5. Pour réappliquer une règle de recherche de l'utilisateur final à tous les incidents DLP existants, cliquez sur **Réappliquer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer des règles d'affectation

Utilisez cette section pour créer des règles d'affectation. Affectez ensuite les Data Loss Prevention Incident Response incidents (IR DLP) à des groupes d'utilisateurs, des utilisateurs finaux, des gestionnaires ou à un utilisateur de l'incident.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser des règles d'affectation pour affecter des incidents DLP IR à des groupes d'utilisateurs, des utilisateurs finaux ou à des gestionnaires. L'affectation des incidents DLP se produit lorsque les conditions de la règle d'affectation sont remplies.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Règles d'affectation**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Règle d'affectation DLP

Champ	Description
Nom	Nom de la règle d'affectation.
Actif	Option permettant d'indiquer si la règle d'affectation est active.
Ordre d'exécution	Priorité de la règle d'affectation. Ce champ indique l'ordre dans lequel les règles d'affectation sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle d'affectation associée au numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Description	Description unique de cette règle d'affectation.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour la règle d'affectation, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, supposons que vous créiez une règle d'affectation DLP pour un point de terminaison. Vous pouvez spécifier que la source d'analyse des conditions est un système de fichiers de point de terminaison qui doit être rempli avant d'affecter un incident. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Affecter à	Affectation à l'un des éléments suivants : ◦ Groupe d'utilisateurs ◦ Utilisateur final ◦ Responsable ◦ Utilisateur à partir de l'incident L'affectation a lieu lorsque les conditions du générateur de conditions sont remplies.
Groupe d'utilisateurs	Option permettant de rechercher et de sélectionner un groupe d'utilisateurs auquel affecter les incidents DLP. Ce champ s'affiche lorsque Groupe **d'utilisateurs** est sélectionné dans le champ **Affecter à** . **Remarque :** Vous ne pouvez afficher et sélectionner que les groupes auxquels le rôle sn_dlir.analyst a été affecté.
Utilisateur final	Option permettant d'affecter l'incident DLP à l'utilisateur final. L'affectation a lieu lorsque les conditions du générateur de conditions sont remplies.
Affecter à l'aide des champs de Gestionnaire	Responsable de l'utilisateur final Ce champ s'affiche lorsque **le gestionnaire** est sélectionné dans le champ **Affecter à** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Vous pouvez affecter des incidents DLP à un gestionnaire particulier en sélectionnant l'un des champs du gestionnaire, tel que Nom de famille, E-mail, Ville, Numéro d'employé.
Identificateur de l'utilisateur	L'identificateur utilisateur de l'incident. Ce champ s'affiche lorsque **l'utilisateur de l'incident** est sélectionné dans le champ **Affecter à** . Vous pouvez sélectionner un identificateur d'utilisateur parmi les suivants : ◦ **E-mail du propriétaire des données** ◦ **Destination** ◦ **Fichier créé par** ◦ **Fichier modifié par** ◦ **Propriétaire du fichier** ◦ **Nom d'utilisateur FTP** ◦ **Expéditeur** ◦ **Utilisateur personnalisé à partir de l'incident**
Attribut personnalisé	Option permettant de spécifier un attribut personnalisé à partir de l'incident qui fait référence à un utilisateur. Ce champ s'affiche uniquement lorsque **l'utilisateur personnalisé à partir de l'incident** est sélectionné dans le champ **Identificateur de l'utilisateur** .
Joindre l'évaluation	Option permettant d'indiquer si vous souhaitez joindre une évaluation à l'incident.
État de la réponse pré-évaluation	Option permettant de sélectionner l'état dans lequel l'incident doit se trouver avant que l'utilisateur final ne réponde. Il peut également s'agir d'un état personnalisé. La valeur par défaut est En attente d'évaluation.
État de la réponse post-évaluation	Option permettant de sélectionner l'état dans lequel l'incident DLP doit se trouver une fois que l'utilisateur a répondu. La valeur par défaut est Évaluation terminée.
Avancés	Option avancée permettant d'identifier l'utilisateur final. Ce champ s'affiche uniquement lorsque **l'utilisateur**

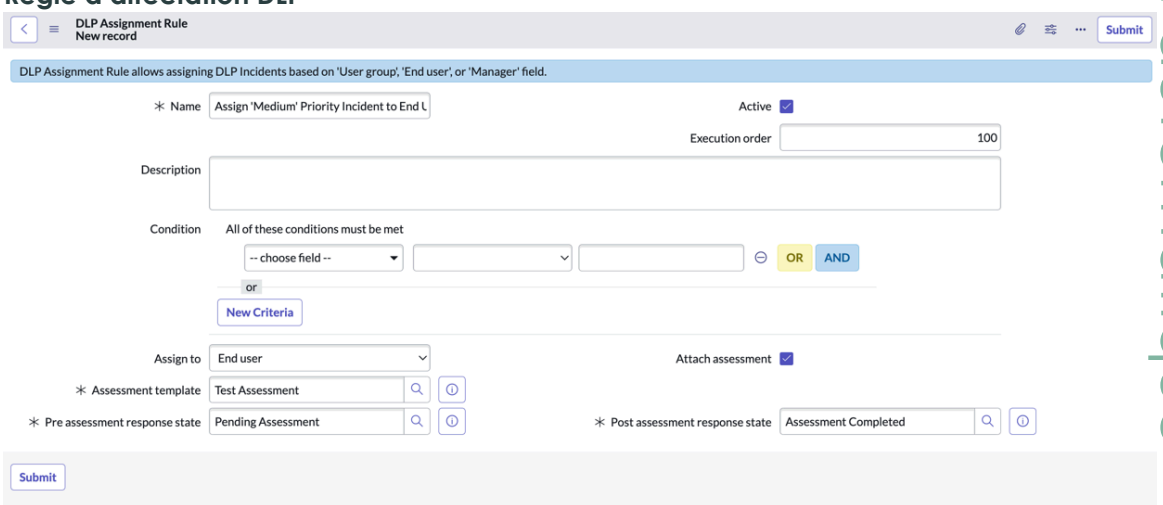
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	personnalisé à partir de l'incident est sélectionné dans le champ **Identificateur de l'utilisateur** . Vous pouvez utiliser l'éditeur de script pour personnaliser et formater les valeurs de champ lors de la création de la règle d'affectation afin d'identifier l'utilisateur final. Ensuite, vous choisissez la personne à qui affecter l'incident DLP, qui peut être un utilisateur final ou le responsable de l'utilisateur final. Par exemple, vous pouvez utiliser le champ de l'adresse e-mail pour identifier l'utilisateur final.

Example
L'exemple suivant montre une règle d'affectation dont le nom est `Affecter un incident de priorité « moyenne » à l'utilisateur final`. Le générateur de conditions exige que la source `d'analyse soit Affecter un incident de priorité « moyenne » à l'utilisateur final` et que le champ `Affecter à` soit défini sur `Utilisateur final`. Ensuite, vous pouvez rechercher l'e-mail de l'utilisateur final.

Règle d'affectation DLP



4. Sélectionnez le champ **Affecter à** de la section de liste connexe à laquelle tous les incidents DLP sont affectés.
   Cliquez sur **Modifier** pour ajouter le groupe d'utilisateurs. Lorsque vous cliquez sur **Modifier** dans la section de liste connexe et que vous sélectionnez un élément dans les colonnes **Collections** , puis que vous ajoutez ce délégataire sélectionné aux colonnes Groupe de la page **Modifier les membres** , puis que vous enregistrez la liste.

   Remarque : Vous ne pouvez afficher et sélectionner que les groupes qui ont été affectés au rôle sn_dlir.analyst à partir de la liste connexe. Vous ne pouvez sélectionner qu'un seul groupe.

5. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez également sélectionner une ou plusieurs règles d'affectation et les réappliquer à tous les incidents DLP existants.

6. Pour réappliquer une règle d'affectation à tous les incidents DLP existants, cliquez sur **Réappliquer**.

Créer des règles de consolidation d'incident

Créez une règle de consolidation des incidents pour regrouper plusieurs incidents de nature similaire sous un seul incident parent.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer
- sn_dlir.analyst et sn_dlir.analyst_read - Afficher (lecture seule)

Pourquoi et quand exécuter cette tâche

L'administrateur DLP définit ces règles de consolidation des incidents pour consolider automatiquement les incidents DLP de même nature sous un seul incident parent. La règle de consolidation des incidents DLP vous permet de consolider les incidents DLP en fonction de la configuration fournie pour la durée de consolidation et l'identification de la consolidation.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Règles de consolidation des incidents DLP**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Règle d'affectation DLP

Champ	Description
Nom	Nom de la règle de consolidation des incidents.
Actif	Option permettant d'indiquer si la règle de consolidation des incidents est active.
Ordre d'exécution	Priorité de la règle de consolidation des incidents. Ce champ indique l'ordre dans lequel les règles de consolidation d'incidents sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle de consolidation des incidents associée au numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Description	Description unique de la règle de consolidation des incidents.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour la règle de consolidation des incidents, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, vous pouvez définir les conditions de cette règle de consolidation des incidents en sélectionnant la condition Source **d'intégration**, **contient**, **Symantec**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Durée de la consolidation	Option permettant de définir la durée de la consolidation d'incidents. Les incidents de cette période avec les mêmes valeurs pour les champs sélectionnés seront regroupés sous le premier incident. Le premier incident correspondant à cette règle sera l'incident parent et les autres incidents seront des incidents enfants.
Consolider les incidents par	Sélectionnez le champ d'incident DLP pour consolider les incidents tout en ayant la même valeur dans le champ sélectionné pour différents incidents. Sélectionnez au moins un champ. Sélectionnez au moins un champ.

L'exemple suivant montre une règle de consolidation des incidents intitulée Consolider les incidents pour l'intégration Symantec. Le générateur de conditions exige que la source d'intégration soit Symantec. L'option **Durée de la condition** est définie sur 1 heure et l'option Nom de politique est sélectionnée pour **Consolider l'incident par**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Au moment de l'ingestion d'un incident Symantec DLP, cette règle est exécutée et, lorsque plusieurs incidents ont le même nom de politique, l'incident est consolidé sous le premier incident ingéré correspondant à cette règle.

4. Cliquez sur **Envoyer**.
   Les incidents consolidés en fonction de la règle de consolidation seront disponibles sous la liste Incidents enfants sur l'espace de travail de l'analyste DLP.

Créer des règles de date d'échéance de la réponse

Configurez les règles de date d'échéance de réponse pour déterminer le délai que vous souhaitez donner à vos utilisateurs finaux pour répondre aux incidents affectés Data Loss Prevention Incident Response (DLP IR).

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

Ce module vous permet de définir les règles de date d'échéance de réponse pour les différents types d'incidents DLP et les règles pour commencer à compter la date d'échéance. Une fois la date d'échéance expirée, les utilisateurs sont informés de l'incident en retard. Vous avez également la possibilité d'escalader l'incident en retard à l'une des situations suivantes :

- Responsable
- Utilisateur personnalisé à partir de l'incident
- Groupe d'utilisateurs

Par exemple, lorsque vous escaladez l'incident en retard vers un gestionnaire et que vous avez spécifié un maximum de trois niveaux d'escalade. Le premier niveau de Gestionnaire est notifié en premier. Si l'incident est à nouveau en retard, le deuxième niveau du Gestionnaire est notifié, suivi du troisième niveau si l'incident est toujours en retard. Si le gestionnaire a un délégué, il a la possibilité d'affecter l'escalade ou l'incident en retard au délégué.

Vous pouvez également créer plusieurs règles de date d'échéance de réponse.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Règles relatives à la date d'échéance de la réponse**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Règle de date d'échéance de la réponse

Champ	Description
Nom	Nom de la règle relative à la date d'échéance de la réponse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Option permettant d'indiquer si la règle de la date d'échéance de la réponse est active.
Échéance dans (jours)	Nombre de jours d'échéance.
Date d'échéance comptée à partir de	Date de début utilisée pour calculer la date d'échéance. La date d'échéance peut être calculée à partir de la première fois que l'utilisateur a été informé de l'incident ou à partir de la date d'affectation de l'incident.
Notifier avant la date d'échéance	Option permettant d'informer l'utilisateur final de l'incident DLP avant la date d'échéance.
Notifier le (jour avant la date d'échéance)	Nombre de jours avant la date d'échéance lorsque la règle déclenche une notification à l'utilisateur final.
Description	Description unique de cette règle de date d'échéance de réponse.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour la règle de date d'échéance de la réponse, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Escalader	Option permettant d'escalader l'incident DLP à quelqu'un si la date d'échéance de la réponse n'a pas été respectée. Pour plus d'informations, voir Ajouter plusieurs utilisateurs pour accéder aux incidents DLP

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Escalader un incident en retard à	Option permettant de spécifier si l'incident doit être escaladé à un gestionnaire, à un utilisateur personnalisé ou à un groupe d'utilisateurs. Ce champ s'affiche uniquement lorsque l'option **Escalader** est activée.
Affecter à l'aide de	Spécifiez comment identifier un gestionnaire. Ce champ est disponible uniquement lorsque **le gestionnaire** est sélectionné dans le champ **Escalader un incident en retard à** .
Niveaux d'escalades maximums	Option permettant de définir le nombre maximal de niveaux d'escalade pour un gestionnaire et un utilisateur personnalisé. En tant que gestionnaire ou utilisateur personnalisé, vous pouvez définir n'importe quel nombre de niveaux d'escalade. Par défaut, trois niveaux d'escalade sont fournis. ◦ En tant que gestionnaire, vous pouvez définir n'importe quel nombre de niveaux d'escalade en mettant à jour la valeur de ce champ. ◦ En tant qu'utilisateur personnalisé, vous pouvez utiliser l'icône + pour définir n'importe quel nombre de niveaux d'escalade.
Attribut personnalisé	Option permettant de spécifier un attribut personnalisé à partir de l'incident qui fait référence à un utilisateur. Ce champ s'affiche uniquement **lorsqu'un utilisateur personnalisé à partir de l'incident** est sélectionné dans le champ **Escalader un incident en retard à** .
Groupe d'utilisateurs	Option permettant de rechercher et de sélectionner un groupe d'utilisateurs auquel escalader les incidents DLP. Ce champ s'affiche uniquement lorsque le **groupe d'utilisateurs** est sélectionné dans le champ **Escalader l'incident en retard à** .

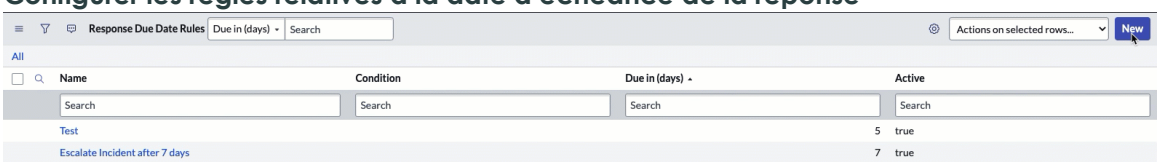
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Vous ne pouvez afficher et sélectionner que les groupes auxquels le rôle sn_dlir.analyst a été affecté.

Example
L'exemple suivant montre la règle de la date d'échéance de la réponse pour déterminer le temps que vous souhaitez donner à vos utilisateurs finaux pour répondre aux incidents affectés Data Loss Prevention Incident Response (DLP). Une fois que l'utilisateur final a été notifié pour la première fois, la date d'échéance de la réponse est dans deux jours. Le générateur de conditions indique que la source d'analyse doit correspondre au système de fichiers du point de terminaison pour poursuivre la création de la date d'échéance de la réponse. L'option d'escalade est sélectionnée. L'incident est remonté au gestionnaire si la date d'échéance de la réponse n'est pas respectée.

Configurer les règles relatives à la date d'échéance de la réponse



4. Cliquez sur **Envoyer**.

Ajouter plusieurs utilisateurs pour accéder aux incidents DLP

Utilisez la fonctionnalité de chaîne d'escalade pour permettre à tous les utilisateurs impliqués dans l'incident d'accéder aux incidents DLP à partir de la vue de liste, bien que l'incident soit affecté à un autre utilisateur.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.read, sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

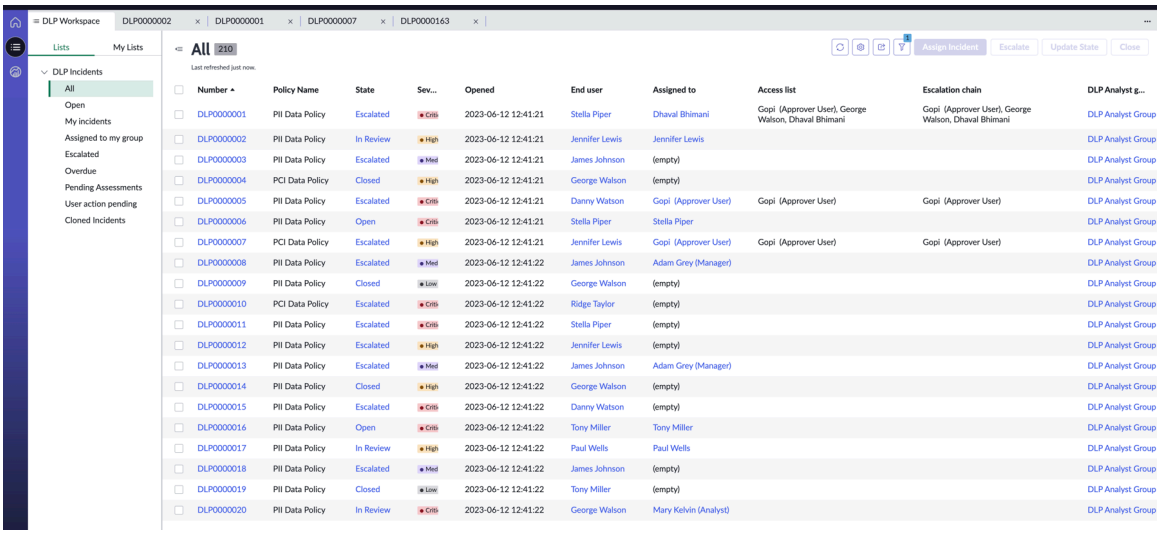
Procédure

1. Accédez à la **DLP** > **Espace de travail de l'analyste DLP**.
   Dans la vue de liste, les utilisateurs et leurs délégués doivent être en mesure d'afficher l'incident DLP sous **l'onglet Incidents escaladés** sur le portail de l'utilisateur final.
2. Ouvrez n'importe quel incident.
3. Cliquez sur **le bouton Escalader** pour escalader un incident.

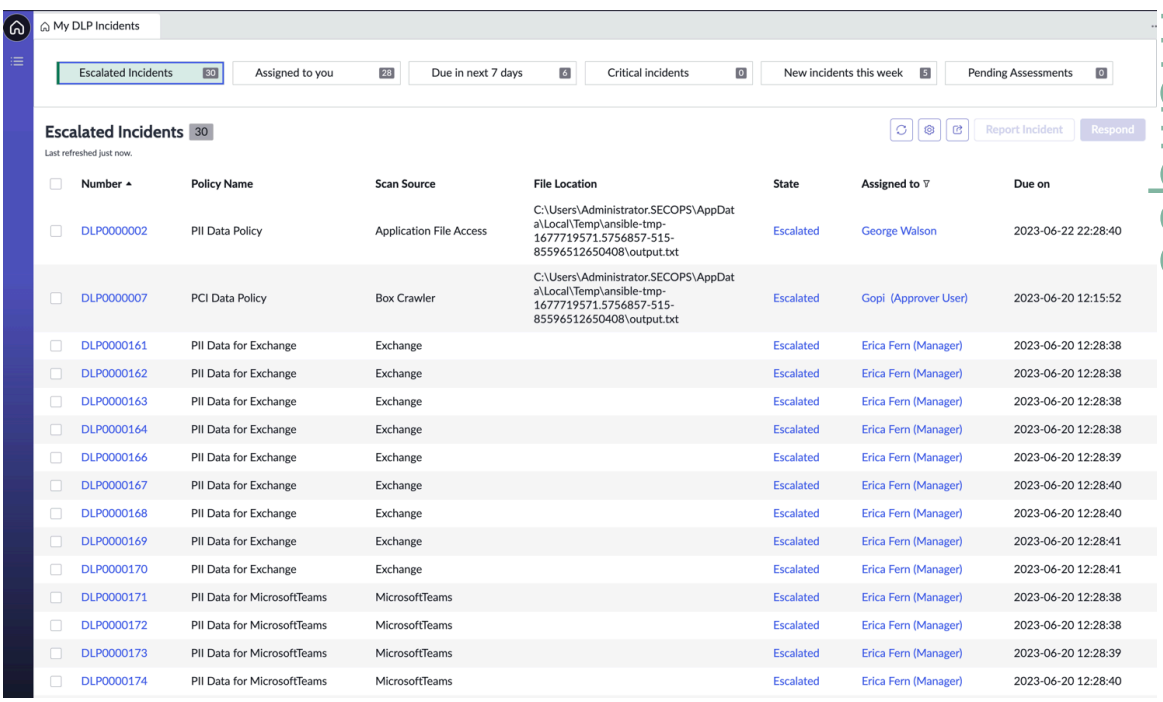
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez l'utilisateur ou le groupe d'utilisateurs dans la liste déroulante.
   Vous pouvez ajouter plusieurs utilisateurs à la chaîne d'escalade. Tous les utilisateurs ayant accès sont répertoriés dans la section Détails de la vue de formulaire et également sous l'onglet **Tous les** incidents. La chaîne d'escalade s'affiche en fonction des paramètres de configuration. Pour plus d'informations, voir Configurer les paramètres avancés



5. Cliquez sur **Envoyer**.
   Une fois l'envoi effectué, l'incident est affecté à un gestionnaire, mais l'utilisateur final peut toujours le consulter.
6. Pour vérifier cela, accédez à **l'espace de travail de l'utilisateur DLP** en tant qu'utilisateur final.
   Tous les incidents affectés à l'utilisateur final s'affichent.
7. Affichez la liste des incidents escaladés sous la section **Incidents escaladés** .



Vous pouvez également afficher la liste d'accès des utilisateurs sous la colonne **Chaîne d'escalade**de la vue de liste.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Ouvrez n'importe quel incident.
9. Cliquez sur le bouton **Répondre** pour soumettre une réponse à l'incident.
10. Sélectionnez la réponse dans la liste déroulante.
11. Cliquez sur **Envoyer**.

Créer des règles d'approbation

Créez des règles d'approbation pour accepter l'approbation de différents niveaux d'utilisateurs approbateurs chaque fois qu'un type avancé d'option de réponse est sélectionné.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

L'administrateur DLP définit ces règles d'approbation pour accorder le consentement sur les demandes envoyées par les utilisateurs finaux pour l'approbation du type avancé d'option de réponse. L'administrateur DLP peut également définir plusieurs niveaux d'approbation à partir d'ici.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Règles d'approbation DLP**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Règle d'affectation DLP

Champ	Description
Nom	Nom de la règle d'approbation.
Actif	Option permettant d'indiquer si la règle d'approbation est active.
Ordre d'exécution	Priorité de la règle d'approbation. Ce champ indique l'ordre dans lequel les règles d'approbation sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle d'approbation associée au numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Description	Description unique de la règle d'approbation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour la règle d'approbation, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, vous pouvez définir les conditions de cette règle de consolidation des incidents en sélectionnant la condition Source **d'intégration**, **contient**, **Microsoft**.
Applicable aux options de réponses	Option permettant de sélectionner l'option de réponse de type avancé. Vous pouvez sélectionner plusieurs options de réponse.
Approbateur	Sélectionnez le type d'utilisateur approbateur que vous souhaitez définir. ◦ **Table des utilisateurs** : sélectionnez cette option si vous souhaitez sélectionner l'utilisateur approbateur à partir de la table Utilisateurs (sys_user). ◦ **Liste d'approbation personnalisée** : sélectionnez cette option si vous souhaitez configurer plusieurs niveaux d'approbateur personnalisé pour une seule demande
Identificateur d'approbateur	Ce champ s'affiche lorsque **la table utilisateur** est sélectionnée pour **l'option Approbateur** . Sélectionnez un champ pour identifier l'approbateur dans la table Utilisateurs (sys_user).
Nombre de niveaux	Ce champ s'affiche lorsque **la table utilisateur** est sélectionnée pour **l'option Approbateur** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Numéro de fin dans ce champ pour définir les niveaux d'approbation. Par exemple, si 3 est ajouté dans le champ Nombre de niveaux et que le gestionnaire est sélectionné dans le champ Identificateur d'approbateur, la demande d'approbation passera à trois niveaux d'approbation.

L'exemple suivant montre la règle d'approbation créée pour l'une des options de réponse avancée. La condition nécessite que le nom de la source d'intégration contienne le mot clé Microsoft qui déclenche ensuite cette configuration.

4. Pour l'option **Approbateur** , sélectionnez **Liste d'approbation personnalisée**.
5. Cliquez sur **Envoyer**.
6. La liste connexe **des niveaux d'approbation** s'affichera dans la vue de formulaire.
7. Dans la section **Niveaux d'approbation** , cliquez sur **Nouveau**.
8. Renseignez les champs du formulaire.

Formulaire Niveau d'approbation

Champ	Description
Nom	Nom du niveau d'approbation.
Actif	Option permettant d'indiquer si le niveau d'approbation est actif.
niveau	Niveau de la règle d'approbation. Ce champ indique l'ordre dans lequel les niveaux d'approbation sont exécutés lorsque deux niveaux ou plus sont configurés. Le niveau d'approbation avec le numéro le plus bas a la priorité la plus élevée. Pour définir le niveau de fonctionnement, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Règle d'approbation	Règle d'approbation pour laquelle vous souhaitez définir cette configuration. Il s'agit d'un champ en lecture seule.
Description	Description unique de la règle d'approbation.
Approbations requises	Sélectionnez une option pour définir si l'approbation de tous les utilisateurs/

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	groupes configurés est requise ou uniquement d'un seul utilisateur.
Approbateurs	Option permettant de sélectionner les approbateurs. **a.** Utilisateurs et groupes : **i. Utilisateurs** : cliquez sur pour ajouter un utilisateur particulier à la liste. Vous pouvez également ajouter un utilisateur à l'aide de son adresse e-mail ou de l'option de recherche. Pour vous ajouter en tant qu'utilisateur auquel les conditions DLP sont applicables, cliquez sur . **ii. Groupes** : cliquez sur l'icône <add_icon> pour ajouter un groupe particulier à la liste. Vous pouvez également ajouter un groupe à l'aide de l'option de recherche. **b. Rechercher à l'aide d'un script** : vous pouvez utiliser l'éditeur de script pour personnaliser et formater les valeurs de champ pendant la création du niveau d'approbation. Par exemple, vous pouvez utiliser le champ d'adresse e-mail pour identifier l'utilisateur approbateur.

9. Cliquez sur **Envoyer**.

Créer des modèles d'instructions de l'utilisateur

Créez et gérez des modèles d'instructions utilisateur pour les incidents DLP afin d'aider les utilisateurs à comprendre les instructions liées à la résolution des incidents et les étapes suivantes impliquées dans le processus de résolution.

Avant de commencer

Le modèle de carte d'instructions de l'utilisateur affiche deux en-têtes différents qui vous fournissent plus d'informations sur un incident spécifique dans la vue de formulaire.

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

Lorsqu'un incident est affecté à l'utilisateur final, l'utilisateur peut être tenu de connaître les instructions supplémentaires sur la façon de répondre aux incidents, de présenter la terminologie aux utilisateurs et de fournir des informations supplémentaires sur l'incident. Ces modèles peuvent guider les utilisateurs pour fournir la réponse précise aux incidents DLP.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Modèles d'instructions de l'utilisateur**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Évaluation des incidents DLP

Champ	Description
Nom	Nom du modèle d'instructions de l'utilisateur.
Description brève	Description unique de ce modèle d'instructions de l'utilisateur.
Actif	Option permettant d'indiquer si le modèle d'instructions de l'utilisateur est actif.
Ordre d'exécution	Priorité du modèle d'instructions de l'utilisateur de l'incident. Ce champ indique l'ordre dans lequel l'ordre est exécuté pour évaluer le modèle d'instructions de l'utilisateur lorsqu'un incident est créé. L'option dotée du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Incidents correspondant à la condition	Les incidents qui correspondent aux conditions définies dans le générateur de conditions s'affichent. Ces conditions sont basées sur les données d'incident DLP. Pour créer une condition pour une instruction utilisateur, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur ET ou OU : Si ET est sélectionné, toutes les conditions doivent être mises en correspondance. Si OU est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Les conditions du générateur de conditions sont sensibles à la casse.
Concerne	Sélectionnez l'utilisateur ou les groupes d'utilisateurs auxquels le modèle s'applique. Les autres options disponibles sont les suivantes : ◦ **Tous les utilisateurs finaux** : cochez cette case si le modèle d'instructions s'applique à tous les utilisateurs. ◦ **Tous les réviseurs des incidents escaladés** : cochez cette case si le modèle s'applique à tous les réviseurs des incidents escaladés. ◦ **Utilisateurs spécifiques** : cliquez sur l'icône pour ajouter un utilisateur particulier à partir de la liste auquel les conditions d'incident DLP sont applicables. Vous pouvez également ajouter un utilisateur à l'aide de son adresse e-mail ou de l'option de recherche. Par exemple, Responsable juridique. Pour vous ajouter en tant qu'utilisateur auquel les conditions DLP s'appliquent, cliquez sur l'icône **Add me (M'ajouter**). ◦ **Groupes d'utilisateurs spécifiques** : cliquez sur l'icône pour ajouter un groupe particulier à partir de la liste auquel les conditions d'incident DLP s'appliquent. Vous pouvez également ajouter un groupe à l'aide de l'option de recherche. Par exemple, Créateurs d'enquêtes.
Modèle d'instructions : Instructions	Ajouter des instructions dans l'éditeur de texte enrichi avec des variables disponibles au niveau de l'incident.

4. Explorez la section **Modèle d'instructions** , entrez l'instruction du modèle et ajoutez des informations au niveau de l'incident sous cette section, si nécessaire.
5. Glissez-déplacez les variables requises pour afficher dynamiquement certains champs.
6. Cliquez sur **Envoyer**.
   Les modèles d'instructions de l'utilisateur sont maintenant créés et vous pouvez cliquer sur n'importe quel en-tête d'instructions de l'utilisateur pour connaître les détails supplémentaires d'un incident DLP.

   Pour plus d'informations, consultez Data Loss Prevention Incident Response Espace de travail de l'utilisateur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les instructions de l'utilisateur de l'interface utilisateur DLP

Configurez les messages de l'interface utilisateur du système pour ajouter des en-têtes d'instructions utilisateur détaillés si nécessaire.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Interface utilisateur du système** > **Messages**.
2. Recherchez **user_instruction_card_heading**.

   Par défaut, user_instruction_card_heading et user_instruction_modal_window_heading sont les deux configurations de messages de l'interface utilisateur mises en service aux utilisateurs.

3. Cliquez sur l'une des instructions utilisateur pour mettre à jour ou modifier.

Créer des modèles d'e-mail

Créez et gérez les modèles d'e-mail préconfigurés pour l'envoi de notifications à vos utilisateurs finaux, groupes d'utilisateurs ou gestionnaires. Avec ces modèles, vous pouvez coacher et communiquer avec vos utilisateurs finaux au sujet Data Loss Prevention Incident Response des incidents (DLP IR).

Avant de commencer
Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

> **Important :** Pour que les analystes puissent afficher les communications par e-mail d'un incident DLP dans le flux d'activité, vous devez ajouter ou ajouter le rôle « sn_dlir.analyst » dans le `glide.ui.activity.email_roles` de propriété système global.

Pourquoi et quand exécuter cette tâche
Les notifications par e-mail sont classées par notifications d'incident envoyées aux utilisateurs finaux, notifications d'escalade envoyées aux gestionnaires ou notifications de date d'échéance. Vous pouvez envoyer des notifications par e-mail concernant les dates d'échéance des incidents DLP ou même former les utilisateurs finaux sur ce qu'ils doivent faire lorsque certaines conditions sont remplies dans le filtre de conditions d'e-mail.
Les modèles d'e-mail DLP vous permettent d'envoyer la notification par e-mail pour les utilisateurs finaux, les gestionnaires et les analystes. Vous pouvez configurer les modèles à envoyer par incident ou sous forme de synthèse. L'objet et le corps de votre e-mail peuvent contenir des variables afin que vous puissiez réutiliser votre contenu existant.

DLP fournit les modèles d'e-mails préconfigurés suivants en fonction des catégories :

- **Modèle d'e-mail DLP : notification d'approbation par incident :** Informez les utilisateurs de l'approbation de leurs demandes.
- **Modèle d'e-mail DLP : notification d'escalade :** Envoyez des notifications d'escalade aux gestionnaires sous la forme de synthèses.
- **Modèle d'e-mail DLP : notification d'approbation en attente** : Notifiez aux approbateurs les éléments en attente.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Modèle d'e-mail DLP : notification d'annulation de demande d'approbation par incident :**Informez les utilisateurs d'une demande d'approbation qui a été annulée par l'équipe d'analystes DLP.
- **Modèle d'e-mail DLP : notification d'achèvement de la réponse de l'utilisateur :** Notifiez l'équipe d'analystes DLP de la réponse soumise par les utilisateurs.
- **Modèle d'e-mail DLP : notification d'incident de l'utilisateur :**Il s'agit d'un modèle par défaut pour la notification de synthèse de l'utilisateur. Envoyez des notifications d'incident aux utilisateurs finaux sous la forme de synthèses tous les quelques jours, même s'il n'y a pas de nouveaux incidents, pour informer les utilisateurs du nombre total d'incidents portant le nom d'un utilisateur particulier. Vous pouvez également envoyer des notifications de synthèse pour informer les utilisateurs des dates d'échéance les plus proches des incidents DLP de gravité critique, élevée, moyenne ou faible.
- **Modèle d'e-mail DLP - Notification d'approbation en attente par incident** : notifier les approbateurs des approbations en attente.
- **Modèle d'e-mail DLP : notification de rejet :** Envoyer une notification de rejet au demandeur.
- **Modèle d'e-mail DLP : notification de la date d'échéance :** Envoyer une notification de date d'échéance de l'incident. Si un incident DLP est affecté à l'utilisateur final et que celui-ci n'a effectué aucune action avant la date d'échéance, une notification par e-mail est envoyée à l'utilisateur final. Vous avez également la possibilité d'escalader l'incident DLP vers un gestionnaire, un utilisateur personnalisé ou un groupe d'utilisateurs si la date d'échéance de la réponse a été dépassée.

  Remarque : Les notifications de date d'échéance doivent être sous forme de synthèses.

- **Modèle d'e-mail DLP - Notification de réponse de l'utilisateur par incident :** Notifier les analystes de la réponse soumise aux utilisateurs par incident.
- **Modèle d'e-mail DLP : notification d'escalade par incident :** Informez les gestionnaires des escalades par incident.
- **Modèle d'e-mail DLP : notification de l'utilisateur par incident :** Informer les utilisateurs de l'affectation par incident.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Modèles d'e-mail**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Modèle d'e-mail DLP

Champ	Description
Nom	Donnez un nom au modèle d'e-mail.
Actif	Option permettant d'indiquer si le modèle d'e-mail DLP est actif. Si cette option n'est pas activée, aucune notification n'est envoyée pour ce modèle d'e-mail.
Catégorie	Catégorie de notification par e-mail. DLP prend en charge les options suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ **Notification d'incident aux utilisateurs finaux** : envoyée lorsque les incidents sont affectés aux utilisateurs finaux. ◦ **Notification d'escalade aux responsables** : envoyée lorsque la date d'échéance de la réponse n'est pas respectée ou affectée manuellement au gestionnaire via le portail des opérations DLP. ◦ **Notification de date d'échéance** : envoyée lorsque la date d'échéance de la réponse n'est pas respectée. ◦ **Notification de réponse de l'utilisateur aux analystes** : envoyée lorsque l'utilisateur final prend des mesures sur l'incident DLP. ◦ **Notification d'approbations en attente** : notifiez aux approbateurs les éléments en attente. ◦ **Notification d'approbation au demandeur** : informez les utilisateurs de l'approbation de leurs demandes. ◦ **Rejeter la notification au demandeur** : informez les utilisateurs du rejet de leurs demandes. ◦ **Annuler la notification au demandeur** : informez les utilisateurs de l'annulation de leurs demandes.
Type	Option permettant d'indiquer si l'e-mail est envoyé par incident ou sous forme de synthèse. **Remarque :** Si vous avez sélectionné **Notification de date d'échéance** dans le champ **Catégorie** , vous ne pouvez utiliser que des synthèses. Sélectionnez cette option.
Description	Description unique pour ce modèle d'e-mail.
Ordre d'exécution	Priorité du modèle d'e-mail. Ce champ indique l'ordre dans lequel les modèles d'e-mail sont exécutés lorsque deux modèles d'e-mail ou plus partagent les conditions de déclenchement. Le modèle d'e-mail avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Condition du modèle	Options dans les conditions de modèle basées sur la table d'incidents DLP. Vous pouvez sélectionner n'importe quel champ d'incident pour créer la condition de déclenchement du modèle d'e-mail. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Utilisateurs cibles	Ciblez les utilisateurs pour le modèle lorsque les conditions sont remplies. Les utilisateurs cibles peuvent être l'un des suivants : ◦ **Tous les destinataires** : Envoyez l'e-mail aux utilisateurs cibles. ◦ **Destinataires dans le groupe :** Envoyez l'e-mail uniquement aux destinataires d'un groupe particulier en utilisant l'option de filtre. ◦ **Destinataires correspondant aux critères** : Envoyez l'e-mail aux utilisateurs cibles qui correspondent aux critères. Vous pouvez utiliser le filtre pour analyser les utilisateurs cibles en fonction des conditions. Par exemple, ville.

Modèle d'e-mail	Modèle d'e-mail que vous pouvez sélectionner. Vous pouvez définir les variables pour réutiliser le contenu existant à ajouter à la notification par e-mail.
	
	Les champs **Catégorie** et **Type** déterminent les variables disponibles pour la sélection. Par exemple, supposons que la catégorie d'e-mail est définie sur Notification d'incident et que le type d'e-mail est une synthèse, alors les variables de sélection sont des champs de synthèse pour prendre en charge l'accumulation de plusieurs incidents DLP.
	
	Voici un exemple de HTML de corps d'e-mail pour chaque modèle d'e-mail :
	◦ **Modèle par défaut pour la notification d'approbation par incident** :
	`Dear ${respondent.first_name},`
	
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	
	`- Date protection team`
	◦ **Demande d'approbation par incident Notification d'annulation**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	``` Dear ${respondent.first_name}, Your request "${end_user_response}" on the DLP incident ${number} has been cancelled. No action is required from you at this point. Data protection team will contact you for any further information required. - Data protection team ``` ◦ **Modèle par défaut pour la notification de date d'échéance** : ``` Dear ${target_user.name}, Following incidents require your response. ${due_days_table} - Data protection team ``` ◦ **Modèle par défaut pour la notification de l'utilisateur Par incident** : ``` Dear ${assigned_to.name}, DLP Incident ${number} is assigned to you. Please review and submit your response. - Data protection team ``` ◦ **Modèle par défaut pour la notification d'incident de l'utilisateur** : ``` Hello ${target_user.name}, You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication. Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_ incidents}. Please log in to the ${link_to_dlp_portal} and submit your response. - Data protection team ```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description

	◦ **Modèle par défaut pour Escalade - Synthèse** :
	`Hi ${target_user.name},`
	
	`The following data security incidents have been escalated to you due to lack of response from the assignees.`
	
	`Please login to the incident response workspace to review the incidents and submit your response.`
	
	`${overdue_table}`
	
	`- Data protection team`
	
	◦ **Modèle par défaut pour l'escalade - Par incident** :
	`Dear ${assigned_to.name},`
	
	`Data security incident ${number} has been escalated to you.`
	
	`Please review and submit your response or assign the incident back to the user.`
	
	`- Data protection team`
	
	◦ **Modèle par défaut pour la notification d'approbation en attente** :
	`Dear ${approver.first_name},`
	
	`Your approval is required for a few requests on data security incidents.`
	
	`Please login to the workspace here and review the requests.`
	
	`- Data protection team`
	
	◦ **Modèle par défaut pour la notification d'approbation en attente par incident** :
	`Dear ${Approver},`
	
	`Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}.`
	
	`Please visit this here to approve or reject the request.`
	
	`- Data Protection Team`

Traduction automatique

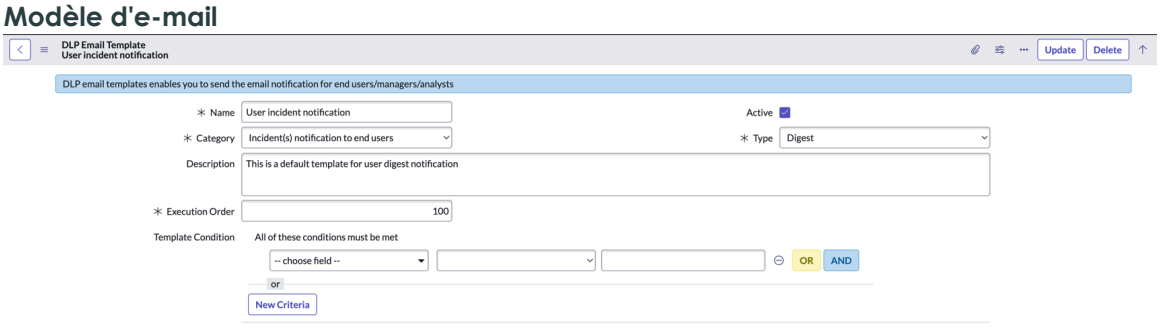
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description

	◦ **Modèle par défaut pour la notification de rejet par incident** :
	`Dear ${respondent.first_name} ${respondent.last_name},`
	
	`This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected.`
	
	`Please review the incident here.`
	
	`- Data protection team`
	
	◦ **Modèle par défaut pour la notification de réponse de l'utilisateur par incident** :
	`Hi ${assigned_to.name},`
	
	`This is to inform you that a response has been submitted for the DLP Incident ${number}.`
	
	◦ **Modèle par défaut pour la notification d'achèvement de la réponse de l'utilisateur** :
	`Hello ${target_user.name},`
	
	`This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication.`
	
	`Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}.`

Example
L'exemple suivant montre le modèle d'e-mail DLP avec les utilisateurs cibles définis comme tous les destinataires.

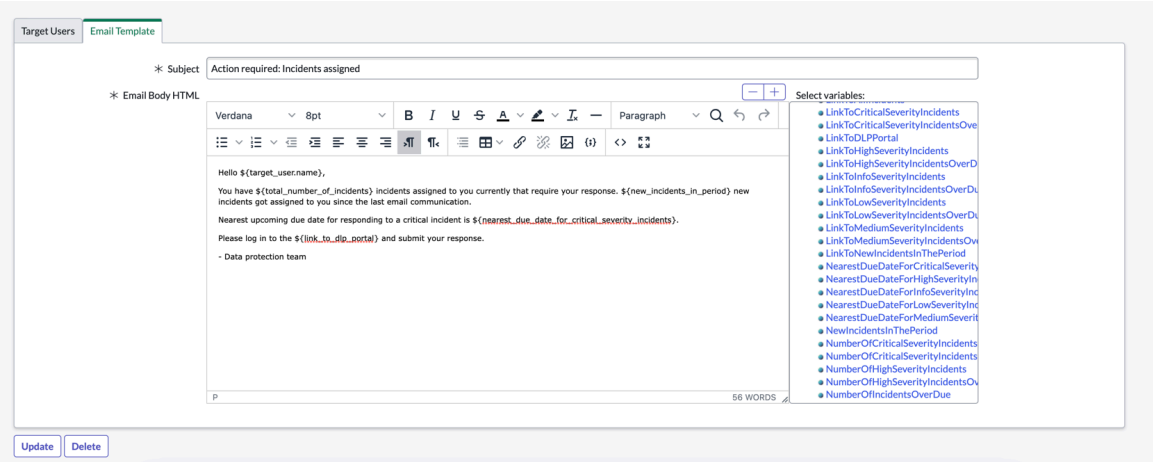
Modèle d'e-mail



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'exemple suivant montre un modèle d'e-mail avec l'objet « Notification d'incident utilisateur » et une variable *new_incidents_in_period*. Le corps de l'e-mail contient plusieurs variables qui sont ajoutées à partir de la colonne Sélectionner des variables.

Variables de modèle d'e-mail



4. Cliquez sur **Envoyer**.

Résultats

L'utilisateur final reçoit un e-mail de notification de synthèse avec tous les champs de variables sélectionnés dans le modèle.

Créer des évaluations

Créez et gérez des évaluations pour permettre aux utilisateurs finaux de répondre aux incidents DLP. Vous pouvez utiliser les évaluations pour recueillir des informations sur les données sensibles exposées ou divulguées à la suite d'incidents DLP.

Créer et gérer des évaluations pour les incidents DLP

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

Les évaluations des incidents DLP vous aident à identifier les menaces potentielles et les vulnérabilités de vos données en fonction de la réponse de l'utilisateur final. Vous pouvez utiliser ces informations pour déterminer les lacunes, les préoccupations et les attentes existantes de vos utilisateurs finaux.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Évaluations**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluation des incidents DLP

Champ	Description
Nom	Nom de l'évaluation de l'incident DLP.
Actif	Option permettant d'indiquer si l'évaluation de l'incident DLP est active.
Description	Description unique pour cette évaluation d'incident DLP.
Introduction d'évaluation	Fournissez une introduction ou un contexte pour votre évaluation. Vous pouvez également utiliser les variables de la section Sélectionner des variables pour afficher dynamiquement certains champs.

4. Cliquez sur **Envoyer**.
5. Après avoir créé une évaluation, ouvrez-la et cliquez sur **Concepteur d'évaluation**.
6. Dans la section Nouvelle évaluation, sélectionnez un type de question d'évaluation sous la section Contrôles.
7. Glissez-déplacez le type de question d'évaluation requis sous la section Nouvelle évaluation.
   Par exemple, vous pouvez glisser-déposer le contrôle **de** choix sous la section Nouvelle évaluation ou Nouvelle catégorie.
8. Pour ajouter d'autres catégories pour l'évaluation, cliquez sur .
9. Pour modifier une catégorie existante, cliquez sur .
10. Après avoir créé les différentes questions d'évaluation pour la première fois, cliquez sur **Enregistrer**, puis sur **Publier**.

Créer des règles d'option de réponse aux incidents

Créez les règles d'option de réponse aux incidents que l'utilisateur final ou l'analyste peut utiliser lors de la réponse à un incident.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer le type de réponse qu'un utilisateur final doit effectuer en fonction du type d'incident DLP. L'application DLP Incident Response du système de base fournit les options de réponse suivantes aux utilisateurs :

- Évaluation terminée
- Contenu supprimé
- Fichier supprimé
- Fichier chiffré
- Contenu masqué

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Signaler un faux positif
- Signaler un propriétaire incorrect
- Requis pour le processus business
- Autorisations examinées

Par exemple, supposons qu'un utilisateur final signale un incident DLP comme un faux positif. L'état de cet incident est alors automatiquement marqué comme fermé, car l'état cible que vous avez configuré est fermé.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Règles de l'option de réponse aux incidents**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Règles de l'option de réponse aux incidents

Champ	Description
Nom	Nom de l'option de réponse à un incident.
Actif	Option permettant d'indiquer si l'option de réponse à un incident est active.
Ordre d'exécution	Priorité de l'option de réponse à un incident. Ce champ indique l'ordre dans lequel les options de réponse aux incidents sont exécutées lorsque deux options de réponse aux incidents ou plus partagent les conditions de déclenchement. L'option de réponse aux incidents associée au numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Description	Description unique de cette option de réponse à l'incident.
État cible par défaut	L'état cible par défaut que vous avez configuré.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour les options de réponse aux incidents, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne.

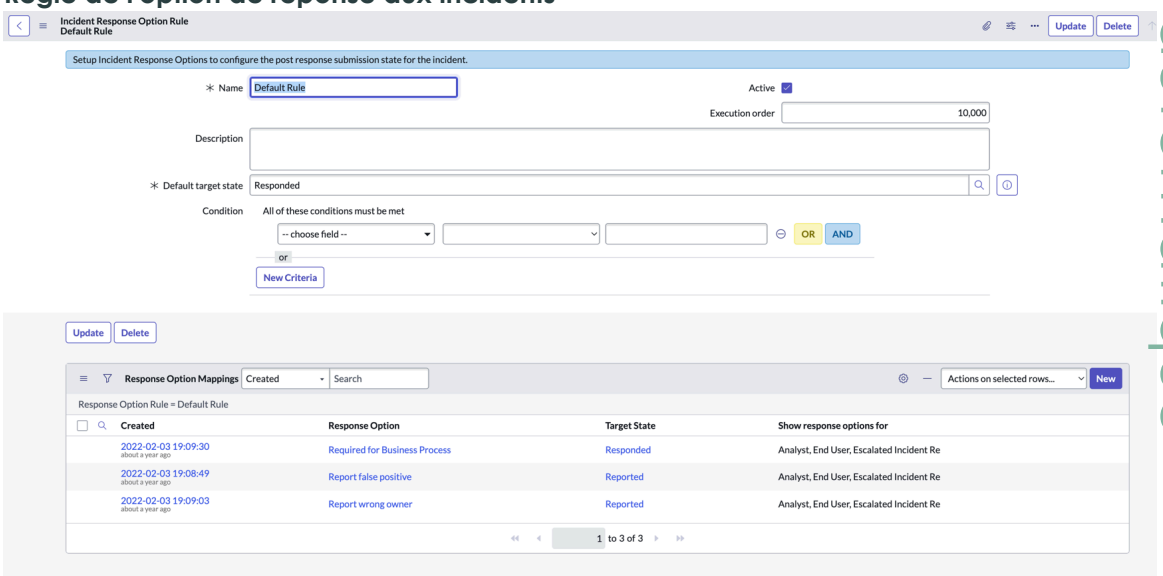
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU** : ◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.

Example

L'exemple suivant montre la configuration de l'action de l'utilisateur final pour un point de terminaison. La condition exige que la source d'analyse soit un système de fichiers de point de terminaison qui déclenche ensuite cette configuration d'action de l'utilisateur final. Le mappage montre que les options de réponse disponibles pour l'utilisateur final sont le Signaler un propriétaire incorrect, Signaler un faux positif et Fichier supprimé.

Règle de l'option de réponse aux incidents



4. Dans la section **Mappages des options de réponse** , cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire.

Formulaire Mappage d'option de réponse

Règle de l'Option de réponse	Nom de la règle d'option de réponse aux incidents. Par exemple, `SharePoint` implique que la source de numérisation est SharePoint. Vous pouvez entrer le nom

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	de la réponse à un incident ou effectuer une recherche à l'aide de la fonction de recherche.
Option en matière de réponse	Option permettant de sélectionner l'option de réponse. Vous pouvez soit saisir l'option de réponse, soit effectuer une recherche à l'aide de la fonction de recherche.
État cible	État cible de l'incident DLP une fois que l'utilisateur final a sélectionné l'action appropriée. **Remarque :** **a.** Le champ **État cible** s'affiche uniquement lorsque vous sélectionnez **l'option de réponse** de **type : de base**. Pour en savoir plus sur la configuration des types d'état cibles, reportez-vous à la section Configurer l'option de réponse pour vos incidents DLP. **b.** Lorsqu'une option de réponse de **type avancé** est sélectionnée, vous ne pouvez pas définir l'état cible et elle est masquée. L'état cible sera affecté en fonction de l'état personnalisé configuré à partir du sous-flux du concepteur de flux.
Afficher les options de réponse pour	Option permettant de déterminer les rôles d'utilisateur pour lesquels afficher les options de réponse. Vous pouvez choisir entre **Analyste**, **Utilisateur final** et **Analyste-réviseurs escaladés** en utilisant l'option de déverrouillage. Vous êtes autorisé à choisir un ou tous les rôles.

Action de mappage d'option de réponse



6. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'option de réponse pour vos incidents DLP

Utilisez cette fonctionnalité pour configurer le type de réponse qu'un utilisateur final ou un analyste doit effectuer.

Avant de commencer

L'application de système de base Réponse aux incidents DLP fournit les options de réponse suivantes :

1. Évaluation terminée
2. Contenu supprimé
3. Fichier supprimé
4. Fichier chiffré
5. Contenu masqué
6. Signaler un faux positif
7. Signaler un propriétaire incorrect
8. Demander une libération de quarantaine par e-mail

   Remarque : Cette option est disponible pour les enregistrements DLP Microsoft Exchange.

9. Requis pour le processus business
10. Autorisations examinées

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Options de réponse**.

   Par défaut, le système de base fournit deux types d'option de réponse :

   a. **Basique** : option de réponse manuelle soumise par l'utilisateur.

   b. **Avancé** : une option de réponse automatisée déclenche un sous-flux du concepteur de flux lorsque l'utilisateur soumet l'option de réponse.

2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire d'option de réponse de type : Basique

Champ	Description
Nom	Saisissez le nom de l'option de réponse à un incident.
Type	Option permettant de sélectionner le type d'option de réponse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire d'option de réponse de type : Avancé

Champ	Description
Nom	Saisissez le nom de l'option de réponse à un incident.
Type	Option permettant de sélectionner l'option de réponse. Par défaut, ce champ affiche les deux types d'options suivants : ◦ **Basique** : lorsque vous sélectionnez cette option lors de la création d'une nouvelle option de réponse, vous devrez peut-être ajouter un nom d'option de réponse et le type. ◦ **Avancé** : lorsque vous sélectionnez cette option, vous pouvez sélectionner les champs suivants : ▪ **Flux** : sélectionnez le flux secondaire du concepteur de flux. ▪ **Nécessite un Serveur MID** : cochez cette case si le flux sélectionné utilise Serveur MID.
Flux	Sélectionnez le flux Flow Designer requis pour activer l'application MID et l'option MID. Lorsque vous créez un flux secondaire pour l'option de réponse, ajoutez les entrées de flux secondaire suivantes : **a. Nom** : ▪ dlp_incident ▪ mid_server_capability ▪ mid_server_application **b. Type** : ▪ Référence (vers la table d'incidents DLP) ▪ ID système pour l'application MID Server et l'aptitude de MID Server
Nécessite un serveur MID	Option permettant de déterminer cette configuration de MID Server. En cochant la case **Exige un serveur MID** , **Application de Serveur MID** et **Aptitude de Serveur MID** , vous pouvez configurer l'application MID et l'aptitude MID.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

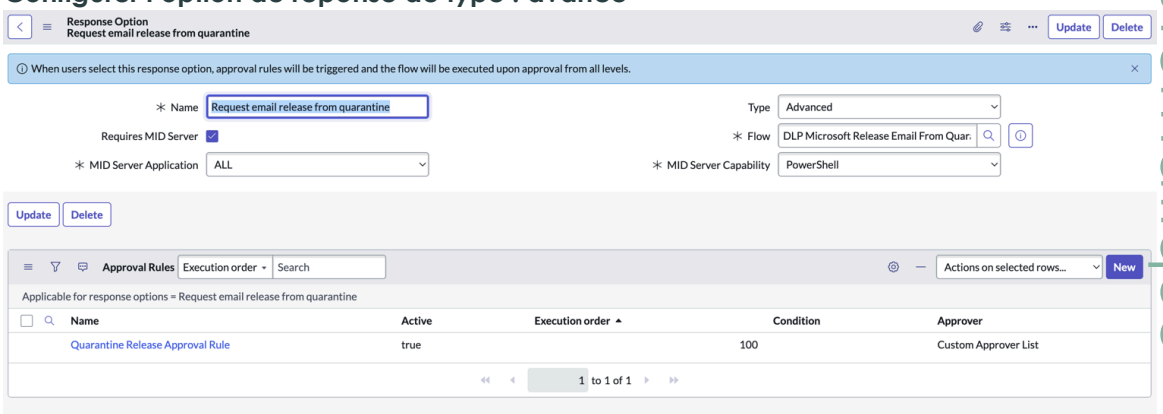
Champ	Description
	Remarque : En fonction de la configuration de l'application de Serveur MID et de l'aptitude de Serveur MID, et si un MID Server est en cours d'exécution, seule l'option de réponse sera visible dans l'espace de travail.
Application de Serveur MID	Sélectionnez l'application de Serveur MID requise dans la liste déroulante.
Capacité du serveur MID	Sélectionnez l'aptitude du serveur MID requise dans la liste déroulante.

Remarque : Si aucun MID Server n'est disponible pour l'aptitude de MID Server sélectionnée, l'option de réponse n'est pas visible. Si vous voulez un MID Server spécifique dans la liste, vous devez configurer l'application MID et l'afficher dans la liste, puis au moins un MID Server configuré doit être opérationnel à partir des applications MID sélectionnées et doit avoir l'aptitude du serveur MID sélectionnée.

4. Cliquez sur **Envoyer**.

Remarque : Si vous créez un type **avancé** d'option de réponse, la liste connexe **Règles d'approbation** est renseignée pour vous permettre de configurer la règle d'approbation de cette nouvelle option de réponse. Pour plus d'informations, consultez Créer des règles d'approbation.

Configurer l'option de réponse de type : avancé



Créer des configurations du graphique des âges

Configurez le graphique d'âge qui s'affiche dans le Data Loss Prevention Incident Response portail Ops (DLP IR). Ce graphique affiche le nombre d'incidents ouverts par nombre de jours.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Configuration du graphique des âges**.
2. Examinez les entrées du graphique des âges dans la table suivante et personnalisez les entrées en fonction de votre environnement.

Formulaire de configurations du graphique des âges DLP

Nom	Condition
0 à 30 jours	Âge de l'incident ouvert, compris entre 0 et 30 jours.
31 à 60 jours	Âge de l'incident ouvert, compris entre 31 et 60 jours.
61 à 90 jours	Âge de l'incident ouvert, compris entre 61 et 90 jours.
90 jours et plus	Âge de l'incident ouvert supérieur à 90 jours.

3. Ajoutez une nouvelle configuration de graphique des âges en cliquant sur **Nouveau**.
4. Dans le champ Nom, entrez un **nom** pour la configuration du graphique d'âge DLP.
5. Définissez les conditions pour la configuration du graphique des âges DLP.

   a. Pour ajouter des conditions, cliquez sur **ET** ou **OU**.
      - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
      - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

      Remarque : Les conditions du générateur de conditions sont sensibles à la casse.

   b. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.

6. Cliquez sur **Envoyer**.

Créer des configurations de délégués d'utilisateurs

Empêchez certains cadres de l'organisation de recevoir des notifications sur les incidents qui leur sont affectés ou qui leur sont remontés.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

Imaginez un scénario dans lequel le cadre est un utilisateur qui appartient à un groupe de direction ou de direction. Le cadre ne doit pas recevoir d'e-mails concernant l'affectation ou l'escalade des incidents. Un utilisateur délégué peut alors prendre les mesures nécessaires au nom du dirigeant.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois qu'un utilisateur a affecté une personne particulière, Henry, en tant que délégué, un autre utilisateur ne peut plus affecter Henry en tant que délégué. De même, un délégué ne peut pas affecter un autre utilisateur en tant que délégué.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Configuration du délégué**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire de configuration du délégué

Champ	Description
Utilisateur	Nom de l'utilisateur qui a besoin d'un délégué pour les incidents DLP.
Délégué	Nom de l'utilisateur qui peut répondre à l'incident DLP au nom de l'utilisateur final d'origine.

4. Cliquez sur **Envoyer**.

Créer des règles d'identification des récidivistes

Créez des règles d'identification des récidivistes pour identifier les utilisateurs qui répètent le même problème plusieurs fois.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

Vous pouvez identifier les récidivistes à l'aide de certaines règles ou critères. Data Loss Prevention Incident Response Fournit des champs que vous pouvez utiliser pour identifier les récidivistes.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Règles d'identification des récidivistes**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Règles d'identification des récidivistes

Champ	Description
Nom	Nom de la règle d'identification des récidivistes.
Ordre d'exécution	Priorité des règles d'identification des récidivistes. Ce champ indique l'ordre dans lequel les règles d'identification des récidivistes sont exécutées lorsque deux

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

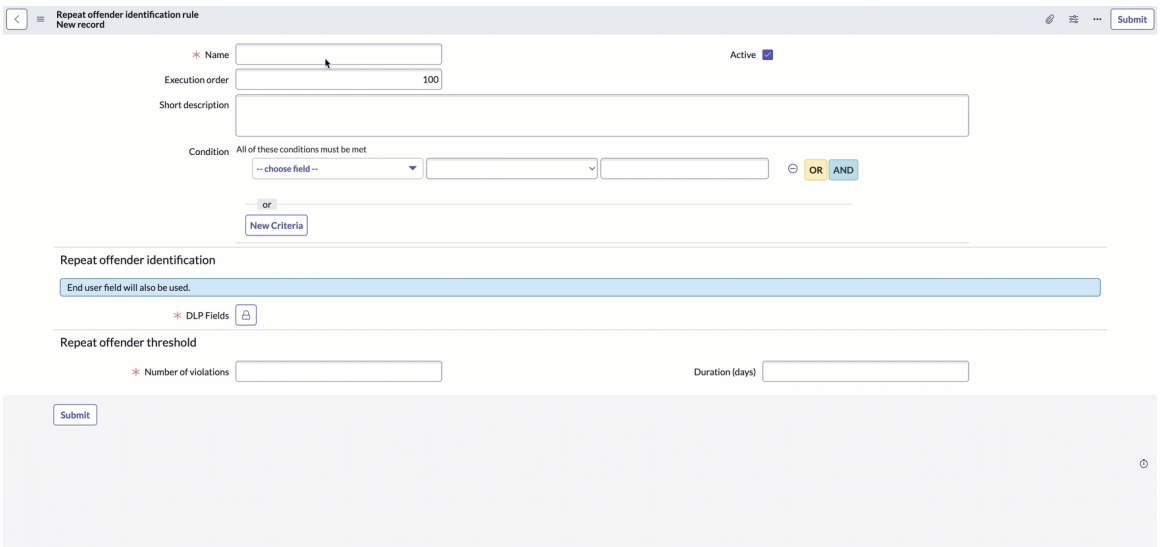
Champ	Description
	règles ou plus partagent les conditions de déclenchement. La règle d'identification des récidivistes avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Description brève	Description unique de cette règle d'identification des récidivistes.
Condition	Conditions dans le générateur de conditions qui sont basées sur la table d'incidents DLP. Vous pouvez sélectionner n'importe quel champ d'incident pour créer la condition de déclenchement de la règle d'identification des récidivistes. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU** : ◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Champs DLP	Identifiez les récidivistes en fonction des champs DLP requis. Cliquez sur à côté des champs DLP pour afficher la liste des champs DLP disponibles. Sélectionnez les champs DLP que vous souhaitez utiliser dans la colonne Disponible et déplacez-les vers la colonne Sélectionné. Par exemple, vous pouvez sélectionner les champs**Nom du fichier** et **Propriétaire du fichier** dans la colonne Disponible et les déplacer vers la colonne Sélectionné. Ensuite, vous pouvez identifier les récidivistes en fonction des champs **Nom du fichier** et **Propriétaire du fichier** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Ainsi, si un utilisateur dépasse le seuil de récidive (nombre d'infractions et durée) et si le même utilisateur correspond aux champs DLP, cet utilisateur particulier est identifié comme récidiviste.
Nombre d'infractions	Définissez la valeur limite du seuil pour les récidivistes. Une fois que l'utilisateur a répété les mêmes actions et dépassé le nombre spécifié d'infractions, l'utilisateur est identifié comme récidiviste.
Durée (en jours)	Définissez le seuil limite de récidive sous la forme de jours. Une fois que l'utilisateur a répété les mêmes actions et dépassé la durée du seuil, il est identifié comme récidiviste.

Identifier les récidivistes



4. Cliquez sur **Envoyer**.

Créer des champs personnalisés

Créez vos champs personnalisés pour les incidents DLP. Vous pouvez créer différents types de champs personnalisés tels que chaîne, numéro, case à cocher, choix, date et heure, et les utiliser dans les formulaires d'incident DLP.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Important : Les champs personnalisés pour les incidents DLP ne sont pris en charge que sur la version San Diego ou ultérieure.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Les champs personnalisés sont associés à des restrictions au niveau des champs, donc s'il existe des restrictions au niveau des champs, elles s'appliquent aux champs personnalisés sur le portail des opérations DLP et le portail de l'utilisateur final.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Champs personnalisés**.
2. Créez un champ personnalisé en cliquant sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Champs personnalisés DLP

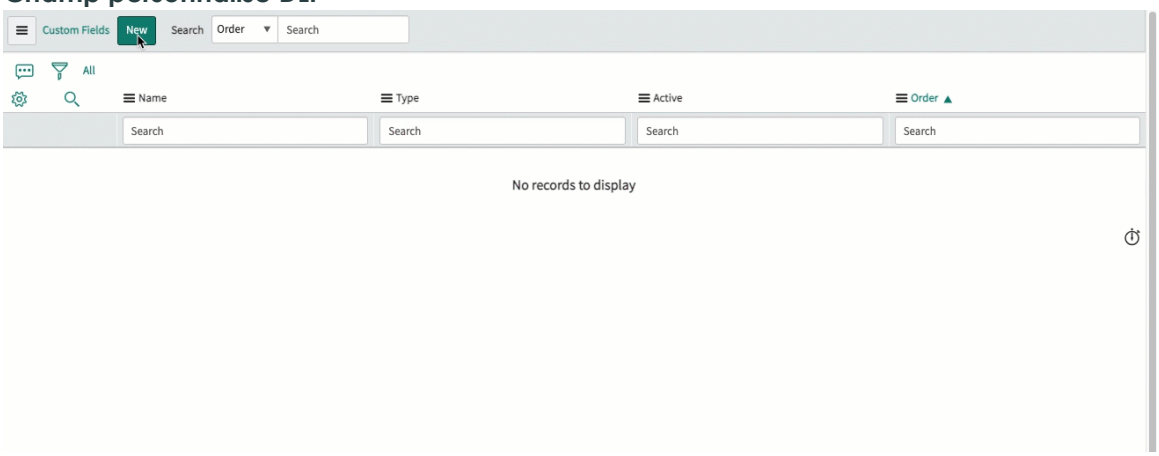
Champ	Description
Nom	Nom du champ personnalisé.
Type	Option permettant de sélectionner le type de champ personnalisé. Vous pouvez choisir l'un des types suivants : ◦ **Chaîne** ◦ **Numéro** ◦ **Case à cocher** ◦ **Choix** Si vous sélectionnez le type de champ personnalisé **Choix**, vous pouvez définir les options de choix du champ personnalisé après avoir créé le champ personnalisé. Pour créer une option de choix de champ personnalisé : **a.** Ouvrez le champ personnalisé requis. **b.** Dans la section Options du champ de choix personnalisé, cliquez sur **Nouveau**. **c.** Dans le champ Nom de l'option, définissez le nom de l'option requis. **d.** Cliquez sur **Envoyer**. ◦ **Date** ◦ **Date/Heure** **Remarque :** Une fois que vous avez sélectionné un type pour votre nouveau champ personnalisé, vous n'êtes pas autorisé à le modifier. Si vous souhaitez modifier le type, vous devez créer à nouveau un nouveau champ personnalisé avec le type requis.
Ordre	Option permettant de choisir l'ordre dans lequel les champs personnalisés doivent être affichés. Vous pouvez définir la valeur d'ordre

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	pour chaque champ personnalisé. Les champs personnalisés sont triés en fonction des valeurs d'ordre que vous définissez. Par défaut, les champs personnalisés sont triés par ordre croissant. Vous pouvez trier les champs personnalisés par ordre décroissant en cliquant sur la colonne **Ordre** .
Actif	Option permettant d'indiquer si le champ personnalisé est actif.
Description	Description du champ personnalisé que vous avez créé.

Champ personnalisé DLP



4. Cliquez sur **Envoyer**.

Configurer les paramètres avancés

Configurez les paramètres avancés afin de pouvoir déterminer les champs de l'incident pour identifier les utilisateurs finaux, entre autres options.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

La configuration des paramètres avancés sur le Data Loss Prevention Incident Response est facultative. Certains paramètres avancés sont les suivants :

- Définissez le nombre maximal d'incidents qui peuvent être envoyés dans un e-mail de synthèse.
- Activez le mode rapide pour envoyer des e-mails plus rapidement.
- Déterminer la verbosité du journal de l'application.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Paramètres avancés**.
2. Renseignez les champs du formulaire.

Formulaire Paramètres avancés

Champ	Description
Les données sensibles à l'origine de l'infraction doivent-elles être affichées sur l'incident ?	Option permettant de choisir si vous souhaitez afficher les données sensibles à l'origine de la violation sur l'incident DLP. Cette option est activée par défaut.
Les données sensibles à l'origine de l'infraction doivent-elles également être affichées sur les incidents enfants ?	Option permettant de choisir si vous souhaitez afficher également les données sensibles à l'origine de la violation sur l'incident enfant DLP. Par défaut, cette option est désactivée.
Liste des champs de l'incident qui sont utilisés pour identifier l'utilisateur final	Liste des champs sur l'incident du module Règle d'affectation qui sont utilisés pour identifier l'utilisateur final. Vous pouvez également spécifier vos propres attributs personnalisés pour identifier l'utilisateur final.
Nombre maximal d'incidents dans un e-mail de synthèse	Nombre maximal d'incidents qui peuvent être envoyés dans un e-mail de synthèse. Par défaut, la valeur est 100.
Durée maximale de la récidive (en jours)	Durée maximale pour identifier un récidiviste. Par défaut, la valeur est de 90 jours.
Mode rapide pour envoyer des e-mails	Option permettant de valider les e-mails et d'identifier les problèmes. Vous pouvez effectuer la validation en activant l'option **Oui** . Cette option est activée par défaut.
Cette propriété est utilisée pour définir le niveau de détail du journal de l'application	Niveau de verbosité du journal de l'application, c'est-à-dire le nom du type d'information. Vous pouvez également mettre à jour la valeur pour les options suivantes : ◦ **erreur** ◦ **avertir** ◦ **infos** ◦ **debug** Par défaut, la valeur est **info**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Exclure les incidents clonés et enfants des rapports	Option permettant d'exclure les incidents clonés et enfants des rapports. Par défaut, cette option est **Oui**.
Jour(s) d'attente pourla suppression du contenu des correspondances sur le stockage cloud après la fermeture de l'incident	Option permettant de choisir le nombre de jours d'attente pour nettoyer le contenu de correspondance des incidents qui sont inactifs pendant une durée spécifique. Par défaut, la valeur est 90. Après 90 jours, si l'incident DLP est inactif, le contenu de la correspondance est nettoyé à partir du stockage dans le cloud.
Affecter un incident au groupe d'analystes DLP après le dernier niveau d'escalade	Cochez cette case pour affecter l'incident à l'analyste après le dernier niveau d'escalade.
Autoriser les utilisateurs à accéder aux incidents après escalade	Cochez cette case pour permettre aux utilisateurs affectés d'accéder à ou aux incidents après l'escalade. Lorsque vous sélectionnez cette option, tous les utilisateurs qui ont été ajoutés à la liste de chaînes d'escalade sont alors en mesure d'accéder à l'incident ou aux incidents.
Autoriser l'analyste à modifier l'évaluation terminée	Cochez cette case pour permettre à l'analyste de modifier l'évaluation terminée. Lorsque vous sélectionnez cette option, les analystes peuvent modifier les évaluations. Lorsqu'elle n'est pas sélectionnée, vous pouvez afficher les évaluations en mode lecture seule.

Traduction automatique

3. Cliquez sur **Enregistrer**.

Surveiller le processus d'exécution de l'intégration DLP

Suivez et surveillez le processus d'ingestion ou d'exécution de l'intégration en cours. Les processus d'exécution de l'intégration contiennent les statistiques relatives au traitement des données et à l'état de l'intégration.

Rôle requis : sn_dlir.admin.

Le processus d'exécution de l'intégration répertorie les détails sur le nombre d'enregistrements ingérés. Par exemple :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Dans l'intégration Symantec, le processus contient à la fois les exécutions d'intégration enfant et parent. L'enregistrement parent indique les données d'ingestion et l'enregistrement enfant indique les appels d'enrichissement et les enregistrements d'attributs personnalisés.
2. Dans l'intégration Microsoft, il n'y a qu'un processus d'ingestion d'enregistrement parent à exécuter.

Processus d'exécution de l'intégration DLP : affiche les entrées de file d'attente, l'état des entrées de file d'attente et les enregistrements extraits.

L'exécution de l'intégration contient la source pour laquelle le profil d'intégration et l'enregistrement d'exécution de l'intégration sont créés, les intervalles d'interrogation des profils, les états et sous-états d'ingestion, ainsi que le nombre d'incidents qui indique le nombre d'enregistrements ingérés.

1. Accédez à la **Administration DLP** > **Exécutions des intégrations**.
2. Sélectionnez l'exécution de l'intégration dans la liste.
3. Accédez au **processus d'exécution de l'intégration DLP**.
4. Affichez l'état d'entrée de file d'attente de l'enregistrement.

Restrictions d'accès aux incidents DLP

Gérez la visibilité d'un incident DLP particulier qui contient des informations sensibles. Vous pouvez utiliser des restrictions d'accès aux incidents pour définir qui peut accéder à un incident DLP particulier et empêcher des utilisateurs ou des groupes spécifiques d'accéder à cet incident.

Créer des restrictions au niveau des champs

Définissez des restrictions au niveau du champ dans les incidents DLP pour protéger les informations sensibles contre leur exposition. Vous pouvez utiliser des restrictions au niveau des champs pour contrôler les utilisateurs ou les groupes qui peuvent accéder à des champs spécifiques dans les incidents DLP.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

Les restrictions de niveau de champ vous permettent d'afficher uniquement certains champs pour des utilisateurs ou des groupes spécifiques, offrant un moyen plus granulaire de contrôler les données auxquelles un utilisateur peut accéder. Vous pouvez créer une restriction au niveau du champ en définissant les conditions de correspondance des incidents DLP, en sélectionnant les utilisateurs ou les groupes auxquels ces conditions s'appliquent, puis en choisissant les champs DLP que ces utilisateurs ou groupes peuvent afficher.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Restrictions d'accès aux incidents** > **Restrictions de niveaux de champs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de restriction au niveau du champ DLP

Champ	Description
Nom	Nom de la restriction au niveau du champ.
Actif	Option permettant d'indiquer si la restriction de niveau de champ est active.
Ordre d'exécution	Priorité des restrictions au niveau du champ. Ce champ indique l'ordre dans lequel les restrictions de niveau de champ sont exécutées lorsque deux restrictions de niveau de champ ou plus partagent les conditions de déclenchement. La restriction de niveau de champ associée au numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Description brève	Description unique de cette restriction de niveau de champ.
Condition de correspondance de l'incident	Options dans l'incident qui correspondent aux conditions définies. Vous pouvez sélectionner n'importe quel champ d'incident pour définir la condition de déclenchement des restrictions au niveau du champ. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU** : ◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, vous pouvez sélectionner le champ Nom de la `politique`et définir la condition `sur dans`, et `Nom de la politique`. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Concerne	Option permettant d'appliquer les conditions de correspondance d'incident à des utilisateurs ou groupes spécifiques. Vous pouvez appliquer les conditions aux éléments suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

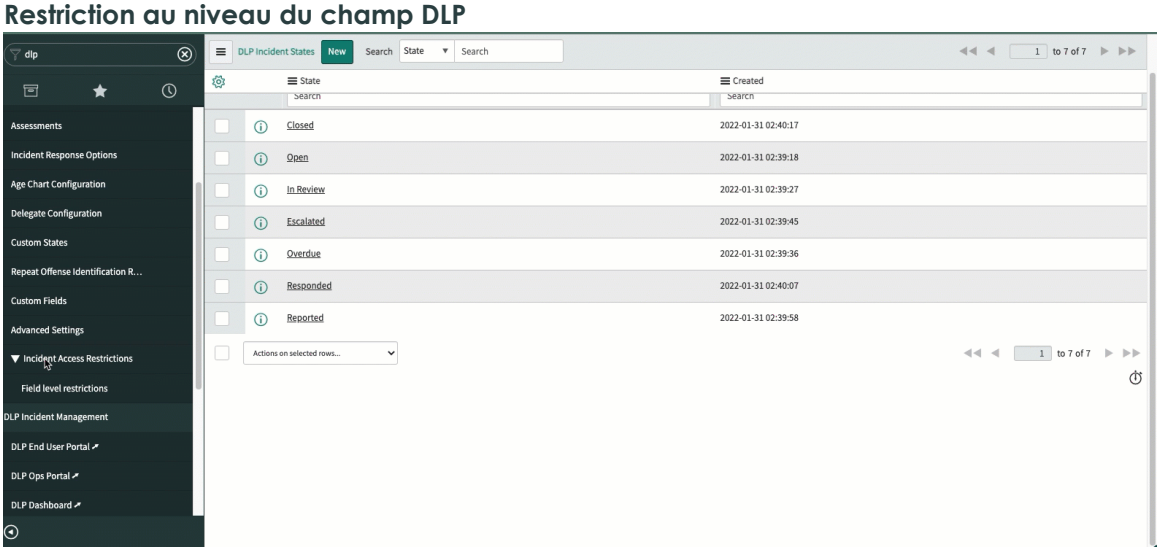
Champ	Description
	◦ **Tous les utilisateurs finaux** : option permettant de sélectionner tous les utilisateurs finaux auxquels les conditions d'incident DLP s'appliquent. ◦ **Tous les réviseurs des incidents escaladés** : option permettant de sélectionner tous les réviseurs des incidents escaladés auxquels les conditions d'incident DLP s'appliquent. Il s'agit de tous les incidents DLP remontés au gestionnaire. ◦ **Utilisateurs** : cliquez sur pour ajouter un utilisateur particulier à partir de la liste auquel les conditions d'incident DLP s'appliquent. Vous pouvez également ajouter un utilisateur à l'aide de son adresse e-mail ou de l'option de recherche. Par exemple, Responsable juridique. Pour vous ajouter en tant qu'utilisateur auquel les conditions DLP sont applicables, cliquez sur ◦ **Groupes** : cliquez sur l'icône IC pour ajouter un groupe particulier à partir de la liste auquel les conditions d'incident DLP sont applicables. Vous pouvez également ajouter un groupe à l'aide de l'option de recherche. Par exemple, Créateurs d'enquêtes.
Autoriser l'accès aux champs suivants uniquement	◦ **Champs DLP** : option permettant de définir les champs DLP pour lesquels vous souhaitez autoriser l'accès aux utilisateurs ou groupes sélectionnés. Sélectionnez les champs DLP auxquels vous souhaitez autoriser l'accès à partir de la colonne Disponible et déplacez-les vers la colonne Sélectionné. **Remarque :** Les utilisateurs ou groupes sélectionnés ne pourront accéder qu'aux champs DLP sélectionnés. Par exemple, vous pouvez sélectionner les champs**Affecté à** et **Ouvert** dans la colonne Disponible et les déplacer vers la colonne Sélectionné. Ensuite, les utilisateurs ou groupes sélectionnés n'ont accès qu'aux champs Affecté à et Ouvert. ◦ **Télécharger les pièces jointes** : option permettant d'indiquer si vous souhaitez autoriser les utilisateurs ou les groupes sélectionnés à télécharger des pièces jointes. ◦ **Champs personnalisés** : option permettant de définir les champs personnalisés que vous souhaitez autoriser l'accès aux utilisateurs ou groupes sélectionnés. Vous pouvez afficher les champs

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	personnalisés que vous avez créés dans la colonne Disponible. Sélectionnez les champs personnalisés auxquels vous souhaitez autoriser l'accès à partir de la colonne Disponible et déplacez-les vers la colonne Sélectionné. **Important :** ▪ Les champs personnalisés pour les incidents DLP ne sont pris en charge que sur la version San Diego ou ultérieure. ▪ Les utilisateurs ou groupes sélectionnés ne pourront accéder qu'aux champs personnalisés sélectionnés.

Restriction au niveau du champ DLP



4. Cliquez sur **Envoyer**.

Créer des restrictions au niveau de l'enregistrement

Définissez des restrictions de niveau d'enregistrement dans les incidents DLP pour protéger les enregistrements sensibles contre leur exposition. Vous pouvez utiliser des restrictions de niveau d'enregistrement pour contrôler les utilisateurs ou les groupes qui peuvent accéder à des enregistrements spécifiques dans les incidents DLP.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read - Affichage (lecture seule).

Pourquoi et quand exécuter cette tâche

Les restrictions de niveau d'enregistrement vous permettent de fournir un accès aux enregistrements uniquement à des utilisateurs ou groupes spécifiques, offrant un moyen plus granulaire de contrôler les enregistrements auxquels un utilisateur peut accéder. Vous pouvez créer une restriction au niveau de l'enregistrement en définissant les conditions de correspondance des incidents DLP, en sélectionnant les utilisateurs ou les groupes auxquels

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ces conditions s'appliquent, puis en choisissant les enregistrements DLP que ces utilisateurs ou groupes peuvent afficher.

Procédure

1. Accédez à la **Tout** > **Administration DLP** > **Restrictions d'accès aux incidents** > **Restrictions de niveaux d'enregistrements**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

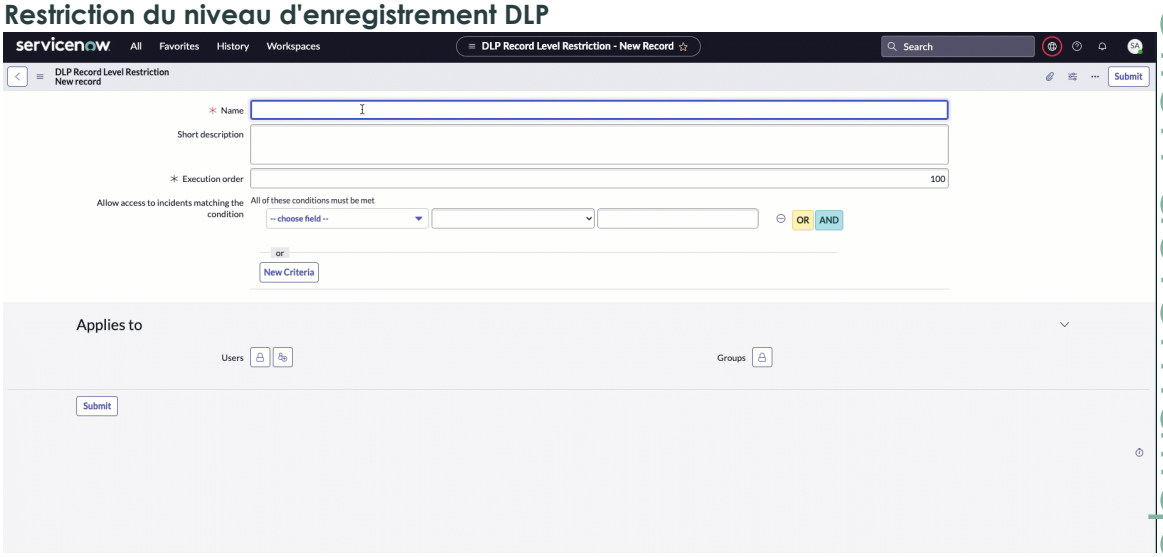
Formulaire de restriction du niveau d'enregistrement DLP

Champ	Description
Nom	Nom de la restriction au niveau de l'enregistrement.
Description brève	Description unique de cette restriction de niveau d'enregistrement.
Ordre d'exécution	Priorité des restrictions de niveau d'enregistrement. Ce champ indique l'ordre dans lequel les restrictions de niveau d'enregistrement sont exécutées lorsque deux restrictions de niveau d'enregistrement ou plus partagent les conditions de déclenchement. La restriction de niveau d'enregistrement associée au numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Autoriser l'accès aux incidents correspondant à la condition	Les options permettent d'accéder aux incidents dans les conditions définies. Vous pouvez sélectionner n'importe quel champ d'incident pour définir la condition de déclenchement des restrictions au niveau de l'enregistrement. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU** : ◦ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ◦ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse. Par exemple, vous pouvez sélectionner le champ `sur Actif`et définir la condition sur `tel quel` et `sur vrai`.
Concerne	Option permettant d'appliquer des restrictions au niveau de l'enregistrement à des utilisateurs ou

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	groupes spécifiques. Vous pouvez appliquer les conditions comme suit : ◦ **Utilisateurs** : cliquez sur pour ajouter un utilisateur particulier à partir de la liste auquel l'enregistrement sélectionné s'applique. Vous pouvez également ajouter un utilisateur à l'aide de son adresse e-mail ou de l'option de recherche. Par exemple, Responsable juridique. Pour vous ajouter en tant qu'utilisateur auquel l'enregistrement s'applique, cliquez sur . Par exemple, Administrateur système. ◦ **Groupes** : cliquez sur pour ajouter un groupe particulier à partir de la liste auquel l'enregistrement sélectionné s'applique. Vous pouvez également ajouter un groupe à l'aide de l'option de recherche. Par exemple, Créateurs d'enquêtes.

Restriction du niveau d'enregistrement DLP



4. Cliquez sur **Envoyer**.

Archivage des incidents DLP

Le Data Loss Prevention Incident Response est doté d'une règle d'archivage dans le système de base pour la table d'incidents DLP. Les enregistrements connexes sont également ajoutés dans le système de base à la règle d'archivage des incidents DLP.

Avant de commencer

Rôle requis : administrateur

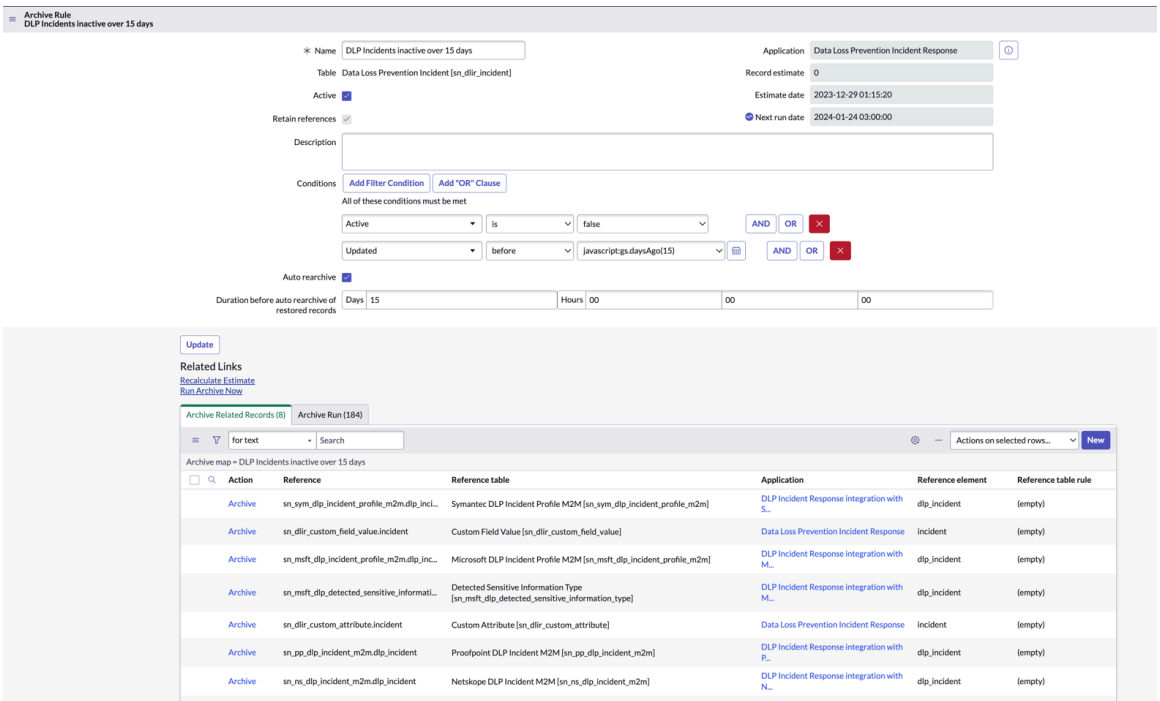
Procédure

1. Accédez à la **Tout** > **Archivage système** > **Règles d'archivage**.
   Les règles d'archivage système qui se trouvent dans le système de base s'affichent.
2. Affichez la règle d'archivage DLP.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : **Incidents DLP inactifs pendant plus de 15 jours** est la règle d'archivage système de base par défaut pour les incidents DLP. Vous pouvez modifier la règle d'archivage si nécessaire. Cette règle signifie que les incidents inactifs au-delà de 15 jours seront automatiquement archivés.



Remarque : Pour plus d'informations sur la façon dont les règles d'archivage sont créées, consultez Créer une règle d'archivage .

3. **Mettez à jour** la règle, si nécessaire.

Archiver les enregistrements connexes DLP

Utilisez la liste connexe Archiver les enregistrements connexes pour les incidents DLP afin d'ajouter les enregistrements connexes à la règle d'archivage.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Archivage système** > **Règles d'archivage**.
2. Sélectionnez la règle d'archivage **Incidents DLP inactifs sur 15 jours** .
3. Accédez à la liste connexe **Enregistrements connexes d'archivage** .
4. Affichez les enregistrements connexes DLP.

Application	Table de référence
Intégration de Symantec à Réponse aux incidents DLP	M2M du profil d'incident Symantec DLP [sn_sym_dlp_incident_profile_m2m]
Data Loss Prevention Incident Response	Valeur du champ personnalisé [sn_dlir_custom_field_value]

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application	Table de référence
Intégration de Microsoft à Réponse aux incidents DLP	M2M du profil d'incident DLP Microsoft [sn_msft_dlp_incident_profile_m2m]
Intégration de Microsoft à Réponse aux incidents DLP	Type d'information sensible détectée [sn_msft_dlp_detected_sensitive_information_type]
Data Loss Prevention Incident Response	Attribut personnalisé [sn_dlir_custom_attribute]
Intégration de Proofpoint à Réponse aux incidents DLP	M2M de l'incident DLP ProofPoint [sn_pp_dlp_incident_m2m]
Intégration de DLP Incident Response à Netskope	M2M de l'incident DLP Netskope [sn_ns_dlp_incident_m2m]
Intégration de Symantec à Réponse aux incidents DLP	Type d'information sensible détectée [sn_sym_dlp_detected_sensitive_information_type]

Remarque : Toutes les tables système telles que les e-mails, les évaluations et les pièces jointes sont automatiquement dirigées vers l'enregistrement DLP archivé.

5. Sélectionnez la règle d'enregistrement connexe d'archivage que vous souhaitez archiver.

Remarque : Pour plus d'informations sur l'ajout d'enregistrements connexes supplémentaires, consultez Archivage des enregistrements connexes DLP sur Now Platform.

Data Loss Prevention Incident Response Gestion des incidents

Utilisez Gestion Data Loss Prevention Incident Response des incidents pour mettre à jour et gérer les incidents en tirant parti de l'espace de travail de l'utilisateur DLP, de l'espace de travail de l'analyste DLP et du tableau de bord DLP.

Data Loss Prevention Incident Response Espace de travail de l'utilisateur

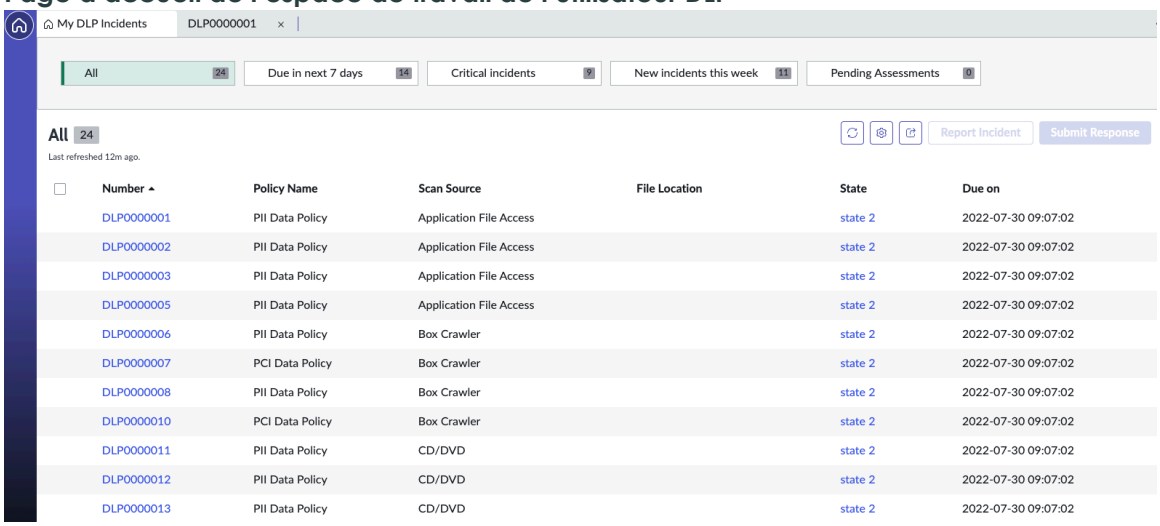
L'espace Data Loss Prevention Incident Response de travail utilisateur (DLP IR) est un espace de travail où les utilisateurs finaux, les gestionnaires et les approbateurs peuvent répondre aux incidents DLP affectés. Les utilisateurs finaux, les gestionnaires et les approbateurs peuvent alors répondre aux incidents en spécifiant les actions correctes.

Vous pouvez également créer et gérer des évaluations pour permettre aux utilisateurs finaux de répondre aux incidents DLP. L'espace de travail se compose d'une page de destination et de vues de listes qui vous permettent de voir les incidents DLP affectés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Page d'accueil de l'espace de travail de l'utilisateur DLP



Signaler des incidents DLP ou y répondre

Accédez à l'espace de travail de l'utilisateur Data Loss Prevention Incident Response (DLP), passez en revue les incidents DLP affectés et signalez les incidents ou répondez-y.

Avant de commencer

Rôle requis :

- Tout utilisateur/employé valide

Procédure

1. Accédez à la **Tout** > **Gestion des incidents DLP** > **Espace de travail de l'utilisateur DLP**. La page Mes incidents DLP s'ouvre dans un nouvel onglet.
2. Cliquez sur une vue de liste pour examiner les incidents qui vous sont affectés.

Vue liste	Description
Tout	Affichez tous les incidents affectés.
Échéance dans les 7 prochains jours	Affichez tous les incidents dus dans les 7 prochains jours.
Incidents critiques	Affichez tous les incidents portant l'étiquette de gravité critique.
Nouveaux incidents de cette semaine	Affichez tous les incidents qui sont affectés cette semaine.
Évaluations en attente	Affichez toutes les évaluations encore en attente.

3. Vous pouvez examiner les incidents DLP de deux manières :

   a. La première consiste à localiser et sélectionner un ou plusieurs incidents DLP que vous souhaitez examiner, puis à cocher la case en regard des incidents.

   b. Choisissez l'option qui vous convient.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

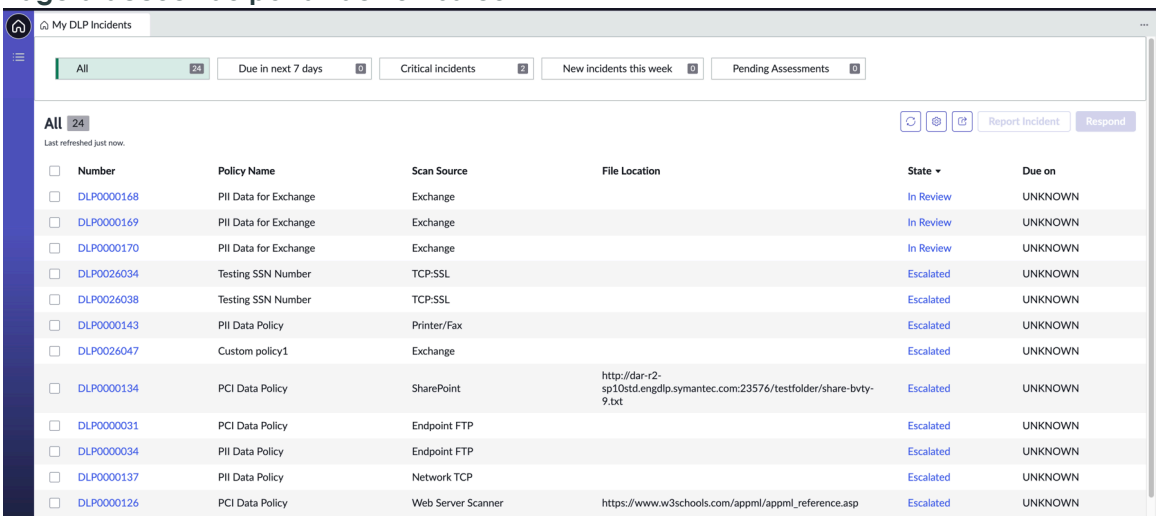
Page d'accueil du portail de l'utilisateur final DLP

Option	Description
Actualiser la liste	Option permettant d'actualiser la liste des incidents DLP si vous avez effectué une mise à jour.
Actions sur la liste	Liste des actions que vous pouvez effectuer. Les choix sont les suivants : ▪ **Enregistrer sous** ▪ **Modifier les colonnes** ▪ **Rétablir la largeur des colonnes** **Remarque :** Lorsque vous avez votre propre liste personnalisée créée dans la section **Mes listes** configurée pour votre espace de travail, vous pouvez également effectuer les actions de liste supplémentaires ci-dessous : ▪ **Renommer** ▪ **Enregistrer** ▪ **Supprimer**
Copier l'URL pour tout	Option permettant de copier les URL de tous les incidents DLP.
Signaler un incident	Action pour signaler l'incident comme faux positif ou propriétaire incorrect. Par exemple, vous pouvez signaler un propriétaire incorrect et suggérer un autre propriétaire ou signaler l'incident comme un faux positif.
Répondre	Répondez à un incident en sélectionnant une option de réponse aux incidents. Par exemple, si un utilisateur supprime un fichier qui enfreint une stratégie DLP, il peut choisir l'option **Fichier supprimé** pour soumettre une confirmation manuelle que le fichier a été supprimé et fournir des commentaires. À partir de là, vous pouvez également sélectionner des options de réponse avancées. Par exemple, **Demander la sortie de quarantaine par e-mail**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Page d'accueil du portail de l'utilisateur DLP



c. La deuxième méthode consiste à cliquer sur un incident DLP particulier pour l'ouvrir. L'onglet **Détails** comprend les sections suivantes :

- Détails : vous pouvez afficher les détails de l'incident DLP tels que le numéro d'incident, la gravité et le nom de fichier.
- Composer : pour ajouter des commentaires sur l'incident DLP visible par tout le monde, saisissez les commentaires dans l'onglet Commentaires. Pour ajouter des commentaires visibles par certaines personnes, saisissez les commentaires dans l'onglet Notes de travail (privées).
- Activité : vous pouvez afficher les détails des différentes activités sur l'incident DLP.
- Pièces jointes : si vous avez des pièces jointes liées à l'incident DLP, cliquez sur **Parcourir** et sélectionnez la pièce jointe sur votre disque local.

  L'onglet **Détails supplémentaires** affiche toutes les informations supplémentaires sur l'incident DLP, y compris les champs personnalisés.

Important :

- Les champs personnalisés pour les incidents DLP ne sont pris en charge que sur la version San Diego ou ultérieure.
- Si des données de champs personnalisés sont disponibles pour un incident DLP particulier, vous pouvez les afficher sous l'onglet **Détails supplémentaires** . S'il n'existe aucun champ personnalisé pour l'incident DLP, la page blanche s'affiche.

- **Type d'information sensible détectée** : affiche les informations sensibles détectées lors de l'incident.

Remarque : Cette liste connexe n'est visible que pour les incidents DLP créés pour les intégrations Microsoft ou Symantec. Dans l'enregistrement d'incident Microsoft ou Symantec, chaque fois que l'utilisateur accède à l'enregistrement de type d'information sensible détectée, le contenu des correspondances en surbrillance relatif à cette intégration s'affiche.

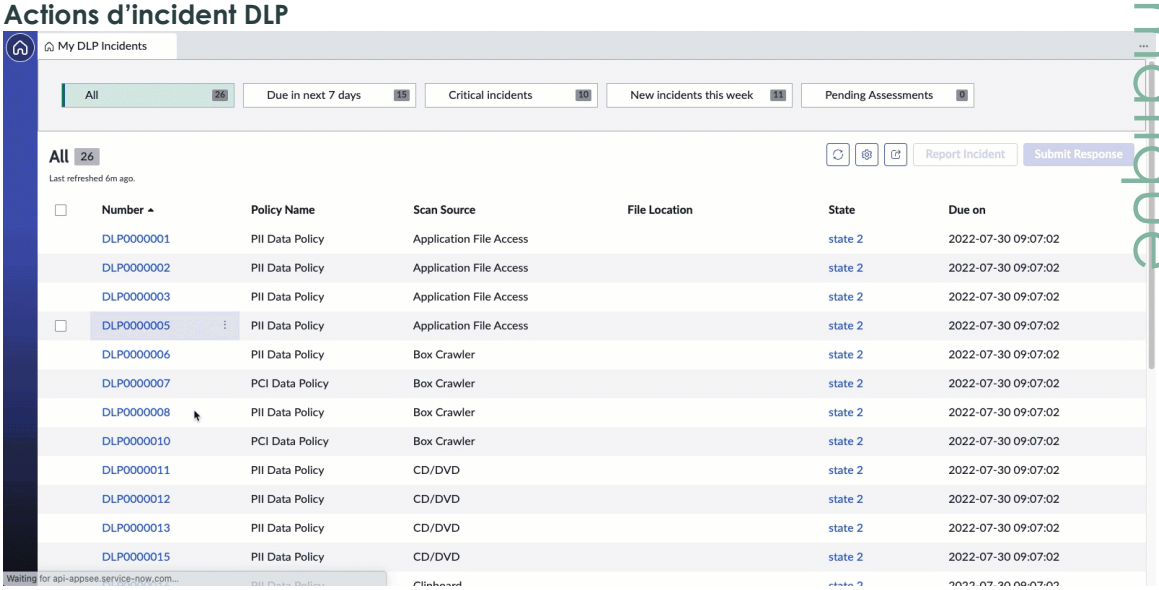
d. Choisissez l'option qui vous convient.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Signaler un faux positif	Action pour signaler que l'incident DLP a été déclenché ou créé de manière incorrecte. Vous pouvez mentionner les raisons pour lesquelles vous avez marqué l'incident comme faux positif dans le champ Commentaires.
Signaler un propriétaire incorrect	Action pour signaler que l'incident DLP a été affecté au mauvais utilisateur. Si vous connaissez le propriétaire correct de l'incident, vous pouvez sélectionner son nom dans le champ Suggérer un propriétaire. Pour ajouter des détails supplémentaires, utilisez le champ Commentaires.
Répondre	Répondez à un incident en sélectionnant une option de réponse aux incidents. Par exemple, si un utilisateur supprime un fichier qui enfreint une stratégie DLP, il peut choisir l'option **Fichier supprimé** pour soumettre une confirmation manuelle que le fichier a été supprimé et fournir des commentaires. À partir de là, vous pouvez également sélectionner des options de réponse avancées. Par exemple, **Demander la sortie de quarantaine par e-mail**.

Actions d'incident DLP



4. Pour effectuer des évaluations, sélectionnez la vue de liste **Évaluations en attente** .

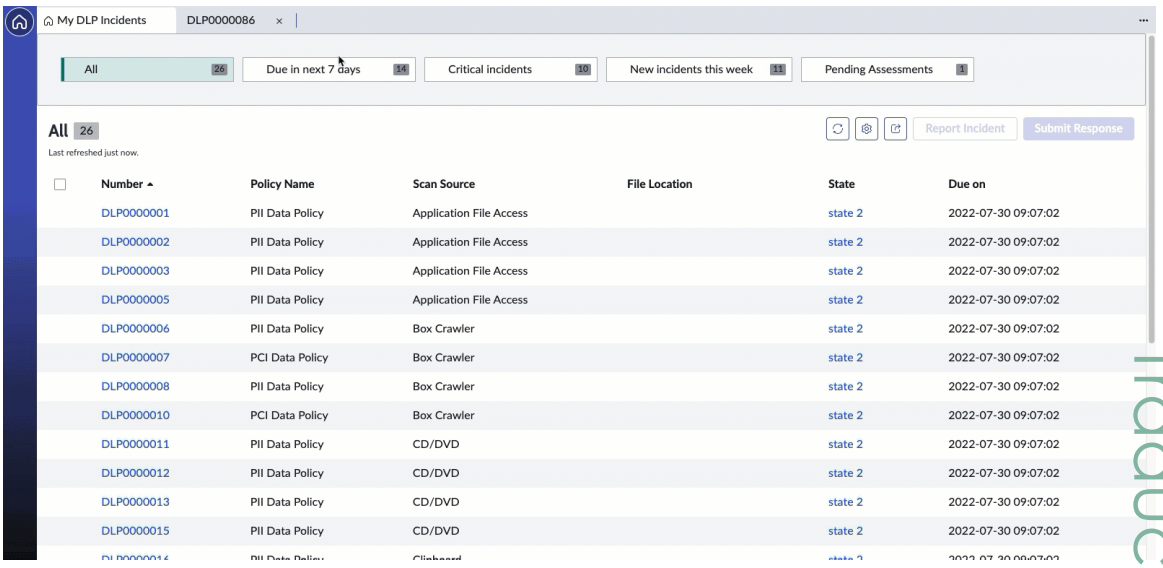
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Cliquez sur un numéro d'évaluation particulier pour l'ouvrir.

b. Répondez aux questions d'évaluation et cliquez sur **Enregistrer** ou **Soumettre** en fonction de vos besoins.

Évaluations DLP



5. Cliquez sur la section **Carte d'instructions** qui s'affiche en haut de tous les champs de la vue du formulaire d'incident DLP pour afficher les informations supplémentaires sur un incident particulier.

Remarque : Cette section de l'espace de travail guide les utilisateurs sur les informations relatives aux incidents, ce qui les aide à comprendre les étapes suivantes de la résolution des incidents.

La carte d'instructions de l'utilisateur affiche deux en-têtes différents qui vous fournissent plus d'informations sur un incident spécifique dans la vue de formulaire. Cliquez sur n'importe quel en-tête d'instructions de l'utilisateur pour connaître les détails supplémentaires.

Pour plus d'informations, consultez Créer des modèles d'instructions de l'utilisateur et Configurer les instructions de l'utilisateur de l'interface utilisateur DLP.

Utiliser le module Mes approbations

Le module Mes approbations sera disponible sur l'espace de travail des utilisateurs DLP pour les utilisateurs connectés. Les utilisateurs peuvent approuver ou rejeter les demandes d'approbation d'affectation à partir d'ici.

Avant de commencer

Rôle requis :

- Utilisateur final
- Responsable
- Approbateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Gestion des incidents DLP** > **Espace de travail de l'utilisateur DLP**.
   La page **Mes incidents DLP** s'affiche dans un nouvel onglet.
2. Cliquez sur le module **Mes approbations** présent sous **le module Mes incidents DLP** .
   La vue de liste Mes approbations s'affiche.

   L'approbateur peut approuver ou rejeter les demandes à partir de la vue de liste de **la page Mes approbations** . On peut approber ou rejeter les demandes multiples à partir de la vue de liste.

   L'approbateur peut afficher les détails de la demande affectée dans la vue de formulaire. En cliquant sur l'action **Approuver** ou **Rejeter** à partir de la vue de formulaire, vous pouvez approuver ou rejeter la demande individuelle.

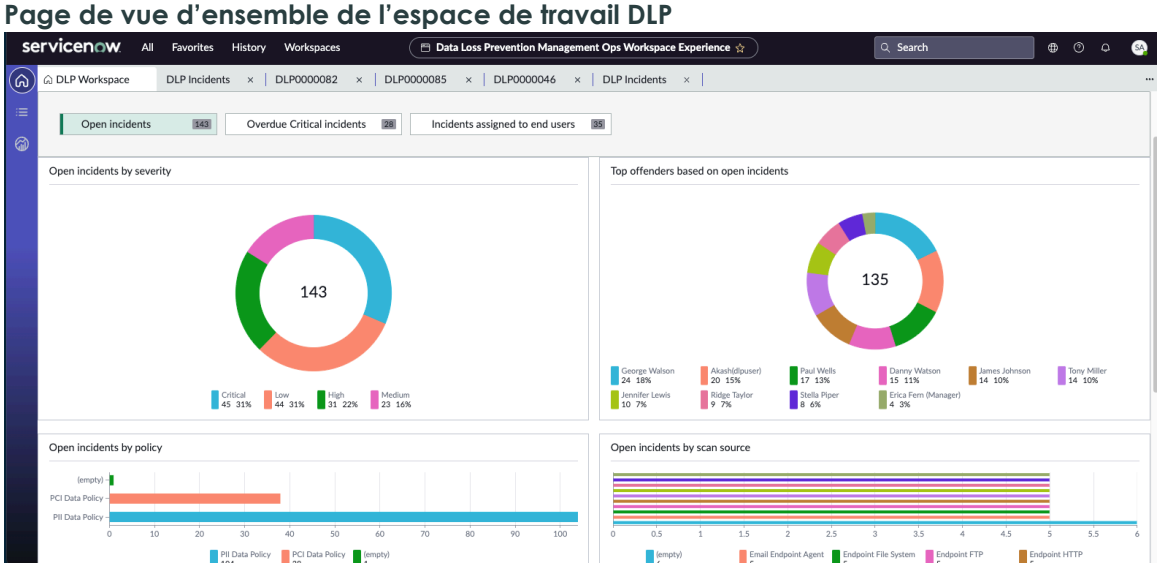
   Remarque : Pour afficher les détails de l'incident DLP, cliquez sur disponible dans le champ **Approuver** .

Data Loss Prevention Incident Response Espace de travail de l'analyste

Utilisez l'espace de travail de l'analyste Data Loss Prevention Incident Response (DLP IR) pour afficher les incidents DLP. Affectez les incidents aux utilisateurs finaux pour qu'ils les résolvent et plus encore.

L'espace de travail DLP se compose d'une page d'accueil avec des tableaux de bord, des vues de listes et des vues de formulaires qui vous permettent de surveiller les incidents DLP.

Page de vue d'ensemble de l'espace de travail DLP



Examiner et affecter vos incidents DLP

Accédez à l'espace de travail de l'analyste Data Loss Prevention Incident Response (DLP IR) afin de pouvoir examiner les incidents DLP et les affecter ou les résoudre. Vous pouvez suivre les tendances des incidents par gravité, des principaux contrevenants, des incidents par source d'analyse et des incidents par politique.

Page d'accueil de l'espace de travail

Vue d'ensemble de l'espace de travail

Avant de commencer

Rôle requis :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_dlir.analyst : modifier et afficher les incidents DLP.
- sn_dlir.analyst_read et sn_dlir.read : afficher les incidents DLP.

Procédure

1. Accédez à la **Tout** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**. La page de la liste Mes incidents ops de l'espace de travail DLP s'ouvre dans un nouvel onglet.
2. Cliquez sur l'icône d'accueil de **l'espace de travail DLP** pour afficher la vue de la page d'accueil de l'espace de travail.
3. Examinez les widgets du tableau de bord pour identifier les tendances par incidents par gravité, les principaux contrevenants, les incidents par source d'analyse et les incidents par politique.
4. Cliquez sur les filtres appropriés sur la page d'accueil pour afficher les widgets par leurs différentes catégories.

Filtres	Description
Incidents ouverts	Affichez tous les incidents ouverts.
Incidents critiques en retard	Affichez les incidents qui ont l'étiquette de gravité critique et qui sont en retard.
Incidents affectés aux utilisateurs finaux	Affichez les incidents affectés aux utilisateurs finaux.

5. Vous pouvez examiner et affecter les incidents DLP de deux façons :

   a. La première consiste à localiser et sélectionner un ou plusieurs incidents DLP que vous souhaitez examiner, puis à cocher la case en regard des incidents.

   b. Choisissez l'option qui vous convient.

Option	Description
Actualiser la liste	Option permettant d'actualiser la liste des incidents DLP lorsque vous effectuez une mise à jour.
Actions sur la liste	Liste des actions que vous pouvez effectuer. Les choix sont les suivants : ▪ **Enregistrer sous** ▪ **Modifier les colonnes** ▪ **Rétablir la largeur des colonnes**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Lorsque vous avez votre propre liste personnalisée créée dans la section **Mes listes** configurée pour votre espace de travail, vous pouvez également effectuer les actions de liste supplémentaires ci-dessous : ▪ **Renommer** ▪ **Enregistrer** ▪ **Supprimer**
Copier l'URL pour tout	Option permettant de copier les URL de tous les incidents DLP.
Afficher le panneau de filtre	Option permettant d'analyser les incidents requis à l'aide de l'option de filtre. **i.** Cliquez sur le filtre en haut à gauche de la page, puis sélectionnez **Vue avancée**. **ii.** Utilisez un filtre existant ou créez le vôtre en ajoutant des conditions qui contiennent un champ, un opérateur et des valeurs. **iii.** Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU** : ▪ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ▪ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. **iv.** Cliquez sur **Mettre à jour**.
Affecter l'incident	Action pour déterminer à qui affecter l'incident DLP. Les choix sont les suivants : ▪ **Affecter l'incident à** : option permettant d'affecter l'incident à un analyste, à un utilisateur final ou à une autre personne. ▪ **Utilisateur** : option permettant de déterminer à quel utilisateur l'incident doit être affecté. ▪ **État de l'incident Réponse pré-utilisateur** : option permettant de déterminer l'état de l'incident avant que l'utilisateur ne réponde. Il peut également s'agir d'un état personnalisé. ▪ **Joindre l'évaluation** : option permettant d'indiquer si vous souhaitez joindre une évaluation à l'incident. Si cette option

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	est activée, les options ci-dessous seront disponibles : ▪ **Modèle d'évaluation** : option permettant de sélectionner un modèle d'évaluation pour l'incident DLP. ▪ **État de l'incident Réponse post-utilisateur** Option permettant de sélectionner l'état dans lequel l'incident DLP doit se trouver une fois que l'utilisateur a répondu.
Répondre	Répondez à un incident en sélectionnant une option de réponse aux incidents. Par exemple, si un utilisateur supprime un fichier qui enfreint une stratégie DLP, il peut choisir l'option **Fichier supprimé** pour soumettre une confirmation manuelle que le fichier a été supprimé et fournir des commentaires. À partir de là, vous pouvez également sélectionner des options de réponse avancées. Par exemple, **Demander la sortie de quarantaine par e-mail**.
Escalader	Action pour escalader l'incident. Vous pouvez escalader l'incident en sélectionnant l'utilisateur vers lequel vous souhaitez l'escalader. Vous pouvez également fournir des informations supplémentaires dans le champ Commentaires.
Mettre à jour l'état	Action pour mettre à jour l'état de l'incident. Vous pouvez mettre à jour l'état de l'incident en sélectionnant l'un des états dans les options déroulantes. Il peut également s'agir d'un état personnalisé.
Fermer	Action pour fermer les incidents. Sélectionnez le **code de fermeture** correspondant dans la liste déroulante et ajoutez des commentaires de fermeture. La fonctionnalité **Fermer** dans Data Loss Prevention Incident Response s'effectue à la fois de manière asynchrone et synchrone à partir de la vue de liste. **i.** Fermeture synchrone : lors de la fermeture des incidents de manière synchrone, cela signifie que l'action de fermeture est exécutée immédiatement. Lorsque vous sélectionnez plusieurs incidents à fermer et si le nombre

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	d'incidents est inférieur ou égal à 100, les incidents sont fermés au premier plan de la vue de liste Incidents DLP. Ici, 100 est la valeur par défaut. **ii.** Fermeture asynchrone : cela implique que la demande de fermeture est envoyée et que l'application exécute la demande en arrière-plan si le nombre d'incidents sélectionnés est supérieur à 100. Vous devez actualiser la vue de liste Incidents DLP pour afficher l'état des incidents mis à jour. **Remarque :** ▪ Le nombre d'incidents sélectionné pour la fermeture asynchrone ou synchrone est configuré à l'aide de la propriété système *sn_dlir.closure_sync_count_limit*. ▪ Par défaut, le nombre d'incidents est défini sur 100.

c. La deuxième méthode consiste à cliquer sur un incident DLP particulier pour l'ouvrir.

- **Onglet Détails** : affiche les sections suivantes :
  - **Détails** : vous pouvez afficher les détails de l'incident DLP tels que le numéro d'incident, la gravité, le nom de fichier, etc. Vous avez également la possibilité de modifier respectivement les champs Gravité, État, Utilisateur final et Groupe d'analystes DLP et de les enregistrer.
  - **Composer** : pour ajouter des commentaires sur l'incident DLP visible par tout le monde, saisissez les commentaires dans l'onglet Commentaires. Pour ajouter des commentaires visibles par certaines personnes, saisissez les commentaires dans l'onglet Notes de travail (privées).
  - **Activité** : vous pouvez afficher les détails des différentes activités sur l'incident DLP.
  - **Pièces jointes** : si vous avez des pièces jointes liées à l'incident DLP, cliquez sur **Parcourir** et sélectionnez la pièce jointe sur votre disque local.
- **Onglet Détails supplémentaires** : affiche toutes les informations supplémentaires sur l'incident DLP, y compris les champs personnalisés.

Important :

- Les champs personnalisés pour les incidents DLP ne sont pris en charge que sur la version San Diego ou ultérieure.
- Vous pouvez utiliser l'onglet **Détails supplémentaires** pour voir si des champs personnalisés ont été créés pour un incident DLP particulier ou non.

- **Onglet Attributs personnalisés** : affiche la liste des attributs personnalisés associés à l'incident DLP.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Autres incidents de l'utilisateur final** : affiche l'incident du même utilisateur final. Vous pouvez consolider les incidents en effectuant l'action **Ajouter en tant qu'incident enfant** à partir de cette liste connexe.
- **Type d'information sensible détectée** : affiche les informations sensibles détectées lors de l'incident.

> **Remarque :** Cette liste connexe n'est visible que pour les incidents DLP créés pour les intégrations Microsoft ou Symantec. Dans l'enregistrement d'incident Microsoft ou Symantec, chaque fois que l'utilisateur accède à l'enregistrement de type d'information sensible détectée, le contenu des correspondances en surbrillance relatif à cette intégration s'affiche.

- **Incidents enfants** : affiche les incidents enfants créés manuellement (en exécutant l'action « Ajouter comme incident enfant ») ou à partir des règles de consolidation DLP. Vous pouvez dissocier l'incident enfant en effectuant l'opération « Dissocier l'incident enfant » de cette liste connexe.
- **Incidents clonés** : affiche les incidents clonés de l'incident parent. En cliquant sur l'action **Cloner l'incident** de la vue de formulaire, vous pouvez créer un nouvel incident cloné.
- **Onglet Évaluations** : affiche la liste des évaluations affectées à l'incident DLP.

d. Choisissez l'option qui vous convient.

Option	Description
Affecter l'incident	Action pour déterminer à qui affecter l'incident DLP. Les choix sont les suivants : ▪ **Affecter l'incident à** : option permettant d'affecter l'incident à un analyste, à un utilisateur final ou à une autre personne. ▪ **Utilisateur** : option permettant de sélectionner l'utilisateur auquel l'incident doit être affecté. ▪ **État de l'incident Réponse pré-utilisateur** : option permettant de sélectionner l'état dans lequel l'incident doit se trouver avant que l'utilisateur ne réponde. Il peut également s'agir d'un état personnalisé. ▪ **Joindre l'évaluation** : option permettant d'indiquer si vous souhaitez joindre une évaluation à l'incident. Si cette option est activée, les options ci-dessous seront disponibles : ▪ **Modèle d'évaluation** : option permettant de sélectionner un modèle d'évaluation pour l'incident DLP. ▪ **État de l'incident après la réponse de l'utilisateur** : option permettant

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	de sélectionner l'état dans lequel l'incident DLP doit se trouver une fois que l'utilisateur a répondu.
Annuler l'approbation	Action pour annuler la demande d'approbation. Cette action est visible par les analystes dans la vue de formulaire uniquement lorsque l'incident DLP est dans l'état **En attente d'approbation** . Les options disponibles sont les suivantes : ▪ **Affecter l'incident à** : option permettant de n'affecter l'incident à personne, à un analyste ou à quelqu'un d'autre. ▪ **Utilisateur** : option permettant de sélectionner l'utilisateur auquel l'incident doit être affecté. ▪ **État de l'incident post-annulation** : option permettant de sélectionner l'état dans lequel l'incident doit se trouver après l'annulation de la demande. ▪ **Commentaires** : pour fournir des détails supplémentaires sur l'annulation.
Affecter une évaluation	Action permettant de joindre une évaluation lors de l'affectation de l'incident. Les choix sont les suivants : ▪ **Modèle d'évaluation** : option permettant de sélectionner un modèle d'évaluation pour l'incident DLP. ▪ **État de l'incident après la réponse de l'utilisateur** : option permettant de sélectionner l'état dans lequel l'incident DLP doit se trouver une fois que l'utilisateur a répondu.
Télécharger le fichier	Action pour télécharger le fichier ou l'e-mail qui contient le contenu en infraction. Cette action peut être effectuée pour les incidents créés pour Microsoft OneDrive, SharePoint Online ou Exchange Online.
Enregistrer	Action pour enregistrer toutes les modifications que vous avez apportées. Vous pouvez modifier les champs Gravité, État et Utilisateur final de l'incident DLP et les enregistrer.
Répondre	Répondez à un incident en sélectionnant une option de réponse aux incidents. Par exemple, si un utilisateur supprime un fichier qui enfreint une stratégie DLP, il peut choisir l'option **Fichier supprimé**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

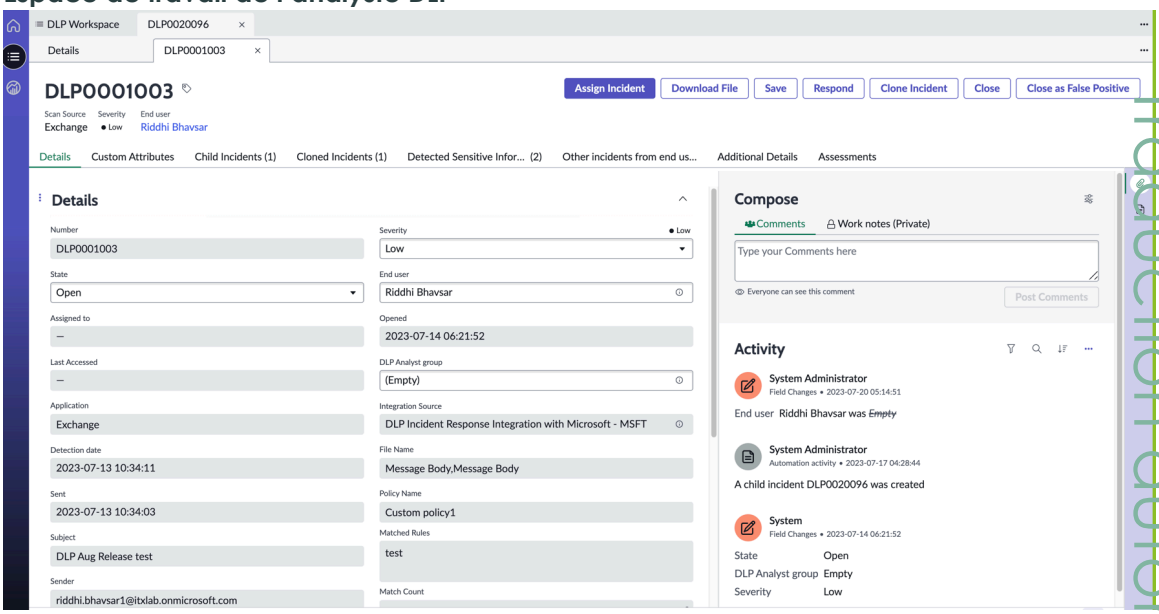
Option	Description
	pour soumettre une confirmation manuelle que le fichier a été supprimé et fournir des commentaires. À partir de là, vous pouvez également sélectionner les options de réponse avancées. **Par exemple : demander la levée de quarantaine par e-mail**.
Escalader	Action pour escalader l'incident. Vous pouvez escalader l'incident en sélectionnant l'utilisateur vers lequel vous souhaitez l'escalader. Vous pouvez également fournir des informations supplémentaires dans le champ Commentaires.
Cloner l'incident	Action pour créer un clone incident si l'enregistrement d'incident a un impact sur plusieurs utilisateurs. Vous pouvez affecter les incidents clonés à plusieurs parties prenantes, telles que le service juridique/informatique. Après avoir créé un enregistrement d'incident clone, un nouvel onglet **Incidents clonés** est créé sous l'incident DLP parent et tous les incidents clonés sont répertoriés dans cette vue. **Remarque :** ▪ Si l'enregistrement d'incident DLP parent est fermé, tous les enregistrements d'incidents clonés se ferment automatiquement. ▪ Si un enregistrement d'incident DLP contient un incident cloné, il ne peut pas être affecté aux utilisateurs finaux. Les enregistrements d'incidents DLP parents ne peuvent être gérés que par les utilisateurs disposant du rôle Analyste. ▪ Vous pouvez également mettre à jour automatiquement l'état parent en fonction de l'état des incidents clonés dans le module Configuration par défaut. Par exemple, si tous les incidents clonés passent à l'état Escaladé, l'incident parent passera également à l'état Escaladé.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Fermer	Action pour fermer l'incident. Vous devez sélectionner le **code de fermeture** correspondant dans la liste déroulante et ajouter des commentaires de fermeture, si nécessaire.
Fermer en tant que faux positif	Action pour fermer l'incident en tant que faux positif. Vous pouvez également ajouter des commentaires supplémentaires avant de fermer l'incident.

Espace de travail de l'analyste DLP



6. Vous pouvez afficher la vue Liste à partir de la page d'accueil en accédant au coin supérieur gauche de la page et en cliquant sur l'onglet **Listes** .
   La catégorie Listes comprend les pages de liste personnalisées et par défaut pour les incidents DLP.
   - **Onglet Listes** : listes par défaut pour les incidents DLP. Les listes par défaut sont les suivantes :
     - Tout
     - Ouvrir
     - Mes incidents
     - Affecté à mon groupe
     - Remonté
     - En retard
     - Évaluations en attente
     - Action de l'utilisateur en attente

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

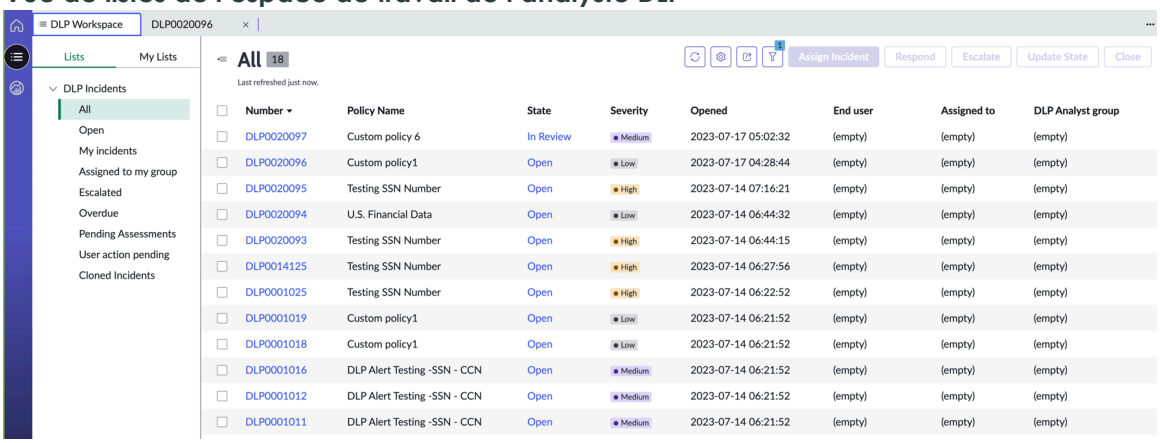
- Incidents clonés
- Incidents archivés

◦ **Onglet Mes listes** : affiche toutes les listes que vous avez renommées et toutes les listes que vous avez créées.

Example

L'exemple suivant montre l'espace de travail DLP avec les catégories de vue de liste. L'option **Toute** la vue de liste est sélectionnée.

Vue de listes de l'espace de travail de l'analyste DLP



Afficher les incidents DLP archivés

Utiliser l'espace de travail de l'analyste DLP pour afficher les incidents DLP archivés

Avant de commencer

Rôle requis :

- sn_dlir.analyst : modifier et afficher les incidents DLP.
- sn_dlir.analyst_read et sn_dlir.read : afficher les incidents DLP.

Procédure

1. Accédez à la **Tout** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
   Par défaut, la section Mes incidents s'affiche.
2. Cliquez sur **Incidents archivés**.
   La liste des incidents DLP archivée s'affiche.
3. Cliquez sur le bouton **Afficher le nombre d'incidents** pour afficher le nombre d'incidents archivés.

Remarque :

◦ Par défaut, le nombre d'incidents archivés est masqué pour améliorer le temps de chargement de la liste. Vous devez cliquer sur le bouton **Afficher le nombre d'incidents** pour afficher le nombre d'incidents. En outre, un message d'information s'affiche pour indiquer le nombre d'incidents.

◦ La propriété système glide.ui.list.seismic.omit.count est activée dans le système de base pour que les incidents archivés masquent le nombre d'incidents dans la liste.

4. Sélectionnez un ou plusieurs incidents DLP que vous souhaitez afficher.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'incident DLP affiche la section des détails de l'incident.

Remarque :

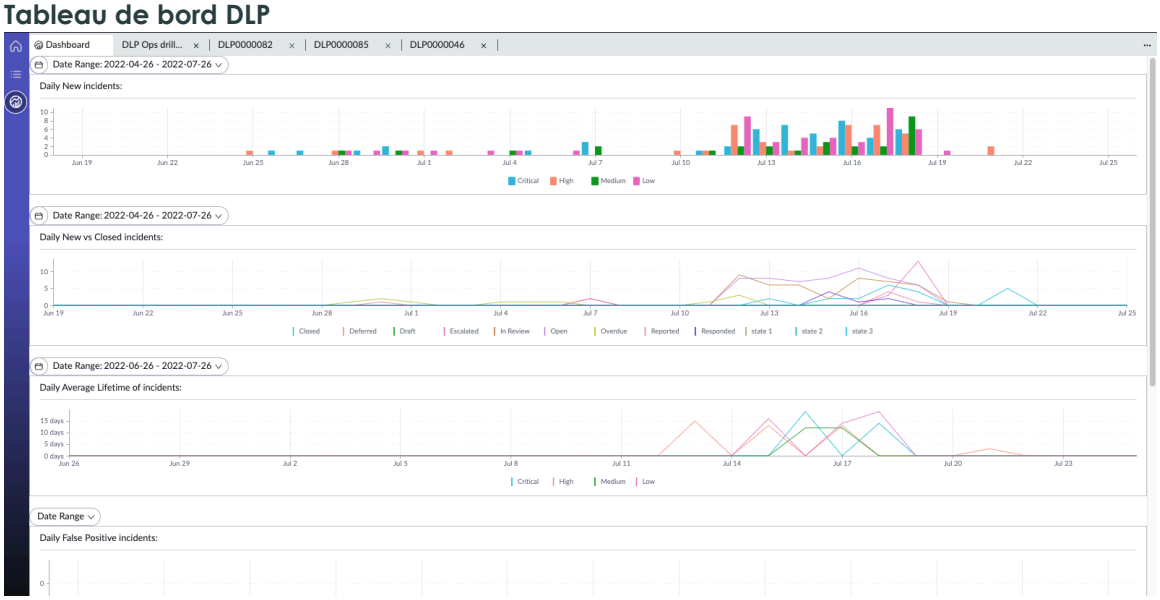
- L'onglet **Autres incidents des utilisateurs finaux** inclut également les incidents archivés.
- **Le contenu de correspondance** est pris en charge pour tous les incidents archivés (qui seront également pris en charge dans toutes les intégrations), mais **le téléchargement du fichier** n'est pris en charge que pour les intégrations Microsoft.

Tableau de bord de Data Loss Prevention Incident Response

Le Data Loss Prevention Incident Response tableau de bord (DLP IR) fournit une vue d'ensemble approfondie de vos incidents DLP et des tendances des incidents quotidiens dans votre instance sous la forme de graphiques graphiques. Ces graphiques vous aident à visualiser, gérer et corriger efficacement les incidents DLP.

Le Data Loss Prevention Incident Response tableau de bord fournit des aperçus clés sur vos incidents DLP quotidiens. Vous pouvez configurer des indicateurs et collecter régulièrement des instantanés de données des incidents correspondant aux conditions dans les propriétés de l'indicateur. Les données collectées sont ensuite visualisées à l'aide de widgets dans le tableau de bord. Pour analyser les incidents DLP à différents intervalles de temps, vous pouvez appliquer différentes plages de dates.

Tableau de bord DLP



Analyser les tendances des incidents quotidiens dans vos incidents DLP

Accédez au Data Loss Prevention Incident Response tableau de bord (DLP IR) pour analyser les tendances quotidiennes de vos incidents DLP et y remédier efficacement.

Avant de commencer

Rôle requis :

- sn_dlir.analyst : modifier et afficher les incidents DLP.
- sn_dlir.analyst_read et sn_dlir.read : afficher les incidents DLP.

Pourquoi et quand exécuter cette tâche

Vous pouvez visualiser les tendances quotidiennes à l'aide de widgets dans le tableau de bord DLP. Les données ou statistiques concernant les tendances quotidiennes de vos incidents DLP sont collectées à partir des propriétés de l'indicateur d'incidents quotidiens

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

définies par votre organisation. Vous pouvez obtenir des aperçus clés en appliquant différentes plages de données pour analyser les incidents DLP à différents intervalles de temps pour les graphiques suivants :

- **Nouveaux incidents quotidiens** : données sur l'ensemble des incidents DLP créés quotidiennement, quel que soit l'état de l'incident. Les incidents DLP sont classés en fonction de leur gravité, notamment moyenne, critique, élevée et faible. Chaque gravité d'incident DLP est représentée par une couleur particulière sur le graphique.
- **Incidents quotidiens nouveaux par rapport aux incidents fermés** : les différents états des incidents DLP et une comparaison entre les nouveaux incidents quotidiens et les incidents fermés quotidiens. La catégorie Nouvelles quotidiennes comprend tous les incidents DLP dont l'état est Ouvert, Brouillon, Escaladé, En cours de révision, En retard, Signalé, Reçu une réponse ou Personnalisé (le cas échéant). La catégorie Incidents fermés inclut les incidents DLP fermés. Chaque état d'incident DLP est représenté par une couleur particulière sur le graphique.
- **Durée de vie moyenne quotidienne des incidents** : la durée de vie d'un incident est la période entre l'ouverture et la fermeture d'un incident DLP spécifique. La durée de vie moyenne quotidienne est calculée uniquement pour les incidents DLP fermés.
- **Incidents de faux positif quotidiens** : données de tous les incidents DLP signalés comme faux positifs quotidiens. Les incidents de faux positif quotidiens sont classés en fonction de leur gravité, et comprend une moyenne, une critique, une élevée et une faible. Chaque gravité quotidienne d'incident faux positif est représentée par une couleur particulière sur le graphique.
- **Âge par rapport à la gravité des incidents** : comparaison des données de tous les incidents DLP, classés par âge et configurés avec la gravité des incidents DLP. La catégorie d'âge inclut tous les incidents DLP dont l'âge est inférieur à celui défini par votre organisation. Pour en savoir plus sur les graphiques des âges, reportez-vous à Créer des configurations du graphique des âges. La gravité des incidents inclut tous les incidents DLP de la catégorie élevée ou faible. Chaque gravité est représentée par une couleur particulière sur le graphique.
- **Incidents escaladés quotidiennement** : données de tous les incidents DLP escaladés quotidiennement. Les incidents escaladés quotidiennement sont classés en fonction de leur gravité, notamment moyenne, critique, élevée ou faible. Chaque gravité d'incident escaladé quotidiennement est représentée par une couleur particulière sur le graphique.

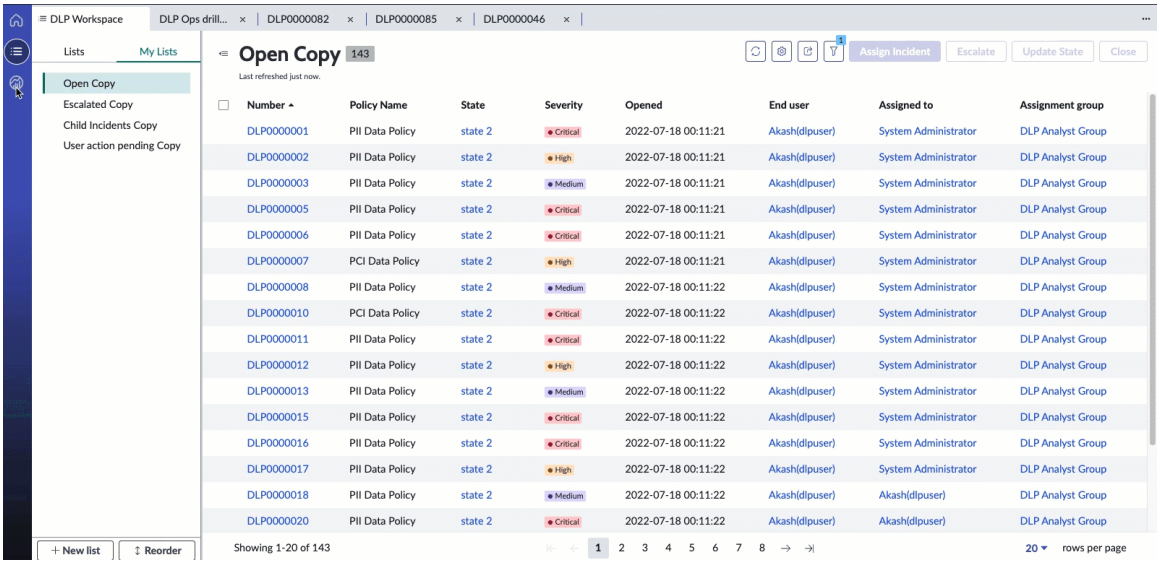
Procédure

1. Accédez à la **Tout** > **Gestion des incidents DLP** > **Tableau de bord DLP**.
   La page Mon tableau de bord DLP s'affiche dans un nouvel onglet de navigateur.
2. Sélectionnez un widget de tableau de bord pour lequel vous souhaitez effectuer une analyse de tendance quotidienne.
   Par exemple, le graphique Nouveaux incidents quotidiens.
3. Examinez les widgets du tableau de bord pour identifier des tendances.
4. Cliquez sur **Plage de dates**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble du tableau de bord DLP



5. Sélectionnez une plage de dates dans le calendrier, puis cliquez sur **Appliquer**.

   Example
   Par exemple, le graphique Nouveaux incidents quotidiens est mis à jour pour la plage de données sélectionnée.

6. Utilisez les filtres sous le graphique pour explorer et effectuer une analyse plus approfondie.

Intégration entrante pour Data Loss Prevention Incident Response

Créez un ou plusieurs incidents DLP à l'aide de l'API REST entrante.

Créer un seul incident DLP

Rôle requis : sn_dlir.api_integration_user.

Pour créer un seul incident DLP, définissez les paramètres suivants selon les besoins :

Champ	Description
Fonction de message REST	*POST*
URL	`https://{instance}/api/now/import/sn_dlir_incident_import`
En-tête de demande	Accepter: *application/json* Type de contenu : *application/json*
Exemple de charge utile	`{ "application_window_title": "<value>", "assigned_to": "<value>", "attachments": "<value>", "data_owner_email": "<value>", "destination": "<value>", "dest_ip": "<value>",`

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	"dest_ip_port": "<value>", "detection_date": "<value>", "endpoint_on_corporate_net": "<value>", "files": "", "file_created": "", "file_created_by": "", "file_location": "", "file_modified_by": "", "file_name": "", "file_owner": "", "file_permissions": "", "ftp_user_name": "", "last_modified": "", "machine_ip": "", "machine_name": "", "match_count": "", "policy_id": "", "policy_name": "", "printer_name": "", "printer_type": "", "print_job_name": "", "recipients": "", "scanned_machine": "", "scan_source": "", "seen_before": "", "sender":"", "source":"", "source_file":"", "source_ip":"", "source_ip_port":"", "subject":"", "url":"", "user_justification":"" }

Exemple de réponse	{
	"import_set": "ISET0010003",
	"staging_table": "sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value": "DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id":
	"7cda322297c2411056a43d1e6253af1f"
	}
	]
	}

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer plusieurs incidents DLP

Rôle requis : sn_dlir.api_integration_user.

Pour créer plusieurs incidents DLP à partir de la même demande, définissez les paramètres suivants selon les besoins :

Champ	Description
Fonction de message REST	*POST*
URL	`https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple`
En-tête de demande	Accepter: *application/json* Type de contenu : *application/json*
Exemple de charge utile	`{ "records": [{ "file_name": "<value>", "file_modified_by": "<value>", "work_notes": "<value>", "url": "<value>", "scan_source": "<value>", "data_owner_email": "<value>", "file_created_by": "<value>", "file_owner": "<value>", "policy_name": "<value>" }, { "dest_ip": "<value>", "dest_ip_port": "<value>", "detection_date": "<value>", "endpoint_on_corporate_net": "<value>", "files": "<value>", "file_created": "<value>", "file_created_by": "<value>", "file_location": "<value>", "file_modified_by": "<value>", "file_name": "<value>", "file_owner": "<value>", }] }`
Exemple de réponse	`{ "import_set_id": "a38f69229734dd1056a43d1e6253af75",`

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description

	<pre>{
	"multi_import_set_id":
	"e78f69229734dd1056a43d1e6253af75"
	}</pre>

Remarque : Par défaut, la transformation est asynchrone. Pour définir la transformation synchrone, créez un nouvel enregistrement dans la table Insertion multiple REST [sys_rest_insert_multiple], sélectionnez la table source comme **sn_dlir_incident_import** et définissez la transformation sur **synchrone**.

Intégrations DLP

Le Data Loss Prevention Incident Response système de base comprend des intégrations à des progiciels tiers de prévention de la perte de données.

Cette section fournit des instructions pour l'activation des modules d'extension et la configuration des intégrations ServiceNow tierces. Vous y trouverez également des directives de base pour le développement de vos propres intégrations, ainsi que des détails sur les intégrations spécifiques incluses dans le système de base.

Configurations d'intégration

Le système de base comprend une série de cartes pour chacune des implémentations d'intégration que vous pouvez activer et utiliser. En outre, des cartes s'affichent pour toutes les intégrations publiées sur le ServiceNow Store qui ont des dépendances sur Opérations de sécurité des modules d'extension. Vous pouvez afficher les cartes d'intégration en sélectionnant **Security Operations** > **Configurations d'intégration**.

Data Loss Prevention Incident Response prend en charge les progiciels tiers de prévention de la perte de données suivants :

Symantec Intégration pour Data Loss Prevention Incident Response

L'intégration Symantec DLP prend en charge l'ingestion des Data Loss Prevention Incident Response incidents créés sur le Symantec Data Loss Prevention Incident Response déploiement. Après l'ingestion, vous pouvez utiliser les fonctionnalités de gestion des incidents pour corriger les incidents DLP.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Vue d'ensemble et fonctionnalités principales

L'intégration Symantec DLP aide les entreprises à suivre l'utilisation et le déplacement des données sensibles sur diverses plateformes.

Cette intégration comprend les fonctionnalités clés suivantes :

- Capacité à créer plusieurs profils d'intégration pour différents Symantec points de terminaison d'API.
- Ingestion planifiée des incidents DLP à partir de Symantec votre ServiceNow instance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Possibilité d'appliquer des filtres d'API pour récupérer les incidents qui correspondent aux critères de filtre et également de spécifier le filtre pour Symantec les incidents DLP qui doivent être importés.
- Mappage des états des incidents DLP dans votre ServiceNow instance aux états des incidents DLP dans Symantec.
- Mettez automatiquement à jour l'état de l'incident lorsque Symantec l'état change dans votre ServiceNow instance.
- Possibilité de personnaliser et de définir le mappage de gravité entre les incidents Symantec DLP et les incidents ServiceNow.

Pour en savoir plus sur l'intégration, consultez la documentation produit Symantec .

Premiers pas avec l'intégration Symantec DLP pour la protection contre la perte de données

Avant de pouvoir utiliser l'intégration, vous devez la télécharger à ServiceNow® Storepartir du fichier .

Liste de vérification

Passez en revue les informations suivantes avant de commencer à configurer votre Symantec intégration DLP pour la protection contre la perte de données.

Liste de vérification

Champ	Description
Vérifiez que vous avez affecté les rôles requis Now Platformd'application , Application de prévention des pertes de données, Application MID.	Les rôles suivants sont utilisés dans l'intégration DLP Symantec sur Now Platform: • L'administrateur (admin) installe les applications à partir de et ServiceNow® Store assigne l'administrateur de la protection contre la perte de données (sn_dlir.admin). • L'utilisateur disposant du rôle sn_dlir.admin peut configurer l'intégration et configurer les profils d'incident. • Les utilisateurs disposant du rôle sn_dlir.analyst auront des rôles de lecture dans l'ensemble de l'intégration.
Affectez les rôles d'utilisateur DLP requis Symantec .	Passez en revue les autorisations et les rôles d'intégration Symantec DLP.
Vérifiez que vous utilisez Symantec DLP 15.8	L'intégration Symantec DLP pour la protection contre la perte de données est testée avec la version 15.8 de la protection contre la perte de Symantec données. **Remarque :** Assurez-vous d'utiliser Symantec DLP 15.8
Vérifiez que l'application ServiceNow® principale requise pour prendre en charge	Vérifiez que les applications DLP et les applications courantes de prise en charge de la sécurité suivantes sont installées et

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Champ	Description
l'intégration DLP Symantec est installée et activée.	activées à partir de ServiceNow Store. Si l'application n'est pas installée, installez-la et activez-la. • Security Support Common • Data Loss Prevention Incident Response

Installer et configurer l'intégration DLP pour la protection contre la Symantec perte de données

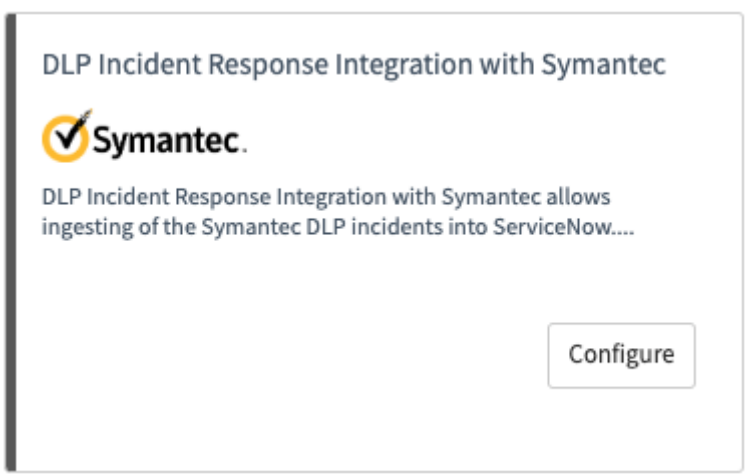
Installez et configurez l'intégration Symantec DLP à ServiceNow® Store partir de sur votre Now Platform instance. Commencez à examiner les incidents DLP à l'aide des données d'incident Symantec DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Téléchargez l'intégration Symantec DLP à partir de et ServiceNow® Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez l'intégration de la réponse aux incidents DLP avec Symantec la tuile et cliquez sur **Configurer**.



4. Renseignez les champs du formulaire.

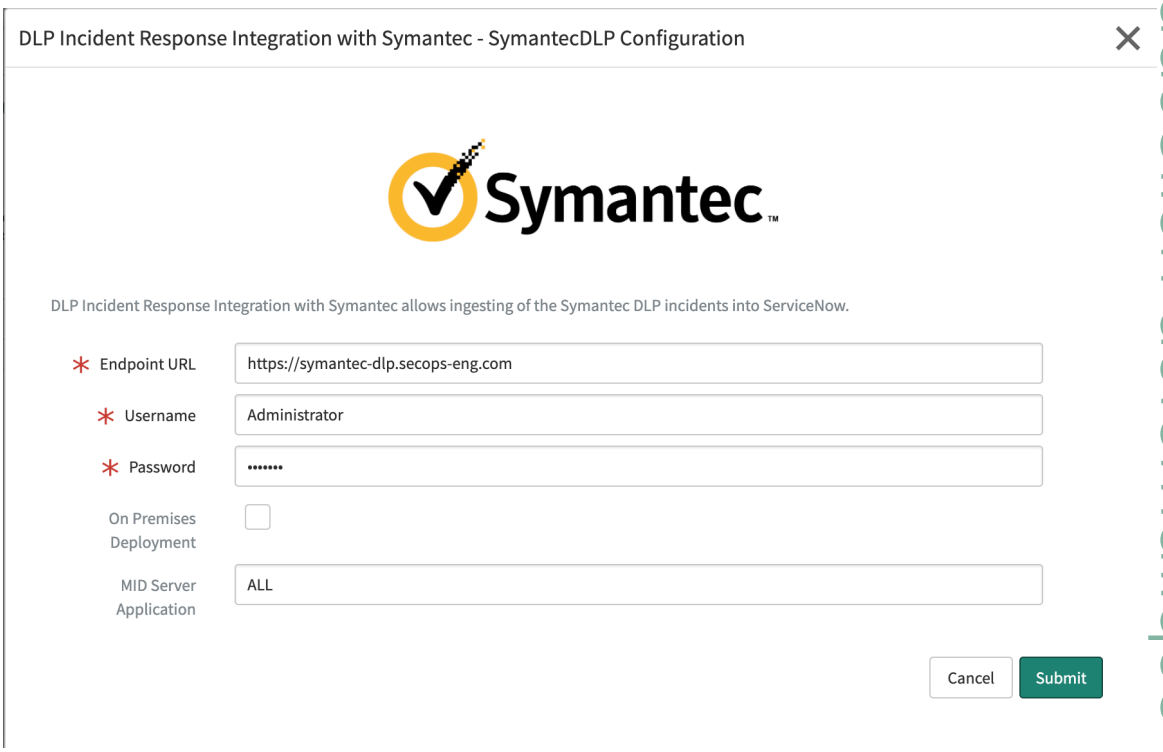
Formulaire de configuration de l'intégration DLP Symantec

Champ	Description
Nom	Nom de la configuration de l'intégration Symantec DLP.
URL du point de terminaison	Symantec Point de terminaison de l'API REST.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom d'utilisateur	Symantec Nom du compte. Pour plus d'informations sur les rôles et autorisations requis, consultez Rôles et autorisations .
Mot de passe	Symantec Mot de passe du compte.
Déploiement sur site	Option que vous pouvez sélectionner si vous Symantec êtes déployé dans une instance locale. Lorsque vous sélectionnez cette option, vous devez utiliser le MID Server pour vous connecter à Symantec.
Application de Serveur MID	Nom de l'application MID utilisée pour communiquer avec Symantec. Ce champ est nécessaire lorsque vous sélectionnez l'option **Déploiement sur site** .



5. Cliquez sur **Envoyer**.

Résultats
Une fois la configuration validée et envoyée, l'intégration Symantec DLP est enregistrée sous forme de vignette sur la page Intégrations de sécurité.

Créer un profil pour Symantec l'intégration DLP

Créez un profil d'incident dans votre Now Platform instance. Déterminez les incidents DLP Symantec qui conviennent à la création d'incidents DLP.

Avant de commencer
Rôle requis : sn_dlir.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Configurez le Now Platform® pour extraire les incidents DLP à partir du Symantec point de terminaison. Stockez ces incidents dans votre ServiceNow® instance en tant qu'incidents DLP.

Procédure

1. Accédez à la **Intégration DLP Symantec** > **Profil d'incident**.
2. Cliquez sur **Nouveau**.
3. Sur le formulaire, renseignez les champs de la section Nom.

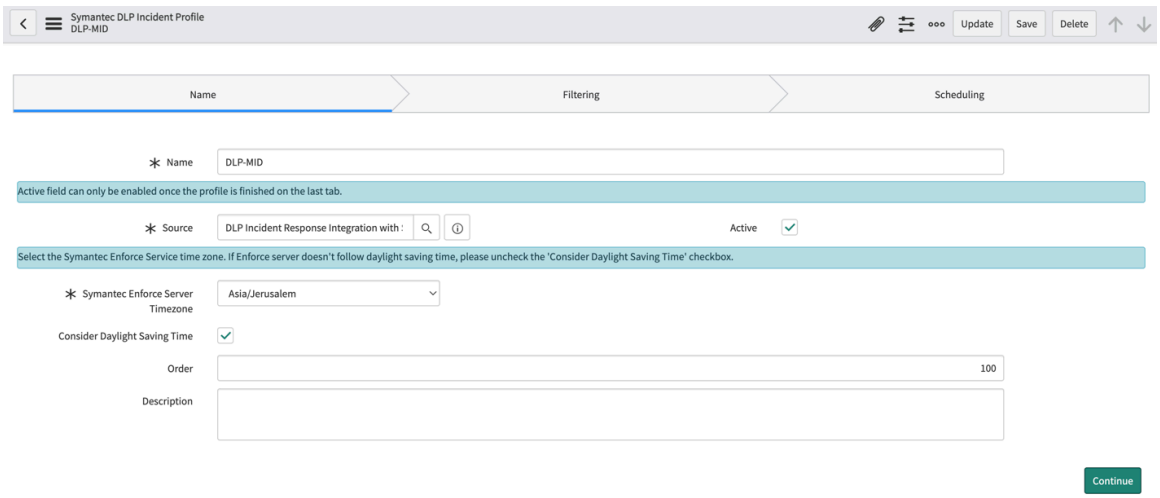
Créer un profil

Champ	Description
Nom	Nom du profil. Ce champ permet d'identifier le profil. **Remarque :** Le nom doit être unique pour chaque profil.
Source	Symantec Instance DLP que vous avez configurée pour ingérer des incidents. Si vous avez configuré plusieurs instances, sélectionnez l'instance appropriée pour les types d'incidents que vous prévoyez d'ingérer pour le profil.
Actif	Option permettant d'indiquer si le profil est actif. Ce champ ne peut être activé qu'après avoir cliqué sur Terminer dans la section **Planification** . Lorsque le profil est actif, cela signifie qu'il Now Platform interroge Symantec activement les incidents DLP. Les incidents DLP correspondants sont créés dans DLP lorsque les conditions de filtrage sont mises en correspondance en fonction des paramètres de planification que vous avez fournis.
Fuseau horaire du serveur Symantec Enforce	Sélectionnez le fuseau horaire du serveur Symantec Enforce dans le profil afin que les incidents ne soient pas manqués en raison de problèmes de fuseau horaire.
Prendre en compte l'heure d'été	Cochez cette case si le serveur d'application suit l'heure d'été.
Ordre	Ordre d'exécution du profil. Le profil dont l'ordre est le plus bas est considéré comme la priorité la plus élevée. Par défaut, la valeur est 100.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Description unique pour ce profil.



Que faire ensuite

Pour passer à la section Filtrage, cliquez sur **Continuer**.

Définir les filtres à appliquer à la création d'incident

Définissez et définissez des conditions de filtre pour analyser les incidents DLP entrants Symantec . Déterminez les incidents qui doivent être créés en tant qu'incidents DLP dans ServiceNow®.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Le filtrage vous aide à isoler les incidents DLP et à limiter le nombre d'incidents DLP que vous créez. Si des critères de filtrage supplémentaires sont définis, seuls les incidents correspondant aux conditions sont créés.

Procédure

1. Cochez **la case Filtre basé sur une API pour l'ingestion d'incidents** afin d'appliquer les filtres d'API et de récupérer les incidents qui correspondent aux critères de filtre.
2. Ajoutez les filtres d'API.
   L'exemple suivant illustre les filtres d'API.

```
{
                "operandOne": {
                    "name": "incidentStatusName"
                },
                "filterType": "string",
                "operator": "EQ",
                "operandTwoValues": [
                    "incident.status.New"
                ]
            }
```

Remarque : Pour plus d'informations sur les filtres d'API sur l'intégration Symantec, consultez Listes d'incidents : paramètres - Détails de l'objet de la demande .

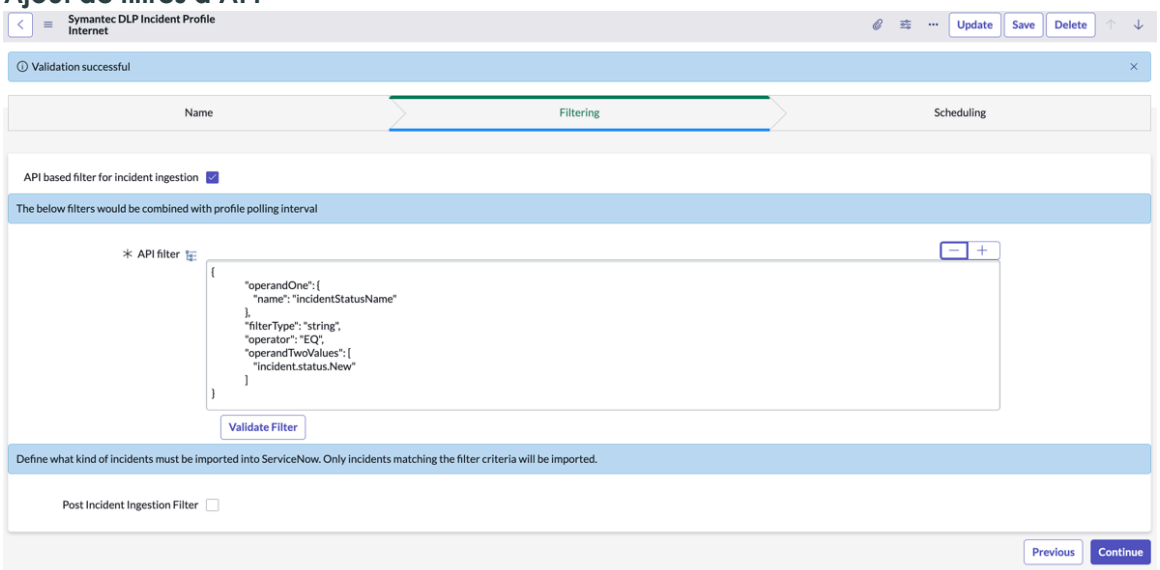
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

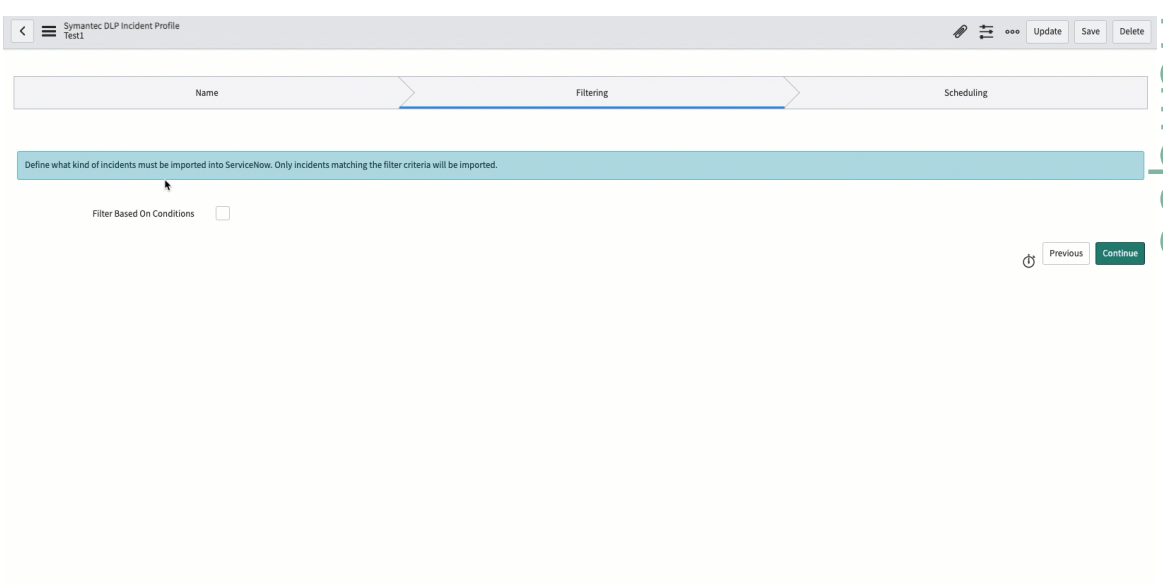
3. Cliquez sur **Valider le filtre** après avoir appliqué les filtres d'API.

> **Remarque :** Si la validation échoue, un message d'erreur s'affiche indiquant que la validation a échoué, et cela se produit lorsque les filtres ne sont pas correctement saisis selon les API Symantec.

Ajout de filtres d'API



4. Cochez la case **Filtre d'ingestion post-incident** pour définir les critères qu'un incident Symantec DLP entrant doit satisfaire pour qu'un incident DLP soit créé.
   Les options du premier champ des conditions de filtre correspondent aux champs disponibles dans l'incident DLP. Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'incident.
5. Dans le générateur de conditions, définissez les filtres dans le champ **Conditions de filtre** .



6. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Cliquez sur **Continuer** pour configurer le calendrier.

Configurer le stockage des fichiers de preuves

Configurez le stockage des fichiers de preuves pour stocker en toute sécurité le fichier de preuves des incidents DLP.

Avant de commencer
Rôle requis : sn_dlir.admin

Vérifiez que les options Corps, Pièces jointes et Message d'origine de l'utilisateur Symantec que vous configurez pour l'intégration Symantec DLP doivent être activées dans la page de configuration des rôles sur le portail Symantec DLP. Pour plus d'informations, consultez la section Attributs d'affichage disponible sur le document Configuration des rôles pour plus d'informations.



Pourquoi et quand exécuter cette tâche
Vous pouvez configurer le stockage des fichiers de preuves pour stocker des fichiers en toute sécurité. Cela fournit une option pour le stockage interne dans l'instance ServiceNow, garantissant que les fichiers sont stockés et chiffrés à l'aide du chiffrement au niveau des colonnes de ServiceNow. Pour plus d'informations, consultez Chiffrement au niveau des colonnes sur la documentation Now Platform.

Lorsqu'un analyste DLP effectue l'action Télécharger les fichiers de preuves pour les incidents DLP à partir de l'espace de travail de l'analyste, le fichier est téléchargé à partir du stockage sélectionné si l'option de stockage de fichier de preuves est activée. Dans le cas contraire, le fichier est téléchargé directement à partir de la source Symantec et n'est pas conservé dans l'instance ServiceNow. Pour plus d'informations, consultez Télécharger les fichiers de preuves.

Remarque : Pour prendre en charge la source d'intégration de l'environnement local, mid_server rôle contiendra le rôle sn_dlir.secure_file_download pour prendre en charge le stockage des fichiers de preuves dans le stockage interne à l'aide du MID Server.

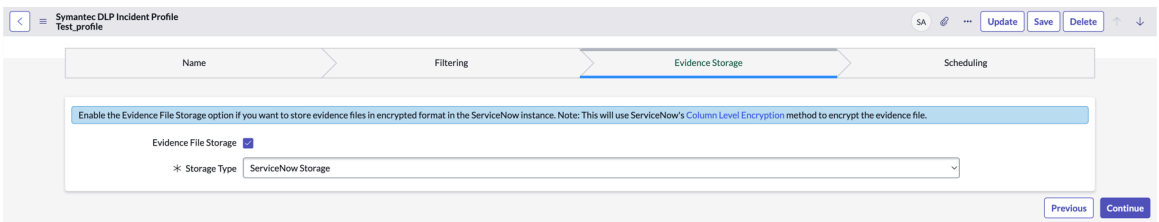
Procédure
1. Accédez à la **Tout** > **Intégration DLP Symantec** > **Profil d'incident**.
2. Cliquez sur la section **Stockage des preuves** sur le formulaire Profil d'incident.
3. Cochez la case **Stockage des fichiers de preuves** pour activer le stockage des fichiers.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez le type de stockage préféré.

Type	Description
Stockage des fichiers de preuves	Option permettant d'activer le stockage des fichiers de preuves.
Type de stockage	Option permettant de sélectionner le type de stockage préféré. **Remarque : Stockage ServiceNow** : stocke les fichiers de preuves dans l'instance ServiceNow dans un format chiffré.



5. Cliquez sur **Continuer** et accédez à la section **Planification** .

Résultats

Les fichiers de preuves sont stockés conformément à la configuration, une fois l'ingestion de l'incident terminée.

Planifier la récupération de l'incident Symantec DLP

Définissez un calendrier pour récupérer les données d'incident et ingérer les Symantec incidents DLP qui correspondent aux critères du profil. Configurez le calendrier pour définir comment et quand vous extrayez les incidents à partir de Symantec.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier la fréquence à laquelle vous procéderez à une interrogation pour les incidents futurs qui correspondent à la configuration du profil d'incident. Pour activer l'ingestion automatisée d'incidents, vous devez configurer la planification et la récupération des incidents avant d'activer le profil. Le profil peut être configuré pour effectuer une récupération ponctuelle à l'aide de la case à cocher **Récupération ponctuelle** . La date historique peut être comprise jusqu'aux trois derniers mois à compter de la date actuelle.

L'intervalle d'interrogation est configuré individuellement pour chaque profil. Les différents intervalles d'interrogation peuvent avoir un impact sur les performances de l'intégration Symantec des incidents DLP. Lors de la planification, prévoyez d'équilibrer la charge du système par rapport à l'urgence d'un incident.

Procédure

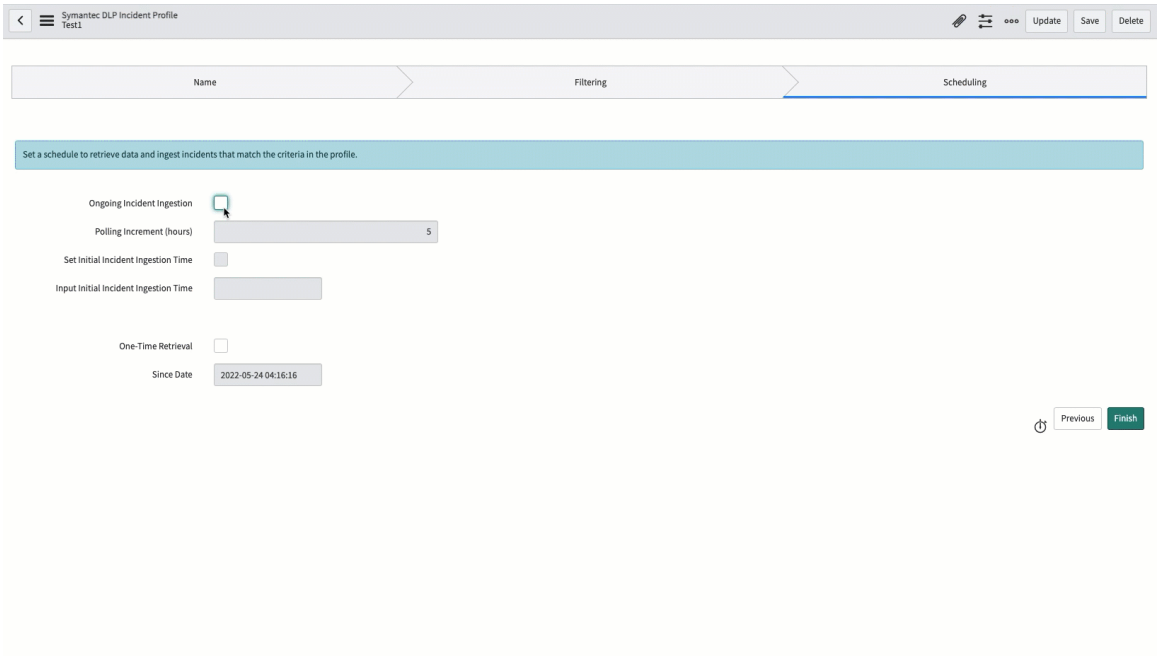
1. Définissez un calendrier pour récupérer les données et ingérer les incidents qui correspondent aux critères du profil.
2. Renseignez les champs du formulaire.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calendrier de l'incident DLP

Champ	Description
Intégration de l'incident en cours	L'ingestion d'incident en cours que l'instance Now Platform extrait de Symantec pour les nouveaux incidents. Les incidents DLP sont créés si des incidents déclenchés sont détectés et que les critères de filtrage de génération d'incident correspondent.
Incrémentation du sondage (minutes)	Fréquence d'interrogation définie en minutes. Ce champ est automatiquement défini sur 300 minutes.
Définir le délai d'intégration de l'incident initial	Option permettant de définir une date et une heure pour l'ingestion initiale. Les ingestions suivantes sont basées sur la période de l'intervalle d'interrogation.
Délai d'intégration de l'incident initial d'entrée	Date et heure que vous spécifiez pour l'ingestion de l'incident.
Délai d'intégration de l'incident initial	Première fois que les données sont ingérées. Vous pouvez voir que les valeurs commencent à s'afficher lorsque le délai d'ingestion initial de l'incident est défini.
Délai d'intégration de l'incident suivant (estimé)	Période suivante pour une ingestion d'incident estimée.
Récupération ponctuelle	Option permettant d'activer l'extraction unique des données historiques. Si ce champ est sélectionné, les données historiques sont extraites de Symantec DLP en fonction de la date ajoutée dans le champ **Depuis date** .
Date de début	Date à partir de laquelle les données sont censées être extraites de Symantec. Ce champ peut être défini sur un maximum de trois mois.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour enregistrer la configuration du profil créée, cliquez sur **Terminer** dans la fenêtre contextuelle.
4. Pour activer le profil, ouvrez le profil créé.
5. Activez **l'option Actif** .
6. Cliquez sur **Mettre à jour**.

Résultats
Une fois le profil créé et activé, les incidents sont récupérés périodiquement selon la configuration définie dans le profil et ajoutés à la table Incidents DLP.

Mappage Symantec des états des incidents DLP à ServiceNow l'état des incidents

Synchroniser l'état des incidents DLP ingérés le ServiceNow avec les incidents DLP du Symantec. Mappez le champ **Statut des incidents ServiceNow** avec le champ **Statut des incidents Symantec** .

Avant de commencer
Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche
L'état de l'incident est récupéré dynamiquement à partir de la source de point Symantec de terminaison qui est ajoutée dans le mappage. Vous devez effectuer un mappage de l'état des incidents un à un.

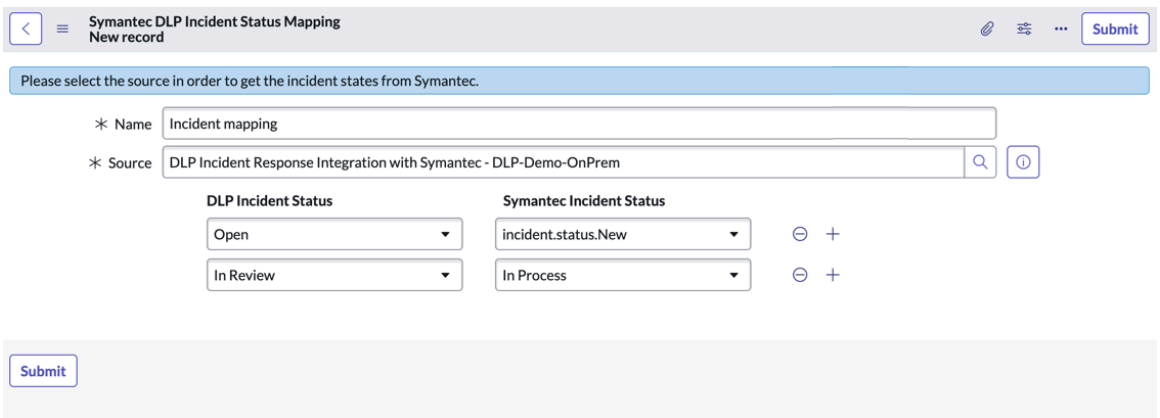
Procédure
1. Accédez à la **Intégration DLP Symantec** > **Mappage de l'état des incidents**.
2. Fournissez un **nom** pour identifier le mappage.
3. Sélectionnez l'intégration **source** à partir de laquelle vous souhaitez récupérer l'état.
4. Mappez **l'état des incidents DLP** avec **l'état des incidents Symantec**.

> **Remarque :** Il n'est pas nécessaire de mapper tous les états, vous pouvez mapper uniquement les états requis.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de l'état des incidents Symantec DLP

Champ	Description
Nom	Nom de l'enregistrement de mappage.
Source	Source de point de terminaison Symantec configurée à partir de laquelle vous souhaitez récupérer l'état de l'incident.
État des incidents DLP	Liste de l'état des incidents DLP.
État des incidents Symantec	Liste des états récupérés à partir de la source (point de terminaison Symantec).



5. Cliquez sur **Envoyer**.

Résultats
Une fois l'enregistrement créé pour le mappage des états des incidents, l'état ServiceNow des ServiceNow incidents est synchronisé avec Symantec l'état des incidents DLP.

Si vous modifiez l'état d'un incident DLP sur votre ServiceNow instance, l'état des incidents DLP associés Symantec sera modifié sur la plateforme source Symantec en fonction du mappage défini dans l'enregistrement.

Mappage de gravité entre les incidents Symantec DLP et les incidents ServiceNow

Utilisez la fonctionnalité de mappage de gravité pour configurer et synchroniser le mappage entre Symantec les incidents et Now Platform® les incidents.

Avant de commencer
Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche
Le mappage de gravité DLP vous permet de mapper la gravité de la source avec la gravité de l'incident DLP. Vous pouvez personnaliser et définir la valeur de gravité de la source et la mapper à la valeur de gravité de l'incident DLP souhaitée.

Procédure

1. Accédez à la **Intégration DLP Symantec** > **Mappage de sévérité d'incident**.

2. Cliquez sur **Nouveau**.

3. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

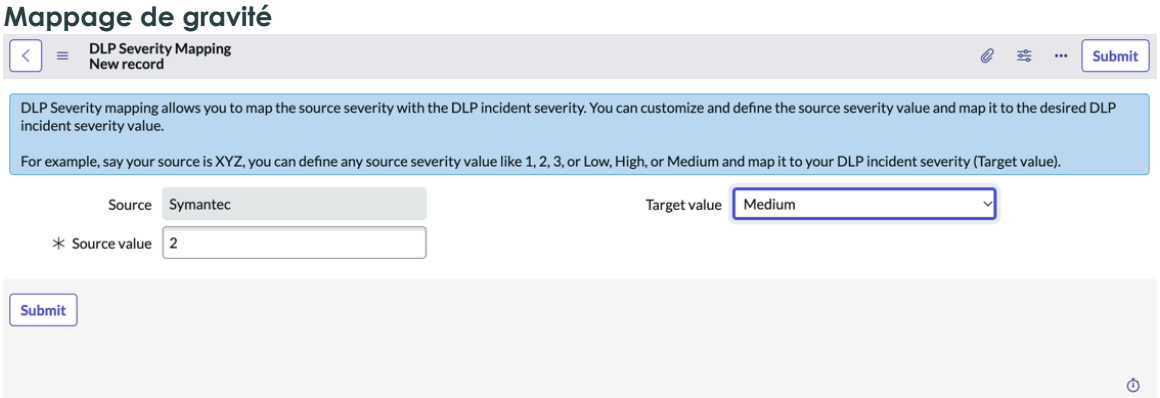
Mappage de gravité DLP

Champ	Description
Source	Source de point de terminaison Symantec configurée à partir de laquelle vous souhaitez récupérer l'incident.
Valeur cible	La valeur cible est l'ID de gravité de l'incident DLP. Les valeurs disponibles sont Critique, Élevée, Moyenne, Faible et Info (utilisée comme gravité de l'information dans Symantec).
Valeur source	La valeur source correspond à la gravité de l'incident Symantec.

Remarque : Dans le système de base, quatre mappages de gravité sont envoyés aux utilisateurs de DLP.

4. Cliquez sur **Envoyer**.

Mappage de gravité



Configurer des règles de réponses intelligentes

Configurez la ou les règles de réponse intelligente Symantec pour effectuer des actions de réponse sur les incidents DLP Symantec ingérés.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Vérifiez que l'utilisateur Symantec que vous configurez pour l'intégration Symantec DLP de ServiceNow doit avoir ces règles de réponse intelligente sélectionnées sur la page **de configuration des rôles** . Pour plus d'informations, consultez la section **Actions** disponible dans le document Configuration des rôles .

Pour la ou les règles de réponse intelligente extraites, l'administrateur DLP peut créer les règles d'option de réponse aux incidents et les mappages d'options de réponse pour configurer les actions de réponse à effectuer sur les incidents DLP Symantec ingérés.

Procédure

1. Accédez à la **Tout** > **Intégration DLP Symantec** > **Règles de réponses intelligentes**. Vous verrez toutes les options de réponse intelligente disponibles pour chaque configuration d'intégration configurée. Pour plus d'informations, Installer et configurer

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'intégration DLP pour la protection contre la Symantec perte de données consultez et suivez la procédure expliquée sur la configuration de l'intégration Symantec : source de configuration si elle n'a pas été configurée.

2. Cliquez sur l'une des règles de réponse intelligente pour ouvrir sa vue de formulaire.

   Suivez Créer des règles d'option de réponse aux incidents cette étape pour créer des règles d'option de réponse aux incidents et des mappages d'options de réponse pour afficher cette règle de réponse intelligente sur le modal de réponse de l'espace de travail DLP.

3. Créez les règles d'approbation pour la règle de réponse intelligente à l'aide de l'onglet **Règles d'approbation** de la liste connexe ou en suivant la procédure expliquée dans la section Configurer les règles d'approbation.
   Les règles d'approbation pour chaque règle de réponse intelligente seront visibles dans la liste connexe des règles d'approbation.
4. Après avoir créé la ou les règles de l'option de réponse aux incidents, vous pouvez voir l'enregistrement dans la liste connexe de l'enregistrement de règle de réponse intelligente.
5. Utilisez le bouton **Actualiser la règle de réponse intelligente** dans la vue de liste pour mettre à jour manuellement la source.
   Les règles de réponse intelligentes ajouteront, mettront à jour ou supprimeront automatiquement chaque jour pour chaque source.

Exécuter les règles de réponses intelligentes

Utilisez cette fonctionnalité pour exécuter des règles de réponse intelligentes pour les incidents DLP Symantec.

Avant de commencer

Vous devez configurer les règles de réponse intelligente en suivant la procédure expliquée ici dans cette section, Configurer des règles de réponses intelligentes.

Rôle requis : sn_dlir.admin

Remarque :

Les options de réponse sur l'espace de travail sont disponibles pour l'utilisateur final, l'analyste ou le gestionnaire en fonction de la configuration mentionnée dans la section Configurer l'option de réponse pour vos incidents DLP.

Procédure

1. Accédez à la **Tout** > **DLP** > **Espace de travail de l'utilisateur DLP**.
2. Ouvrez n'importe quel incident Symantec DLP.
3. Cliquez sur **Répondre**.
4. Sélectionnez l'option de réponse dans la liste déroulante Réponse.
   Les options de réponse seront visibles en fonction de la configuration de la **règle d'option de réponse aux incidents** et des **mappages d'options de réponse**.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Envoyer**.

> **Remarque :** Vous pouvez également configurer la ou les règles d'approbation pour les options de réponse en suivant la procédure expliquée dans la Créer des règles d'approbation section. Lorsqu'une règle d'approbation est configurée pour la règle de réponse intelligente, le flux d'approbation est déclenché en premier et après avoir reçu toutes les approbations, le flux d'option de réponse intelligente est déclenché. L'état de l'incident DLP sera mis à jour en fonction de l'état cible du mappage de l'option de réponse après l'exécution réussie de l'option de réponse.

Télécharger les fichiers de preuves

Téléchargez les fichiers de preuves d'incidents DLP qui enfreignent la politique DLP sur Symantec.

Avant de commencer

Téléchargez ce fichier sur votre ordinateur local à partir de l'espace de travail de l'analyste DLP IR et de l'espace de travail de l'utilisateur final DLP IR. L'action Télécharger les fichiers n'est disponible que pour les approbateurs dans l'espace de travail de l'utilisateur final DLP IR.

Rôle requis :

- sn_dlir.analyste
- sn_dlir.secure_file_download (n'importe quel approbateur disposant de ce rôle)

Procédure

1. Accédez à la **Tout** > **Intégration DLP Symantec** > **Paramètre**.
2. Activer **Le téléchargement du fichier en infraction de l'incident signalé doit-il être autorisé** ?
   Une fois que vous avez activé cette propriété, vous pouvez maintenant voir l'action **Télécharger le fichier** sur DLP Analyst Workspace pour n'importe quel incident DLP Symantec.
3. Accédez à la **Tout** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
4. Ouvrez un enregistrement d'incident DLP ingéré à partir d'une source Symantec.
5. Cliquez sur **Télécharger le fichier**.

> **Remarque :** Le fichier qui a enfreint la stratégie DLP de Symantec sera téléchargé sur l'ordinateur local de l'utilisateur.

   Pour que l'approbateur affiche l'action Télécharger le fichier, suivez les étapes mentionnées ci-dessous :

6. Accédez à la **Tout** > **Gestion des incidents DLP** > **Espace de travail de l'utilisateur DLP**.
   La page Mes incidents DLP s'affiche dans un nouvel onglet.
7. Sélectionnez **le module Mes approbations** disponible sous le module Mes incidents DLP.
   La vue de liste Mes approbations s'affiche.
8. Ouvrez un enregistrement de demande d'approbation qui est déclenché pour l'incident DLP Symantec.
9. Cliquez sur l'icône d'informations (i) disponible dans le champ Incident DLP de la vue de formulaire.
10. Cliquez sur **Télécharger le fichier**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Une fois cette action effectuée, le fichier de preuves au format ZIP (si l'incident comporte des violations dans plusieurs composants et/ou si les données du message d'origine sont également disponibles) ou un seul fichier (si l'incident comporte des violations dans un seul composant ou si seules les données du message d'origine sont disponibles) est téléchargé sur l'ordinateur local de l'utilisateur.

Remarque : En tant qu'administrateur DLP, vous pouvez contrôler l'accès à l'action Télécharger le **fichier** en désactivant l'option **Si le téléchargement du fichier en infraction de l'incident signalé est autorisé** à partir de la page **Paramètres avancés** . Pour plus d'informations, consultez Configurer les paramètres avancés pour Data Loss Prevention Incident Response .

Configurer les paramètres d'intégration Symantec DLP

Modifiez les propriétés système par défaut de l'intégration Symantec DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Accédez à la **Intégration DLP Symantec** > **Paramètres**.
2. Modifiez les paramètres suivants selon vos besoins.

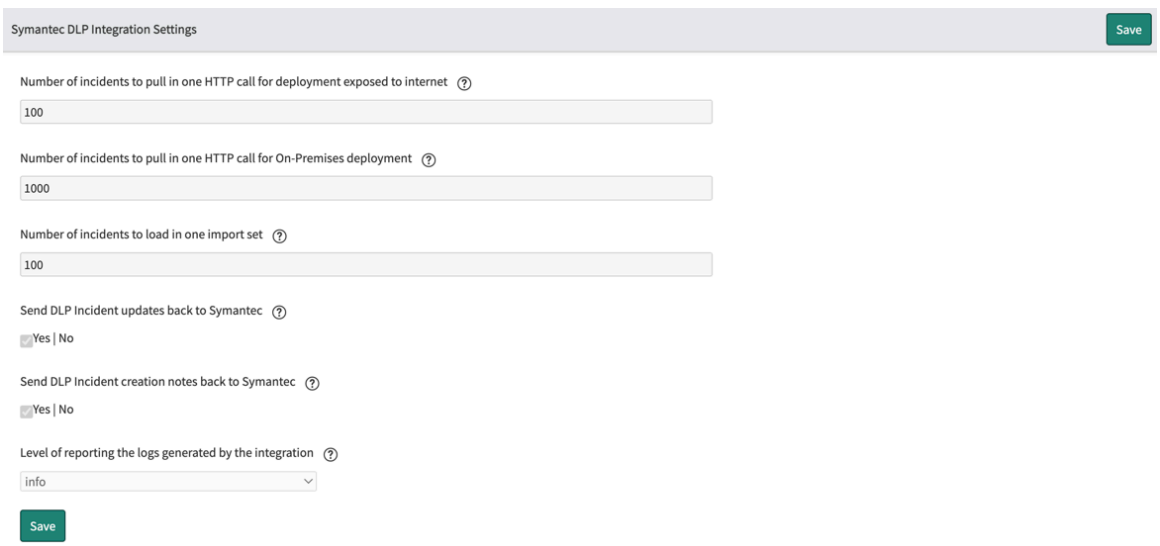
Paramètres

Champ	Description
Appliquer une limite au nombre d'incidents à extraire dans un appel HTTP pour un déploiement sur site sn_sym_dlp.page_size_on_prem	Nombre maximal d'incidents à extraire dans un appel HTTP pour un déploiement sur site de Symantec. ◦ Type : nombre entier ◦ Valeur par défaut : 1 000
Appliquer une limite au nombre d'incidents à extraire dans un appel HTTP pour un déploiement exposé à Internet sn_sym_dlp.page_size_on_internet	Nombre maximal d'incidents à extraire dans un appel HTTP pour Symantec un déploiement exposé à Internet. ◦ Type : nombre entier ◦ Valeur par défaut : 100
Nombre d'incidents à charger dans un jeu d'importation sn_sym_dlp.incidents_per_attachment	Nombre d'enregistrements à stocker dans un fichier joint pour le traitement. ◦ Type : nombre entier ◦ Valeur par défaut : 100
Renvoyer les mises à jour des incidents DLP à Symantec sn_sym_dlp.incident_update	Cette propriété vous permet de restreindre toute synchronisation d'état entre ServiceNow les Symantec incidents DLP. ◦ Type : booléen ◦ Valeur par défaut : **vrai**
Envoyer des notes de création d'incidents DLP à Symantec sn_sym_dlp.incident_creation_notes	Cette propriété vous permet de renvoyer une note à Symantec dès qu'un incident est créé dans ServiceNow.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Type : booléen ◦ Valeur par défaut : **vrai**
Niveau de génération de rapports des journaux générés par l'intégration sn_sym_dlp.logging.verbosity	Propriété qui définit la génération de rapports des journaux générés par l'intégration.



3. Cliquez sur **Enregistrer**.

Séparation de domaine dans l'intégration Symantec DLP

Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Support : basique.

Fonctionnement de Séparation de domaine avec Symantec l'intégration DLP

Procédez comme suit pour réaliser Séparation de domaine :

- Créez un utilisateur avec le rôle requis dans le domaine respectif.
- Exécutez les procédures d'intégration DLP Symantec dans le domaine approprié.

Intégration de Data Loss Prevention Incident Response à Proofpoint

L'intégration Proofpoint DLP prend en charge l'ingestion des incidents de protection contre la perte de données créés sur le déploiement de prévention de la Proofpoint perte de données. Après l'ingestion, vous pouvez utiliser les fonctionnalités de gestion des incidents pour corriger les incidents DLP.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Vue d'ensemble et fonctionnalités principales

L'intégration Proofpoint DLP aide les entreprises à suivre l'utilisation et le déplacement des données sensibles sur diverses plateformes.

Cette intégration comprend les fonctionnalités clés suivantes :

- Création de plusieurs profils pour différents Proofpoint points de terminaison.
- Automatisation de la création d'incidents DLP.
- Mappage du champ État de l'incident DLP au champ État de l'incident Proofpoint DLP.
- Filtrage des incidents DLP Proofpoint .
- Ingestion d'incidents dans votre ServiceNow instance dès leur création sur Proofpoint le locataire DLP.
- Proofpoint L'intégration DLP prend en charge à la fois les points de terminaison et le type d'e-mail des incidents.
- Mises à jour automatiques du statut de l'incident DLP et des commentaires pour la Proofpoint création d'incidents DLP, ainsi que pour le changement d'état et la fermeture du ServiceNow côté.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
Proofpoint site web de la documentation produit	Documentation produit Proofpoint
ServiceNow® site web de la documentation produit	Site web de la documentation produit ServiceNow

Mise en route de l'intégration Proofpoint pour la protection contre la perte de données

L'intégration Proofpoint DLP prend en charge l'ingestion des incidents de prévention de la perte de données créés sur le locataire de prévention de la Proofpoint perte de données. Après l'ingestion, les fonctionnalités de gestion des incidents qui corrigent les incidents DLP seront utilisées.

Liste de vérification

Passez en revue les informations suivantes avant de commencer à configurer votre Proofpoint intégration DLP pour la protection contre la perte de données.

Liste de vérification

Champ	Description
Vérifiez que vous avez affecté les rôles requis Now Platform et Data Loss Prevention Incident Response d'application.	Les rôles suivants sont utilisés dans l'intégration Proofpoint DLP de :Now Platform

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Champ	Description
	• L'administrateur (admin) installe les applications à partir de et ServiceNow® Store affecte l'administrateur de la prévention des pertes de données (sn_dlir.admin). • L'utilisateur disposant du rôle sn_dlir.admin peut configurer l'intégration et configurer les profils d'incident. • Les utilisateurs disposant du rôle sn_dlir.analyst ont des rôles de lecture dans l'intégralité.
Affectez les rôles d'utilisateur DLP requis Proofpoint .	Passez en revue les autorisations et les rôles d'intégration Proofpoint DLP.
Vérifiez que vous utilisez Proofpoint DLP 1.0.1 ou une version ultérieure.	L'intégration Proofpoint DLP pour la protection contre la perte de données est testée avec Proofpoint la prévention de la perte de données, version 1.0.1 ou ultérieure.
Vérifiez que l'application principale de l'utilisateur final requise pour prendre en charge l'intégration Proofpoint DLP est installée et activée.	Vérifiez que les applications DLP et les applications courantes de prise en charge de la sécurité suivantes sont installées et activées à partir du ServiceNow magasin. Si l'application n'est pas installée, installez-la et activez-la. • Security Support Common • Data Loss Prevention Incident Response

Installer et configurer l'intégration pour la protection contre la Proofpoint perte de données

Installez et configurez l'intégration Proofpoint DLP à ServiceNow® Store partir de sur votre Now Platform instance. Commencez à examiner les incidents DLP à l'aide des données d'incident Proofpoint DLP.

Avant de commencer

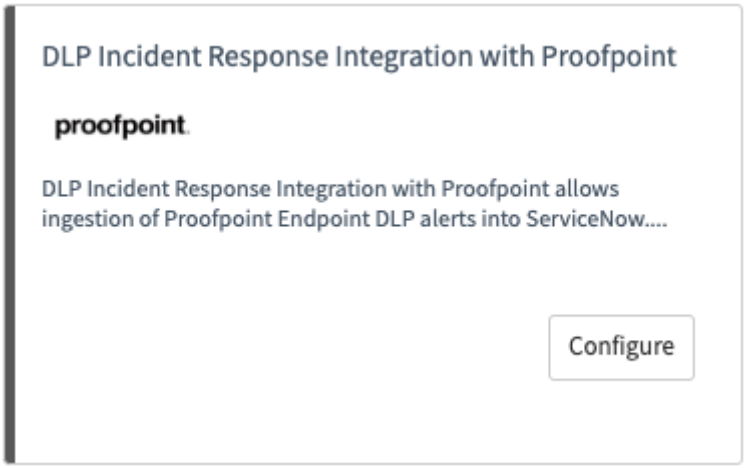
Rôle requis : sn_dlir.admin

Procédure

1. Téléchargez l'intégration Proofpoint DLP à partir de et ServiceNow® Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette `Intégration de la réponse aux incidents DLP avec Proofpoint` , puis cliquez sur **Configurer**.

Traduction automatique

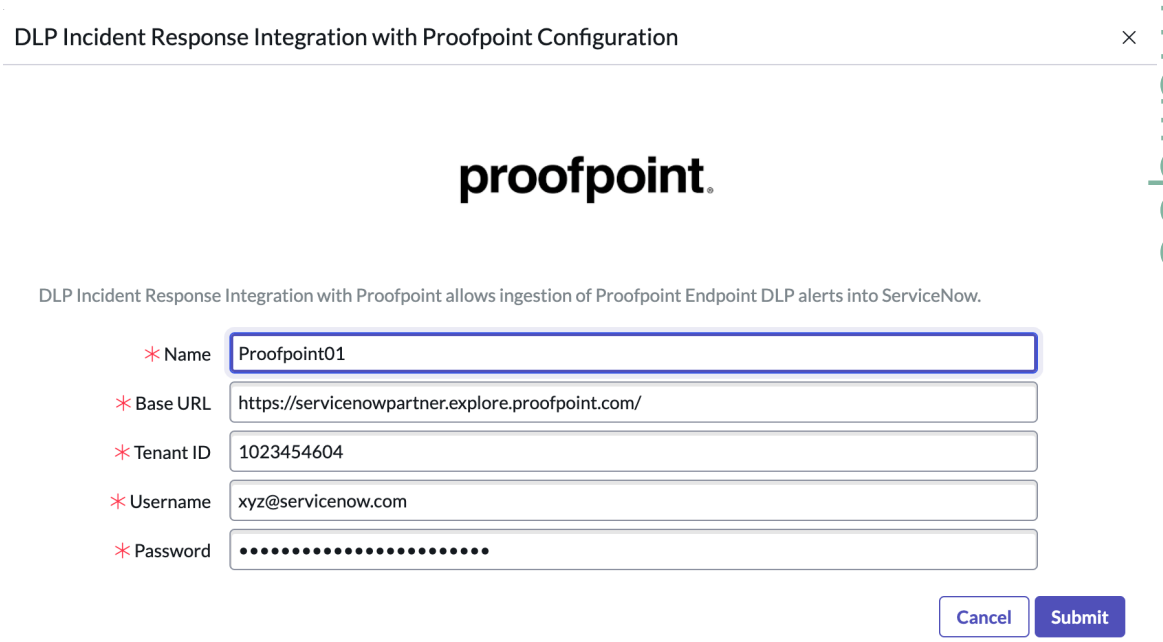
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Renseignez les champs du formulaire.

Proofpoint Formulaire Configuration de l'intégration DLP

Champ	Description
Nom	Nom de la configuration de l'intégration Proofpoint DLP.
URL de base	URL du Proofpoint point de terminaison REST.
ID de locataire	L'ID du Proofpoint locataire à utiliser.
Nom d'utilisateur	Nom d'utilisateur configuré pour votre compte utilisateur sur Proofpoint.
Mot de passe	Mot de passe configuré pour votre compte utilisateur sur Proofpoint.



5. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Une fois la configuration validée et envoyée, l'intégration Proofpoint DLP est enregistrée sous forme de vignette sur la page Intégrations de sécurité.

Configurez le Webhook sur le locataire DLP pour les Proofpoint notifications d'alerte ServiceNow

Configurez un webhook à Proofpoint l'aide du point de terminaison de l'API REST pour commencer à recevoir les alertes du Proofpoint locataire DLP. Votre ServiceNow instance crée des incidents DLP à partir de ces alertes. L'intégration Proofpoint DLP fournit un point de terminaison d'API REST permettant aux utilisateurs finaux de configurer le webhook.

Avant de commencer
Rôle requis : sn_pp_dlp.api_integration_user

Procédure

1. Connectez-vous à **Proofpoint**.
2. Accédez à la **Locataire ProofPoint** > **Application d'administration** > **Intégration** > **Politiques de notification**.
3. Créez une politique de notification avec un nom approprié.
4. Cliquez sur la **stratégie de notification** et gérez les webhooks configurés dans la stratégie de notification.
5. Créez une configuration de webhook en cliquant sur **Ajouter des webhooks**.
6. Sélectionnez le type de webhook **Générique**.
7. Dans Entrée URL, saisissez une URL au format suivant : `https://<Instance_Name>.service-now.com/api/sn_pp_dlp/proofpointalertapi/getalerts`.
8. Conservez la méthode en **mode POST.**
9. Ajoutez les en-têtes suivants au webhook :
   - ```
     Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow
      instance user>
     ```
   - ```
     Name: Content-Type
     Value: application/json
     ```
10. D ne change pas les autres valeurs.
11. Cliquez sur **Enregistrer**.
12. Accédez à la **Locataire ProofPoint** > **Application d'administration** > **Politiques** > **Règles**.
13. Dans la section Actions, sélectionnez les règles pour lesquelles la notification webhook doit être générée.
14. Ajoutez les politiques de notification nouvellement créées qui ont un webhook configuré.
15. Cliquez sur **Enregistrer**.

Créer un profil pour Proofpoint l'intégration DLP

Créez un profil d'incident dans votre Now Platform instance. Déterminez les incidents DLP Proofpoint qui conviennent à la création d'incidents DLP.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche
Configurez le Now Platform pour renseigner les alertes DLP de Proofpoint. Stockez les alertes en tant qu'incidents DLP dans votre ServiceNow instance.

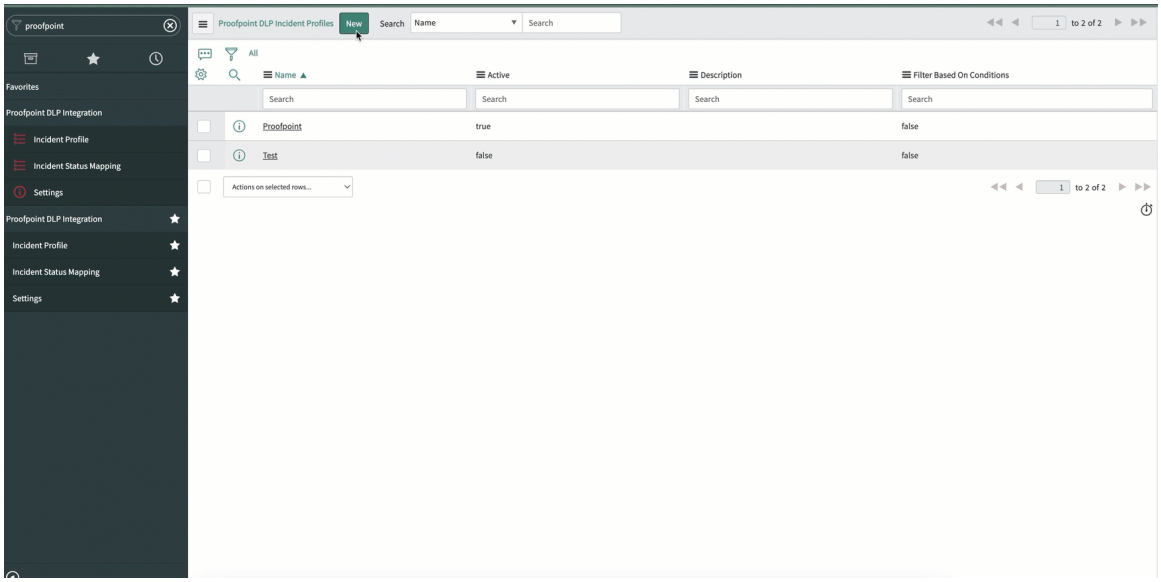
Procédure
1. Accédez à la **Intégration DLP ProofPoint** > **Profil d'incident**.
2. Cliquez sur **Nouveau**.
3. Sur le formulaire, renseignez les champs de la section **Nom** .

Créer un profil pour Proofpoint le formulaire d'intégration DLP

Champ	Description
Nom	Nom du profil. Ce nom vous aide à identifier le profil. **Remarque :** Le nom doit être unique pour chaque profil.
Source	Instance Proofpoint DLP que vous avez configurée pour ingérer des incidents. Si vous avez configuré plusieurs instances, sélectionnez l'instance appropriée pour les types d'incidents que vous prévoyez d'ingérer pour le profil.
Actif	Option permettant d'activer le profil. Lorsque le profil est actif, votre Now Platform instance est prête à recevoir les incidents de Proofpoint.
Description	Description permettant de distinguer ce profil des autres profils.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Continuer** et accédez à la section Filtrage.

Définir les filtres à appliquer à la création d'incident

Définissez et définissez des conditions de filtre pour filtrer les incidents DLP entrants Proofpoint . Contrôlez quels incidents DLP doivent être créés le ServiceNow®.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

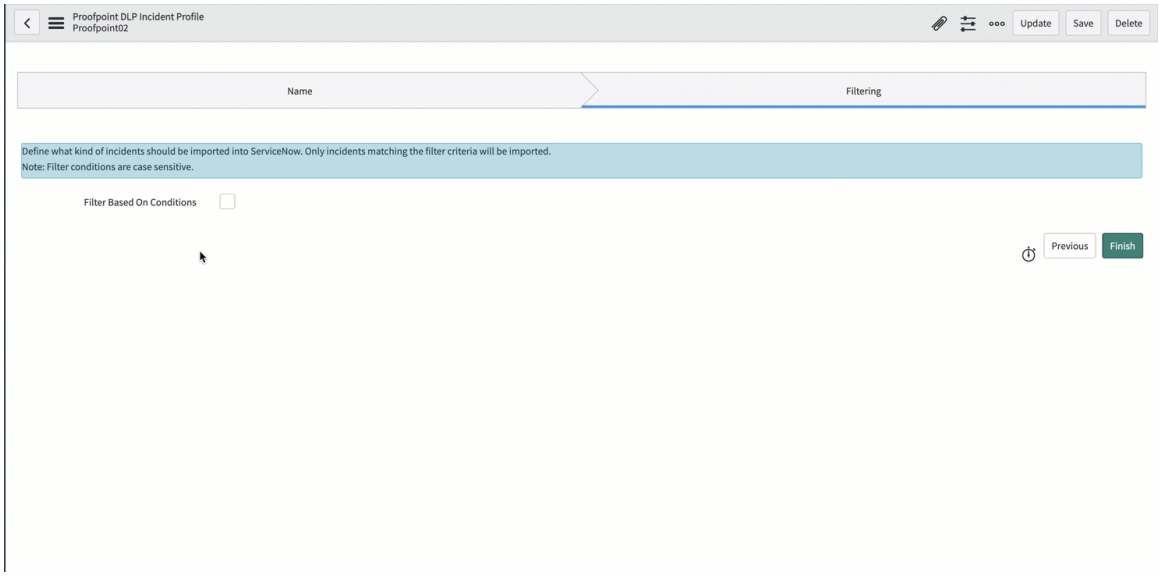
Ce type de filtrage vous aide à isoler les incidents DLP et à limiter le nombre d'incidents DLP que vous créez. Si des critères de filtrage supplémentaires sont définis, seuls les incidents correspondant aux conditions sont créés.

Procédure

1. Sélectionnez l'option **Filtre basé sur les conditions** et définissez les critères qu'un incident DLP entrant Proofpoint doit satisfaire pour qu'un incident de sécurité soit créé.
2. À l'aide des listes et des champs du générateur de conditions, définissez les filtres dans le champ **Conditions de filtre** .

   Les options du premier champ des conditions de **filtre** correspondent aux champs disponibles dans l'incident DLP. Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'incident.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Ajoutez d'autres conditions en cliquant sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. Cliquez sur **Terminer**.

Mapper l'état Proofpoint des incidents DLP à ServiceNow l'état des incidents

Synchronisez l'état des incidents DLP ingérés sur votre ServiceNow instance et les Proofpointincidents DLP du . Mappez l'état de l'incident à l'état de l'incident ServiceNowProofpoint .

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Accédez à la **Intégration DLP ProofPoint** > **Incident** > **Mappage de l'état des incidents**.
2. Fournissez un **nom** pour identifier le mappage.
3. Sélectionnez la vignette **Source** (configuration d'intégration) pour laquelle le mappage d'état doit être appliqué.
4. Mappez **l'état de l'incident DLP ServiceNow** avec **l'état de l'incident Proofpoint**.

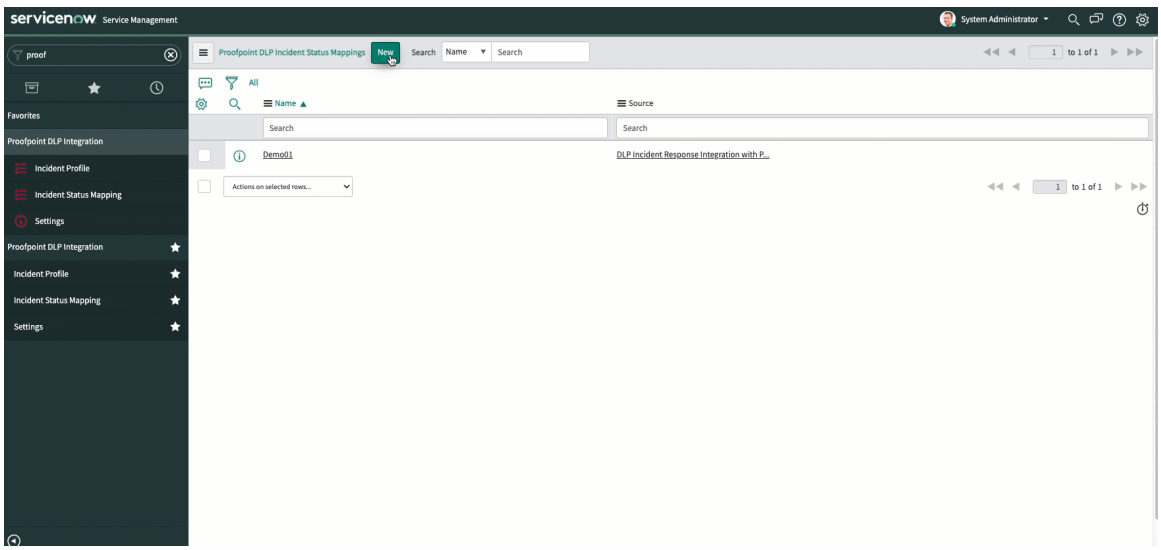
Mapper l'état des incidents DLP Proofpoint avec le formulaire d'état des incidents ServiceNow

Champ	Description
Nom	Espace réservé pour l'enregistrement de mappage.
Source	Source de point de terminaison configurée Proofpoint à partir de laquelle vous souhaitez récupérer l'état de l'incident.
État des incidents ServiceNow	Liste de l'état des incidents DLP.
État de l'incident ProofPoint	Valeurs mappées par défaut pour les états par défaut disponibles dans les incidents

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	DLP. Pour les états personnalisés, l'état par défaut Proofpoint est **Nouveau**. Vous pouvez modifier et ajouter l'état requis Proofpoint dans le champ d'entrée.



5. Cliquez sur **Envoyer**.

Résultats

Un enregistrement pour le mappage est créé avec succès. Les états des incidents sont synchronisés avec Proofpoint les ServiceNow incidents DLP.

Lorsque vous modifiez l'état d'un incident DLP sur votre ServiceNow instance, l'état de l'incident DLP associé Proofpoint est modifié sur la plateforme source Proofpoint selon le mappage défini dans l'enregistrement.

Configurer les Proofpoint paramètres d'intégration DLP

Modifiez les propriétés système par défaut de l'intégration Proofpoint DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Accédez à la **Intégration DLP ProofPoint** > **Paramètres**.

2. Modifiez les paramètres suivants selon vos besoins.

Champ	Description
Délai d'expiration maximal pour les appels HTTP sn_pp_dlp.maximum_http_time_out	Délai d'expiration maximal pour les appels HTTP (en secondes). ◦ Type : nombre entier ◦ Valeur par défaut : 30
Renvoyer les mises à jour des incidents DLP à Proofpoint sn_pp_dlp.incident_update	Cette propriété vous permet de restreindre toute synchronisation de votre ServiceNow instance aux Proofpoint incidents DLP.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Type : booléen ◦ Valeur par défaut : true
Niveau de génération de rapports des journaux générés par l'intégration sn_pp_-dlp.logging.verbosity	Niveau des journaux de reporting générés par l'intégration.

3. Cliquez sur **Enregistrer**.

Résultats
Vos paramètres d'intégration modifiés sont appliqués à l'intervalle d'interrogation suivant, tel que défini dans le profil.

Séparation de domaine dans l'intégration Proofpoint DLP

Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Support : basique.

Fonctionnement de Séparation de domaine avec Proofpoint l'intégration DLP

Procédez comme suit pour réaliser Séparation de domaine :

- Créez un utilisateur avec le rôle requis dans le domaine respectif.
- Exécutez les procédures d'intégration DLP Proofpoint dans le domaine approprié.

Intégration de Data Loss Prevention Incident Response à Netskope

L'intégration Netskope DLP prend en charge l'ingestion des incidents de protection contre la perte de données créés sur le déploiement de prévention de la Netskope perte de données. Netskope DLP aide les entreprises à suivre l'utilisation et le déplacement des données sensibles sur diverses plateformes.

Après l'ingestion, vous pouvez utiliser les fonctionnalités de gestion des incidents pour corriger les incidents DLP.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

- Création de plusieurs profils pour différents Netskope locataires.
- Automatisation de la création d'incidents DLP ServiceNow à partir d'incidents Netskope DLP.
- Filtrage des incidents DLP Netskope .
- Ingestion planifiée des incidents DLP qui créent des Netskope incidents DLP dans ServiceNow.
- Mettez automatiquement à jour l'état Netskope de l'objet lorsque l'état DLP change dans votre instance ServiceNow.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Affichez les détails médico-légaux (contenu contrevenant) de l'incident DLP sur l'espace de travail DLP IR Analyst et l'espace de travail de l'utilisateur final DLP.

  Remarque : Le contenu en infraction ne persiste pas dans ServiceNow. Le contenu est extrait lorsque l'incident est ouvert dans l'espace de travail.

- Téléchargement du fichier de preuves directement à partir de Netskope la demande.

  Remarque : Le fichier de preuves n'est pas conservé dans ServiceNow. Le fichier de preuves est extrait lorsque l'analyste clique sur Télécharger le **fichier** dans l'espace de travail.

- Notification par e-mail aux utilisateurs administrateurs DLP à Netskope l'expiration du jeton.
- Une notification par e-mail est envoyée aux utilisateurs administrateurs DLP si elle dépasse la limite de nouvelles tentatives définie pour les échecs d'appel d'API d'incident.
- Netskope Prend également en charge le processus d'exécution de l'intégration. Pour plus d'informations, consultez Surveiller le processus d'exécution de l'intégration DLP.

Premiers pas avec l'intégration Netskope DLP pour la protection contre la perte de données

Passez en revue les informations suivantes avant de commencer à configurer votre Netskope intégration DLP pour la protection contre la perte de données.

Tâche de configuration	Description
Vérifiez que vous avez affecté l'application Now Platform de prévention des pertes de données requise.	Les rôles suivants sont utilisés dans l'intégration Netskope DLP de :Now Platform • L'administrateur (admin) installe les applications à partir de et ServiceNow Store affecte l'administrateur de la prévention des pertes de données (sn_dlir.admin). • L'utilisateur disposant du rôle sn_dlir.admin peut configurer l'intégration et configurer les profils d'incident. • Les utilisateurs disposant du rôle sn_dlir.analyst auront des rôles de lecture dans l'ensemble de l'intégration.
Affectez les privilèges requis pour Netskope le jeton d'API v2.	Les privilèges de point de terminaison suivants sont utilisés dans la tokenisation de l'API Netskope v2. • Lecture : /api/v2/incidents/dlpincidents • Lire : /api/v2/events/dataexport/events/incident • Lecture + écriture : /api/v2/incidents/update
Vérifiez que l'application principale de l'utilisateur final requise pour prendre en	Vérifiez que les applications DLP et les applications courantes de prise en charge de la sécurité suivantes sont installées et

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
charge l'intégration Netskope DLP est installée et activée.	activées à partir du ServiceNow magasin. Si l'application n'est pas installée, installez-la et activez-la. • Security Support Common • Data Loss Prevention Incident Response

Installer et configurer l'intégration DLP pour la protection contre la Netskope perte de données

Installez et configurez l'intégration DLP à partir de l'instance NetskopeServiceNow Store #Now Platform . Vous pouvez commencer à enquêter sur les incidents DLP à l'aide des données d'incident Netskope DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

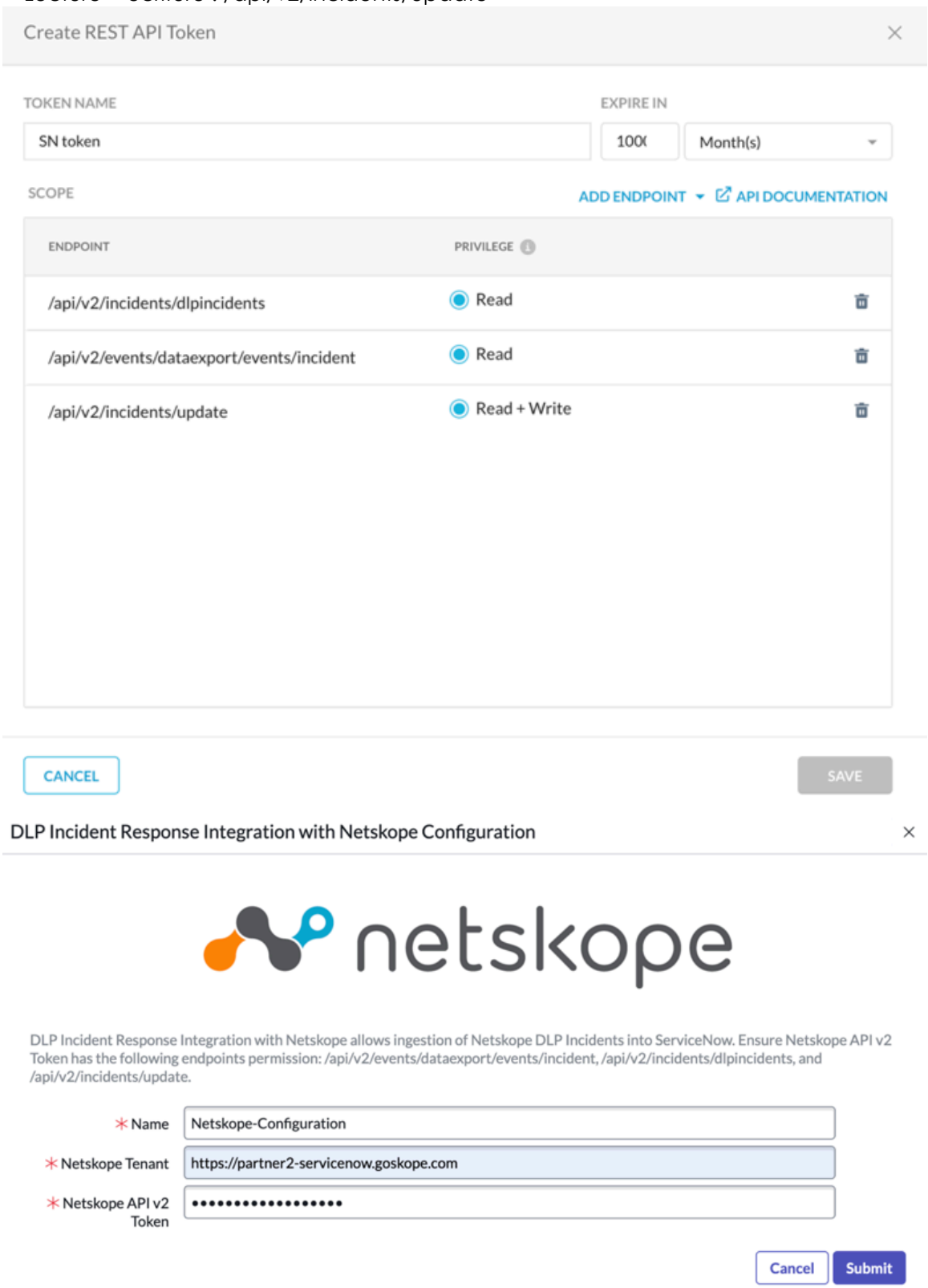
1. Téléchargez l'intégration Netskope DLP à partir de et ServiceNow Store installez-la.
2. Accédez à **Opérations de sécurité** > **Intégrations** > **Configurations d'intégration**
3. Recherchez `la vignette Intégration de la réponse aux incidents DLP avec Netskope` , puis cliquez sur **Configurer**.
4. Renseignez les champs du formulaire.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Assurez-vous que votre Netskope jeton d'API v2 dispose des privilèges de point de terminaison ci-dessous :

- Lecture : /api/v2/incidents/dlpincidents
- Lire : /api/v2/events/dataexport/events/incident
- Lecture + écriture : /api/v2/incidents/update



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom de la configuration de l'intégration Netskope DLP.
Locataire Netskope	L'URL Netskope de base pour le Netskope locataire.
Jeton de l'API Netskope v2	Jeton configuré pour l'API REST v2 sur votre compte utilisateur à l'adresse Netskope.

5. Cliquez sur **Envoyer**.

Résultats
Une fois la configuration validée et envoyée, l'intégration Netskope DLP est enregistrée sous forme de vignette sur la page Intégrations de sécurité.

Créer un profil pour Netskope l'intégration DLP

Créez un profil d'incident dans votre Now Platform instance.

Avant de commencer
Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche
Configurez Now Platform pour récupérer les incidents DLP à partir Netskope du point de terminaison. Stockez les incidents dans votre ServiceNow instance en tant qu'incidents DLP.

Procédure
1. Accédez à la **Intégration DLP Netskope** > **Profil d'incident**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Créer un profil

Champ	Description
Nom	Nom du profil. Le nom doit être unique pour chaque profil. Ce nom vous aide à identifier le profil.
Source	Netskope Instance DLP que vous avez configurée pour ingérer des incidents. Si vous avez configuré plusieurs instances, sélectionnez l'instance appropriée pour les types d'incidents que vous prévoyez d'ingérer pour le profil. **Remarque :** Un seul profil actif est autorisé par source.
Actif	Indicateur indiquant que le profil est actif.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Ce champ n'est disponible qu'une fois que vous avez cliqué sur **Terminer** dans la dernière section Planification. Lorsque le profil est actif, votre Now Platform instance interroge Netskope activement les incidents DLP. Les incidents DLP correspondants sont créés en tant qu'incidents DLP ServiceNow lorsque les conditions de filtrage sont mises en correspondance en fonction des paramètres de planification que vous avez fournis.
Ordre	Ordre d'exécution du profil. Le profil dont l'ordre est le plus bas est considéré comme la priorité la plus élevée. Par défaut, la valeur est 100.
Description	Description destinée à vous aider à distinguer ce profil des autres profils.

4. Cliquez sur **Continuer** et accédez à la section Filtrage.

Définir les filtres à appliquer à la création d'incident

Définissez et définissez des conditions de filtre pour filtrer les incidents DLP entrants Netskope . Contrôlez lesquels de ces incidents doivent être créés en tant qu'incidents DLP sur votre ServiceNow instance.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Ce type de filtrage vous aide à isoler les incidents DLP et à limiter le nombre d'incidents DLP que vous créez. Si des critères de filtrage supplémentaires sont définis, seuls les incidents correspondant aux conditions sont créés.

Procédure

1. Sélectionnez l'option **Filtre basé sur les conditions** et définissez les critères qu'un incident DLP Netskope entrant doit satisfaire pour qu'un incident DLP soit créé.
2. À l'aide des listes et des champs du générateur de conditions, définissez les filtres dans le champ **Conditions de filtre** .

   Les options du premier champ des conditions de **filtre** correspondent aux champs disponibles dans la table d'importation **d'incidents DLP Netskope** . Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'incident.

3. Ajoutez d'autres conditions en cliquant sur **ET** ou **OU**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
- Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

4. Cliquez sur **Continuer** et accédez à la section Planification.

Planifier la récupération des Netskope incidents DLP

Définissez un calendrier pour récupérer Netskope les incidents DLP qui correspondent aux critères du profil.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier la fréquence à laquelle vous interrogerez les nouveaux Netskope incidents nets qui correspondent à la configuration du profil d'incident. Pour activer l'ingestion automatisée d'incidents, vous devez configurer la planification et la récupération des incidents avant d'activer le profil. Le profil peut être configuré pour effectuer une récupération ponctuelle à l'aide de la case à cocher **Récupération ponctuelle** . La date historique peut être antérieure d'un mois.

Procédure

1. Configurez le calendrier pour définir comment et quand vous extrayez les incidents à partir de Netskope.
2. Renseignez les champs du formulaire.

Planifier les Netskope incidents DLP

Champ	Description
Intégration de l'incident en cours	Ingestion d'incident en cours que votre Now Platform instance extrait Netskope pour les nouveaux incidents. Si des incidents déclenchés correspondant aux critères de filtrage des incidents sont détectés, des incidents DLP sont créés.
Incrémentation du sondage (minutes)	Fréquence d'interrogation définie en minutes. Cette valeur par défaut est définie sur **5**.
Définir le délai d'intégration de l'incident initial	Option permettant de définir l'ingestion d'incident initiale en fonction de la date et de l'heure configurées. Vous pouvez utiliser cette option pour définir une date et une heure spécifiques pour l'ingestion initiale. Les ingestions suivantes sont basées sur la période de l'intervalle d'interrogation.
Délai d'intégration de l'incident initial d'entrée	Date et heure que vous spécifiez pour l'ingestion de l'incident.
Délai d'intégration de l'incident initial	La première fois que des données sont ingérées.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : La valeur n'est visible que si l'option **Définir le délai d'intégration de l'incident initial** est sélectionnée.
Délai d'intégration de l'incident suivant (estimé)	Délai d'intégration estimé de l'incident suivant.
Récupération ponctuelle	Option permettant d'activer l'extraction unique des données historiques. **Remarque :** Si cette option est sélectionnée, les données historiques sont extraites de DLP en fonction de Netskope la date ajoutée dans Depuis la **date**.
Date de début	Date à partir de laquelle les données sont extraites à partir de Netskope. **Remarque :** Au maximum, les données des 30 derniers jours peuvent être extraites à partir de .Netskope

3. Cliquez sur **Terminer**.
4. Dans la fenêtre contextuelle, enregistrez la configuration du profil créée en cliquant sur **Terminer**.
5. Activez le profil.
   a. Ouvrez le profil créé.
   b. Définissez **Actif** sur **vrai**.
   c. Cliquez sur **Mettre à jour**.

Résultats
Une fois l'activation du profil créée, les incidents sont récupérés périodiquement selon la configuration définie dans le profil. Les incidents seront ajoutés à la table Incidents DLP.

Mappage de l'état des incidents DLP avec Netskope

La section de mappage de l'état des incidents permet aux utilisateurs de fournir les mappages entre l'état de l'incident DLP dans ServiceNow et Netskope l'état de l'objet.

Avant de commencer
Le mappage sera utilisé lors de l'ingestion d'un incident DLP de Netskope vers ServiceNow, ainsi que lors de la synchronisation de tout changement d'état d'un incident DLP dans ServiceNow vers Netskope.

Synchronisez l'état des incidents DLP ingérés sur ServiceNow avec l'incident DLP de Netskope. Mappez le champ État de l'incident ServiceNow avec le champ État de l'objet Netskope .

Rôle requis : sn_dlir.admin

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous devez créer un mappage de l'état de l'incident et de l'état Netskope ServiceNow un à un.

Procédure

1. Accédez à la **Intégration DLP Netskope** > **Mappage de l'état des incidents**.
2. Fournissez un nom pour identifier le mappage.
3. Sélectionnez l'intégration source.
4. Mappez l'état de l'incident DLP à Netskope l'état de l'objet (l'état en Netskope double peut également être mappé).
   La synchronisation de l'état de ServiceNow vers Netskope sera désactivée si vous ne créez pas d'enregistrement de mappage.

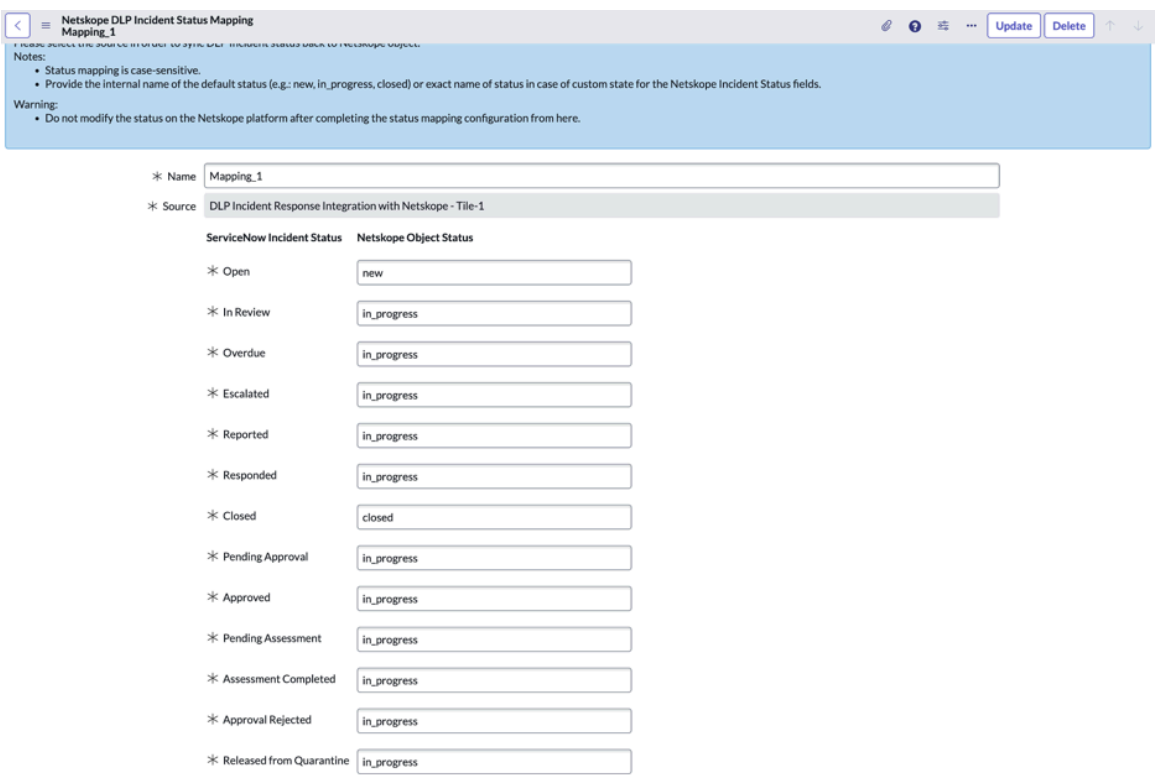
> **Important :** Vous devez mapper tous les Netskope états des objets à tous les états ServiceNow. Sélectionnez la source afin de resynchroniser l'état de l'incident DLP avec l'objet Netskope .

Les informations et les messages d'alerte suivants s'affichent lorsque vous mappez l'état des incidents, examinez les messages et poursuivez.

Remarque :

- Le mappage d'état est sensible à la casse.
- Indiquez le nom interne de l'état par défaut (par exemple : nouveau, in_progress, fermé) ou le nom exact de l'état en cas d'état personnalisé pour les champs État de l'objet Netskope .

> **Avertissement :** Ne modifiez pas l'état sur la Netskope plateforme après avoir terminé la configuration du mappage d'état à partir d'ici.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Netskope Mappage de l'état des incidents DLP

Champ	Description
Nom	Nom de l'enregistrement de mappage.
Source	Source de point de terminaison configurée Netskope à partir de laquelle vous souhaitez synchroniser l'état de l'incident.
État des incidents DLP	Indique l'état de la liste des incidents DLP.
Netskope État de l'objet	Indique la liste de l'état de l'objet Netskope .

5. Cliquez sur **Envoyer**.

Résultats

Une fois l'enregistrement créé avec succès pour le mappage de statut, chaque fois qu'il y a une mise à jour de l'état de l'incident DLP ServiceNow, il la reflète automatiquement de Netskope côté conformément au mappage.

Remarque : Si vous modifiez directement l'état d'un incident DLP sur Netskope le locataire, la synchronisation de l'état de SN à Netskope ne fonctionnera pas compte tenu des limitations de l'API. Assurez-vous de mapper soigneusement l'état de tous les incidents DLP avec Netskope l'état de l'objet.

Configurer les Netskope paramètres d'intégration DLP

Modifiez les propriétés système par défaut de l'intégration Netskope DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Accédez à la **Intégration DLP Netskope** > **Paramètres**.
2. Modifiez les paramètres suivants selon vos besoins.

Configurer les Netskope paramètres d'intégration DLP

Champ	Description
Le téléchargement du fichier en infraction de l'incident signalé doit-il être autorisé sn_ns_dlp.enable_file_download.	Option permettant de choisir si vous souhaitez activer le téléchargement du fichier. Cette option est activée par défaut.
Délai d'expiration maximal pour les appels HTTP, en secondes sn_ns_dlp.maximum_http_time_out.	Délai d'expiration maximal pour les appels HTTP, en secondes. Ce champ est automatiquement défini sur 30.
Nombre maximal de nouvelles tentatives à effectuer en cas d'échec d'API. sn_ns_dlp.maximum_retry.	Nombre maximal de nouvelles tentatives à effectuer en cas d'échec d'API. La valeur par défaut est 3.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Niveau de génération de rapports des journaux générés par l'intégration sn_ns_dlp.logging.verbosity.	Définissez le niveau des journaux de reporting générés par l'intégration. Ce champ est automatiquement défini sur **Info**.

3. Cliquez sur **Enregistrer**.

Résultats
Vos paramètres d'intégration modifiés sont appliqués à l'intervalle d'interrogation suivant, tel que défini dans le profil.

Télécharger les fichiers de preuves

Télécharger des fichiers qui enfreignent la politique DLP sur Netskope. Téléchargez ce fichier sur votre ordinateur local à partir de l'espace de travail de l'analyste DLP IR et de l'espace de travail de l'utilisateur final DLP IR pour les approbateurs.

Avant de commencer
Rôle requis :

- sn_dlir.analyste
- sn_dlir.secure_file_download (n'importe quel approbateur disposant de ce rôle)

Pourquoi et quand exécuter cette tâche
Vous devez activer le téléchargement de fichiers avant Netskope de continuer.

Procédure

1. Accédez à la **Tout** > **Intégration DLP Netskope** > **Paramètres**.
2. Activer la propriété **Le téléchargement du fichier en infraction de l'incident signalé doit-il être autorisé** ?
   Le bouton **Télécharger le fichier** s'affiche dans l'espace de travail de l'analyste DLP IR et dans l'espace de travail de l'utilisateur final DLP IR.
3. Accédez à la **Tout** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
4. Ouvrez un enregistrement d'incident DLP qui est ingéré à partir de la Netskope source.
5. Cliquez sur **Télécharger le fichier**.
   Le fichier qui enfreint la politique DLP sur le Netskope sera téléchargé sur l'ordinateur local de l'utilisateur.

> **Remarque :** L'administrateur DLP peut contrôler l'accès à l'action Télécharger le **fichier** pour toutes les intégrations en désactivant l'option Le **téléchargement du fichier en infraction de l'incident signalé doit-il être autorisé** à partir de la page **Paramètres avancés** de l'Administration DLP. Pour plus d'informations, consultez Configurer les paramètres avancés.

Notifications pour les utilisateurs sur le mécanisme de nouvelle tentative

Netskope l'intégration retente le nombre de fois configuré en cas d'échecs d'API pendant l'ingestion d'incidents DLP.

Lorsque la limite maximale de nouvelles tentatives est dépassée, Netskope l'intégration envoie une notification par e-mail aux utilisateurs qui ont le rôle Administrateur DLP (sn_dlir.admin).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois que vous avez terminé l'installation et la configuration de l'intégration, fournissez le rôle d'administrateur DLP (sn_dlir.admin) aux utilisateurs qui doivent être informés lorsque la limite maximale de nouvelles tentatives est dépassée.

Une fois la limite maximale de nouvelles tentatives dépassée, le profil ignore l'ingestion pendant une durée maximale d'une heure. Le nombre maximal de nouvelles tentatives est configuré à l'aide de la propriété : `Nombre maximal de nouvelles tentatives à effectuer pour les échecs d'API`. Pour plus d'informations, consultezConfigurer les Netskope paramètres d'intégration DLP.

Notifications par e-mail à l'expiration des informations d'identification

Lorsque le jeton utilisé dans l'instance ServiceNow expire, Netskope l'intégration envoie une notification par e-mail aux utilisateurs ayant le rôle Administrateur DLP (sn_dlir.admin).

Une fois la configuration de l'intégration terminée, fournissez le rôle d'administrateur DLP (sn_dlir.admin) aux utilisateurs qui doivent être informés si le jeton a expiré.

Si le jeton expire, l'ingestion de données pour les profils associés sera suspendue jusqu'à ce que la configuration d'intégration Netskope soit mise à jour avec un jeton valide.

Vous devez créer un jeton ou renouveler l'ancien Netskopele , puis mettre à jour le jeton sur l'instance ServiceNow . Si vous renouvelez le jeton en prolongeant le délai d'expiration, l'application Netskope détecte automatiquement le renouvellement et poursuit la collecte de données. Si vous créez un jeton, vous devez le mettre à jour dans la configuration.

Séparation de domaine dans l'intégration Netskope DLP

Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Support : basique.

Fonctionnement de Séparation de domaine avec Netskope l'intégration DLP

Procédez comme suit pour réaliser Séparation de domaine :

- Créez un utilisateur avec le rôle requis dans le domaine respectif.
- Exécutez les procédures d'intégration DLP Netskope dans le domaine approprié.

Data Loss Prevention Incident Response avec Microsoft

Le Data Loss Prevention Incident Response avec Microsoft fournit un cadre de travail de base pour importer des incidents de protection contre la perte de données (DLP) à partir de plusieurs sources telles que Microsoft les applications de portée (Microsoft Teams, Exchange Online, SharePoint Online, OneDrive Entreprise). Les appareils de point de terminaison permettent un workflow de rattrapage impliquant les utilisateurs finaux, les responsables et l'équipe des opérations DLP avec une affectation et des remontées automatisées des incidents.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .

Fonctionnalités principales

Utilisez les fonctionnalités clés de cette intégration pour effectuer les actions suivantes :

- Créez plusieurs profils pour différents comptes.
- Automatiser la création d'incidents DLP IR .
- Mappez les champs d'événement aux champs d'incident Microsoft DLP IRDLP IR .
- Filtrer Microsoft DLP IR les événements.
- Planifiez l'ingestion des DLP IR événements qui créent DLP IR des incidents périodiquement.
- Stockez le contenu correspondant de chaque événement DLP Microsoft dans un stockage cloud externe.
- Supprimer le contenu correspondant au stockage cloud externe lors de la suppression de l'incident dans ServiceNow.DLP IR
- Téléchargez des fichiers pour DLP IR les incidents de type Exchange, OneDrive et SharePoint.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
Microsoft site web de la documentation produit	Site web de la documentation produit Microsoft
ServiceNow site web de la documentation produit	Site web de la documentation produit ServiceNow

Prise en main de l'intégration Microsoft DLP IR pour la protection contre la perte de données

Passez en revue les informations suivantes avant de commencer à configurer votre Microsoft DLP IR intégration pour la protection contre la perte de données.

Liste de vérification

Tâche de configuration	Description
Obtenir les informations d'identification Microsoft Purview pour extraire les données d'événement et les informations d'identification de compte de stockage AWS/Azure pour stocker le contenu de la correspondance Enregistrer une application auprès de Microsoft Identity Platform	Enregistrez une application sur la plateforme Microsoft Azure à partir d'ici pour obtenir l'ID client, le secret client et l'ID de locataire. Pour en savoir plus sur les rôles requis pour créer une application, consultez Conditions préalables . Pour en savoir plus sur les autorisations/rôles d'API requis sur une application Microsoft Azure pour la configurer sur ServiceNow l'intégration DLP Microsoft, consultez le tableau suivant.
Autorisations requises pour que l'utilisateur Azure obtienne l'accès de l'objet blob en	L'utilisateur Azure doit avoir le rôle **Contributeur de données d'objet blob de**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
lecture/écriture/suppression sur le stockage Azure	**stockage** pour lire, écrire et supprimer des objets blob sur le stockage Azure.
Autorisations requises pour que l'utilisateur AWS obtienne l'accès à l'objet en lecture/ écriture/suppression sur AWS Storage	Une politique doit être créée qui donne l'accès en liste, en lecture, en écriture et en suppression pour l'objet dans AWS S3 Storage.
Affectez et vérifiez si vous disposez des rôles requis pour Now Platform les rôles d'administration des pertes de données.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • Le rôle administrateur installe l'intégration à partir du ServiceNow Store rôle sn_dlir.admin et lui attribue le rôle. • Le rôle sn_dlir.admin effectue les tâches suivantes : ◦ Configure l'intégration. ◦ Configure les profils d'incident.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration Microsoft DLP IR sont installées et activées avant de configurer cette intégration.	Vérifiez que les applications courantes et la sécurité suivantes DLP IR prennent en charge les applications courantes sont installées et activées à partir du ServiceNow Store. Si ce n'est pas le cas, installez-le et activez-le dans l'application. • Security Support Common • Data Loss Prevention Incident Response

Autorisations/rôles API requis sur une application Microsoft Azure

Vous avez besoin des autorisations/rôles d'API suivants sur une application Microsoft Azure pour la configurer sur **ServiceNow** *l'intégration DLP Microsoft.*

API	Nom d'autorisation	Type	Description	Pour quelle fonctionnalité ServiceNow est-elle requise ?	Le consentement de l'administrateur est-il requis ?
API de gestion Office 365	ActivityFeed.ReadDlp	Application	Lisez les événements de politique DLP, y compris	Pour ingérer les événements DLP de MSFT Purview vers ServiceNow.	Oui

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisations/rôles API requis sur une application Microsoft Azure

Vous avez besoin des autorisations/rôles d'API suivants sur une application Microsoft Azure pour la configurer sur **ServiceNow** *l'intégration DLP Microsoft.*

(suite)

API	Nom d'autorisation	Type	Description	Pour quelle fonctionnalité ServiceNow est-elle requise ?	Le consentement de l'administrateur est-il requis ?
			les données sensibles détectées.	**Remarque :** Cette autorisation est indispensable pour obtenir les données MSFT dans ServiceNow.	
Microsoft Graph API	Fichiers.Lecture.Tout	Application	Lisez les fichiers de toutes les collections de sites auxquelles vous pouvez accéder.	Télécharger le fichier : pour télécharger la pièce jointe sur l'instance ServiceNow à l'origine de l'événement DLP à partir de OneDrive ou SharePoint **Remarque :** Ceci est facultatif. Vous pouvez ignorer cette autorisation d'API si vous ne souhaitez pas autoriser les analystes à télécharger la pièce jointe à l'origine de l'événement DLP.	Oui
	Courrier.Lecture	Application	Lire le courrier dans toutes les boîtes aux lettres.	Télécharger le fichier : pour télécharger le contenu de l'e-mail (corps et pièce jointe) sur l'instance ServiceNow à l'origine de l'événement DLP à partir d'Exchange.	Oui

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisations/rôles API requis sur une application Microsoft Azure

Vous avez besoin des autorisations/rôles d'API suivants sur une application Microsoft Azure pour la configurer sur **ServiceNow** *l'intégration DLP Microsoft.*

(suite)

API	Nom d'autorisation	Type	Description	Pour quelle fonctionnalité ServiceNow est-elle requise ?	Le consentement de l'administrateur est-il requis ?
				Remarque : Ceci est facultatif. Vous pouvez ignorer cette autorisation API si vous ne souhaitez pas autoriser les analystes à télécharger le contenu de l'e-mail (corps, pièce jointe) à l'origine de l'événement DLP.	
	Utilisateur.Lecture	Délégué	Connectez-vous et lisez le profil d'utilisateur.	Il s'agit de l'autorisation par défaut qui sera disponible pour toutes les nouvelles applications.	Non

Informations sensibles détectées (facultatif)

Le contenu de la correspondance est stocké en externe dans le stockage Azure Blob ou la catégorie Amazon S3 et est extrait du stockage externe lorsque l'utilisateur consulte un incident.

L'une des autorisations suivantes est requise si les utilisateurs souhaitent afficher le contenu des correspondances/les informations sensibles détectées dans l'application DLP Core :

1. Si vous êtes un Microsoft Azure utilisateur, vous devez avoir le rôle Contributeur de données d'objet blob de stockage pour lire, écrire et supprimer des objets blob sur le stockage Azure.
2. Si vous êtes un utilisateur Amazon S3, vous devez créer une politique qui donne l'accès à la liste, en lecture, en écriture et en suppression pour l'objet dans Amazon S3 Storage.

Installer et configurer l'intégration DLP de Microsoft

Installez et configurez l'intégration de Réponse aux incidents DLP avec Microsoft DLP à ServiceNow® Store partir de votre Now Platform instance. Commencez à examiner les incidents DLP à l'aide des données d'événement Microsoft DLP.

Traduction automatique

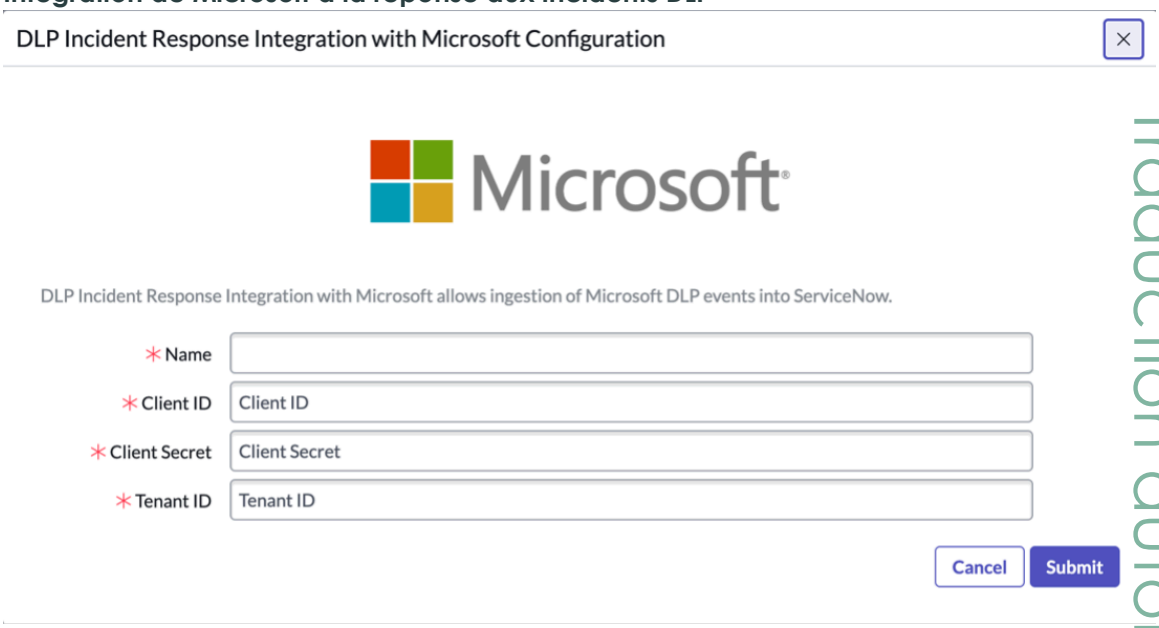
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_dlir.admin

Procédure
1. Téléchargez l'intégration Microsoft DLP à partir de et ServiceNow® Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Configurez l'intégration DLP Microsoft .

   a. **Recherchez la vignette Intégration de la réponse aux incidents DLP avec Microsoft** et cliquez sur **Configurer**.

Intégration de Microsoft à la réponse aux incidents DLP



   b. Renseignez les champs du formulaire.

Formulaire de configuration de l'intégration DLP Microsoft

Champ	Description
Nom	Nom de la configuration de l'intégration Microsoft DLP.
ID client	ID client de l'application créée sur le portail Microsoft Azure.
Secret client	Secret client de l'application créée sur le portail Microsoft Azure.
ID de locataire	ID de locataire de l'utilisateur.

   c. Cliquez sur **Envoyer**.

   Une fois la configuration validée et envoyée, l'intégration Microsoft DLP est enregistrée sous forme de vignette sur la page Intégrations de sécurité.

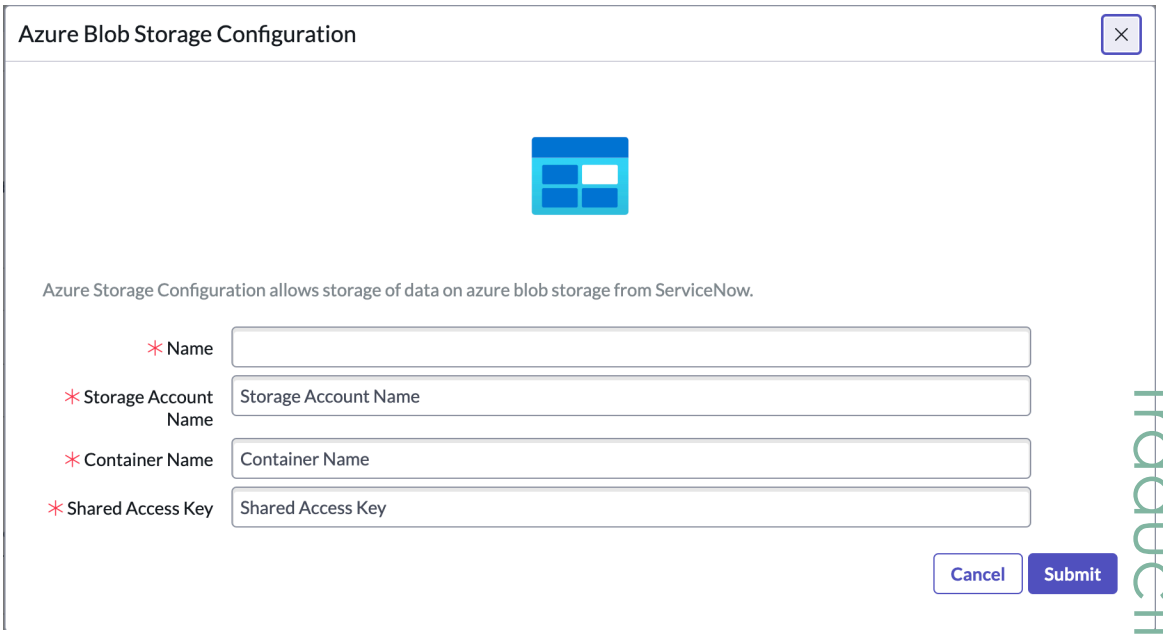
4. Mettez à jour la configuration du stockage Azure.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Sur la page Intégrations de sécurité, recherchez **la vignette Configuration du stockage Azure** .

b. Dans la vignette Configuration du stockage Azure, cliquez sur **Mettre à jour**.



c. Renseignez les champs du formulaire.

Formulaire de configuration du stockage Azure

Champ	Description
Nom	Nom de la configuration de stockage Azure.
Nom du compte de stockage	Nom du compte de stockage créé sur le portail Azure
Nom du conteneur	Nom du conteneur créé dans le compte de stockage sur le portail Azure.
Clé d'accès partagé	Clé d'accès partagée pour le compte de stockage.

d. Cliquez sur **Envoyer**.

Une fois que vous avez validé et soumis la configuration, la configuration du stockage Azure est enregistrée sous forme de vignette sur la page Intégrations de sécurité.

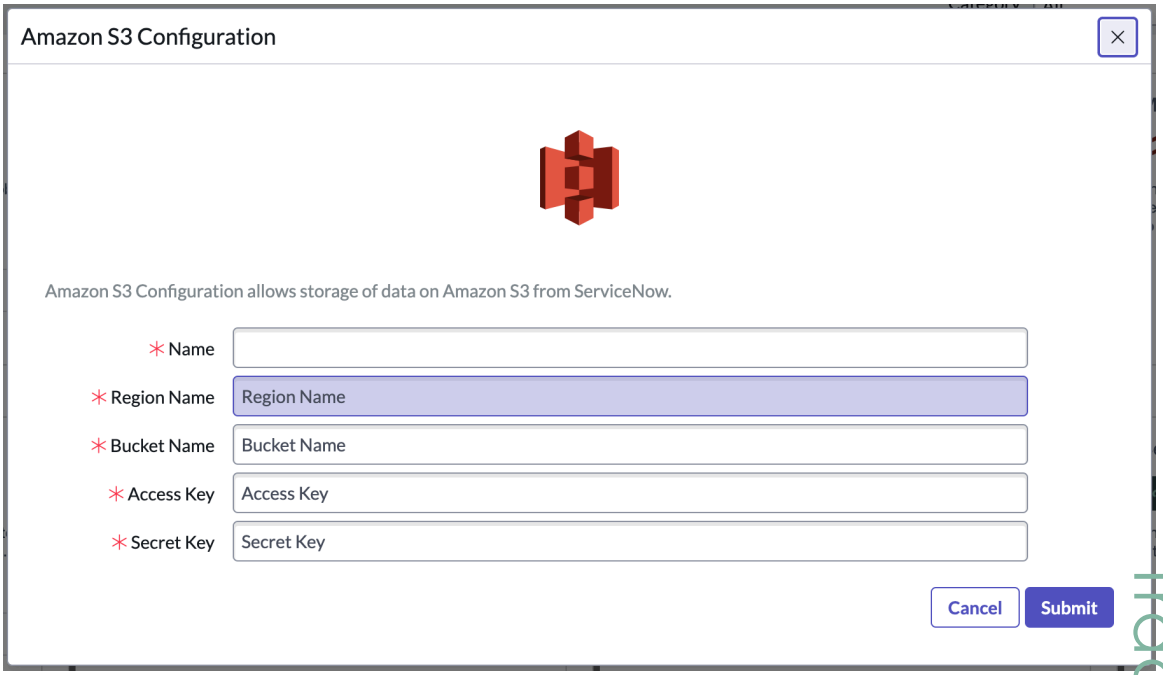
5. Mettez à jour la configuration du stockage AWS.

a. Sur la page Intégrations de sécurité, recherchez **la vignette Configuration du stockage AWS** .

b. Dans la vignette AWS Storage Configuration (Configuration du stockage AWS), cliquez sur **Mettre à jour**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Renseignez les champs du formulaire.

Formulaire Configuration du stockage AWS

Champ	Description
Nom	Nom de la configuration de stockage AWS.
Nom de la région	Nom de la région du compte de stockage AWS.
Nom du compartiment	Nom de la catégorie créée sur le portail AWS.
Clé d'accès	Clé d'accès avec accès en lecture, écriture et suppression.
Clé secrète	Clé partagée avec accès en lecture, écriture et suppression

d. Cliquez sur **Envoyer**.

Résultats
Une fois la configuration validée et envoyée avec succès, celle-ci est enregistrée sous forme de vignette sur la page Security Integrations.

Créer un profil d'incident pour Microsoft l'intégration DLP

Créez un profil d'incident dans votre Now Platform instance pour récupérer les données à partir de Microsoft Purview et ajouter les données à la table d'incident ServiceNow DLP IR .

Avant de commencer
Rôle requis : sn_dlir.admin (créer, modifier et supprimer)

sn_dlir.analyst : afficher (lecture seule)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Configurez le Now Platform® pour récupérer les événements à partir de Purview Microsoft . Stockez ces événements dans la DLP IR table Incident de votre ServiceNow® instance.

Procédure

1. Accédez à la **Intégration DLP de Microsoft** > **Profil d'incident**.
2. Cliquez sur **Nouveau**.
3. Sur le formulaire, renseignez les champs de la section Nom.

Formulaire Créer un profil

Champ	Description
Nom	Nom du profil. Ce champ permet d'identifier le profil. **Remarque :** Le nom doit être unique pour chaque profil.
Source	Instance Microsoft DLP IR que vous avez configurée pour ingérer des incidents. Si vous avez plusieurs configurations d'intégration, sélectionnez l'enregistrement de configuration d'intégration approprié pour les types d'incidents que vous prévoyez d'ingérer pour le profil.
Actif	Option permettant d'indiquer si le profil est actif. Ce champ ne peut être activé qu'après avoir cliqué sur le champ **Terminer** dans la section Planification. Lorsque le profil est actif, cela implique qu'il Now Platform interroge Microsoft DLP IR activement les événements en fonction de la configuration définie dans le profil.
Ordre	Ordre d'exécution du profil. Le profil dont l'ordre est le plus bas est considéré comme la priorité la plus élevée. Par défaut, la valeur est 100.
Description	Description unique pour le profil.

Que faire ensuite

Pour passer à la section Filtrage, cliquez sur **Continuer**.

Définir les filtres à appliquer à la création d'incident

Définissez et définissez des conditions de filtre pour filtrer les événements DLP Microsoft entrants. Contrôlez lesquels de ces événements doivent être créés en tant qu'incidents DLP IR sur votre ServiceNow instance.

Avant de commencer

Rôle requis : sn_dlir.admin (créer, modifier et supprimer)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sn_dlir.analyst : afficher (lecture seule)

Pourquoi et quand exécuter cette tâche

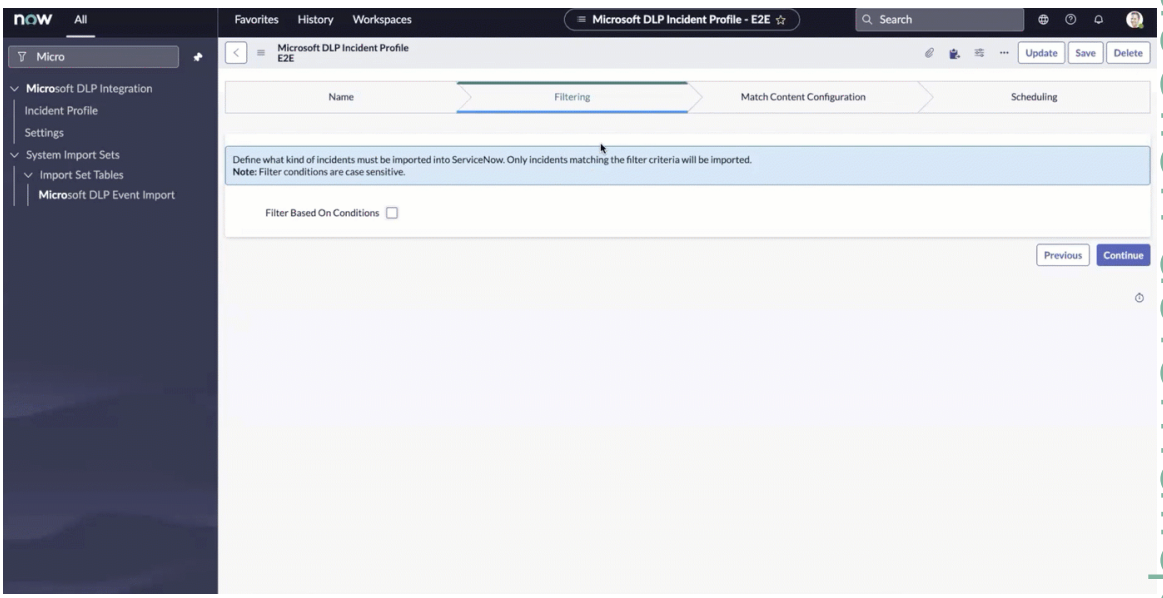
Ce type de filtrage vous aide à isoler les événements DLP Microsoft afin de limiter le nombre d'incidents DLP IR que vous créez. Si les critères de filtrage sont définis, seuls les événements qui correspondent aux conditions sont créés en tant qu'incidents DLP.

Procédure

1. Sélectionnez l'option **Filtre basé sur les conditions** .
2. À l'aide des listes et des champs du générateur de conditions, définissez les filtres dans le champ **Conditions de filtre** .

   Définissez les critères qu'un événement DLP entrant Microsoft doit satisfaire pour qu'un incident DLP soit créé.

   Les options du premier champ des conditions de **filtre** correspondent aux champs disponibles dans l'événement DLP Microsoft. Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'événement.



3. Ajoutez d'autres conditions en cliquant sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. Cliquez sur **Continuer** et accédez à la section Configuration du contenu de la correspondance.

Configurer le contenu de la correspondance pour l'incident

Fournissez la configuration pour stocker les informations sensibles sur le stockage externe dans le cloud, tel qu'Azure Storage ou la catégorie AWS S3, afin de récupérer ce contenu lors d'un chargement tout en accédant à l'incident DLP IR.

Avant de commencer

Rôle requis : sn_dlir.admin (créer, modifier et supprimer)

sn_dlir.analyst : afficher (lecture seule)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Sur la barre de progression, cliquez sur l'étape **Configuration du contenu de la correspondance** .
2. Renseignez les champs du formulaire.

Faire correspondre la configuration du contenu

Champ	Description
Stocker le contenu correspondant	Option permettant de stocker le contenu correspondant sur le stockage cloud. **Important :** Si cette option n'est pas sélectionnée, le contenu de correspondance de politique pour les incidents DLP n'est pas visible dans l'espace de travail DLP. L'activation de cette option garantit que le contenu des correspondances renvoyé dans les incidents DLP est stocké dans le stockage cloud externe (par exemple, Azure, AWS). Vous pouvez également récupérer et afficher le contenu de la correspondance chaque fois qu'un incident DLP est ouvert dans l'espace de travail. Pour en savoir plus sur la configuration du stockage externe dans le cloud, reportez-vous à la section Installer et configurer l'intégration DLP de Microsoft.
Supprimer le contenu de la correspondance lors de la suppression de l'incident	Option permettant de supprimer le contenu de correspondance d'incident du stockage externe dans le cloud. Cette option n'est visible que lorsque le champ **Contenu de la correspondance de stockage** est sélectionné.
Informations d'identification externes dans le cloud	Le stockage externe dans le cloud où le contenu de la correspondance est stocké. Vous pouvez vous référer aux informations d'identification externes dans le cloud ajoutées pour la configuration du stockage. Cette option n'est visible que lorsque le champ **Contenu de la correspondance de stockage** est sélectionné.

3. Cliquez sur **Continuer** et accédez à la section Planification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Planifier la récupération d'incident DLP IR Microsoft

Définissez un calendrier pour récupérer les données d'incident et ingérer les Microsoft DLP IR incidents qui correspondent aux critères du profil. Configurez le calendrier pour définir comment et quand vous extrayez les incidents à partir de Microsoft.

Avant de commencer

Rôle requis : sn_dlir.admin (créer, modifier et supprimer)

sn_dlir.analyst : afficher (lecture seule)

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier la fréquence à laquelle vous procéderez à une interrogation pour les incidents futurs qui correspondent à la configuration du profil d'incident. Pour activer l'ingestion automatisée d'incidents, vous devez configurer la planification et la récupération des incidents avant d'activer le profil. Le profil peut être configuré pour effectuer une récupération ponctuelle à l'aide de la case à cocher **Récupération ponctuelle** . La date historique peut être comprise jusqu'aux trois derniers mois à compter de la date actuelle.

L'intervalle d'interrogation est configuré individuellement pour chaque profil. Les différents intervalles d'interrogation peuvent avoir un impact sur les performances de l'intégration d'incident Microsoft DLP IR . Lors de la planification, prévoyez d'équilibrer la charge du système par rapport à l'urgence d'un incident.

Procédure

1. Définissez un calendrier pour récupérer les données et ingérer les incidents qui correspondent aux critères du profil.
2. Renseignez les champs du formulaire.

Calendrier du formulaire d'incident DLP

Champ	Description
Intégration de l'incident en cours	Ingestion d'incident en cours que l'instance Now Platform extrait de Microsoft pour les nouveaux incidents. DLP IR Les incidents sont créés si des incidents déclenchés sont détectés et que les critères de filtrage de génération d'incident correspondent.
Incrémentation du sondage (minutes)	La fréquence d'interrogation de Microsoft. Ce champ est automatiquement défini sur 300 minutes.
Définir le délai d'intégration de l'incident initial	Option permettant de définir une date et une heure pour l'ingestion initiale. Les ingestions suivantes sont basées sur la période de l'intervalle d'interrogation. Cette option n'est visible que lorsque le champ **Ingestion d'incident en cours** est sélectionné.
Délai d'intégration de l'incident initial d'entrée	Date et heure que vous spécifiez pour l'ingestion de l'incident.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Si la valeur est définie, la récupération des données à partir de Microsoft commencera à partir de la date ultérieure ajoutée. ◦ Ce champ n'est visible que lorsque **l'option Définir le délai d'ingestion initial** est sélectionnée.
Délai d'intégration de l'incident initial	Première fois que les données sont ingérées. Vous pouvez voir que les valeurs commencent à s'afficher lorsque le délai d'ingestion initial de l'incident est défini.
Délai d'intégration de l'incident suivant (estimé)	La période suivante pour une ingestion d'incident estimée.
Récupération ponctuelle	Option permettant d'activer les extractions ponctuelles de données historiques. Si ce champ est sélectionné, les données historiques sont extraites de Microsoft DLP IR en fonction de la date ajoutée dans le champ **Depuis date** .
Date de début	Date à partir de laquelle les données sont censées être récupérées à partir de Microsoft. Ce champ peut être défini sur un maximum de 7 jours.

3. Enregistrez la configuration de profil créée en cliquant sur **Terminer** dans la fenêtre contextuelle.
4. Activez le profil.
   a. Ouvrez le profil créé.
   b. Activez l'option **Actif** .
   c. Cliquez sur **Mettre à jour**.

Résultats
Une fois le profil créé et activé, les incidents sont récupérés périodiquement selon la configuration définie dans le profil et ajoutés à la table Incidents DLP.

Configurer les paramètres d'intégration Microsoft DLP IR

Modifiez les propriétés système par défaut de l'intégration Microsoft DLP IR .

Avant de commencer
Rôle requis : sn_dlir.admin

Procédure
1. Accédez à la **Intégration DLP de Microsoft** > **Paramètres**.
2. Modifiez les propriétés suivantes selon vos besoins.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de l'intégration DLP de Microsoft

Champ	Description
Délai maximal pour les appels HTTP (sn_pp_dlp.maximum_http_time_out)	Délai d'expiration maximal pour les appels HTTP (en secondes). ◦ Type : nombre entier ◦ Valeur par défaut : 30
Niveau de génération de rapports des journaux générés par l'intégration (sn_pp_dlp.logging.verbosity)	Niveau de journaux de reporting générés par l'intégration, c'est-à-dire le nom du type d'informations. Vous pouvez également mettre à jour la valeur pour les options suivantes : ◦ **erreur** ◦ **avertir** ◦ **info** ◦ **debug** ◦ **arrêt** Par défaut, la valeur est **info**.
Destination des rapports des journaux générés par l'intégration (sn_pp_dlp.logging.destination)	Destination des journaux générés par l'intégration. Vous pouvez également mettre à jour la valeur pour les options suivantes : ◦ **Db** ◦ **fichier** ◦ **aucun** Par défaut, la valeur est **db**.

3. Cliquez sur **Enregistrer**.

Résultats
Vos paramètres d'intégration modifiés sont appliqués à l'intervalle d'interrogation suivant, tel que défini dans le profil.

Demander la sortie de quarantaine de l'e-mail

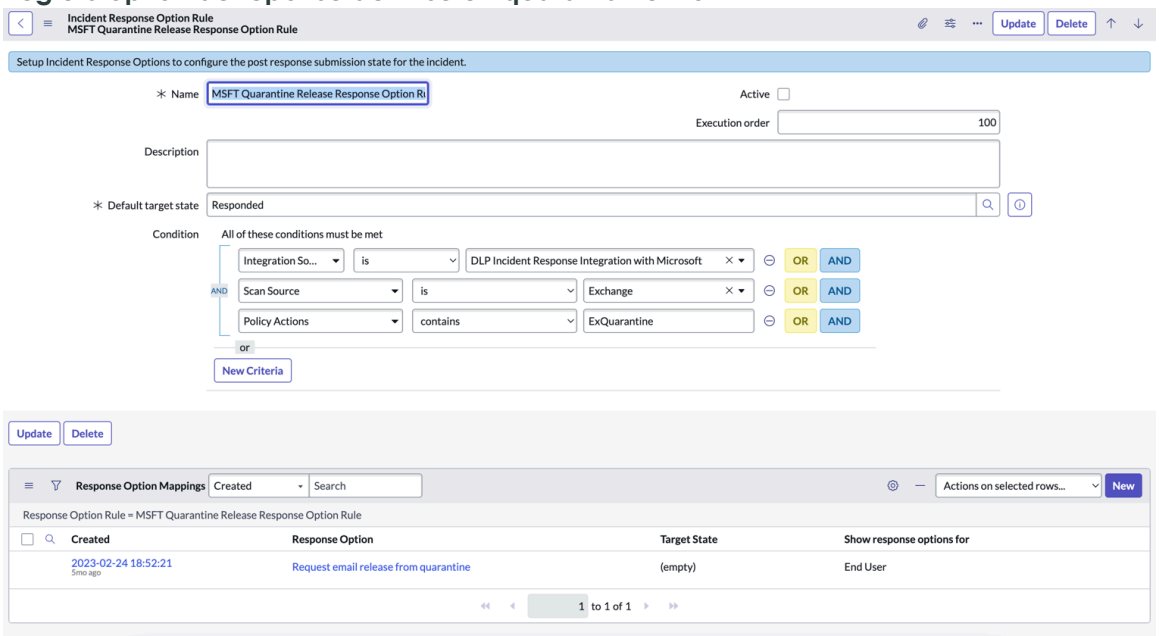
Utilisez cette fonctionnalité pour libérer l'e-mail qui est mis en quarantaine à partir du portail de conformité Microsoft Purview.

Avant de commencer
Par défaut, le système de base fournit l'option **de réponse Demander la libération de l'e-mail de quarantaine** et la **règle d'option de réponse de libération de quarantaine MSFT** pour sortir l'e-mail de quarantaine. La **règle d'approbation de mise en quarantaine** est également configurée pour cet enregistrement par défaut afin de tirer parti de la fonctionnalité d'approbation de cette action. Pour en savoir plus, consultez Créer des règles d'option de réponse aux incidents, Configurer l'option de réponse pour vos incidents DLP et Créer des règles d'approbation.

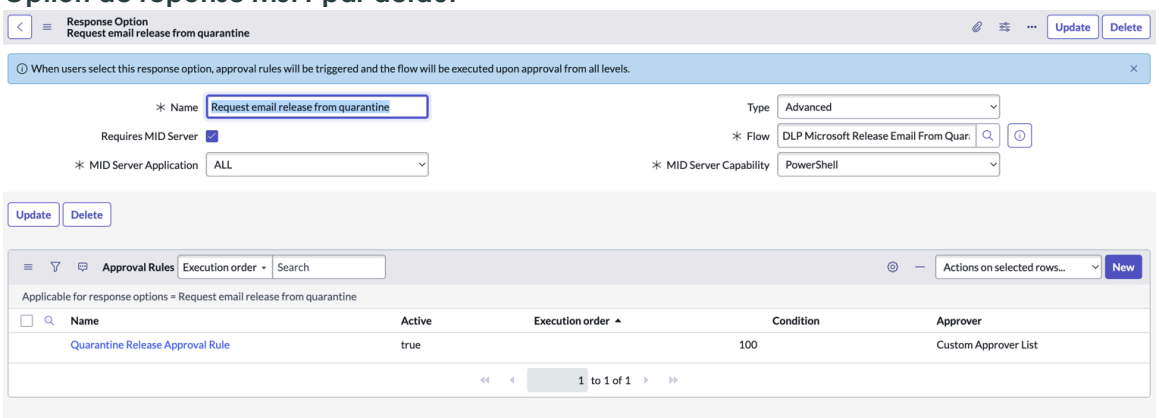
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règle d'option de réponse de mise en quarantaine MSFT



Option de réponse MSFT par défaut



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous utilisez cette option de réponse, assurez-vous que le MID Server est opérationnel avec l'aptitude PowerShell. Si un MID Server n'est pas opérationnel et ne dispose pas de la fonctionnalité PowerShell, l'utilisateur final ne peut pas sélectionner l'action **Demander la libération de l'e-mail de la quarantaine** dans l'espace de travail des utilisateurs DLP. Pour plus d'informations, consultez Créer des règles d'option de réponse aux incidents et Configurer l'option de réponse pour vos incidents DLP.

- Si vous voulez un MID Server spécifique dans la liste, vous devez configurer l'application MID et l'afficher dans la liste, puis au moins un MID Server configuré doit être opérationnel à partir des applications MID sélectionnées et doit avoir la capacité Power Shell.
- Pour que vous puissiez utiliser l'option Sortir de quarantaine, vous avez besoin d'autorisations d'API. Sur la page des autorisations d'API Microsoft, vérifiez **Office 365 Exchange Online** > **Exchange.ManageAsApp** est répertorié et contient les valeurs suivantes :
  - ▪ **Type** : **Application**.
  - ▪ **Consentement de l'administrateur requis** : **oui**.
  - ▪ **État** : la valeur incorrecte actuelle **n'est pas accordée pour <Organisation>** pour l'entrée **Office 365 Exchange Online** > **Exchange.ManageAsApp** et modifiez la valeur d'état. Pour plus d'informations sur les autorisations d'API, consultez Affecter des autorisations d'API à l'application sur le site de documentation de Microsoft.

    Remarque : Cette étape est requise pour se connecter à Exchange Online à l'aide du principe de service.

- Vous devez également avoir besoin **du rôle d'administrateur de sécurité** dans Service Principle,
  - Recherchez les **rôles et les administrateurs Microsoft Entra ID** dans le portail Microsoft Azure, ajoutez l'affectation à l'application inscrite (principe de service), puis suivez la procédure expliquée dans la documentation Microsoft sur l'affectation d'un rôle .
- Cette option s'applique uniquement aux incidents Microsoft Exchange dont l'option **Action de politique** est **ExQuarantine** dans la vue du formulaire d'incident.

Rôle requis : utilisateur final

La procédure suivante explique comment soumettre cette action à partir de l'espace de travail de l'utilisateur DLP.

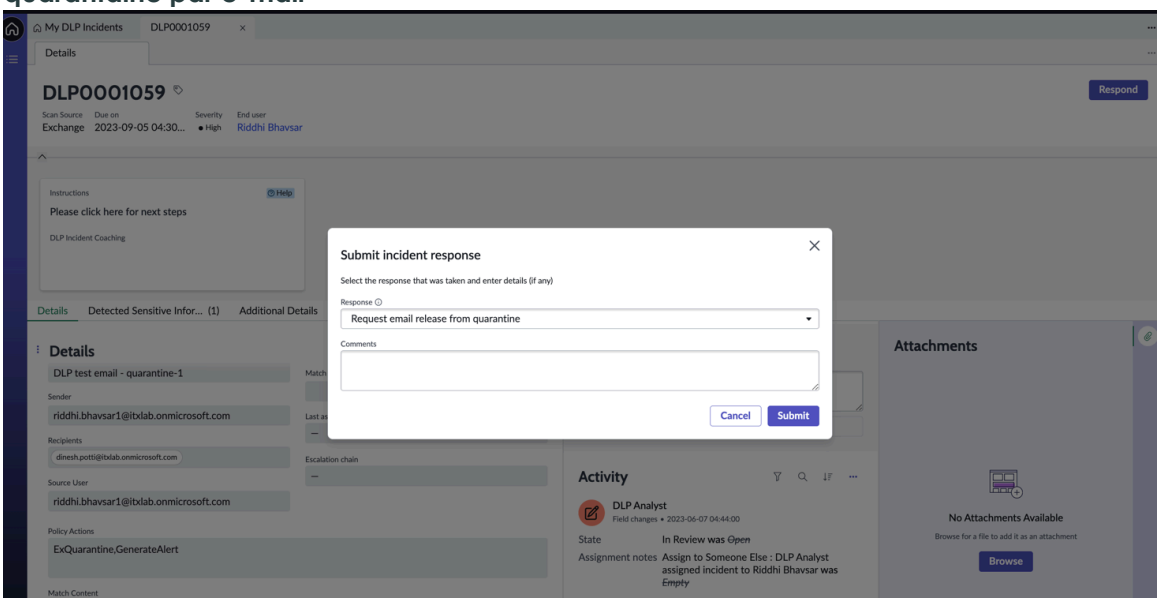
Procédure

1. Accédez à la **DLP** > **Espace de travail de l'utilisateur DLP**.
2. Ouvrez n'importe quel incident DLP Microsoft Exchange.
   Vérifiez que **l'action de politique** relative à l'incident est définie sur ExQuarantine.
3. Cliquez sur **Répondre**.
4. Sélectionnez **l'option Demander la sortie du courrier de quarantaine** dans la liste déroulante Réponse.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Soumettre une réponse à un incident : demander l'option de sortie de quarantaine par e-mail



5. Cliquez sur **Envoyer**.

> **Remarque :** Lorsqu'une règle d'approbation est configurée pour cette action, le flux d'approbation est déclenché en premier et après avoir reçu toutes les approbations, le flux Demander la libération de l'e-mail de quarantaine est déclenché et l'e-mail est sorti de quarantaine. L'état de l'incident DLP sera mis à jour sur **Sorti de quarantaine** après une diffusion réussie.

Télécharger des fichiers pour les incidents DLP de type Exchange Online, OneDrive et SharePoint

Téléchargez des fichiers ou des e-mails qui enfreignent la stratégie DLP sur Microsoft Purview. Téléchargez ce fichier ou envoyez un e-mail sur votre ordinateur local à partir de la DLP IR vue Incident. Vous pouvez télécharger les fichiers pour DLP IR les incidents de type Source de l'analyse Exchange Online, OneDrive et SharePoint.

Avant de commencer

Rôle requis :

- sn_dlir.admin, sn_dlir.analyst
- N'importe quel approbateur valide

Procédure

1. Accédez à la **Tout** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Ouvrez un enregistrement d'incident DLP de type Source de l'analyse, Exchange Online, OneDrive ou SharePoint qui est ingéré à partir d'une source Microsoft.
3. Cliquez sur **Télécharger le fichier**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le fichier ou l'e-mail qui a enfreint la politique DLP du côté de Microsoft Purview sera téléchargé sur l'ordinateur local de l'utilisateur.

Remarque : L'administrateur DLP peut contrôler l'accès à l'action Télécharger le **fichier** en désactivant le paramètre **Le téléchargement du fichier en infraction de l'incident signalé doit-il être autorisé** à partir de la page Paramètres avancés ? Pour plus d'informations, consultez Configurer les paramètres avancés.

Séparation de domaine dans l'intégration Microsoft DLP

Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Support : basique.

Fonctionnement de Séparation de domaine avec Microsoft l'intégration DLP

Procédez comme suit pour réaliser Séparation de domaine :

- Créez un utilisateur avec le rôle requis dans le domaine respectif.
- Exécutez les procédures d'intégration DLP Microsoft dans le domaine approprié.

Opérations de sécurité Fonctionnalité commune

Chaque fois que l'un des modules d'extension pour les applications principales Opérations de sécurité (Réponse aux incidents de sécurité, Réponse aux vulnérabilités, Renseignements sur les menaces, ou Configuration Compliance) est activé, le module d'extension Security Support Common est activé. Ce module d'extension charge divers modules qui fournissent des fonctionnalités communes à toutes les Opérations de sécurité applications.

Remarque : Seuls les utilisateurs disposant de la propriété [sn_sec_cmn.admin] peuvent afficher et utiliser le Opérations de sécurité module. Ce rôle est hérité lorsqu'un rôle administratif vous est affecté dans l'une Opérations de sécurité des applications.

Security Operations Modules

Fonctionnalité	Description
Référence de Security Operations Integrations, Intégrations de Renseignements sur les menaces, Intégrations de Réponse aux vulnérabilités	Plusieurs intégrations sont incluses dans les Opérations de sécurité applications (Réponse aux incidents de sécurité, Renseignements sur les menaces, et Réponse aux vulnérabilités). Cette section fournit des instructions pour l'activation des modules d'extension et la configuration des intégrations ServiceNow tierces. Vous y trouverez également des directives de base pour le développement de vos propres intégrations, ainsi que des détails sur les intégrations spécifiques incluses dans le système de base.
Opérations de sécurité Traitement des e-mails	Vous pouvez configurer l'intégration des informations provenant de systèmes de détection externes, assurer la granularité du traitement des

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalité	Description
	enregistrements des opérations de sécurité, traiter les e-mails sans correspondance et empêcher la duplication des enregistrements à l'aide Traitement des e-mailsde .
Groupes	• **Groupes de filtres** Créez et utilisez des groupes de filtres pour localiser les enregistrements de n'importe quelle table sur votre instance. Par exemple, vous pouvez créer un groupe de tous les ordinateurs du même fabricant. Vous pouvez également filtrer les éléments de configuration (CI) qui présentent des vulnérabilités similaires ou qui se trouvent dans une plage d'adresses IP de sous-réseau particulière. • **Escalades** Vous pouvez créer un parcours d'escalade des incidents de sécurité pour les problèmes nécessitant une plus grande attention ou une expertise. Une fois qu'un groupe d'escalade existe, un bouton apparaît sur tous les incidents de sécurité de ce groupe.
Balises de sécurité	**Balises** : les règles de balise de sécurité permettent de filtrer l'accès aux balises de sécurité.
Workflows	• **Voir les workflows de sécurité** Vous pouvez afficher les nombreux workflows inclus dans les applications Security Operations. Vous pouvez créer des workflows à partir de modèles et dans l'éditeur de workflow. • **Déclencheurs de workflow** Opérations de sécurité Les déclencheurs de workflow contiennent une condition sur une table. Tous les workflows associés à l'enregistrement de déclencheur de workflow s'exécutent lorsque la condition est remplie.
Utilités	• **Mappage des données d'enrichissement** Mappage des données d'enrichissement transforme les données de XML, JSON ou Propriétés de fichiers en ServiceNow enregistrements. Opérations de sécurité Les workflows utilisent des cartes de données

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalité	Description
	d'enrichissement et fournissent des données de sortie aux incidents de sécurité. • **Transformations de valeurs de champs** Transforme les valeurs de champ client uniques en valeurs de champ reconnues par Opérations de sécurité l'analyse des e-mails, l'enrichissement des données ou les tables utilisant des cartes de champs. Prend en charge les champs de choix, les références et aligne les données externes sur la terminologie et le format standard de votre nouvel enregistrement. • **Mappage de champs** Opérations de sécurité Les tables peuvent être mappées vers et à partir d'autres tables, liant un incident de sécurité à un ticket du service clientèle ou un problème à d'autres parties du Opérations de sécurité système. Par exemple, vous pouvez intégrer un module d'extension à une Réponse aux incidents de sécurité tâche. • **Orchestration sur demande** Au cours Réponse aux incidents de sécurité de l'analyse, un analyste de sécurité peut vouloir effectuer une tâche qui est générée par un workflow d'incident de sécurité. Par exemple, exécutez un vidage de processus sur un CI particulier. Cela peut être accompli avec l'orchestration à la demande. • **Groupes de systèmes d'exploitation** N/A. • **Registre des applications SecOps** N/A.
CMDB	**Règles d'identificateur de CI** : les identificateurs de CI sont des règles utilisées pour rechercher un élément de configuration (CI) dans la CMDB qui contient des informations correspondantes provenant d'une intégration tierce. Ces règles définissent les champs qui contiennent des données correspondantes et l'ordre de priorité selon lequel ils sont évalués. La valeur **d'ordre** la plus basse est évaluée en premier.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer et définir des groupes de filtres dans Security Operations

Créez et utilisez des groupes de filtres pour localiser les enregistrements de n'importe quelle table sur votre instance. Par exemple, vous pouvez créer un groupe de tous les ordinateurs du même fabricant. Vous pouvez également filtrer les éléments de configuration (CI) qui présentent des vulnérabilités similaires ou qui se trouvent dans une plage d'adresses IP de sous-réseau particulière.

Avant de commencer

Rôle requis : sn_sec_cmn.write

Pourquoi et quand exécuter cette tâche

Les groupes de filtres peuvent contenir des enregistrements mis à jour dynamiquement, une série d'enregistrements statiques qui ne sont pas filtrés à l'aide de conditions ou une combinaison d'enregistrements statiques et mis à jour dynamiquement. Certains groupes de filtres sont inclus dans le système de base, par exemple, les exclusions de CI.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Groupes** > **Groupes de filtres**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Le nom du groupe de filtres.
Actif	Box pour activer le groupe.
Description	Description du groupe de filtres.
Adresses IP de réseau	Adresse IP de réseau qui contient les adresses IP des CI que vous souhaitez ajouter au groupe. Ce champ s'affiche uniquement si vous avez sélectionné l'élément de configuration [cmdb_ci] ou une table qui étend l'élément de configuration dans le champ **Table** .
Masque de sous-réseau	Sous-réseau qui contient les adresses IP des CI que vous souhaitez ajouter au groupe, par exemple, 255.255.255.0. Ce champ s'affiche uniquement si vous avez sélectionné l'élément de configuration [cmdb_ci] ou une table qui étend l'élément de configuration dans le champ **Table** .
Table	Table sur laquelle filtrer.
Condition	Utilisez le créateur de conditions pour définir les critères à filtrer.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
   Un onglet **Conditions avancées** s'affiche.

   D'autres onglets apparaissent en fonction du type de table que vous avez spécifié dans le champ **Table** , comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Onglets affichés
Élément de configuration [cmdb_ci] ou une table qui étend la table d'éléments de configuration	**CI ajoutés manuellement** et **CI correspondants**
Tâche [task] ou table étendant la table de tâches	**Tâches ajoutées manuellement** et **tâches correspondantes**
Une table non associée à un CI ou à une tâche	**Enregistrement ajouté manuellement**

5. Pour définir d'autres conditions pour votre groupe de filtres :

a. Cliquez sur **Conditions avancées**.

b. Insérez une nouvelle ligne dans la liste **incorporée des conditions de groupe de filtres supplémentaires** pour sélectionner d'autres groupes de filtres prédéfinis que vous souhaitez combiner avec le groupe de filtres en cours de mise à jour.
Si vous souhaitez que le groupe de filtres sélectionné filtre les enregistrements en fonction d'un champ de référence, un champ mappé est automatiquement sélectionné lors de l'enregistrement actuel.

> **Remarque :** La valeur **du champ mappé** ne peut pas être modifiée à partir de la liste **incorporée des conditions de groupe de filtres supplémentaires** . Pour modifier le champ, cliquez sur l'icône afin d'ouvrir l'enregistrement.

c. Cliquez sur **Mettre à jour**.

6. Pour ajouter manuellement d'autres CI ou tâches au groupe de filtres :

a. Cliquez sur l'onglet **CI ajoutés manuellement** ou **Tâches ajoutées manuellement** .

b. Cliquez sur **Modifier**.

c. Sélectionnez les CI ou les tâches que vous souhaitez ajouter.

d. Cliquez sur **Enregistrer**.

7. Pour afficher les CI ou les tâches qui correspondent à vos critères de sélection :

a. Cliquez sur l'onglet **CI correspondants** ou **Tâches correspondantes** .

b. Si vous avez modifié les critères, actualisez la liste en cliquant avec le bouton droit de la souris dans l'en-tête du formulaire et en sélectionnant **Actualiser la liste**.

Transformation des données partagées

Les modules d'extension Réponse aux incidents de sécurité, Réponse aux vulnérabilités, et Renseignements sur les menaces partagent des caractéristiques communes, pour les données de relation et les règles de duplication, utilisées pour importer des informations externes et internes dans Opérations de sécurité.

Analyse des e-mails, Règles de duplicationpuis Mappage de champs prenez des données d'entrée (un e-mail, un fichier JSON ou XML, ou un enregistrement) et transformez ces données au format approprié pour créer un nouvel enregistrement. Chacune de ces fonctionnalités extrait les données à sa manière, mais elles sont transformées en nouvel enregistrement à l'aide d'un grand nombre des mêmes processus.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Données de relation

Lorsque vous ajoutez des informations à une liste connexe (comme un observable associé dans un incident de sécurité), vous pouvez créer un enregistrement de relation composé d'une table m2m. Parfois, il y a des données supplémentaires sur cet enregistrement de relation à définir. Par exemple, un observable étant une adresse IP source (par opposition à une adresse IP de destination). Ces informations sont placées dans le champ **Données** de relation du formulaire **Transformation de champ** utilisé par **Analyse des e-mails** ou dans une liste connexe **Champs de mappage de champs** dans le formulaire **Mappage de champs** .

Le champ **de données de relation** est généralement vide. Il est le plus souvent utilisé pour les adresses IP sur les observables dans **l'analyse des e-mails**.

Vous pouvez transformer les données de n'importe quel ServiceNow enregistrement en n'importe quel autre ServiceNow enregistrement à l'aide des **champs de mappage de champs** de la fonctionnalité **de mappage de champs** . Par exemple, pour transformer les données d'un incident en incident de sécurité, ou d'un incident de sécurité en PRB.

Règles de duplication de Security Operations

Permet Règles de duplication de gérer les enregistrements en double pour la sécurité, la vulnérabilité, les IoC, etc.

Les règles de duplication ont deux objectifs. Ils empêchent la création d'un trop grand nombre d'enregistrements en double et, lorsqu'un doublon est détecté, ils spécifient quels champs de l'enregistrement sont mis à jour. Seuls les doublons actifs sont recherchés. Si l'enregistrement n'est pas actif, par exemple, si l'incident est fermé, tout nouveau problème identique devient un nouvel incident.

Les règles de duplication sont utilisées par **l'analyse des e-mails**, **le mappage de champs** et **le mappage des données d'enrichissement**.

Information associée

Créer des analyseurs d'e-mails dans Security Operations

Mappez les tables aux tables avec le mappage de champs Security Operations

Créer des règles de duplication dans Opérations de sécurité

Vous pouvez l'utiliser Règles de duplication pour identifier les nouveaux e-mails, données d'enrichissement ou cartes de champs avec des enregistrements en double actifs et les traiter de manière appropriée.

Avant de commencer

Rôle requis : sn_sec_cmn.write

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Règles de duplication**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient :

Règle de duplication

Champ	Description
Nom	Nom de la règle de duplication.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Table	Table où les enregistrements sont créés et utilisés pour déterminer la duplication.
Identification des champs	Sélectionnez un ensemble de champs qui indiquent un incident de sécurité en double, un observable, une vulnérabilité, etc., lorsque les valeurs de ces champs sont identiques.
Action relative à la duplication	Régit la façon de gérer les e-mails en double. Les choix possibles sont les suivants : Créer en tant qu'enfant Crée un enregistrement en tant qu'enfant de l'original. Le champ liant l'enfant au parent est le champ **Parent**. Ne pas créer ni mettre à jour des enregistrements (par défaut) Ne fait rien. Ignore les doublons. Mettre à jour l'enregistrement en double Met à jour les champs de l'enregistrement existant comme spécifié dans **Actions de duplication.** **Remarque :** Si vous choisissez **Mettre à jour l'enregistrement en double**, la liste connexe **Actions de duplication** s'affiche.
Actif	Cochez cette case pour activer la règle.
Description	Décrit le but et l'application de cette règle de duplication ; lorsqu'elle doit être utilisée, par exemple une règle conçue pour les observables basés sur l'adresse IP ou les incidents de sécurité du pare-feu.

4. Cliquez avec le bouton droit dans l'en-tête de l'enregistrement et sélectionnez **Enregistrer** ou cliquez sur **Mettre à jour**.
5. Pour définir des actions de duplication, si vous avez choisi **Mettre à jour l'enregistrement en double**, cliquez sur **Nouveau** pour créer des actions de duplication pour chaque champ que vous souhaitez mettre à jour dans l'incident.
6. Remplissez ou modifiez les champs du formulaire pour décrire la mise à jour du champ :

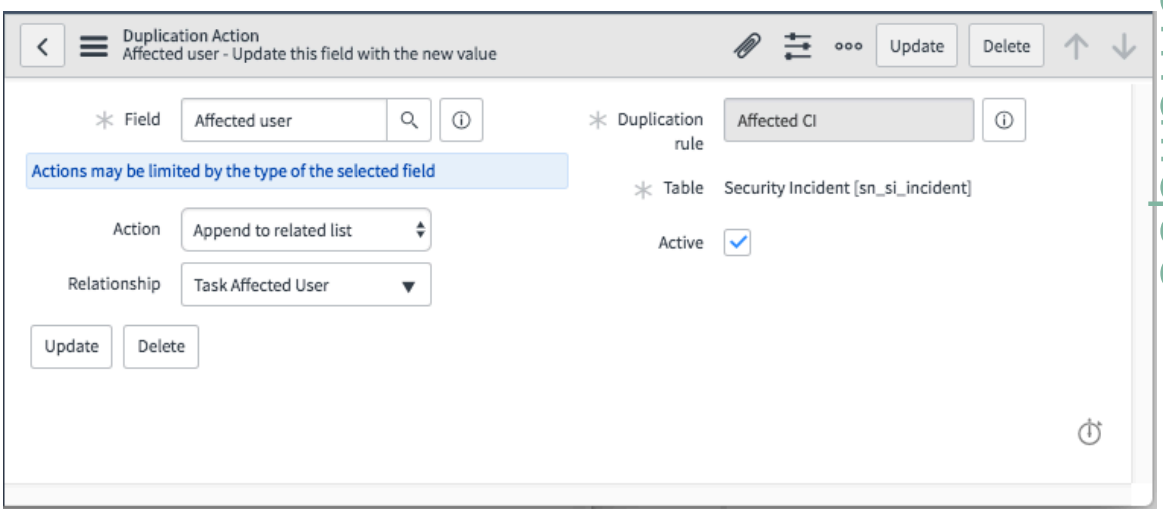
Actions de duplication

Champ	Description
Champ	Nom du champ à utiliser pour l'action de duplication.
Action	Les actions prises en charge varient selon le type de champ. Les choix possibles sont les suivants : Mettre à jour ce champ avec la nouvelle valeur Remplace la valeur précédente dans l'enregistrement existant par cette valeur. Ajouter la nouvelle valeur à une liste séparée par des virgules, si elle est unique Traite la valeur comme une entrée dans une liste séparée par des virgules et ajoute les nouvelles données (le cas échéant)

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

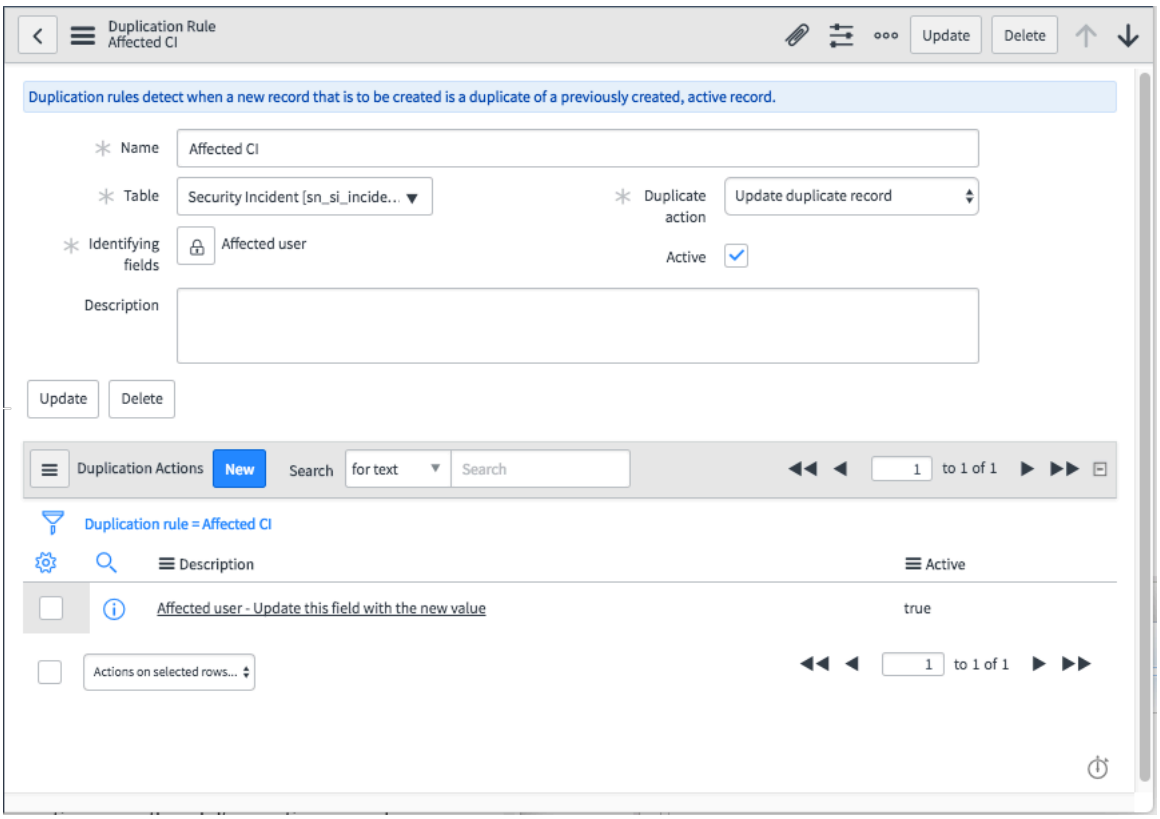
Champ	Description
	comme une nouvelle entrée dans cette liste. Si les données sont déjà dans la liste, elles ne sont pas ajoutées deux fois. Ajouter la nouvelle valeur à ce champ Ajoute la nouvelle valeur à la fin du texte existant dans le champ. Ajouter un à un champ de compteur Ajoute un au champ numérique. Définir le champ à la date d'aujourd'hui Définit le champ sur la date et l'heure actuelles. Ajouter à la liste connexe Ajoute l'enregistrement connexe avec cette valeur à la liste connexe de l'enregistrement actuel. S'affiche lorsqu'il existe une table plusieurs à plusieurs, avec une colonne du même type, liée à la table en cours de mise à jour. Par exemple, **CI affecté** ou **Utilisateur affecté**.
Relation	[Facultatif] Ce champ s'affiche uniquement lorsque l'action **Ajouter à la liste connexe** est choisie. Il s'agit du nom de la liste connexe que vous souhaitez associer à cette règle.
Règle de duplication	Règle dont cette action fait partie.
Table	Table où les enregistrements sont créés. S'affiche à titre d'information uniquement.
Actif	Cochez cette case pour activer l'action.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Envoyer**.



Opérations de sécurité Traitement des e-mails

Vous pouvez configurer l'intégration des informations provenant de systèmes de détection externes, assurer la granularité du traitement des enregistrements des opérations de sécurité, traiter les e-mails sans correspondance et empêcher la duplication des enregistrements à l'aide Traitement des e-mailsde .

Traitement des e-mails se compose des fonctionnalités suivantes :

Fonctionnalité	Description
Analyse des e-mails	Générez de nouveaux Opérations de sécurité enregistrements à partir d'e-mails du système externe.
Règles de duplication	Identifie les nouveaux e-mails contenant des incidents connus et les traite de manière appropriée.
Propriétés	Spécifie les comptes utilisés comme entrée pour Analyse des e-mails la sécurité, la vulnérabilité et les IoC. Assure la granularité du traitement Opérations de sécurité des enregistrements.
E-mails sans correspondances	Répertorie les e-mails qui ne correspondent à aucun Opérations de sécurité enregistrement.

Propriétés d'e-mail Opérations de sécurité

Les e-mails Propriétés spécifient les boîtes de réception utilisées comme entrée pour Analyse des e-mails importer des informations à partir de systèmes de détection externes afin de créer des enregistrements pour la sécurité, la vulnérabilité et les IoC. Vous pouvez configurer un compte général pour tous les systèmes de détection externes à utiliser, ou des comptes

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de messagerie individuels pour Réponse aux incidents de sécurité, Renseignements sur les menaces, ou Réponse aux vulnérabilités.

Créer des Opérations de sécurité propriétés d'e-mail

Vous pouvez spécifier des adresses de messagerie pour les rapports et contrôler le comportement automatique de la messagerie à l'aide de la messagerie .Propriétés

Avant de commencer

Rôle requis : sn_sec_cmn.admin
Configurez des outils de détection externes pour envoyer des e-mails dans votre boîte de réception d'analyse des e-mails.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Traitement des e-mails** > **Propriétés**.
2. Entrez vos boîtes aux lettres des destinataires comme il convient :
   Il s'agit d'adresses e-mail entrantes à traiter par **l'analyse des e-mails**, plutôt que par **des actions entrantes**.

Propriétés de l'analyse des e-mails

Champ	Description
Boîte de réception des Opérations de sécurité outils	Adresse e-mail complète pour Opérations de sécurité. Par exemple, secops_support@yourcompany.com.
Boîte de réception des outils des incidents de sécurité	Adresse e-mail complète pour Réponse aux incidents de sécurité. Par exemple, sir_support@your.company.com.
Boîte de réception des Réponse aux vulnérabilités outils	Adresse e-mail complète pour Réponse aux vulnérabilités. Par exemple, vuln_resp@yourcompany.com.
Boîte de réception des Renseignements sur les menaces outils	Adresse e-mail complète pour Renseignements sur les menaces. Par exemple, threat_intel@yourcompany.com.

3. Cliquez sur **Enregistrer**.

Opérations de sécurité Analyse des e-mails

Générez de nouveaux Opérations de sécurité enregistrements à partir de systèmes de détection externes à l'aide de Analyse des e-mails. Cette fonctionnalité fournit une méthode d'intégration d'informations provenant d'outils externes tels que la détection de programmes malveillants, la détection de vulnérabilité, les pare-feu, la connaissance des menaces, etc.

Comment les e-mails sont-ils analysés ?

Tout système capable d'envoyer un e-mail peut créer Opérations de sécurité des enregistrements, par exemple, des incidents de sécurité, des demandes, des éléments vulnérables, des vulnérabilités, des observables d'incident de sécurité, des méthodes d'attaque, etc.

Tous les Opérations de sécurité modules d'extension (Réponse aux incidents de sécurité, Renseignements sur les menaces, et Réponse aux vulnérabilités) ont une propriété (**email_to**) qui définit l'adresse e-mail à laquelle les intégrations externes doivent envoyer des e-mails,

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à analyser par les analyseurs d'e-mails. Reportez-vous à **Traitement des e-mails** > **Propriétés** pour plus d'informations.

Un e-mail envoyé à l'une Opérations de sécurité des adresses e-mail est stocké dans une table d'événements d'e-mail. Ces e-mails sont traités pour déterminer s'ils correspondent à un analyseur d'e-mails.

Les e-mails qui ont une correspondance sont marqués et les règles de transformation et de duplication créent ou mettent à jour un Opérations de sécurité enregistrement. L'e-mail est lié à cet enregistrement et marqué comme `correspondant`.

Les e-mails qui ne correspondent pas sont répertoriés en E-mails sans correspondances tant qu'enregistrement Opérations de sécurité . Ils peuvent être examinés pour aider à construire des analyseurs d'e-mails pour gérer ces e-mails. Une action de retraitement vous permet d'exécuter à nouveau l'e-mail sans correspondance dans les analyseurs. Le journal d'e-mail d'origine est lié à cet enregistrement.

Les règles de duplication pour la transformation d'e-mail gèrent plusieurs e-mails relatifs au même problème. Ces règles définissent ce qui constitue un enregistrement en double et peuvent empêcher la création d'enregistrements en double. Lorsqu'un doublon est détecté, la règle spécifie l'action à entreprendre : aucune action (ne pas créer de nouvel enregistrement), créer le nouvel enregistrement en tant qu'enregistrement enfant de l'enregistrement existant ou mettre à jour l'enregistrement existant. Lors de la mise à jour, la règle de duplication spécifie quels champs de l'enregistrement existant sont mis à jour.

Remarque : Un Opérations de sécurité analyseur d'e-mails fonctionne conjointement avec les actions entrantes de la plateforme et ne les remplace pas. Il ne prend pas en charge la définition de valeurs sur les champs indirects, par exemple, **sys_journal_field** entrées.

Par défaut, les événements d'e-mail sont supprimés après 30 jours.

Plusieurs enregistrements

Les systèmes de détection externes (détecteurs de logiciels malveillants, vulnérabilités, etc.) peuvent envoyer des e-mails qui signalent plusieurs éléments à la fois. L'analyseur d'e-mail prend en charge les séparateurs dans l'e-mail.

Par exemple, un détecteur de logiciels malveillants pourrait vous envoyer un rapport par e-mail sur tous les systèmes de votre réseau infectés par un logiciel malveillant particulier, avec d'abord des informations sur le programme malveillant, puis une liste des systèmes affectés.

Exemple d'e-mail malveillant

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 20380285098260923490723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
==========
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
==========
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
==========
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans cet exemple, lorsque le **séparateur d'enregistrement** est défini dans votre **Transformation d'e-mail**en tant que **==========**, il divise l'e-mail en quatre sections qui sont évaluées séparément. Cela crée un incident de sécurité pour chacun des trois systèmes affectés.

Remarque : La section d'en-tête est détectée, mais aucun système n'est affecté, elle est donc utilisée dans les trois enregistrements et ne crée pas de quatrième enregistrement.

Les transformations de champ extraient les données de chaque section. Si un élément dans l'en-tête ou le pied de page de l'e-mail s'applique à tous les enregistrements, comme Hachage de programme malveillant, Nom du programme malveillant et Type dans cet exemple, la transformation de champ correspondant doit définir la **valeur Rechercher** en une valeur qui effectue une recherche dans le corps **de l'e-mail, soit au début d'une ligne dans le corps de l'e-mail** , soit **n'importe où dans le corps de l'e-mail**.

Les transformations de champdoivent être définies sur rechercher **au début d'une ligne dans la section des enregistrements ou dans la seconde** des données définies dans chaque section, telles que le système, l'adresse IP ou l'état. Les options de section d'enregistrement ne sont disponibles que lorsqu'un séparateur d'enregistrement est défini dans la transformation d'e-mail.

Lors de l'analyse d'un e-mail avec un séparateur défini, les enregistrements ne sont créés que pour les sections ayant au moins un élément de données spécifiques à la section.

Dans cet exemple, trois enregistrements sont créés, même s'il y a quatre sections définies. La première section est un en-tête, et il lui manque quoi que ce soit de spécifique à un seul système. Si l'un des champs de la première section est renseigné (Système, IP ou État), un enregistrement est également créé pour cette section.

Information associée

- Créer des analyseurs d'e-mails dans Security Operations
- Opérations de sécurité Mappage des données d'enrichissement
- Opérations de sécurité Mappage de champs

Créer des analyseurs d'e-mails dans Security Operations

Analyse des e-mails Crée Opérations de sécurité des enregistrements à partir de votre e-mail pour la sécurité, la vulnérabilité et les observables afin d'accélérer la réponse aux menaces et les mesures correctives.

Avant de commencer

- Configurez des outils de détection externes pour envoyer des e-mails à une adresse e-mail centrale.
- Définissez l'adresse e-mail dans les propriétés de Security Operations. Pour plus d'informations, consultez Créer des Opérations de sécurité propriétés d'e-mail.
- Affectez un compte d'utilisateur à cette adresse e-mail et donnez à cet utilisateur des contrôles d'accès de sécurité pour créer et mettre à jour les enregistrements d'événements d'e-mail.
- Ayez devant vous une copie de l'e-mail concerné provenant de votre outil de détection externe.
- Décidez du type d'enregistrement que vous souhaitez créer : incident de sécurité, enregistrement de vulnérabilité, tâche, etc. Ce choix détermine la table que vous sélectionnez.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Analyse des e-mails**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

> **Remarque :** Si plusieurs champs sont spécifiés, tous doivent correspondre à l'e-mail pour créer un enregistrement.

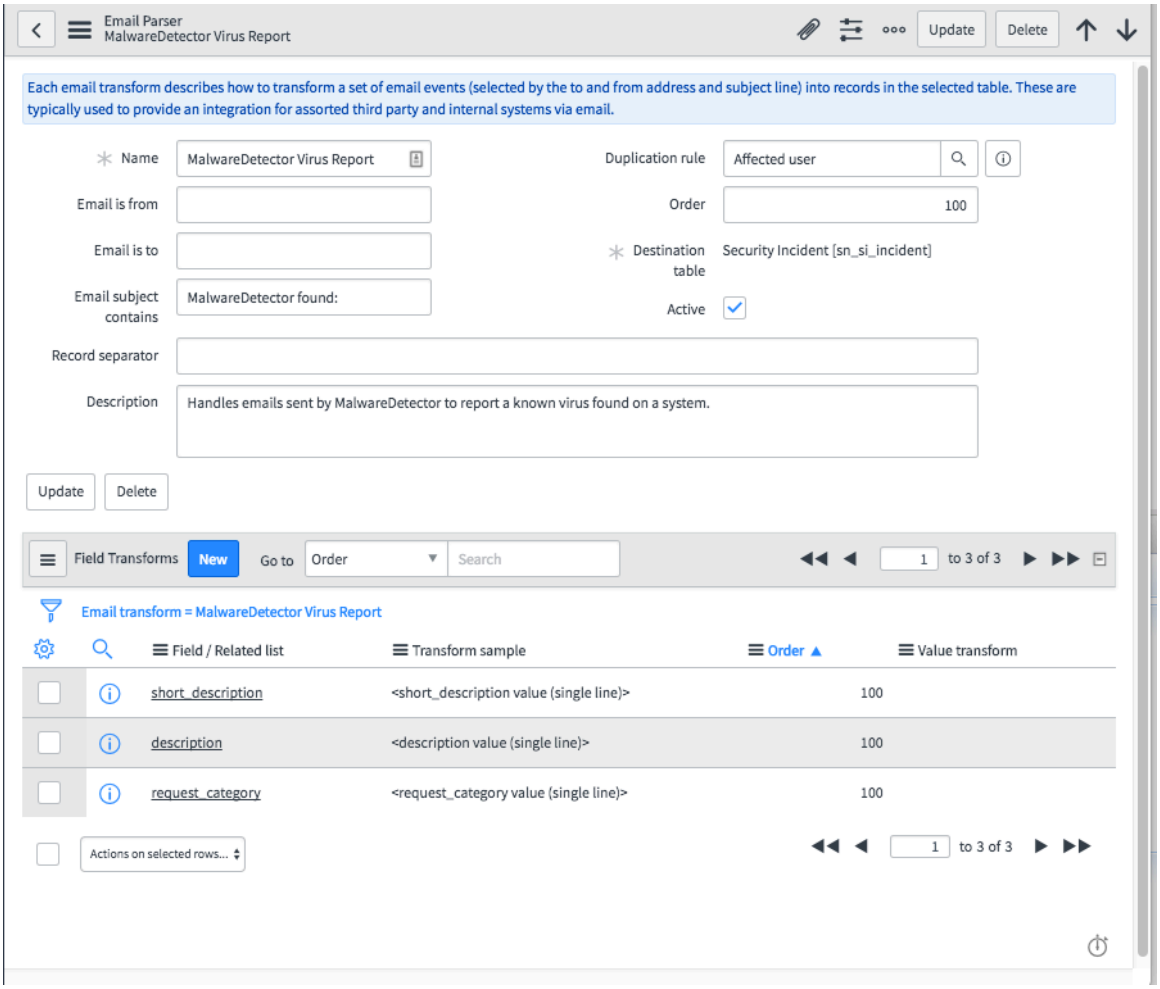
Analyseur d'e-mail

Champ	Description
Nom	Le nom de l'analyseur d'e-mails.
L'e-mail provient de	S'il est renseigné, seuls les e-mails provenant de cette adresse sont transformés par cet analyseur d'e-mails.
L'e-mail est destiné à	S'il est renseigné, seuls les e-mails provenant de cette adresse sont transformés par cet analyseur d'e-mails.
L'objet de l'e-mail contient	S'ils sont renseignés, seuls les e-mails dont l'objet contient cette phrase sont transformés par cet analyseur d'e-mail.
Règle de duplication	Régit la façon de gérer les e-mails en double pour tous les e-mails traités par cette transformation. Pour plus d'informations, consultez Transformation des données partagées.
Ordre	Dans quel ordre considérer les transformations. La première transformation d'e-mail correspondante est utilisée. En règle générale, vous souhaitez configurer les analyseurs d'e-mails les plus spécifiques dans les numéros inférieurs, avec quelques solutions de secours. Donnez aux analyseurs d'e-mails fourre-tout des numéros **de commande** plus élevés afin qu'ils s'exécutent si rien d'autre ne correspond. La valeur par défaut est 100. Lorsque tout correspond, l'analyseur d'e-mails le plus spécifique (correspond **de**, **à** et **objet**) est utilisé.
Table de destination	Table dans laquelle vous souhaitez créer des enregistrements.
Actif	Indique si cette transformation est active, en cours d'utilisation ou non active. Si elle n'est pas cochée, aucun e-mail n'est transformé avec ce code.
Séparateur d'enregistrements	Lorsque les e-mails traités par cet analyseur d'e-mails créent plusieurs enregistrements, ce champ contient le séparateur entre les informations de ces enregistrements. Consultez Opérations de sécurité Analyse des e-mails pour plus d'informations.
Description	Description de cet analyseur d'e-mails, avec quel outil il fonctionne, objectif, etc.

4. Lorsque vous avez terminé vos saisies, faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
   Un onglet **Transformations de champ** s'affiche. Cet onglet montre comment les champs individuels de la table de destination sont définis en fonction du contenu de l'e-mail.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Pour ajouter **des transformations de champ**, procédez comme suit.
   a. Dans l'onglet **Transformations de champ** , cliquez sur **Nouveau**.
   b. Renseignez les champs du formulaire comme il convient.

Option	Description
Champ	**Description**
Stocker la valeur dans un champ ou une liste connexe	Sélectionnez où trouver la valeur. Les choix sont les suivants : ◦ Stocker la valeur dans un champ du nouvel enregistrement ◦ Lier à cette valeur dans une liste connexe ◦ Lier à cette valeur, ce qui crée un nouvel enregistrement si un enregistrement correspondant n'existe pas **Remarque :** Si la table de destination ne possède aucune liste connexe, ce champ n'est pas affiché.
Champ	Sélectionnez le champ à renseigner avec cette valeur.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Pour les champs de choix, les correspondances avec les choix existants sont établies à l'aide de l'étiquette ou de la valeur de choix sous-jacente. Si aucune correspondance n'est trouvée, le champ est défini, mais aucune nouvelle entrée n'est ajoutée à la liste de choix. Pour plus d'informations, consultez Listes de choix . Pour les champs de référence, une entrée n'est définie que lorsqu'une valeur correspondant au nom d'affichage de l'enregistrement ou à un `sys_id` valide est trouvée. Pour plus d'informations, consultez Champs de référence .
Liste connexe	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou **Lier à cette valeur, la création d'un nouvel enregistrement si aucun enregistrement correspondant n'existe**, ce champ spécifie la liste connexe à laquelle ajouter des informations.
Champ de valeur	Lorsque la **valeur stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou **Lier à cette valeur, la création d'un nouvel enregistrement si aucun enregistrement correspondant n'existe**, ce champ spécifie le champ dans la table affichée dans la liste connexe. Il est utilisé pour rechercher et trouver un enregistrement existant. Par exemple, si votre liste connexe est **celle des CI affectés**, ce champ peut contenir le **nom** ou le **nom de domaine complet**, ou tout autre champ de l'enregistrement de CI à utiliser pour rechercher le CI ajouté à la liste **des CI affectés** .
Données de relation	Lorsque la **valeur stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe**, un enregistrement est créé pour lier cet enregistrement (comme un incident de sécurité) à la valeur (un CI, un observable, etc.). Ce champ spécifie toutes les informations sup-

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	plémentaires (paires de champ et valeur) qui doivent être ajoutées à l'enregistrement de liaison. Par exemple, lors de l'ajout d'un observable pour une adresse IP source, spécifiez que cette adresse IP est la source et non l'adresse IP de destination. Pour plusieurs valeurs, utilisez un séparateur ^, par exemple, type= Source IP^Active=true.
Données de nouvel enregistrement	Lorsque la **valeur stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur, ce qui crée un nouvel enregistrement. Si aucun enregistrement correspondant n'existe, si aucun enregistrement connexe correspondant à** la valeur analysée n'est trouvé, un enregistrement est créé. Ce champ spécifie les données statiques à ajouter à cet enregistrement. **Pour les CI affectés**, si aucun CI correspondant n'est trouvé, un enregistrement de CI est créé. Lorsque cela se produit, la valeur trouvée dans l'e-mail est définie sur le champ **Valeur** dans l'enregistrement CI. Vous pouvez définir des données supplémentaires : une note indiquant pourquoi le CI a été créé, des informations sur le type de CI avec lesquels vous travaillez, etc. Un exemple serait : description=Created by Malware Scanner email parser^type=autodetect.
Rechercher la valeur	Sélectionnez l'emplacement dans l'e-mail à rechercher. Les choix sont les suivants : ◦ **Au début d'une ligne dans le corps de l'e-mail** ◦ **N'importe où dans le corps de l'e-mail** ◦ **Dans la ligne d'objet de l'e-mail** ◦ **Toujours la valeur statique** Lorsque vous avez défini un **séparateur d'enregistrement**, d'autres options (**n'importe où dans la section d'enregistrement** et **au début d'une ligne dans la section d'enregistrement) vous permettent d'effectuer une** recherche uniquement dans la section actuelle et non dans l'ensemble du corps de l'e-mail (voir Opérations de sécurité Analyse des e-mails pour plus d'informations. Les informations contenues dans un en-tête ou un pied de page, s'appliquant à tous les enregistrements, sont recherchées dans

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	l'ensemble du corps de l'e-mail. Les informations qui diffèrent d'un enregistrement à l'autre ne sont recherchées que dans la section.
Séparateur de valeur	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou **Lier à cette valeur, créant un nouvel enregistrement si aucun enregistrement correspondant n'existe**, ce champ spécifie le séparateur à utiliser pour les listes d'éléments. par exemple, une virgule ou un point-virgule lorsque les données de l'e-mail sont une liste d'adresses IP.
Préfixe de valeur	Texte qui précède toujours la valeur placée dans ce champ à extraire.
Fin de la valeur	Sélectionnez ce qui indique la fin de la valeur. Les choix sont les suivants : **Fin de ligne**, **Fin de l'e-mail** (affiche tout le texte restant dans l'e-mail), **Jusqu'à** (s'arrête lorsqu'il trouve le texte spécifié) ou **Jusqu'à** (s'arrête lorsqu'il trouve le texte spécifié).
Suffixe de valeur	Lorsque la **fin de la valeur** est définie sur **Jusqu'à**, ce champ spécifie le texte qui suit toujours la valeur placée dans ce champ. Par exemple, la recherche d'une valeur qui vient après « L'ordinateur affecté est » et avant « . » analysera « AB123 » à partir de « Le virus du lapin dément a été trouvé. L'ordinateur concerné est AB123. L'heure estimée de l'infection était 15h45 » dans un courriel.
Transformation de valeur	Choisissez l'entrée de transformation de champ à appliquer. Convertit la valeur trouvée dans l'e-mail en une valeur différente, utilisée pour remplir les champs de choix, parfois de référence, et d'autres champs.
Ordre	Ordre dans lequel les transformations de champ s'exécutent, de la plus basse à la plus élevée. Une transformation de champ avec une entrée d'ordre de 100 est d'abord tentée. Ce n'est que si cette transformation de champ ne parvient pas à trouver une valeur qu'une transforma-

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	tion de champ d'ordre supérieur (200) sur le même champ s'exécute.
Transformation d'e-mail	Transformation à laquelle appartient cette transformation de champ.
Table de destination	Table de destination de la transformation d'e-mail. Il contient des données d'information issues de la transformation d'e-mail.
Actif	L'option par défaut est cochée. Lorsque cette option est activée, la transformation de champ est activée. Décochez cette case pour désactiver la transformation de champ.

a. Cliquez sur **Envoyer**.
Le nouvel enregistrement est utilisé pour analyser les informations contenues dans l'e-mail en un nouvel enregistrement.

Information associée

Créer des règles de duplication dans Opérations de sécurité

Créer des Opérations de sécurité transformations de valeurs de champ

Définir les Réponse aux vulnérabilités notifications par e-mail

Modifier des enregistrements d'e-mail dans Opérations de sécurité

Ajoutez ou créez des transformations dans vos enregistrements d'événements d'e-mail existants.

Avant de commencer

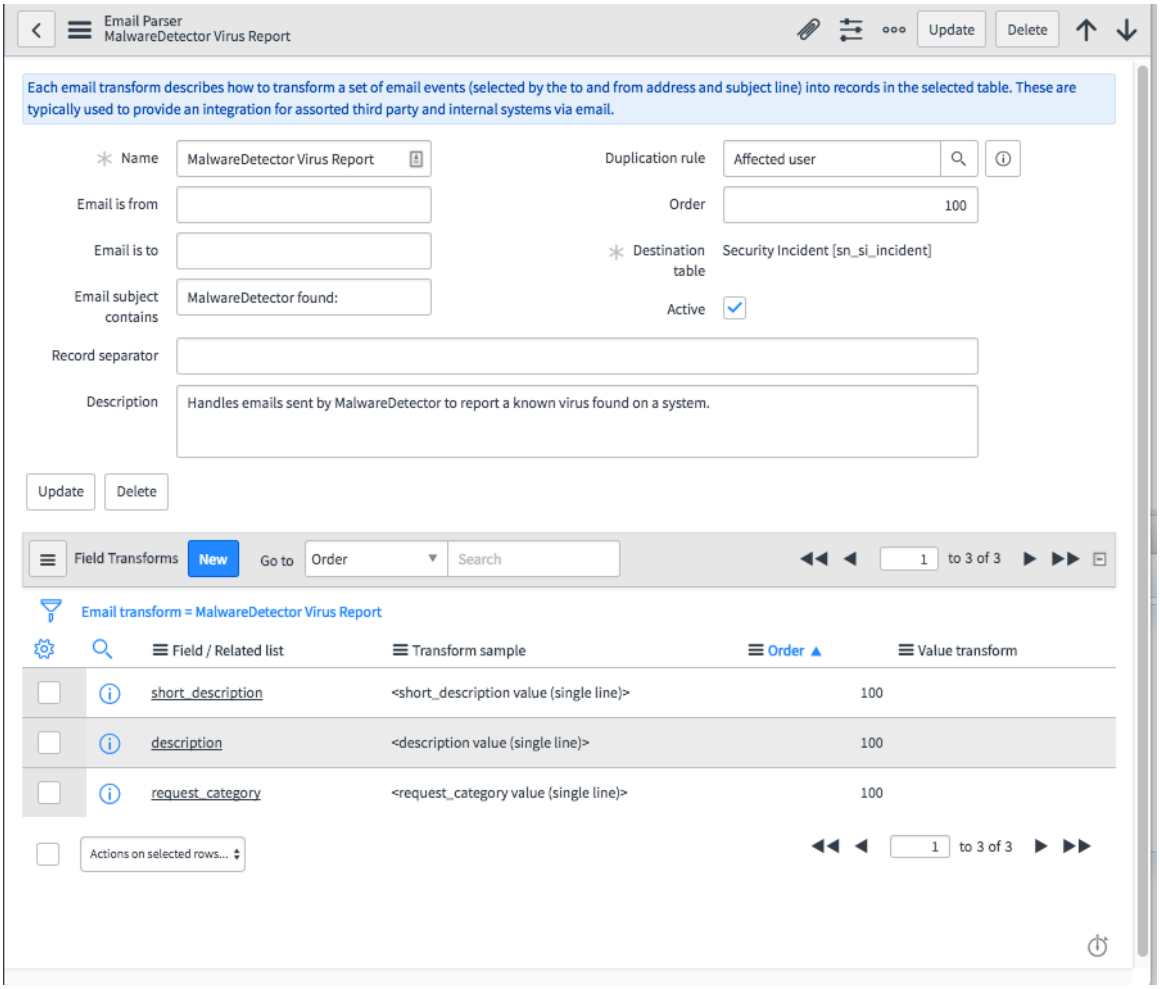
Rôle requis : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Analyse des e-mails**.
2. Cliquez sur l'analyseur d'e-mail pour effectuer la modification.
Si l'enregistrement est en lecture seule, cliquez sur le lien ici dans le message d'en-tête.
Vous êtes redirigé vers la forme modifiable de la transformation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Modifiez les champs comme il convient.
4. Pour modifier **les transformations de champ**, cliquez dans le champ et modifiez-les selon vos besoins.
5. Cliquez sur **Mettre à jour.**

Événements d'e-mail sans correspondance Opérations de sécurité

Le marqueur « correspondant » des événements d'e-mail qui ne correspondent pas à un analyseur d'e-mail n'est pas défini. Vous pouvez afficher ces enregistrements d'événements d'e-mail à partir de la E-mails sans correspondances liste, pour révéler les systèmes de détection externes dont les e-mails ne sont pas encore analysés.

Lorsque vous créez des analyseurs d'e-mails, vous pouvez tenter de traiter à nouveau l'événement d'e-mail (à partir du formulaire ou de la liste) pour valider un nouvel analyseur d'e-mail.

Afficher et traiter à nouveau les e-mails Security Operations sans correspondance

Vous pouvez vérifier E-mails sans correspondances les filtres abandonnés ou en tant que candidats à un nouveau filtre afin de maintenir ou d'améliorer le taux de détection des menaces par e-mail.

Avant de commencer

Rôle requis : sn_sec_cmn.read

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **E-mails sans correspondances**.
   Si des e-mails sans correspondance ont été trouvés, ils sont répertoriés.
2. Les champs du formulaire sont les suivants :

Événements d'e-mail de sécurité

Champ	Description
De	Adresse e-mail de l'expéditeur.
À	Adresse e-mail des destinataires.
Objet	Ligne d'objet de l'e-mail.
Corps	Contenu du corps de l'e-mail.
En correspondance	Indique si cet événement d'e-mail a une correspondance.

3. Pour traiter à nouveau cet e-mail, créez un enregistrement d'e-mail ou modifiez un enregistrement d'e-mail existant pour correspondre aux informations contenues dans cet e-mail.
   Consultez Créer des analyseurs d'e-mails dans Security Operations.
4. Revenir à **Security Operations** > **E-mails sans correspondances**.
5. Cliquez sur **Retraiter l'événement d'e-mail** pour tenter de traiter cet e-mail.
   Cela vous renvoie à la E-mails sans correspondances liste principale. Si le nouvel enregistrement d'e-mail correspond, l'événement d'e-mail n'est plus dans la liste. Un message indique s'il a été mis en correspondance ou non.

Opérations de sécurité Mappage de champs

Opérations de sécurité Les tables peuvent être mappées vers et à partir d'autres tables, liant un incident de sécurité à un ticket du service clientèle ou un problème à d'autres parties du Opérations de sécurité système.

Le mappage de champs définit le mappage utilisé lorsqu'un enregistrement de la table source est utilisé pour créer un nouvel enregistrement dans la table de destination. Généralement utilisées pour créer un incident de sécurité à partir d'un autre enregistrement, ces cartes définissent les champs d'un incident de sécurité insérés dans un nouveau problème ou les champs d'un incident client existant renseignent un nouvel incident de sécurité.

Mappez les tables aux tables avec le mappage de champs Security Operations

Opérations de sécurité vous offre une granularité de mappage de champs plus fine afin que vous puissiez mapper une Opérations de sécurité table à n'importe quelle autre table.

Avant de commencer

Rôle requis : sec_cmn.write

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Utilités** > **Mappage de champs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

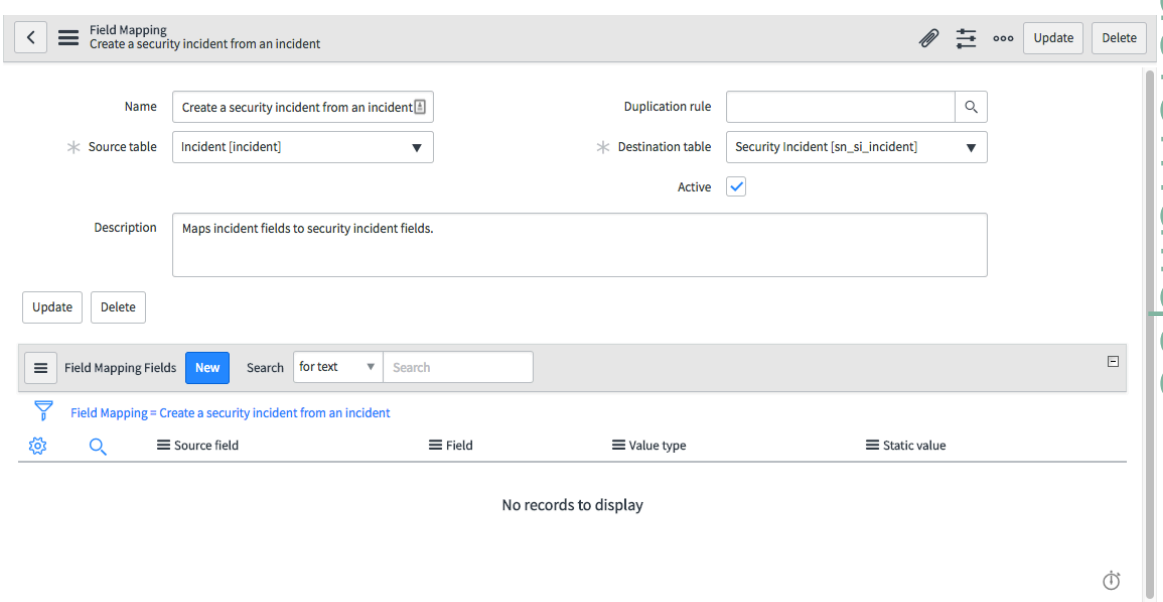
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de champs

Champ	Description
Nom	Nom de la carte de champs.
Table source	Table qui fournit les données à utiliser pour créer un enregistrement dans la table de destination.
Règle de duplication	Régit la manière de gérer les enregistrements sources susceptibles de générer un enregistrement en double. Pour plus d'informations, consultez Transformation des données partagées.
Table de destination	Table dans laquelle les nouveaux enregistrements sont créés.
Actif	Cochez cette case pour activer le mappage. **Remarque :** Un seul mappage entre les tables peut être actif à la fois. Si deux cartes contiennent les mêmes tables, l'ancienne version est automatiquement désactivée.
Description	Description de la carte de champs.

4. Lorsque vous avez terminé vos saisies, faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
   L'onglet Champs de mappage de champs s'affiche. Cet enregistrement définit les données qui sont placées dans le champ cible, dans les enregistrements créés par cette transformation de champ.



5. Cliquez sur **Nouveau**.
6. Renseignez les champs du formulaire comme il convient.

Option	Description
Champ	**Description**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Stocker la valeur dans un champ ou une liste connexe	Sélectionnez où trouver la valeur. Les choix sont les suivants : ◦ Ajouter une nouvelle valeur dans un champ de l'enregistrement ◦ Lier à cette valeur dans une liste connexe ◦ Lier à cette valeur, ce qui crée un enregistrement si un enregistrement correspondant n'existe pas **Remarque :** Si la table de destination ne possède aucune liste connexe, ce champ n'est pas affiché.
Champ	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Ajouter une nouvelle valeur dans un champ de l'enregistrement** , ce champ spécifie le champ à renseigner. **Remarque :** Pour les champs de choix, les correspondances avec les choix existants sont établies à l'aide de l'étiquette ou de la valeur de choix sous-jacente. Si aucune correspondance n'est trouvée, le champ est défini, mais aucune nouvelle entrée n'est ajoutée à la liste de choix. Pour plus d'informations, consultez Listes de choix . Pour les champs de référence, une entrée n'est définie que lorsqu'une valeur correspondant au nom d'affichage de l'enregistrement ou à`un sys_id` valide est trouvée. Pour plus d'informations, consultez Champs de référence .
Liste connexe	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou **Lier à cette valeur, la création d'un nouvel enregistrement si aucun enregistrement correspondant n'existe**, ce champ spécifie la liste connexe à laquelle ajouter des informations.
Champ de valeur	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou **Lier**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	à cette valeur, créant un nouvel enregistrement si aucun enregistrement correspondant n'existe, ce champ spécifie le champ dans la table affichée dans la liste connexe, qui est utilisé pour rechercher et rechercher un enregistrement existant. Par exemple, si votre liste connexe est celle **des CI affectés**, ce champ peut contenir **le nom** ou le **nom de domaine complet**, ou tout autre champ de l'enregistrement de CI qui doit être utilisé pour rechercher le CI est ajouté à la liste **des CI affectés** .
Données de relation	Lorsque la **valeur stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe**, un nouvel enregistrement est créé pour lier cet enregistrement (comme un incident de sécurité) à la valeur (un CI, un observable, etc.). Ce champ spécifie toutes les informations supplémentaires (paires de champs et de valeurs) qui doivent être ajoutées à cet enregistrement de liaison. Par exemple, en ajoutant un observable pour une adresse IP source, vous pouvez spécifier que cette adresse IP est l'adresse IP source, plutôt que l'adresse IP de destination. Pour plusieurs valeurs, utilisez un séparateur ^, par exemple, type= Source IP^active=true.
Données de nouvel enregistrement	**Lorsque la valeur stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur, un nouvel enregistrement est créé si aucun enregistrement correspondant n'existe, si aucun enregistrement** associé correspondant à la valeur analysée n'est trouvé, un nouvel enregistrement est créé. Ce champ spécifie les données statiques à ajouter à cet enregistrement. Par exemple, pour **les CI affectés**, si nous ne trouvons pas le CI, ce paramètre indique qu'un nouveau CI est créé). La valeur trouvée dans l'enregistrement source est définie sur le champ **Valeur** dans l'enregistrement CI. Vous pouvez définir des données supplémentaires : une note indiquant pourquoi ce CI a été créé, des informations sur le type de CI avec lequel vous travaillez. Voici un exemple : `description=Créé par un programme malveillant rapport d'incident^type=autodetect`
Séparateur de valeur	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	cette valeur dans une liste connexe ou **Lier à cette valeur, la création d'un nouvel enregistrement si aucun enregistrement correspondant n'existe**, ce champ spécifie le séparateur à utiliser pour les listes d'éléments, généralement une virgule ou un point-virgule.
Type de valeur	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Ajouter une nouvelle valeur dans un champ de l'enregistrement** , ce champ spécifie le type de valeur. Les choix sont les suivants : ◦ **Enregistrement du champ source** ◦ **Ajouter au champ en tant que nouvelle ligne** ◦ **Valeur statique** ◦ **Valeur statique plus valeur du champ d'enregistrement source**
Champ source	Choisissez le champ source qui contient la valeur à placer dans le champ de destination ou dans la liste connexe sélectionnée.
Champ statique	Valeur statique pour le champ.
Transformation de valeur	Choisissez l'entrée de transformation de la valeur de champ à appliquer. Il est utilisé pour mapper les champs de choix entre les enregistrements, par exemple, en convertissant le jeu de choix de **catégorie** pour un incident de sécurité en champ **Type** approprié pour une demande de changement.
Table de destination	Renseigné automatiquement avec la table de destination.
Mappage de champs	Renseigné automatiquement avec la carte de champs parent.
Table source	Renseigné automatiquement avec la table source.

7. Cliquez sur **Envoyer**.

Opérations de sécurité Transformations de valeurs de champs

Transforme les valeurs de champ client uniques en valeurs de champ reconnues par Opérations de sécurité l'analyse des e-mails, l'enrichissement des données ou les tables utilisant des cartes de champs. Prend en charge les champs de choix, les références et aligne les données externes sur la terminologie et le format standard de votre nouvel enregistrement.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez mapper des données pour des champs tels que Catégorie, État ou Groupe d'affectation dans les valeurs utilisées dans la table Security Operations. Par exemple, mappez « En cours d'analyse » vers « Travail en cours ».

Créer des Opérations de sécurité transformations de valeurs de champ

L'option Transformations de valeurs de champs définit une transformation entre les données sources fournies et la valeur de remplacement à utiliser.

Avant de commencer

Rôle requis : sn_sec_cmn.basic ou sn_si.basic

Pourquoi et quand exécuter cette tâche

Définissez chaque entrée de transformation à appliquer soit lorsqu'il y a une correspondance avec la valeur de recherche, soit lorsque la valeur de recherche est contenue dans les données sources fournies, soit lorsqu'aucune correspondance n'est trouvée. Définissez une valeur par défaut lorsqu'aucune correspondance n'est trouvée. Si aucune valeur par défaut n'est définie et qu'aucune correspondance n'est trouvée, les données sources d'origine sont utilisées.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Utilités** > **Transformations de valeurs de champs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Transformations de valeurs de champs

Champ	Description
Nom	Nom de la transformation de la valeur de champ.
Description	Description de la carte de champs.
Entrées de transformation de la valeur de champ	Liste des entrées dans la table. **a.** Sous **Remplacer les données**, double-cliquez sur « Insérer une nouvelle ligne ». **b.** Choisissez l'une des options suivantes : Lorsque la date de ce champ correspond à Lorsque les données de ce champ contiennent Lorsqu'aucune autre entrée de transformation ne correspond aux données (par défaut) **c.** Cliquez sur la coche verte. **d.** Double-cliquez sous **Valeur de recherche**, ajoutez votre valeur de recherche. **e.** Cliquez sur la coche verte. **f.** Double-cliquez sous **Valeur de remplacement** , puis ajoutez la ServiceNow valeur correspondante. **g.** Répétez l'opération si nécessaire.
Actif	Cochez cette case pour activer la transformation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Périmètre de l'application.

4. Cliquez sur **Envoyer**.

Opérations de sécurité Mappage des données d'enrichissement

Mappage des données d'enrichissement transforme les données de XML, JSON ou Propriétés de fichiers en ServiceNow enregistrements. Opérations de sécurité Les workflows utilisent des cartes de données d'enrichissement et fournissent des données de sortie aux incidents de sécurité.

Opérations de sécurité comprend plusieurs cartes de données d'enrichissement, déclenchées par divers workflows, par exemple, Workflow Security Operations Integrations - Obtenir les statistiques réseau et Intégration des commandes système Security Operations : workflow Obtenir les processus en cours d'exécution. La sortie de la carte de données d'enrichissement à partir Opérations de sécurité des workflows est affichée dans l'onglet **Données d'enrichissement** du formulaire d'incident de sécurité.

Créer une Opérations de sécurité carte de données d'enrichissement

Transformez les données au format JSON, XML ou Propriétés fichier en enregistrements à ServiceNow l'aide de cartes de données d'enrichissement.

Avant de commencer
Rôle requis : sn_sec_cmn.write

Pourquoi et quand exécuter cette tâche
Les cartes de données d'enrichissement existantes sont utilisées par les workflows fournis dans Opérations de sécurité. Vous pouvez afficher la liste sous **Mappage des données d'enrichissement**. Pour utiliser une carte, vous avez besoin d'un déclencheur, soit une règle métier, soit un workflow.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Utilités** > **Mappage des données d'enrichissement**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs comme il convient.

Création d'une carte de données d'enrichissement

Champ	Description
Nom	Nom de ce mappage de données d'enrichissement.
Format d'entrée	Choisissez un format dans la liste : JSON (par défaut) XML Format du fichier de propriétés
Clé de préfixe	Utilisez cette propriété pour limiter le jeu de données d'entrée à une clé spécifiée. La racine de l'ensemble de données

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d'entrée est définie sur cette clé. Dans cet exemple, si vous avez saisi file_info, les valeurs d'entrée seront limitées aux valeurs comprises dans file_info. <?xml version="1.0" encoding="UTF-8"?> <malware> <version>2.0</version> <file_info> <malware>yes</malware> <sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1> <filetype>PE</filetype> <sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a930</sha256> <md5>ee8c91751b3010e38c479cf9ab09827a</md5> <size>546304</size> </file_info> </malware>
Application	Périmètre de l'application.
Règle de duplication	Règle définissant quand un enregistrement est considéré comme un doublon et quelles actions effectuer avec les enregistrements dupliqués.
Table de destination	Choisissez une table dans la liste.
Actif	Cochez cette case pour activer la carte.
Description	Entrez une description de la carte des données d'enrichissement.

4. Cliquez sur **Envoyer**.
   L'onglet Champs de mappage des données d'enrichissement s'affiche.
5. Cliquez sur **Nouveau**.
6. Renseignez les champs du formulaire comme il convient.

Champs de mappage des données d'enrichissement

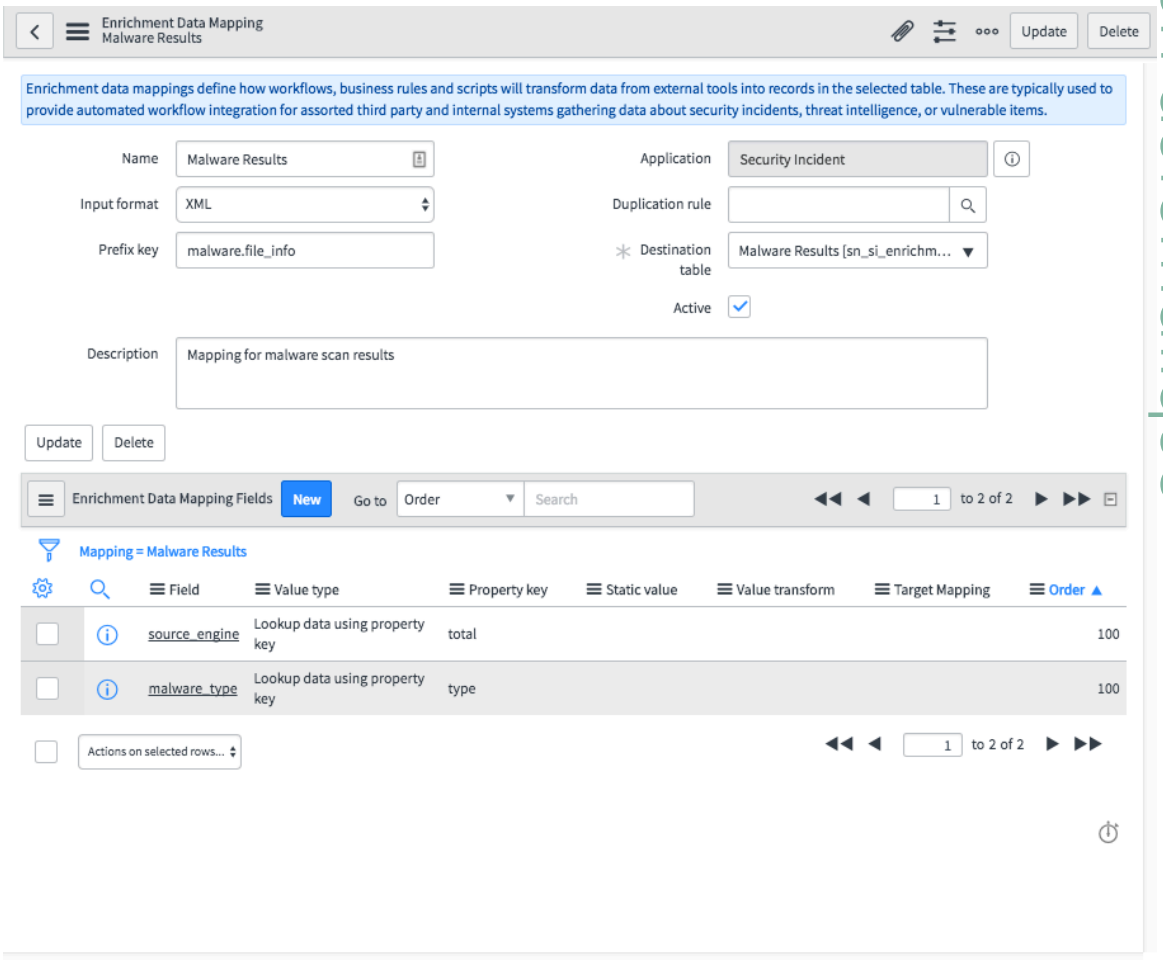
Champ	Description
Champ	Nom du mappage de données d'enrichissement.
Type de valeur	Choisissez dans la liste : Rechercher des données à l'aide de la clé de propriété Valeur statique

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Valeur statique plus données de la clé de propriété Le champ est un tableau ou un objet (imbrication de données brutes) Chaque choix a des entrées différentes. Les valeurs de champ et les tableaux ou objets nécessitent une clé de propriété.
Clé de propriété	Détermine la clé de recherche des données d'entrée et la valeur écrite dans le champ cible.
Transformation de valeur	Transformation de la valeur de champ qui mappe une valeur à une autre.
Application	Périmètre de l'application.
Ordre	Dans quel ordre considérer le mappage. La première correspondance est utilisée. La valeur par défaut est 100.
Mappage	Nom du mappage de données d'enrichissement.
Table de destination	Table vers laquelle les champs à mapper vont.

7. Cliquez sur **Envoyer**.
   Voici un exemple de mappage de données d'enrichissement.



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opérations de sécurité Escalade définie par l'utilisateur

Vous pouvez créer un parcours d'escalade des incidents de sécurité pour les problèmes nécessitant une plus grande attention ou une expertise. Une fois qu'un groupe d'escalade existe, un bouton apparaît sur tous les incidents de sécurité de ce groupe.

Créer un groupe d'escalade Opérations de sécurité défini par l'utilisateur

Escaladez un incident de sécurité jusqu'à n'importe quel groupe associé à l'incident à l'aide des escalades.

Avant de commencer

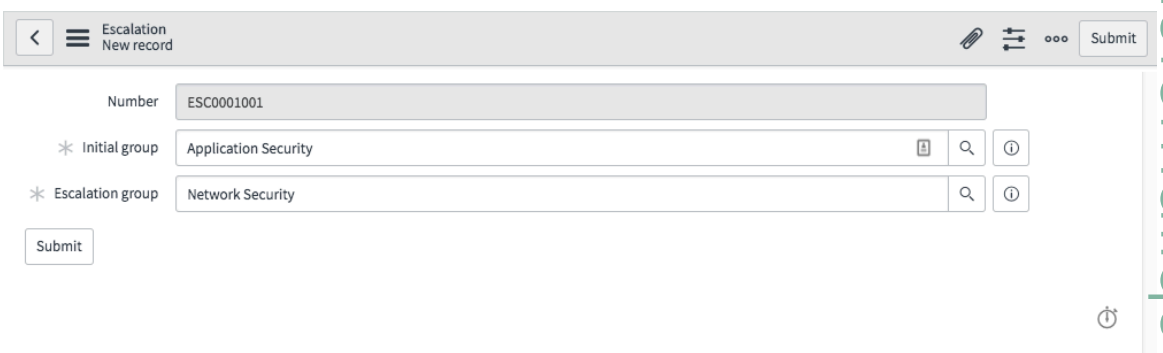
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Groupes** > **Escalades**.
2. Cliquez sur**Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Escalades

Champ	Description
Numéro	Numéro d'incident d'escalade (champ généré automatiquement).
Groupe initial	Sélectionnez le groupe auquel appartient cet incident de sécurité.
Groupe d'escalade	Sélectionnez le groupe auquel escalader l'incident de sécurité.

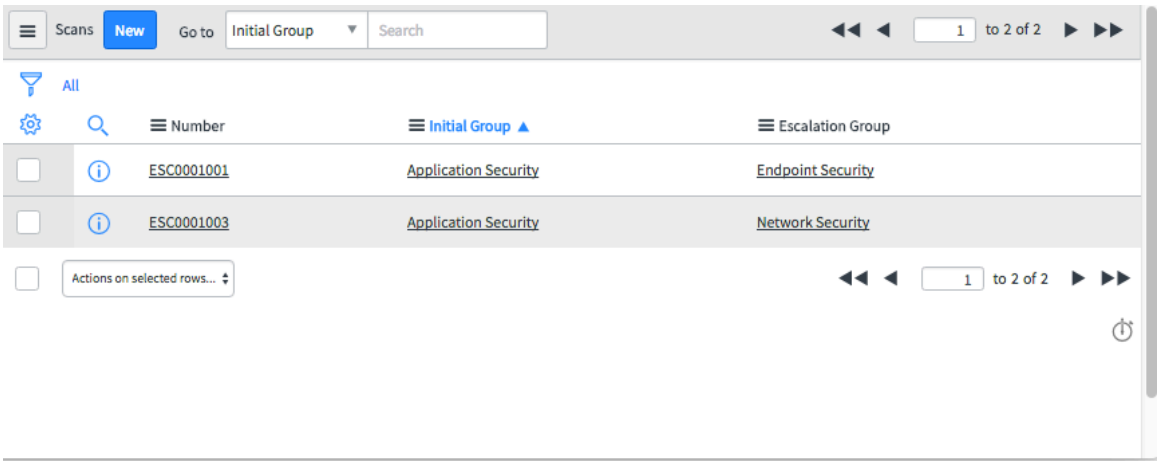


4. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un groupe d'escalade est disponible pour tous les incidents de sécurité dans le groupe initial. Vous pouvez créer plusieurs groupes.



Créer des remplacements de propriété séparés par domaine

Lorsque vous utilisez Séparation de domaine, vous pouvez créer des remplacements des propriétés des opérations de sécurité existantes qui vous permettent de personnaliser les fonctions des applications dans chacun de vos domaines.

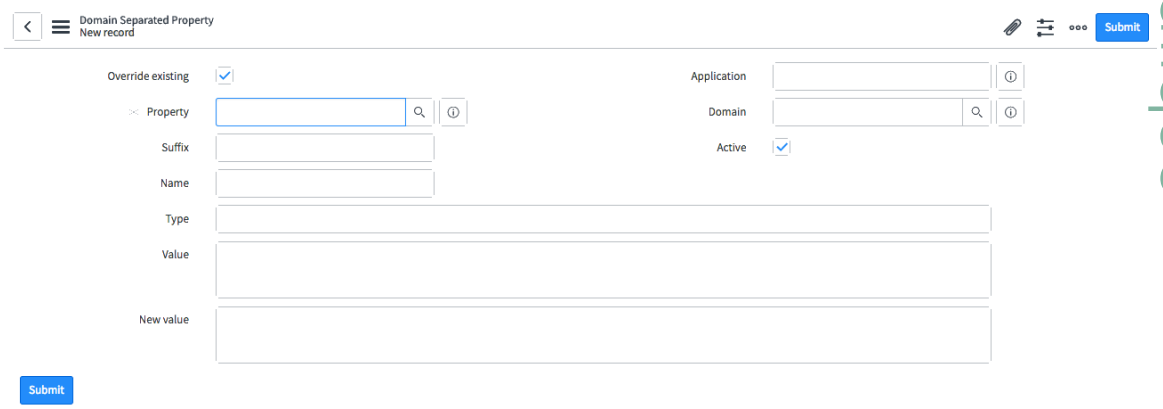
Avant de commencer

Nécessite l'activation de l'option Prise en charge de domaine : extensions de domaine .
Vous pouvez également en savoir plus sur la visionneuse de remplacement de domaine .

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Utilités** > **Propriétés séparées par les domaines**.
2. Cliquez sur **Nouveau**.



3. Renseignez les champs du formulaire.

Formulaire de propriété Séparation de domaine

Champ	Description
Remplacer l'existant	Cochez cette case pour créer une valeur spécifique au domaine pour une propriété existante.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Sélectionnez l'application qui contient la propriété que vous souhaitez remplacer.
Propriété	Sélectionnez la propriété de l'application sélectionnée pour laquelle vous souhaitez créer un remplacement spécifique au domaine.
Domaine	Sélectionnez le domaine pour lequel vous créez ce remplacement de propriété.
Actif	Activez ou désactivez le remplacement.
Suffixe	Affiche le suffixe de la propriété.
Nom	Affiche le nom de la propriété.
Type	Affiche le type de propriété.
Valeur	Affiche la valeur actuelle définie pour la propriété.
Nouvelle valeur	Entrez une nouvelle valeur pour la propriété à appliquer à ce domaine.

4. Cliquez sur **Envoyer**.
   Le remplacement de propriété est appliqué à la propriété sélectionnée dans le domaine spécifié. Lorsque la logique de cette propriété est déclenchée, le système recherche les remplacements de propriétés séparées par domaine. Si un contournement pour le domaine est trouvé, la nouvelle valeur est utilisée. Sinon, la valeur du domaine par défaut est utilisée.

Information associée

Présentation de Séparation de domaine

Créer un groupe de systèmes d'exploitation

Les groupes de systèmes d'exploitation sont utilisés pour mapper un système d'exploitation à des types de processus et à des scripts spécifiques dans Réponse aux incidents de sécurité les workflows. Les scripts définissent la façon dont les processus en cours d'exécution pour les groupes de systèmes d'exploitation définis sont récupérés. De nouveaux systèmes d'exploitation peuvent être ajoutés selon les besoins.

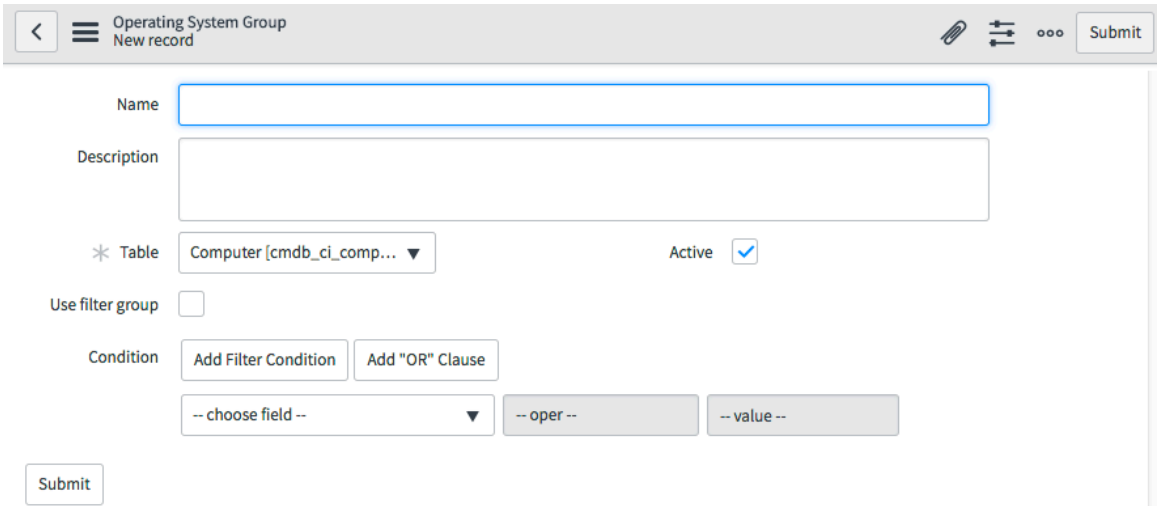
Avant de commencer

Rôle requis : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Utilités** > **Groupes de systèmes d'exploitation**.
   Le système de base comprend des scripts pour trois systèmes d'exploitation :
   - Système d'exploitation basé sur BSD
   - Système d'exploitation basé sur POSIX
   - Système d'exploitation Windows
2. Cliquez sur **Nouveau**.

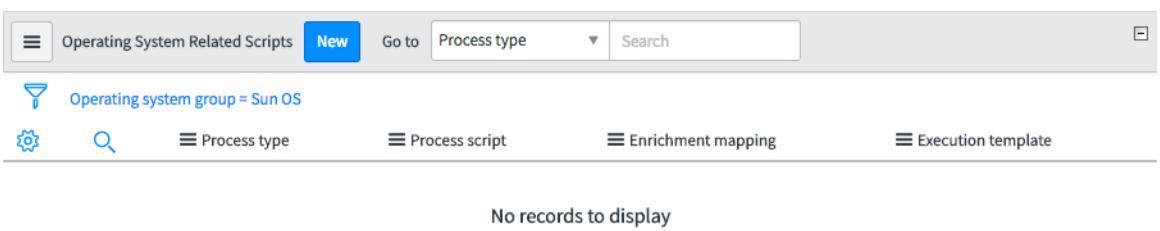
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom du groupe de systèmes d'exploitation.
Description	Description du groupe de systèmes d'exploitation.
Table	Table affectée.
Actif	Cochez cette case pour activer le groupe de systèmes d'exploitation.
Utiliser un groupe de filtres	Activez cette case à cocher pour utiliser un groupe de filtres afin de localiser les enregistrements correspondants dans la table sélectionnée.
Groupe de filtres	Sélectionnez le groupe de filtres pour localiser les enregistrements correspondants dans la table sélectionnée. Ce champ s'affiche uniquement si vous avez coché la case **Utiliser un groupe de filtres** .
Condition	Le champ Les champs Générateur de conditions s'affichent uniquement si vous n'avez pas coché la case **Utiliser un groupe de filtres**.

4. Faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
La liste connexe Scripts associés au système d'exploitation s'ouvre.



5. Cliquez sur **Nouveau**.

6. Sélectionnez les scripts qui correspondent aux workflows que vous utilisez pour obtenir des statistiques d'exécution sur les processus, les services et/ou le réseau.

7. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Joindre un fichier de script à un fichier synchronisé Serveur MID

Configurer des groupes et des balises de sécurité

Vous pouvez affecter des balises aux incidents de sécurité, aux tâches de réponse, aux éléments vulnérables, aux observables, aux IoC et aux tickets de sécurité afin de créer des métadonnées sur l'enregistrement répondant et de définir qui doit avoir accès à des types spécifiques de contenu de sécurité. Les balises peuvent être ajoutées aux groupes de sécurité pour les organiser.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Balises de sécurité** > **Groupes**.
   Trois groupes de classification par défaut sont inclus dans le système de base.
   - **Liste d'autorisation d'enrichissement/liste de refus** : ce groupe définit si un enregistrement doit être traité comme un enregistrement de liste d'autorisation ou de liste de refus. Les enregistrements de liste d'autorisation sont généralement moins importants et peuvent donc être ignorés. Les enregistrements de liste de refus présentent généralement un intérêt plus élevé.
   - **Balise META** : ce groupe est fourni en tant que données de démonstration. Vous pouvez l'utiliser pour créer des balises de classification personnalisées qui sont utilisées par les applications des opérations de sécurité.
   - **Traffic Light Protocol (Protocole de feux tricolores**) : ce groupe est utilisé pour s'assurer que les informations sensibles sont partagées avec le bon public. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité. Pour chaque couleur, vous pouvez attribuer les rôles d'accès en lecture/écriture appropriés. Lors du partage d'observables avec un cercle de sécurité approuvé, la balise affectée au profil de cercle de sécurité approuvé détermine quels observables balisés TLP peuvent être partagés avec le cercle, comme suit :
     - **TLP : BLANC :** Seuls les observables avec TLP :WHITE peuvent être partagés avec un profil TLP :WHITE.
     - **TLP : VERT :** Les observables avec TLP :GREEN et TLP :WHITE peuvent être partagés dans un profil TLP :GREEN.
     - **TLP : AMBRE :** Les observables avec TLP : AMBER, TLP : GREEN et TLP : WHITE peuvent être partagés dans un profil TLP : AMBER.
     - **TLP : ROUGE :**Tous les observables, quelle que soit leur balise TLP, peuvent être partagés avec un profil TLP :RED, car TLP :RED est la balise TLP la mieux classée.

     Remarque : Vous pouvez ajouter d'autres couleurs TLP, mais toutes les couleurs en plus des quatre couleurs incluses sont considérées comme non valides par le Forum pour les équipes de sécurité et de réponse aux incidents (FIRST).
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Entrez le nom du groupe de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Autoriser les sélections multiples	Cochez cette case si vous souhaitez pouvoir attribuer plusieurs balises de sécurité à un enregistrement qui partage un groupe.
Actif	Activer ou désactiver le groupe.
Description	Entrez une description de ce groupe.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**. La liste connexe des balises de sécurité s'affiche.
5. Dans la liste connexe Balises de sécurité, cliquez sur **Nouveau**.
6. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom de la balise de classification.
Groupe de balises de sécurité	Si la balise a été créée à l'aide du bouton **Nouveau** dans la liste connexe du groupe, ce champ est défini par défaut sur le groupe actuel. Si nécessaire, vous pouvez ajouter la balise à un autre groupe, mais cette option est facultative.
Ordre	Spécifier l'ordre dans lequel la balise apparaît sur les formulaires ou dans une liste.
Couleur	Sélectionnez la couleur de cette balise.
Appliquer l'accès restreint	Cochez cette case pour affecter les rôles de lecture et/ou d'écriture nécessaires aux utilisateurs pour lire ou écrire dans les enregistrements qui comportent cette balise de sécurité.
Actif	Activez ou désactivez la balise.
Description	Description de cette balise.
Rôles (accès en lecture)	Pour attribuer l'accès en lecture à une balise de sécurité, cliquez sur l'icône de verrouillage, sélectionnez les rôles d'accès appropriés, puis cliquez à nouveau sur l'icône de verrouillage. Ce champ s'affiche uniquement si vous avez coché la case **Appliquer l'accès restreint** .
Rôles (accès en écriture)	Pour attribuer l'accès en écriture à une balise de sécurité, cliquez sur l'icône de verrouillage, sélectionnez les rôles d'accès appropriés, puis cliquez à nouveau sur l'icône de verrouillage. Ce champ s'affiche uniquement si vous avez coché la case **Appliquer l'accès restreint** .

7. Répétez l'opération autant de fois que nécessaire pour créer d'autres balises de sécurité.
8. Cliquez sur **Mettre à jour**.

Remarque : Vous pouvez également créer de nouvelles balises en accédant à **Security Operations** > **Balises de sécurité** > **Balises**. La procédure est la même.

Créer des règles de balise de sécurité

Les règles de balise de sécurité permettent de filtrer l'accès aux balises de sécurité.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Balises de sécurité** > **Balises**.
2. Choisissez ou créez une balise de sécurité.
3. Dans l'onglet **connexe Règles de balise de sécurité** , cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom de la règle de balise de sécurité.
Balise de sécurité	La balise de sécurité à joindre à la règle.
Actif	Activez ou désactivez la balise de sécurité.
Description	Description de cette règle.

5. Déterminez **le filtrage des enregistrements.**
6. Renseignez les champs du formulaire comme il convient.

Champ	Description
Utiliser un groupe de filtres	Associe le groupe de filtres à la règle.
Table	La table qui doit contenir la règle.
Condition	Ajoutez une ou plusieurs conditions de filtre.

7. Cliquez sur **Envoyer**.

Importer les règles de balise de sécurité

Vous pouvez importer des règles de balise de sécurité à partir d'autres tables de votre déploiement.

Avant de commencer

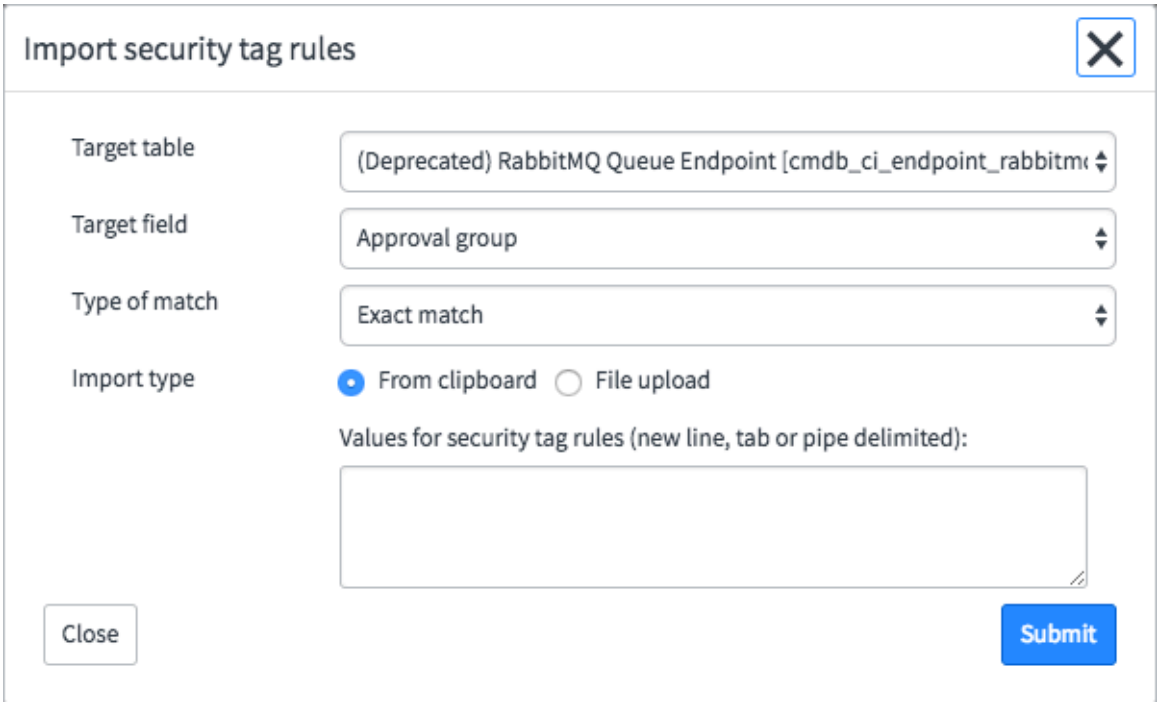
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Balises de sécurité** > **Balises**.
2. Choisissez ou créez une balise de sécurité.
3. Cliquez sur le lien connexe **Importer les règles de balise de sécurité** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Table cible	Choisissez la table à utiliser pour importer des règles.
Champ cible	Choisissez le champ à utiliser pour importer les règles.
Type de correspondance	Choisissez comment faire correspondre les règles importées aux **balises de sécurité** à partir de : Correspondance exacte (par défaut) Contient Commence par Se termine par Expression régulière
Type d'importation	Choisir: À partir du presse-papiers Copiez une liste de valeurs délimitées dans la zone de texte. Les valeurs sont analysées en balises de sécurité. À partir du chargement du fichier Chargez un fichier avec des valeurs délimitées. Les valeurs sont analysées en balises de sécurité. Ajoutez des valeurs pour les règles de balise de sécurité à l'aide de délimiteurs de nouvelle ligne ou de barre verticale.

5. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Annotations de sécurité

Une annotation de sécurité est une note d'explication ou de commentaires ajoutée à un élément de configuration, à un observable ou à une utilisation sur un incident de sécurité.

Plusieurs annotations de sécurité sont disponibles pour les utilisateurs et les observables (nécessite le module d'extension Renseignements sur les menaces). Des rapports sur les annotations de sécurité sont également disponibles.

Créer des annotations de sécurité pour les CI

Les annotations sur les CI vous permettent de suivre l'activité des incidents. Vous pouvez ajouter des annotations à un ou plusieurs CI.

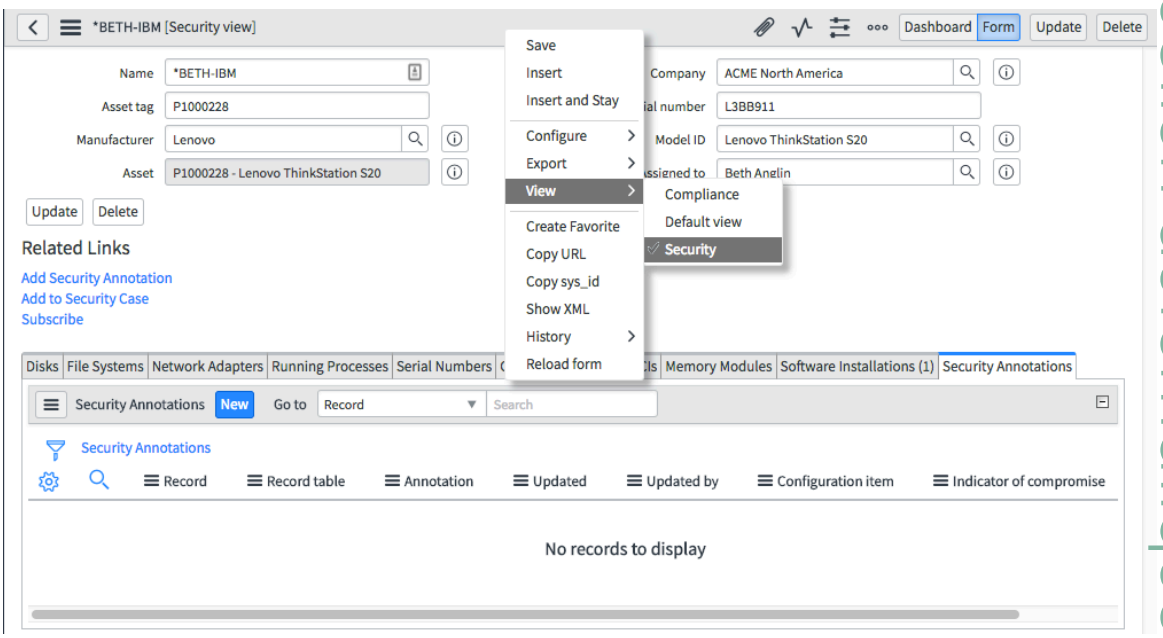
Avant de commencer

Rôle requis : administrateur

Procédure

1. À partir d'un incident de sécurité ou de la table d'éléments de configuration, ouvrez un CI.

2. Faites un clic droit dans l'en-tête, puis choisissez **Vue** > **Sécurité**.



3. Dans l'onglet de la liste connexe **Annotations de sécurité** , cliquez sur **Nouveau**.

4. Saisissez une annotation.
Les annotations peuvent être dans n'importe quel format texte.

5. Cliquez sur **Envoyer**.

> **Remarque :** Vous pouvez ajouter la même annotation à plusieurs CI en sélectionnant des CI dans la liste, en choisissant **Ajouter une annotation de sécurité**, en saisissant une annotation dans n'importe quel format texte, puis en cliquant sur **Soumettre**.

Créer des annotations de sécurité pour les observables

Vous pouvez sélectionner un ou plusieurs observables et leur appliquer des annotations de sécurité à l'aide du menu de choix **Actions sur les lignes sélectionnées** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

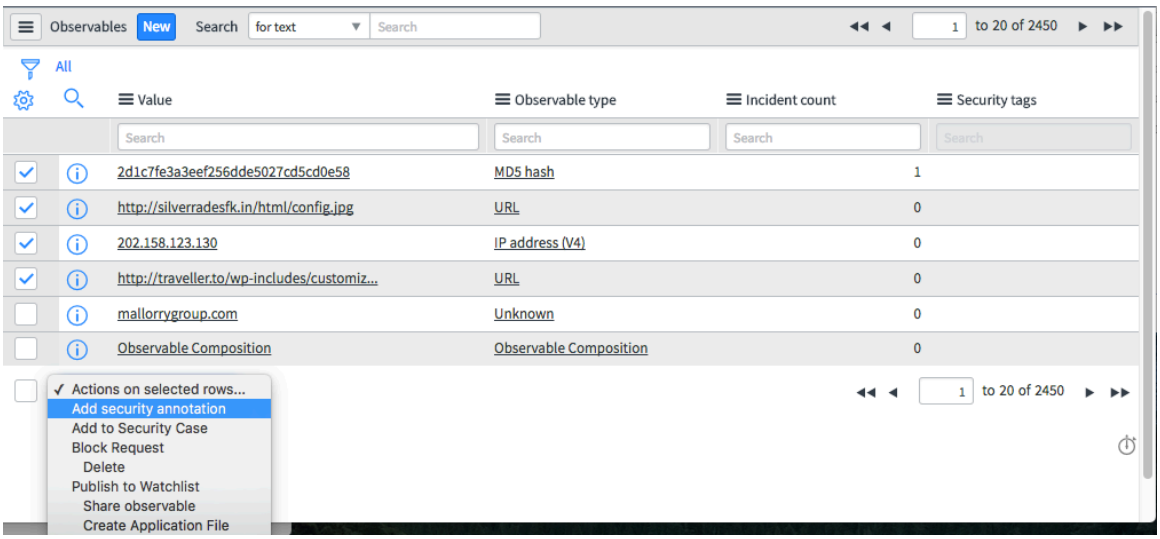
Avant de commencer

- Nécessite le module d'extension et l'activation Renseignements sur les menaces . Le module d'extension Renseignements sur les menaces est disponible sous la forme d'un abonnement distinct.

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Renseignements sur les menaces** > **Observables**
2. Sélectionnez un ou plusieurs observables dans la liste.
3. Dans le menu déroulant **Actions sur les lignes sélectionnées** , choisissez **Ajouter une annotation de sécurité**.



4. Saisissez une annotation.
   Les annotations peuvent être dans n'importe quel format texte.
5. Cliquez sur **Envoyer**.

Créer des annotations de sécurité pour les utilisateurs

Vous pouvez sélectionner un ou plusieurs utilisateurs et leur appliquer des annotations de sécurité à l'aide du menu de choix **Actions sur les lignes sélectionnées** .

Avant de commencer

Nécessite le module d'extension et l'activation Renseignements sur les menaces . Le module d'extension Renseignements sur les menaces est disponible sous la forme d'un abonnement distinct.

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Utilisateurs**
2. Sélectionnez un ou plusieurs utilisateurs dans la liste.
3. Dans le menu déroulant **Actions sur les lignes sélectionnées** , choisissez **Ajouter une annotation de sécurité**.
4. Saisissez une annotation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les annotations peuvent être dans n'importe quel format texte.

5. Cliquez sur **Envoyer**.

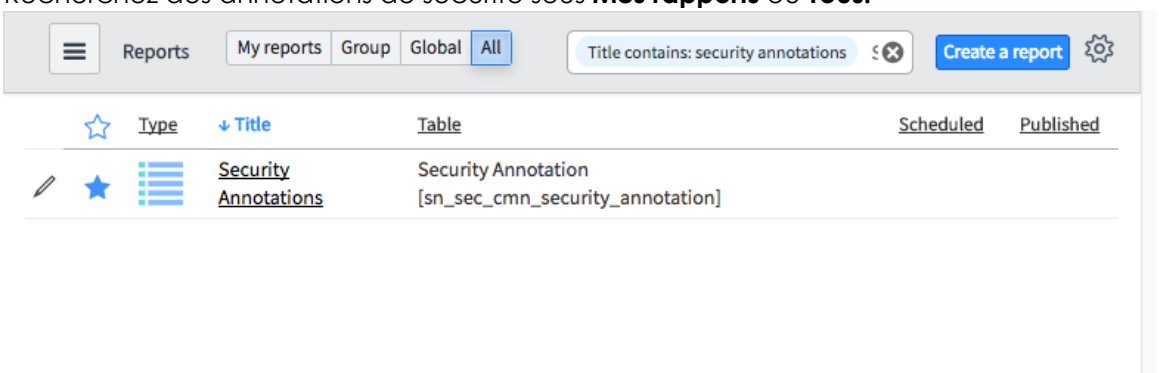
Afficher les rapports d'annotations de sécurité

Le rapport Annotations de sécurité présente les détails stockés dans la table Annotations de sécurité [sn_sec_cmn_security_annotations]. Vous pouvez personnaliser les colonnes du rapport et regrouper les données comme bon vous convient.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Rapports** > **Afficher/Exécuter**.
2. Recherchez des annotations de sécurité sous **Mes rapports** ou **Tous.**



Information associée

Afficher la liste des rapports

Composants installés avec Security Support Common

Plusieurs types de composants sont installés avec Security Support Common. Ils fournissent des fonctionnalités communes à utiliser dans les différentes applications de sécurité, telles que Réponse aux incidents de sécurité.

Localisation et affichage des composants installés

Pour plus d'informations sur la localisation et l'affichage des composants installés, reportez-vous Afficher les composants installés avec Security Support Common à la section

Afficher les composants installés avec Security Support Common

Plusieurs types de composants sont installés lorsque vous activez le module d'extension, notamment mais sans s'y limiter, les tables, les rôles d'utilisateur et les Security Support Common modules.

Localisation des composants

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Si vous souhaitez limiter la liste des composants installés aux rôles, travaux planifiés et tables pour l'application Security Support Common, procédez comme suit :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les listes filtrées pour les composants installés avec une application

Filtrez la table Fichiers d'applications afin que seuls les rôles, les travaux planifiés et les tables installés avec une application s'affichent. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés sur l'instance et dans la table de métadonnées. Procédez comme suit pour afficher les listes filtrées à partir de la table Fichiers d'applications.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, cliquez sur **ET**, puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Rechercher Opérations de sécurité

Vous pouvez trouver rapidement des informations dans n'importe quelle Opérations de sécurité application à l'aide de l'icône de recherche dans l'en-tête de l'écran. Zing est le moteur d'indexation et de recherche de texte qui effectue toutes les recherches de texte dans votre instance.

Avant de commencer

Rôle requis : sn_si.read ou supérieur

Procédure

1. Cliquez sur l'icône de recherche ( ) dans le coin supérieur droit de l'écran.
2. Saisissez les critères que vous souhaitez utiliser pour effectuer la recherche, puis appuyez sur **Entrée**.
   si vous avez activé le module d'extension Réponse aux incidents de sécurité , les critères de recherche que vous avez saisis présentent tout texte de description brève, CI, adresse IP ou URL correspondant dans vos incidents de sécurité, Réponse aux incidents de sécurité tâches ou demandes de sécurité. Si les modules d'extension Réponse aux vulnérabilités ou Renseignements sur les menaces sont activés, les résultats de la recherche incluent les vulnérabilités, les éléments vulnérables, les entrées vulnérables, les observables, les IoC et les modes/méthodes d'attaque.

Information associée

Introduction à la recherche

Recherche de texte Zing

Référence de Security Operations Integrations

Les développeurs et les partenaires ServiceNow peuvent utiliser les informations de cette section pour mieux comprendre les fonctionnalités sous-jacentes des intégrations tierces, y compris les directives de développement, les options d'intégration et les workflows.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Opérations de sécurité Directives de développement de l'intégration

La ServiceNow plate-forme fournit plusieurs mécanismes pour développer des intégrations avec des systèmes externes. La ServiceNow Opérations de sécurité suite de produits ajoute des fonctionnalités d'intégration destinées à rationaliser le processus d'intégration avec des systèmes externes axés sur la sécurité.

La plupart des concepts abordés dans ce guide supposent une certaine familiarité avec les fonctionnalités standard ServiceNow . Pour s'intégrer à la Opérations de sécurité suite, une connaissance minimale des concepts suivants ServiceNow est requise :

- Includes de script
- Services Web entrants/sortants
- Sources de données
- Numéros des jeux d'importation
- Cartes de transformation

Programme de partenariat technologique

Toutes les exigences relatives à la certification des applications ou les directives données dans la documentation du programme de partenariat technologique remplacent les informations contenues dans ce guide. Ce guide ne remplace pas la documentation du programme de partenariat technologique et sert uniquement de complément à la documentation existante.

Pour plus d'informations, consultez l'article de blog sur le cours de formation du programme de partenariat technologique .

Types d'intégrations ServiceNow fournies

Les Opérations de sécurité applications (Réponse aux incidents de sécurité, Renseignements sur les menaceset Réponse aux vulnérabilités) peuvent être intégrées de manière transparente à d'autres ServiceNow applications pour améliorer leurs fonctions.

Les intégrations suivantes sont fournies dans le système de Opérations de sécurité base.

Intégration de Security Incident Response – Event Management

Les options de l'application Gestion des événements ont été étendues pour prendre en charge Réponse aux incidents de sécurité. Le Réponse aux incidents de sécurité Gestion des événements module d'extension de support analyse automatiquement le contenu des événements pour Gestion des événements renseigner les champs dans les incidents de sécurité.

Cas d'utilisation couvert :

Création d'événements de sécurité dans le Gestion des événements système à partir d'outils d'information et Gestion des événements de sécurité (SIEM)

Options utiles fournies :

- Fonctionnalité de gestion des événements : corrélation d'événements, règles d'événements et règles d'alerte
- Mappage automatique des valeurs de additional_information à l'incident de sécurité résultant

Ressources:

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation d'assistance Security Incident Event Management

Documentation de Gestion des événements

Réponse aux incidents de sécurité : intégration de l'API de jeu d'importation

En plus de l'utiliser Gestion des événements pour transmettre par push des événements liés à la sécurité, l'application Réponse aux incidents de sécurité fournit une API de jeu d'importation qui permet la création directe d'incidents de sécurité. Le point de terminaison REST pour le jeu d'importation des incidents de sécurité est http://localhost:8080/api/now/import/sn_si_incident_import.

Cette technique d'intégration est utile lorsque a) Gestion des événements n'est pas installé, ou b) il est souhaité de créer simplement des incidents de sécurité sans passer par le flux d'alerte > d'incident de sécurité d'événement > qui est requis lors de l'utilisation Gestion des événementsde .

Cas d'utilisation couvert :

Création d'incidents de sécurité directement à partir des outils SIEM.

Options utiles fournies :

Correspondance automatique des CI lors de la création d'un incident de sécurité sur la base d'une adresse IP, d'un NetBIOS ou d'un nom de domaine complet.

Ressources:

Documentation de l'API Import Set de plateforme

Documentation des ensembles de données à importer des services Web d'incident de sécurité

Threat Intelligence : rechercher l'intégration de la source

Les sources de recherche offrent la possibilité d'envoyer des données à des sources de recherche externes pour déterminer si ces données sont malveillantes. Généralement, ces données sont une adresse IP, une URL, un fichier ou un hachage de fichier.

Cas d'utilisation couvert :

Recherchez une adresse IP, une URL, un fichier ou un hachage avec un service de recherche externe.

Options utiles fournies :

- Manière cohérente de demander des recherches à partir d'éléments de catalogue et d'incidents de sécurité.
- Capacités de limitation et d'étranglement des débits fournies avec peu ou pas de codage.
- Création automatique d'entrées observables d'indicateurs de compromis (IoC) pour tous les problèmes détectés par les sources de recherche.

Threat Intelligence : intégration de la source des menaces

Les sources de menace offrent la possibilité d'extraire des données des référentiels externes de Threat Intelligence. Ces données sont ensuite importées dans les différentes tables d'indicateurs de compromission qui existent dans le système. Les collections TAXII et les listes de blocage simples sont prises en charge nativement. Pour ajouter de nouvelles collections TAXII (ou des profils basés sur un service de découverte ou de gestion de collection), il suffit

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'ajouter une entrée. De même, l'ajout d'une nouvelle liste de blocage simple à colonne unique consiste à entrer un nouvel enregistrement et à fournir l'URL de la liste de blocs. Pour des ensembles de données plus complexes, une intégration personnalisée peut être fournie pour passer un appel à une URL et analyser la réponse.

Cas d'utilisation couvert :

Récupérez les données d'une source de renseignements sur les menaces pour les charger dans des tables IoC.

Options utiles fournies :

- Prise en charge des listes de blocage simples et des collections TAXII sans codage.
- Mécanisme simple d'exécution de messages REST pour récupérer des données.
- Récupération/traitement des données découplées pour la réutilisation des composants d'intégration.
- Prise en charge native du traitement des données transmises renvoyées aux sources de données (et aux jeux d'importation/cartes de transformation).
- Prend en charge plusieurs demandes de données par intégration (pour les appels paginés) avec la possibilité de transmettre le contexte aux appels suivants

Ressources:

Définir une source de menace

Vulnerability Response : intégration de l'invocation de scanner

L'invocation du scanner de vulnérabilité est un point d'entrée d'intégration légère qui prend en charge l'invocation d'analyses de vulnérabilité à partir de l'instance. Un scanner de vulnérabilité tiers est appelé de manière asynchrone pour planifier une analyse à la recherche d'éléments de configuration ou d'adresses IP.

Cas d'utilisation couvert :

Effectuez une demande à un scanner tiers pour analyser un CI (à l'aide des informations d'hôte dérivées du CI) ou une adresse/des adresses IP.

Options utiles fournies :

- Cadre de travail simple pour la définition des implémentations de scanner.
- Manière cohérente de demander des analyses à partir d'éléments de catalogue, d'incidents de sécurité et d'éléments vulnérables.
- Mise à jour automatique des tâches avec le résultat de l'invocation de l'analyse.

Vulnerability Response : intégration de données

Les intégrations de données de vulnérabilité sont destinées à récupérer des données de vulnérabilité à partir de systèmes de vulnérabilité tiers. Les sorties attendues de ces intégrations sont des entrées de vulnérabilité et des éléments vulnérables. Cette intégration permet aux scanners de vulnérabilité tiers de fonctionner indépendamment, en s'attendant à ce que les vulnérabilités puissent être traitées et suivies au sein de l'instance.

Cas d'utilisation couverts :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Récupérer les bibliothèques de vulnérabilité
- Récupérer les paires vulnérabilité/CI
- Synchroniser les CI avec le système de gestion des vulnérabilités

Options utiles fournies :

- Récupération/traitement des données découplées pour la réutilisation des composants d'intégration.
- Prise en charge native du traitement des données transmises renvoyées aux sources de données (et aux jeux d'importation/cartes de transformation).
- Prend en charge plusieurs demandes de données par intégration (pour les appels paginés) avec la possibilité de transmettre le contexte aux appels suivants.

Ressources:

Documentation sur l'intégration des données de vulnérabilité

Opérations de sécurité Configurations d'intégration

La plupart des intégrations incluses dans le système de base nécessitent peu ou pas de configuration et fonctionnent de la même manière. Toutefois, Qualys Cloud Platformcertaines intégrations nécessitent des étapes distinctes pour la configuration de l'intégration. D'autres prennent en charge différents ensembles de types d'analyse et de recherche et différentes limites de taux.

Cette section décrit les différences entre les intégrations prises en charge et vous dirige vers plus de documentation, si nécessaire.

- Intégration Carbon Black: vous permet d'enquêter sur les incidents de sécurité et d'y répondre en utilisant les API Carbon Black pour interroger et interagir avec les points de terminaison associés aux incidents de sécurité.
- Anti-robot Check Point - Intégration de l'analyseur d'e-mail: utilise un analyseur d'e-mails qui utilise les notifications par e-mail de Check Point Anti-bot pour créer des incidents de sécurité.
- Intégration de l'enrichissement des incidents Elasticsearch: recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.
- Have I been pwned? intégration: permet de rechercher rapidement la liste des comptes piratés (adresses e-mail et noms d'utilisateur) via un service RESTful.
- HPE Security ArcSight ESM - Intégration de l'analyseur d'e-mails: utilise un analyseur d'e-mails qui utilise les notifications par e-mail de HPE ArcSight ESM pour créer des incidents de sécurité.
- HPE ArcSight Logger - Intégration de l'enrichissement des incidents: recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.
- IBM QRadar : intégration de l'enrichissement d'incident: recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.
- McAfee ESM - Intégration de l'analyseur d'e-mails: utilise un analyseur d'e-mails qui utilise les notifications par e-mail de McAfee ESM pour créer des incidents de sécurité.
- McAfee ESM : intégration de l'enrichissement des incidents: recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vue d'ensemble de l'intégration OPSWAT Metadefender: permet de télécharger les données de menace, détectées par le scanner tiers Metadefender, dans l'application pour le suivi, la hiérarchisation et la Renseignements sur les menaces résolution.
- Palo Alto Networks - AutoFocus intégration: Palo Alto Networks AutoFocus, un service cloud de renseignements sur les menaces, vous permet de rechercher des informations de session relatives aux observables d'incident de sécurité.
- Palo Alto Networks - Firewall intégration: Palo Alto Networks Firewall vous permet de configurer et de maintenir des pare-feu pour prévenir les menaces connues et inconnues sur le réseau, le cloud et les points de terminaison.
- Palo Alto Networks - WildFire intégration: l'intégration de Wildfire vous permet d'interroger par programmation des tâches d'analyse sur Wildfire et de récupérer les résultats historiques via une interface d'API XML simple.
- Présentation de Qualys Vulnerability Integration: Qualys Cloud Platform est utilisé dans Réponse aux vulnérabilités.
- Splunk - Intégration de l'enrichissement pour les incidents: recherche vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.
- Intégration de VirusTotal: utilisé dans Renseignements sur les menaces. Pour utiliser cette source de recherche, vous devez activer le module d'extension VirusTotal Integration.
- Configuration de l'intégration de l'API WhoisXML: fournit des données cohérentes et bien structurées à partir d'une recherche Whois. Maintient des données Whois précises accessibles 24h/24 et 7j/7.

Activer et configurer les intégrations tierces

Vous pouvez activer les modules d'extension pour les intégrations tierces et les configurer pour une utilisation à partir du même écran.

Avant de commencer

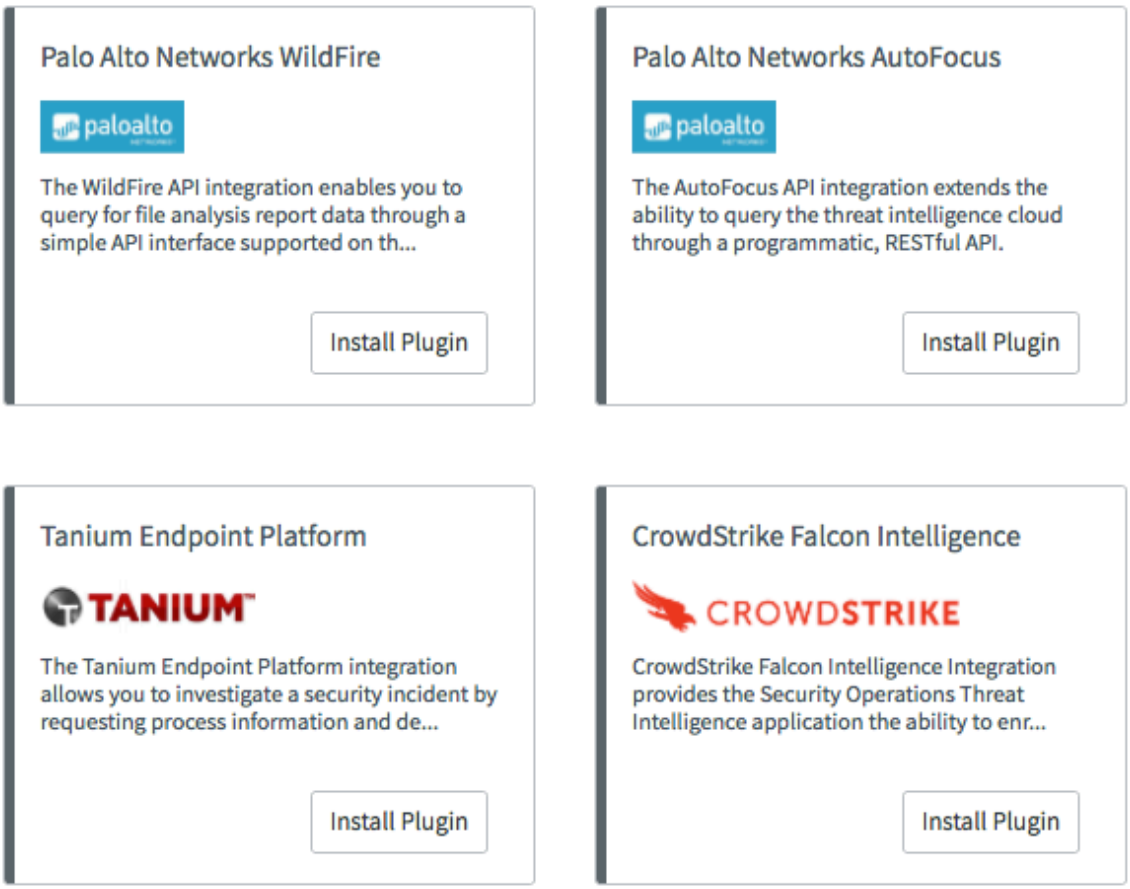
Rôle requis : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes, semblable au groupe de cartes suivant. Vous pouvez pointer vers n'importe quelle carte pour obtenir une description de l'intégration.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

2. Pour installer le module d'extension pour une intégration donnée, cliquez sur **Installer le module d'extension**.

   a. Dans le formulaire Module d'extension système, examinez les détails du module d'extension et cliquez sur le lien connexe **Activer/Mettre à niveau** .

   b. Cliquer sur **Activer**.
   Lorsque l'activation est terminée, l'écran Security Integration s'affiche à nouveau et le bouton de l'intégration que vous avez activée s'intitule **Configurer**.

3. Cliquez sur **Configurer**.

   Remarque : Si vous configurez le , reportez-vous à la Qualys Vulnerability Integrationsection Installation et prise en charge des Réponse aux vulnérabilités applications.

4. Saisissez la **clé API**.
5. Cliquez sur **Envoyer**.

Créer une intégration

Vous pouvez créer une intégration et ajouter la carte d'intégration associée à l'écran Intégrations de sécurité. Cette procédure est destinée aux partenaires qui créent des intégrations tierces.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_sec_cmn.admin

Audience: Les partenaires qui créent des intégrations tierces.

Procédure

1. Dans le filtre de navigation, saisissez sn_sec_core_integration_item.list et appuyez sur la touche **Entrée** .
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom de l'intégration.
ID de module d'extension	Le module d'extension qui doit être activé pour utiliser l'intégration.
Ordre	Indique l'ordre d'affichage de cette carte d'intégration.
Texte de la bannière	Cliquez sur le lien, sélectionnez une image ou un logo à afficher dans la carte d'intégration, puis cliquez sur **OK**.
Installé	Champ en lecture seule qui indique si le module d'extension a déjà été installé.
Configurable	Indique si vous pouvez configurer l'intégration.
Catégories	Utilisé pour filtrer les cartes d'intégration.
Description brève	Une description de l'intégration qui apparaît dans l'info-bulle de la carte.
Description	Une description plus longue de l'intégration.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**. La liste connexe **Integration and Configurations (Intégration et configurations**) s'affiche. Vous pouvez utiliser cette liste connexe pour définir les options de configuration de l'intégration. Ces options s'affichent lorsque vous cliquez sur le bouton **Configuration** sur la carte d'intégration associée.
5. Cliquez sur **Nouveau**.
6. Renseignez les champs du formulaire comme il convient.

Champ	Description
Étiquette	Nom de l'élément d'intégration.
Nom	Le module d'extension qui doit être activé pour utiliser l'intégration.
Intégration	Affiche l'intégration pour laquelle vous définissez les éléments d'intégration
Ordre	Indique l'ordre dans lequel cet élément d'intégration apparaît.
Type	Dans la liste, sélectionnez le type de champ : ◦ Chaîne ◦ Entier ◦ Décimal

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Date ◦ Booléen ◦ Mot de passe ◦ IPv4 ◦ IPv6 ◦ URL
Valeur	Entrez la valeur associée au **type** sélectionné. Si une valeur non valide pour le **type** sélectionné est saisie, aucun enregistrement n'est récupéré lors de l'exécution de l'intégration. Par exemple, si vous sélectionnez le type d'URL et saisissez la valeur 12.32.23.10, aucun enregistrement n'est récupéré.

7. Cliquez sur **Envoyer**.

Conseils pour l'écriture d'intégrations

Évitez certains des pièges que vous pouvez rencontrer lors de l'écriture de vos propres intégrations en suivant ces directives.

Utiliser les fonctionnalités de la plateforme ServiceNow dans la mesure du possible

Dans la plupart des cas, les options d'intégration intégrées aux Opérations de sécurité applications (Réponse aux incidents de sécurité, Renseignements sur les menaces, et Réponse aux vulnérabilités) visent à améliorer ou à rationaliser les fonctionnalités d'intégration de plateforme existantes ServiceNow . Lors de l'écriture d'intégrations, assurez-vous toujours d'utiliser la fonctionnalité de plateforme lorsqu'elle existe. Voici quelques fonctionnalités courantes ServiceNow qui peuvent être utilisées plutôt que de « rouler vous-même ».

- Services Web sortants : pour la plupart des interactions avec des systèmes tiers, la communication se fait par le biais de services Web. Dans ce cas, utilisez les services Web sortants de la plateforme (REST et SOAP sont pris en charge).
- Une carte des sources de données/des ensembles d'importation/de transformation – pour le traitement des données et l'insertion dans ServiceNow des tables, le mécanisme privilégié consiste à utiliser les sources de données et les composants associés.

Utiliser les cadres de travail d'intégration de Security Operations dans la mesure du possible

Étant donné que Opérations de sécurité les mécanismes d'intégration ont résolu de nombreux problèmes courants, il n'est pas nécessaire de réimplémenter les fonctionnalités de base pour chaque intégration. Par exemple, les données de vulnérabilité et les cadres de travail des sources de menace prennent en charge la gestion de plusieurs pages et la transmission de ces données à des sources de données/transformations/ jeux d'importation. De même, l'infrastructure d'analyse ou de recherche de source fournit une fonctionnalité configurable de limitation des taux. En règle générale, lors de l'implémentation d'une fonctionnalité ou d'un ensemble de fonctionnalités, vérifiez si le cadre de travail d'intégration existant Opérations de sécurité couvre votre cas d'utilisation. Si c'est le cas, utilisez ce cadre.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étendre les cadres de travail d'intégration des opérations de sécurité existants selon les besoins

La plupart des tables et des scripts utilisés par Opérations de sécurité les frameworks d'intégration étaient destinés à être étendus pour répondre aux besoins futurs. Si un cas d'utilisation est rencontré lors de l'écriture d'une intégration, étendez une table ou un script d'intégration pour mieux correspondre à ce cas d'utilisation.

Fournir des commentaires à ServiceNow pour les problèmes rencontrés pendant l'intégration

Au fur et à mesure qu'une intégration est en cours de développement ou de test, assurez-vous de fournir des commentaires lorsque des problèmes sont rencontrés. Même si une solution de contournement est nécessaire, Service et assistance client le personnel peut apporter une amélioration dans les versions futures qui pourrait atténuer le problème pour les intégrations futures.

Essai sous charge raisonnable

Un problème courant avec les intégrations est qu'elles ne sont pas équipées pour gérer des charges réalistes. Étant donné que chaque intégration est une application incluse dans le périmètre, la plateforme impose davantage de limitations pour garantir la stabilité du système. Ces limitations peuvent entraîner l'arrêt de tâches ou d'appels d'API de longue durée. Vous pouvez vous assurer que les processus de longue durée ou les processus qui traitent beaucoup de données sont gérés de manière appropriée en réduisant le temps nécessaire à chaque appel ou processus (généralement en fournissant un moyen de paginer les demandes d'API ou de segmenter de grands ensembles de données).

Dépannage de l'intégration

Ces suggestions de dépannage peuvent vous aider à résoudre les problèmes courants que vous pouvez rencontrer lors de la configuration ou de l'exécution d'intégrations.

Remplacer un certificat SSL tiers non approuvé ou expiré

Lorsqu'une connexion SSL est requise dans une intégration, il peut arriver que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou ait expiré. Vous pouvez le remplacer ou ajouter un nouveau certificat.

Avant de commencer
Rôle requis : sn_ti.write

Procédure

1. Procurez-vous le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.

   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
   Par exemple : `https://<3rdparty>/`.

   b. Cliquez sur l'icône de cadenas dans la ligne d'adresse.

   c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .

   d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.

f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
Il doit commencer par `-----BEGIN CERTIFICATE` ----- et se terminer par `-----END CERTIFICATE`-----.

2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et Créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Cliquez sur **Enregistrer**.
Les autres champs de l'enregistrement sont générés automatiquement.

Cadre de travail des options d'intégration 2.0

Le nouveau cadre de travail des options d'intégration 2.0 a été repensé pour permettre l'implémentation des intégrations de manière simple et cohérente. Cela garantit une expérience cohérente pour des types d'intégrations similaires (par exemple, recherche de réputation d'un observable).

Le nouveau cadre de travail comporte des fonctionnalités implémentées à l'aide de flux .

Les avantages de la mise en œuvre améliorée du cadre sont les suivants :

- Les flux d'aptitudes qui incluent uniquement des composants de niveau métier sans logique spécifique d'implémentation.
- Les flux d'aptitudes acceptent désormais un large éventail d'entrées et de formats pour une flexibilité maximale (par exemple, des références d'observables, des références de CI, des tâches, des combinaisons de tables ou de sys_id).
- La limitation ou l'étranglement des taux sur les exécutions d'intégration sont désormais faciles à configurer (ce qui élimine la nécessité d'utiliser du code personnalisé ou des modifications apportées aux workflows d'implémentation).
- Des fonctionnalités améliorées d'audit et de suivi des exécutions permettent désormais d'améliorer la génération de rapports et le dépannage.
- Des fonctions robustes de gestion des erreurs sont intégrées dans les flux d'aptitudes pour éviter de dupliquer les routines d'implémentation.
- Possibilité de configurer le déclenchement conditionnel des options ou des intégrations. Cela permet de lancer automatiquement des automatisations en fonction de la catégorie d'incident.
- Une condition de filtre par défaut a été introduite sur toutes les options pour filtrer les observables répertoriés avant que des entrées ne soient fournies aux intégrations.

Remarque : Ce nouveau cadre de capacité ne met pas à jour le cadre de capacité actuel. Les deux cadres peuvent fonctionner en parallèle. Pour obtenir des instructions sur la manière d'exploiter le nouveau cadre de travail d'aptitude, reportez-vous aux sections Utilisation du nouveau cadre de travail d'aptitude avec une intégration installée et Utilisation du nouveau cadre de travail d'aptitude avec un flux.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations et composants pris en charge

Le module d'extension Security Incident Response inclut tous les flux d'aptitudes répertoriés dans Integration Capabilities Framework 2.0 et des filtres standard de haut niveau que vous pouvez activer ou désactiver en fonction de vos besoins.

Remarque : Si vous souhaitez utiliser le nouveau Cadre de travail d'intégration d'aptitude avec la version New York, vous devez installer le module d'extension ServiceNow Centre d'intégration Starter Pack Installer. Contactez le service client pour obtenir de l'aide pour l'installation.

Versions d'application prises en charge

À partir de Security Incident Response 10.0, les intégrations suivantes sont prises en charge :

Application	Version minimale requise
Intégration de Security Operations Hybrid Analysis	10.0.0
Intégration PhishTank de Security Operations	10.0.0
Intégration de Security Operations ThreatCrowd	10.0.0
Intégration de CrowdStrike Intelligence pour opérations de sécurité	10.0.0
Opérations de sécurité : « Est-ce que j'ai été victime d'une attaque ? » Intégration	10.0.0
Intégration MetaDefender pour Security Operations	10.0.0
Intégration future enregistrée d'Opérations de sécurité	10.0.0
Intégration de VirusTotal pour opérations de sécurité	10.0.0
Security Operations : inverser l'intégration de Whols	10.0.0

À partir de Security Incident Response 10.4, les intégrations suivantes sont prises en charge :

Application	Version minimale requise
Intégration de Security Operations RiskIQ	10.0.0
Intégration Shodan de Security Operations	10.0.0
Intégration Whois de Security Operations	10.0.0
Intégration de Security Operations Carbon Black	10.3.1
Intégration de la recherche Splunk pour Opérations de sécurité	10.3.0
Intégration ArcSight Logger pour Security Operations	10.3.0

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application	Version minimale requise
Intégration McAfee ESM pour Security Operations	10.3.0
Intégration Elasticsearch pour Security Operations	10.3.0
Intégration d'IBM QRadar pour Security Operations	10.3.1
Hôte CrowdStrike Falcon pour Security Operations	10.3.0

Composants inclus

Le nouveau Cadre d'intégration des capacités comprend les éléments suivants :

- **Options** : toutes les options suivantes qui existent dans le produit aujourd'hui sous forme de workflows ont été repensées à l'aide de flux :
  - **Demande de bloc** : fournit un moyen de bloquer les observables associés à un incident de sécurité sur un pare-feu, un proxy web ou un autre point de contrôle. Cette option est utilisée au cours des enquêtes de réponse à un incident pour contenir une menace identifiée.
  - **Recherche et suppression d'e-mails** : fournit un moyen de rechercher un serveur de messagerie pendant un examen de sécurité et, si nécessaire, de supprimer les e-mails du serveur.
  - **Enrichir l'élément de configuration** : fournit un moyen général d'enrichir les éléments de configuration avec des informations supplémentaires provenant de différentes sources. Cette fonctionnalité est utilisée au cours des enquêtes de réponse à un incident pour enrichir les données associées à un incident de sécurité.
  - **Enrichir les observables** : fournit un moyen général d'enrichir les observables avec des informations supplémentaires provenant de diverses sources. Cette option est utilisée au cours des enquêtes de réponse à un incident pour contenir une menace identifiée.
  - **Ingestion d'événement** : fournit un moyen général de créer un incident de sécurité en mappant les événements d'une source d'intégration à un incident de sécurité.
  - **Obtenir les statistiques réseau** : récupère une liste des connexions réseau actives à partir d'un point de terminaison ou d'un hôte. Cette option sert à enrichir les incidents au cours des enquêtes.
  - **Obtenir les processus en cours d'exécution** : récupère une liste des processus en cours à partir d'un point de terminaison ou d'un hôte. Cette option sert à enrichir les incidents au cours des enquêtes.
  - **Isoler l'hôte** : fournit un moyen d'isoler un point de terminaison ou un hôte associé à un incident de sécurité. Isoler l'hôte est exécuté sur un élément de configuration (CI).
  - **Publier dans la liste de surveillance** : fournit un moyen d'ajouter des observables associés à un incident de sécurité à une liste de surveillance qui surveille les événements de sécurité et génère des alertes. Cette option est utilisée dans le cadre de la réponse à un incident au cours des enquêtes.
  - **Recherche de perceptions** : recherche des instances d'observables dans différents SIEM ou d'autres magasins de journaux. Cette fonctionnalité est utilisée pour déterminer la présence d'IoC malveillants dans votre environnement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Recherche de menace** : effectue des recherches de renseignements sur les menaces pour déterminer si un observable donné est associé à une menace de sécurité connue. Cette option est utilisée dans le cadre de la réponse à un incident au cours des enquêtes.

- **Nouvelles tables** :
  - sn_sec_cmn_capability : aptitude et flux qui implémentent l'aptitude.
  - sn_sec_cmn_capability_implementation : flux d'implémentation réel qui fournit les services de l'aptitude.
  - sn_sec_cmn_capability_execution : enregistrement d'exécution d'une option lors de l'exécution.
  - sn_sec_cmn_capability_implementation_execution : enregistrement d'exécution d'une implémentation d'option lors de l'exécution.
  - sn_sec_cmn_filter_condition : conditions de filtre qui peuvent être appliquées pendant l'exécution à l'aptitude ou à l'implémentation d'une aptitude.
- **Include script** : CapabilityProcessor : gère tout le code de traitement pour le framework.
- **Limite du taux** : Capacité max. Demande simultanée par période : définit le nombre d'intégrations qui peuvent être exécutées en parallèle.
- **Implémentation de l'aptitude du processus de tâche planifiée** : s'exécute toutes les 15 secondes et peut être désactivée dans la page Propriétés de l'administration de la sécurité (**Incident de sécurité** > **Administration** > **Propriétés**.
  - Active ou désactive la tâche planifiée, Implémentations des aptitudes de processus : Cette tâche planifie et gère automatiquement les flux d'exécution de l'implémentation des aptitudes.
  - Active ou désactive les recherches ou enrichissements automatisés : paramètre qui active ou désactive la tâche planifiée qui effectue la recherche automatisée des menaces ou l'enrichissement des observables lorsque des éléments observables sont ajoutés aux incidents de sécurité dans le cadre de travail d'aptitude actuel.
  - Active ou désactive la tâche planifiée, Rechercher des observables d'incident de sécurité : cette tâche planifie automatiquement une tâche de recherche de menace ou d'enrichissement des observables lorsque des éléments observables sont ajoutés à un incident de sécurité.

Configurations dans le nouveau cadre de travail d'aptitude

Cette section décrit les configurations disponibles dans le nouveau cadre de travail.

Avant de commencer

Rôle requis : sn_si.admin, flow_designer, action_designer

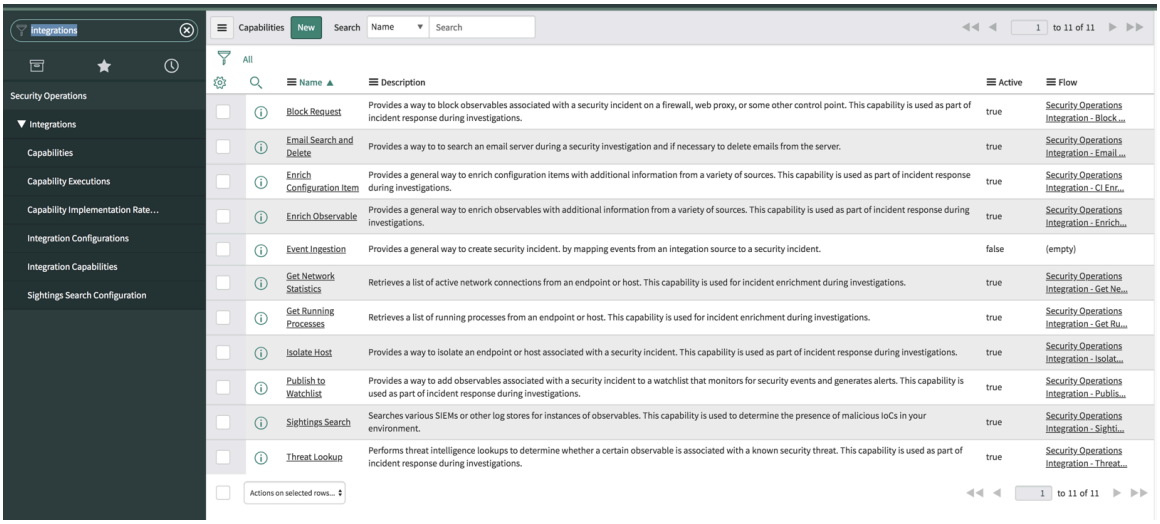
Procédure

1. Accédez à la **Tout** > **Security Operations** > **Intégrations** > **Aptitudes**.

   Remarque : Version 10.4 : À partir de la version 10.4 de Security Incident Response, le nom du menu **Options** a été remplacé par **Options d'intégration (flux).**

2. Les options disponibles avec le système de base s'affichent.

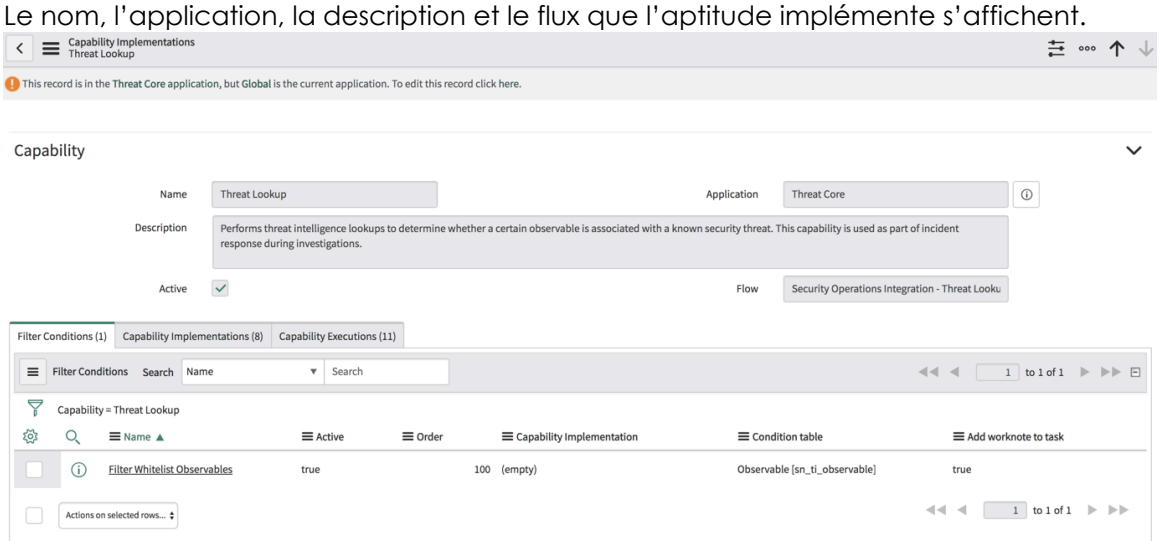
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :

Il s'agit des options fournies avec le système de base. Vous pouvez utiliser les options ou les personnaliser selon vos besoins. Les étapes suivantes décrivent comment configurer une option et les intégrations implémentées pour elle.

3. Cliquez sur le lien dans la colonne Nom pour configurer une option.
Le nom, l'application, la description et le flux que l'aptitude implémente s'affichent.



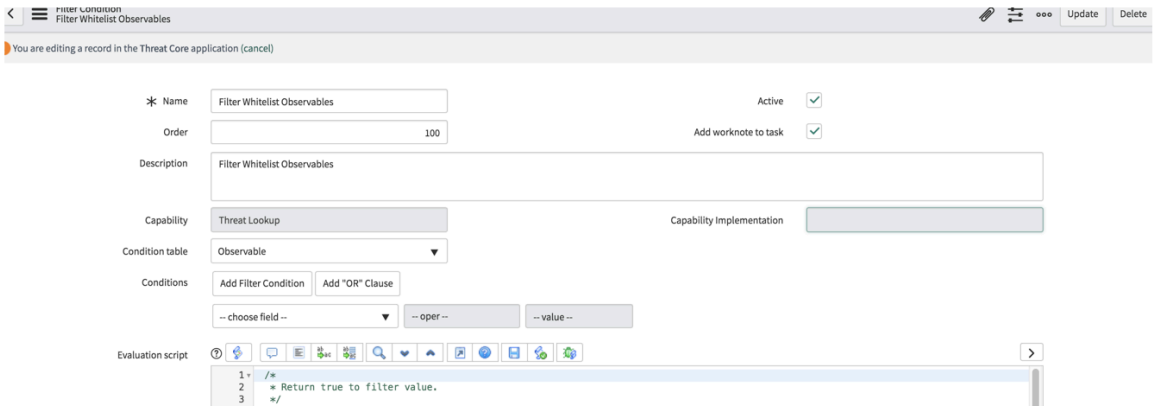
4. Cochez la case **Actif** pour activer l'option.

- **Conditions de filtre au niveau de l'aptitude : lorsqu'une aptitude d'intégration** implémente un flux, les conditions de filtre associées au flux sont exécutées avant le lancement du flux d'aptitude. Par exemple, l'option Recherche de menace inclut la condition Filtrer les éléments observables sur liste d'autorisation, comme indiqué ci-dessus. Cliquez sur le lien Nom pour modifier la condition de filtre.

  Remarque : Cochez la case **Ajouter une note de travail à la tâche** pour ajouter des notes de travail afin d'inclure des informations sur les conditions de filtre utilisées.

Traduction automatique

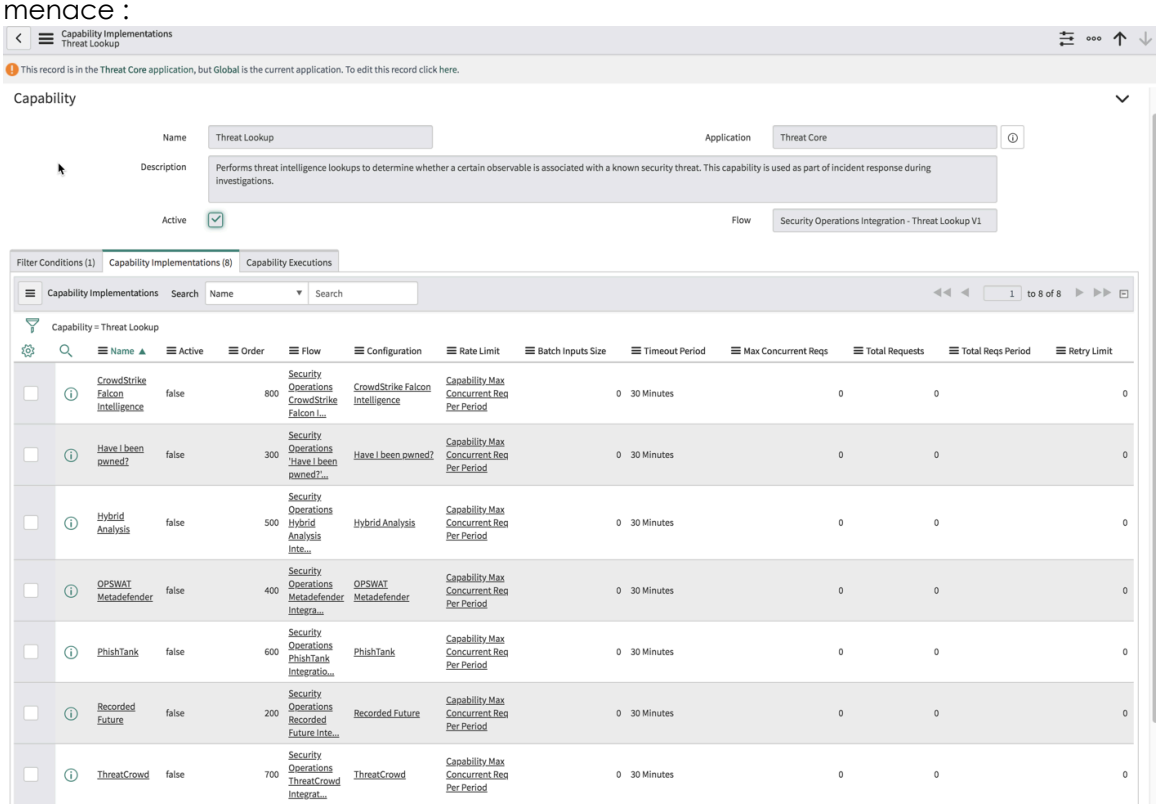
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez définir des conditions de filtre ou un script, ou une combinaison des deux. Dans l'exemple ci-dessus, un script est utilisé pour définir les conditions de filtre. Lorsque le flux d'aptitude est exécuté, le script recherche les observables sur liste d'autorisation et les supprime de la table.

Remarque : Les conditions de filtre définies ici s'appliquent à toutes les intégrations actives définies dans l'onglet **Implémentations d'aptitudes** .

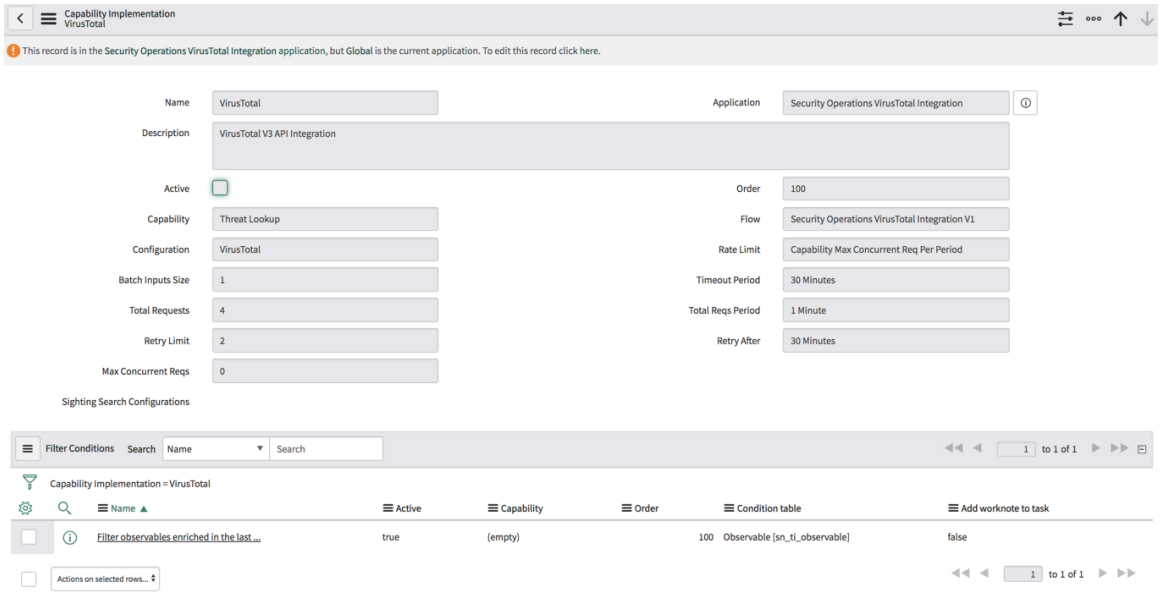
- **Implémentations d'aptitudes** : cliquez sur l'onglet **Implémentations d'aptitudes** . Les implémentations (intégrations) qui ont été configurées pour cette option s'affichent. L'exemple ci-dessous montre les intégrations configurées pour l'option Rechercher une menace :



5. Cliquez sur le lien Nom pour afficher l'implémentation de l'aptitude.
   Le nom, l'application, la description et le flux que l'aptitude implémente s'affichent.
6. Cochez la case **Actif** pour activer l'option.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



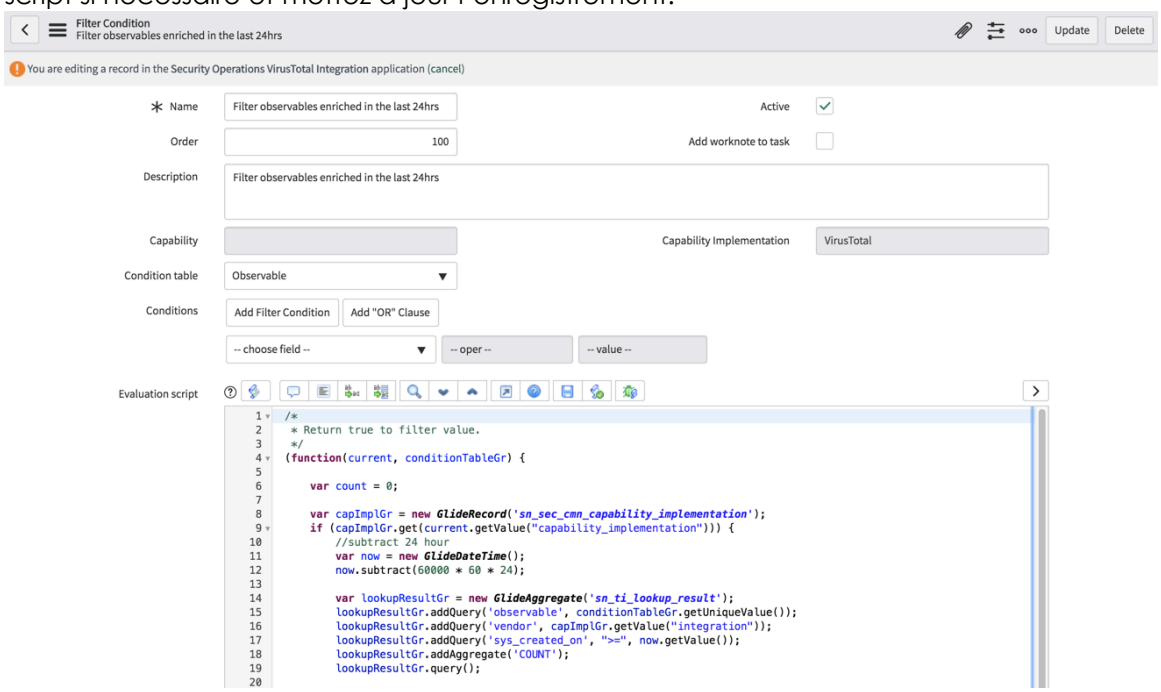
Vous pouvez spécifier les détails suivants :

Nom de champ	Description
Actif	Cochez cette case pour activer la désactivation de cette intégration. **Remarque :** Si vous configurez cette intégration à l'aide de la vignette d'intégration dans **Security Operations** > **Intégrations** > **Configurations des intégrations**, ce marqueur est automatiquement réglé sur **Actif**.
Ordre	Indique l'ordre dans lequel les intégrations sont exécutées.
Option	Aptitude implémentée par cette intégration.
Flux	Flux secondaire qui implémente l'aptitude.
Configuration	La configuration d'intégration pour cette option. **Remarque :** Initialement défini sur la configuration par défaut fournie avec le système de base. Lorsqu'une intégration est configurée à l'aide de la vignette d'intégration sur la page **Configurations d'intégration** , cette valeur est automatiquement réinitialisée sur la nouvelle configuration créée.
Limite du taux	Indique le nombre d'intégrations qui peuvent être exécutées au moment de l'exécution (en parallèle ou par unité de temps).
Taille des entrées par lots	Taille d'entrée par lots pour chaque exécution. Par exemple, pour une intégration de recherche d'observations, vous pouvez regrouper les observables en lots de 50 afin que les requêtes générées ne deviennent pas trop volumineuses. 0 indique qu'il n'y a pas de limite.
Délai d'expiration	Durée maximale avant l'annulation du flux d'implémentation de l'aptitude. 0 indique qu'il n'y a pas de délai d'expiration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description
Nombre total de demandes	Nombre total de demandes d'exécution de l'implémentation. Ce champ, associé au champ Nombre total de demandes au cours de la période, peut être utilisé pour limiter le nombre de demandes au service. Par exemple, vous pouvez limiter ce nombre à 4 requêtes par minute.
Nombre total de demandes au cours de la période	Nombre total de demandes d'exécution autorisées par période.
Nombre limite de nouvelles tentatives	Nombre de nouvelles tentatives autorisées pour une demande d'exécution ayant échoué. Cette limite s'applique si le marqueur **Nouvelle tentative** est défini dans votre intégration pour réessayer une demande d'exécution lorsqu'une condition est remplie. Par exemple, une nouvelle demande est effectuée lorsque vous avez dépassé votre limite de licence pour ce service pendant une période donnée ou lorsque le service est en panne.
Recommencer après	Période après laquelle une nouvelle tentative est effectuée pour une demande d'exécution ayant échoué.
Nombre maximal de demandes simultanées	Nombre maximal de demandes d'exécution d'implémentation simultanées. 0 indique qu'il n'y a aucune limite.
Configurations de recherche de perceptions	Les requêtes de recherche de perception par défaut qui peuvent être exécutées.

Cliquez sur le lien Nom dans la section Conditions de filtre pour configurer les conditions définies pour l'implémentation. Ajoutez ou supprimez des conditions de filtre, modifiez le script si nécessaire et mettez à jour l'enregistrement.



© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du nouveau cadre de travail d'aptitude avec une intégration installée

Cette section décrit comment utiliser le nouveau cadre de travail pour une intégration existante.

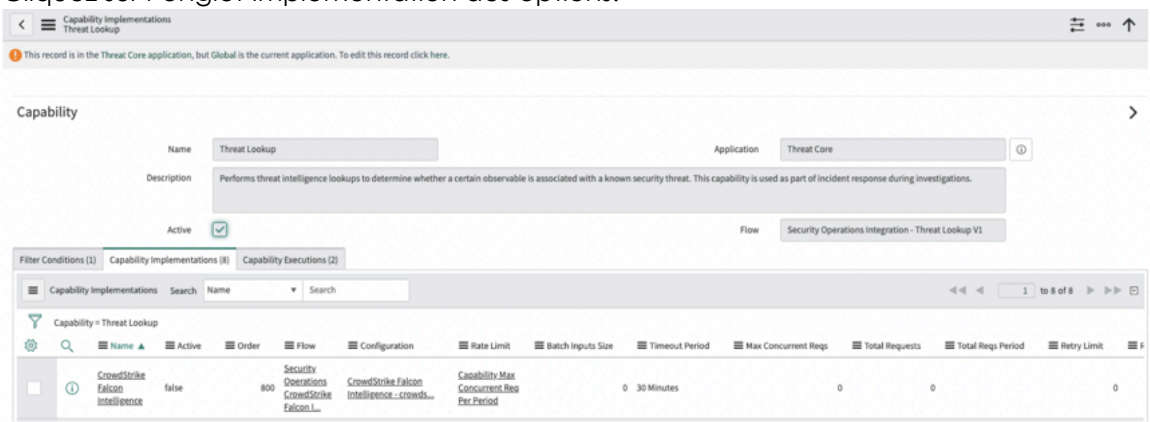
Suivez les étapes ci-dessous pour activer une intégration déjà installée et configurée (voir la liste des intégrations prises en charge dans Intégrations et composants pris en charge) afin d'utiliser le nouveau cadre de travail d'aptitude.

Remarque : Integration Capability Framework 2.0 disponible avec Security Incident Response 10.0.2 prend en charge les implémentations pour les options **Recherche de menace** et **Enrichissement des observables** . Les implémentations d'autres fonctionnalités seront disponibles dans une version ultérieure.

Avant de commencer

- Rôle requis : sn_si.admin
- Réponse aux incidents de sécurité 10.0.2

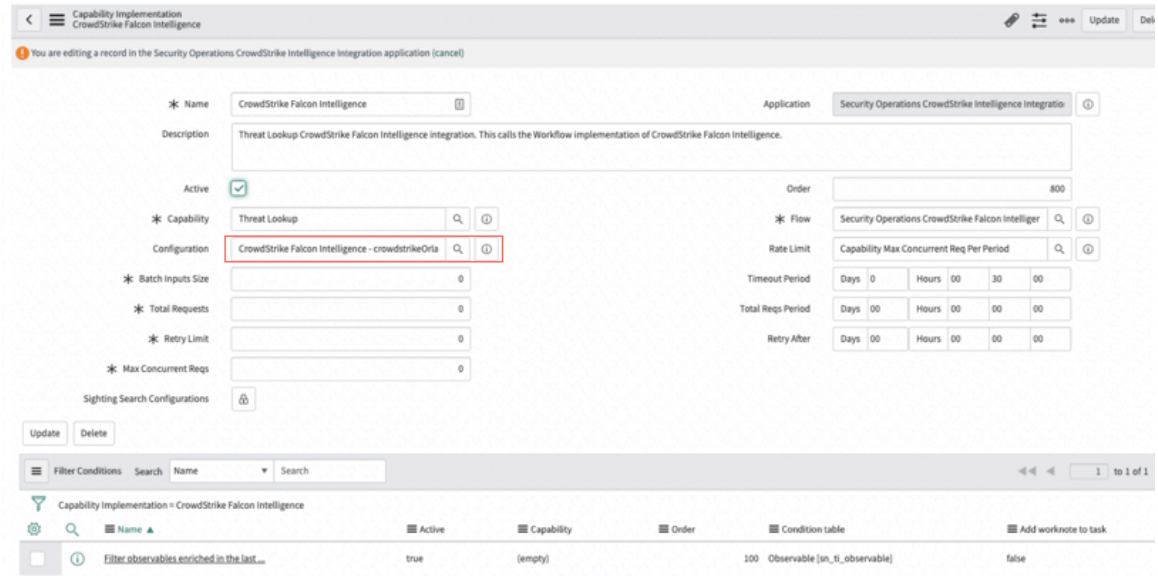
1. Accédez à la **Security Operations** > **Intégrations** > **Aptitudes**.
2. Cliquez sur **l'aptitude de recherche de menace** .
3. Cliquez sur l'onglet Implémentation des options.



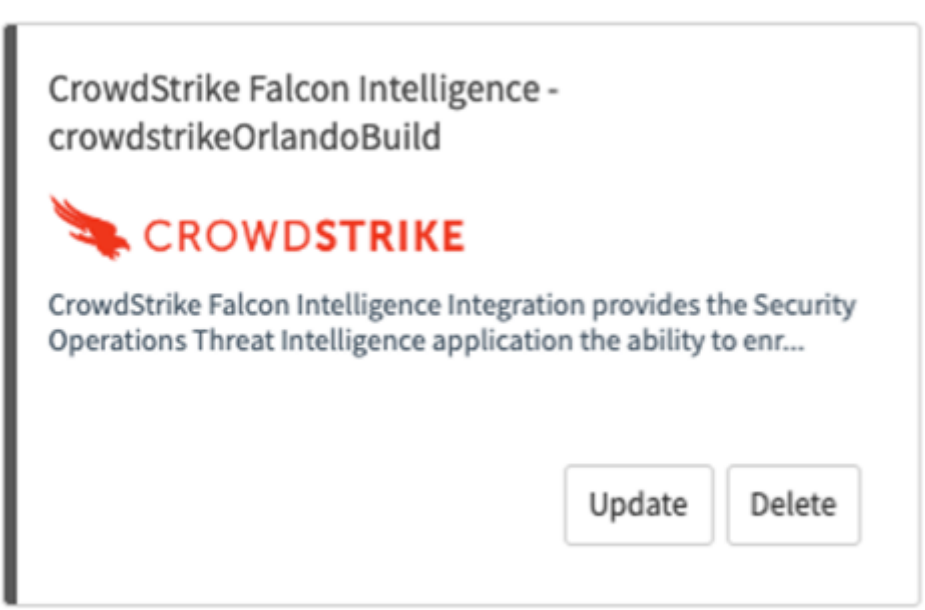
4. 4. Afficher l'enregistrement d'implémentation de l'aptitude pour l'intégration d'intérêt (exemple : Crowdstrike Falcon Intelligence). La colonne **Actif** doit avoir la valeur **Faux**.
5. Cliquez sur le lien **Nom** pour afficher l'enregistrement d'implémentation.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Sélectionnez la case à cocher **Activé**.
7. Assurez-vous que l'enregistrement d'implémentation pointe vers l'enregistrement de configuration approprié (le nom de la mosaïque pour l'intégration dans **Configurations d'intégration** > **Afficher les configurations (Oui)**).



8. L'implémentation est activée pour une utilisation avec le nouveau cadre de travail.

Remarque : Toutes les intégrations prises en charge lors de leur installation avec Réponse aux incidents de sécurité 10.0.2 seront automatiquement activées dans le nouveau cadre de travail d'aptitude d'intégration.

Utilisation du nouveau cadre de travail d'aptitude avec un flux

Suivez les étapes ci-dessous pour créer un flux et appeler le flux secondaire fourni par le nouveau cadre de travail d'aptitude.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

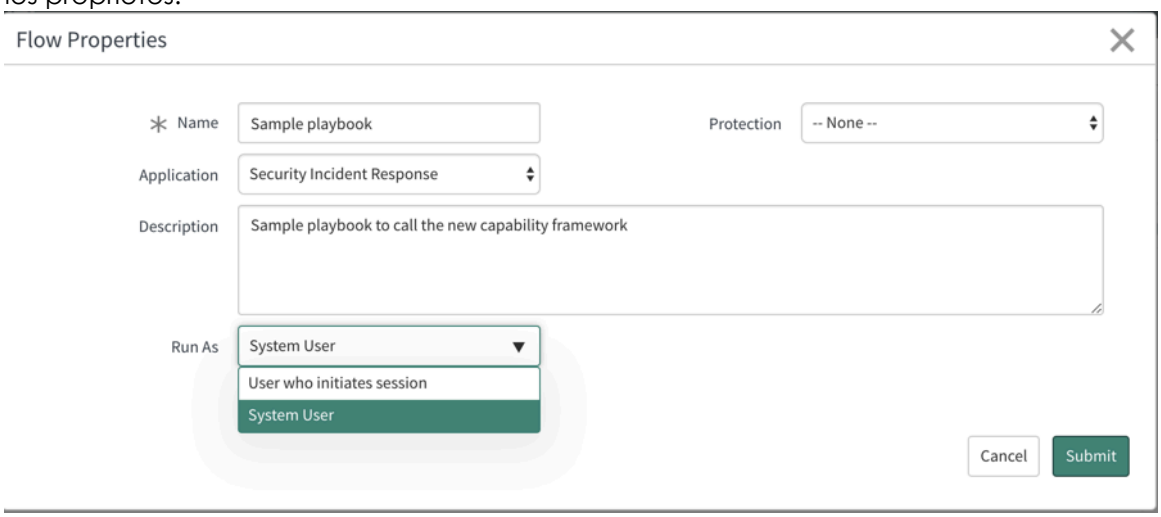
Avant de commencer

- Rôle requis : sn_si.admin, flow_designer, action_designer
- Installez l'une des intégrations prises en charge (reportez-vous à la section Intégrations et composants pris en charge)

Les étapes ci-dessous décrivent comment créer un exemple de flux et appeler l'un des flux secondaires fournis avec le nouveau cadre de travail d'aptitude.

Procédure

1. Accédez à la **Tout** > **Concepteur de flux** > **Concepteur**.
2. Cliquez sur **Nouveau** pour créer un nouveau flux et fournir les informations nécessaires pour les propriétés.



Remarque : Sélectionnez **Utilisateur système** dans la liste de choix Exécuter en tant que, comme illustré dans l'image ci-dessus.

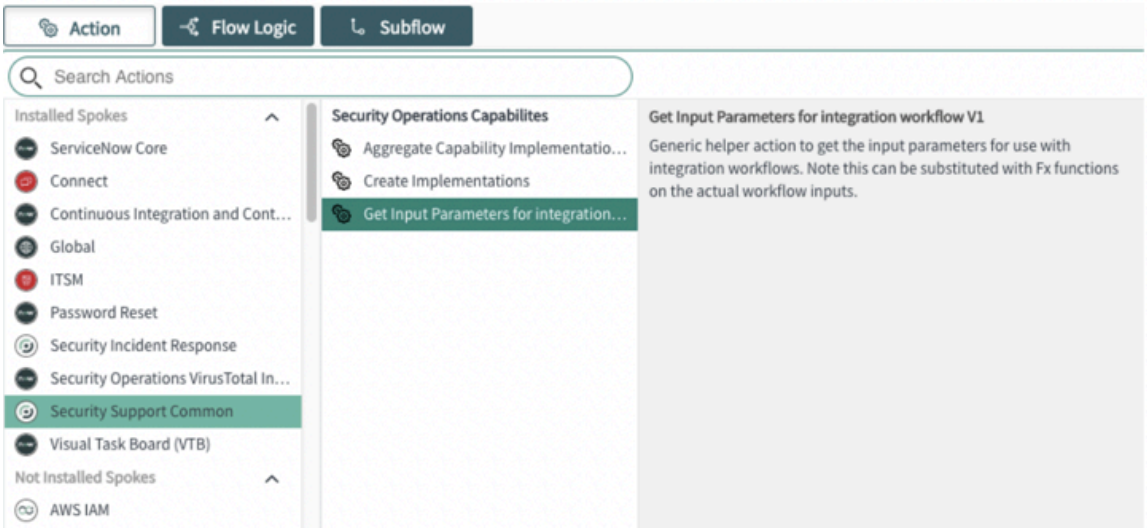
3. Sélectionnez une condition de déclenchement pour le flux (un déclencheur courant est la création d'un enregistrement d'incident de sécurité pour une certaine catégorie d'incident).



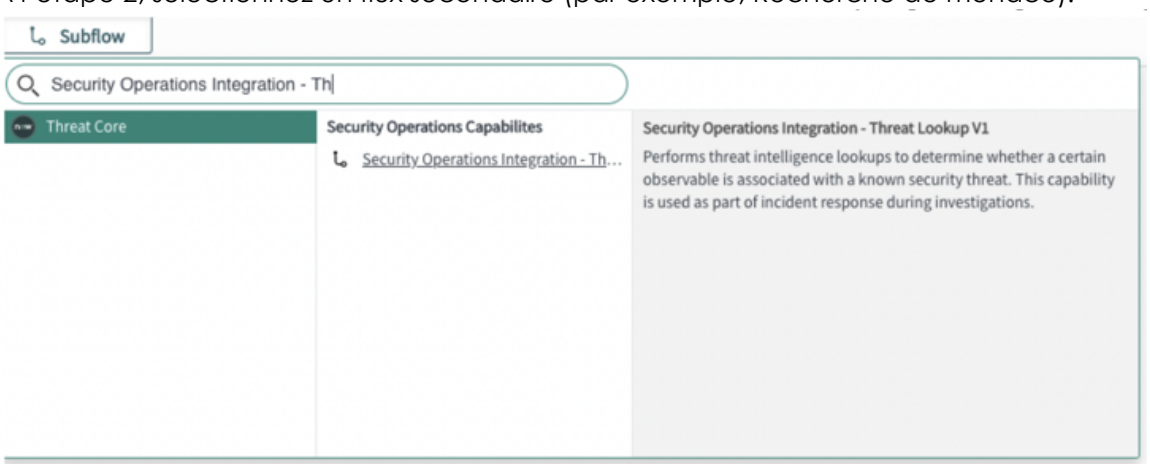
4. À l'étape 1 du flux, sélectionnez une action pour obtenir des entrées de l'incident de sécurité (par exemple, des observables).
   Vous pouvez sélectionner une action parmi les actions fournies avec le système de base avec le spoke commun de prise en charge de la sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. À l'étape 2, sélectionnez un flux secondaire (par exemple, Recherche de menace).



6. Configurez le flux secondaire que vous avez sélectionné comme indiqué ci-dessous :



7. Enregistrez et publiez le flux.

Dépannage des flux d'aptitude d'intégration

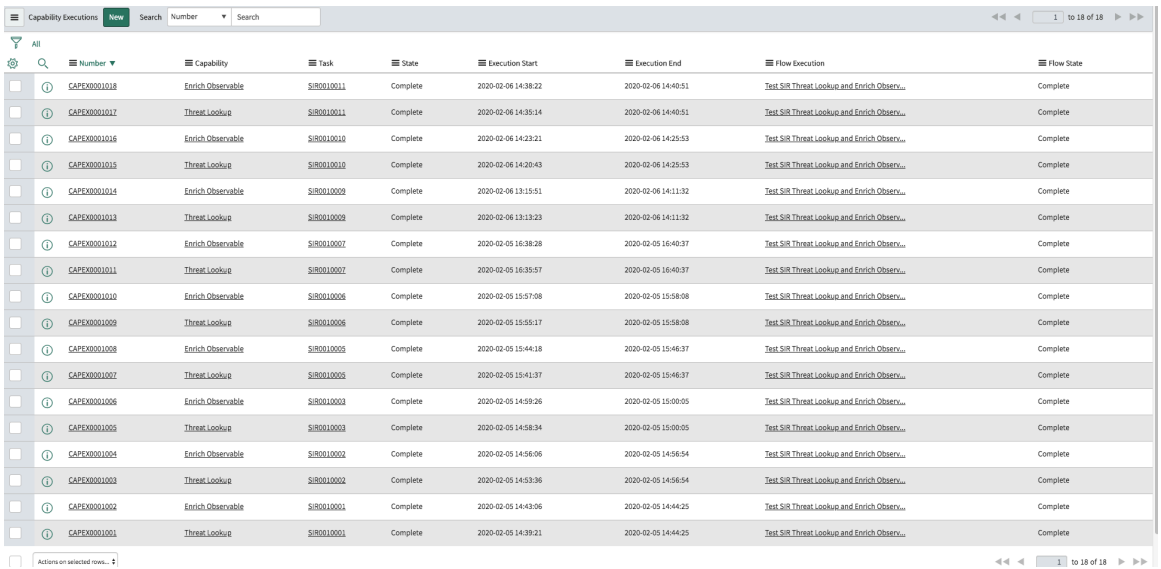
L'option Exécutions d'aptitudes fournit des informations détaillées sur chaque aptitude qui a été exécutée.

Remarque : Les exécutions terminées sont archivées au bout de 30 jours.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Security Operations** > **Intégrations** > **Exécutions de l'aptitude.**.



2. Cliquez sur le lien Exécutions de l'aptitude pour afficher des détails supplémentaires.

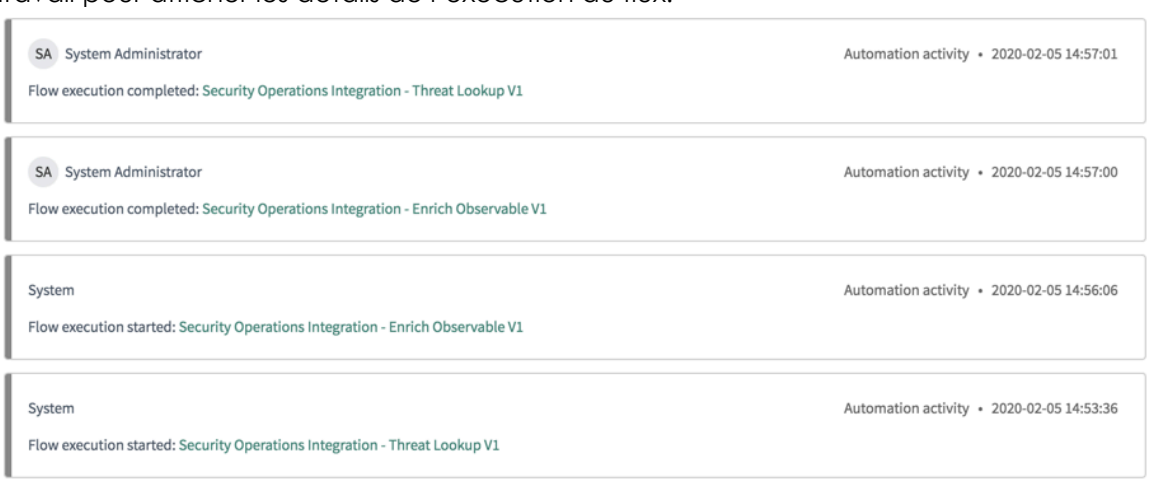
Enregistrement d'incident de sécurité Notes de travail

Lorsque des observables ont été ajoutés à un incident de sécurité et que la condition de déclenchement du flux est remplie, les flux secondaires Recherche de menace et Enrichissement des observables sont lancés et les notes de travail suivantes sont ajoutées à l'incident de sécurité :

- L'exécution du flux a commencé : Security Operations Integration - Enrichir les observables V1
- Exécution du flux terminée : Security Operations Integration - Enrichir les observables V1
- L'exécution du flux a commencé : Security Operations Integration – Threat Lookup V1
- Exécution du flux terminée : Security Operations Integration – Threat Lookup V1

Pour afficher ces notes de travail, connectez-vous en tant qu'utilisateur avec les rôles *sn_si.admin* ou *sn_si.analyst*, ainsi que *flow_designer* et *action_designer*.

Accédez à la page d'enregistrement d'incident de sécurité et cliquez sur ces notes de travail pour afficher les détails de l'exécution du flux.



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

API REST pour l'intégration tierce dans Security Operations

Le Opérations de sécurité système de base comprend une série d'API REST scriptées qui permettent aux clients et aux partenaires de s'intégrer facilement à un déploiement existant Opérations de sécurité . Les API vous permettent de collecter des données provenant de l'extérieur de votre système (par exemple, un script Python est utilisé pour recevoir des données de VirusTotal) et de les renvoyer à votre instance.

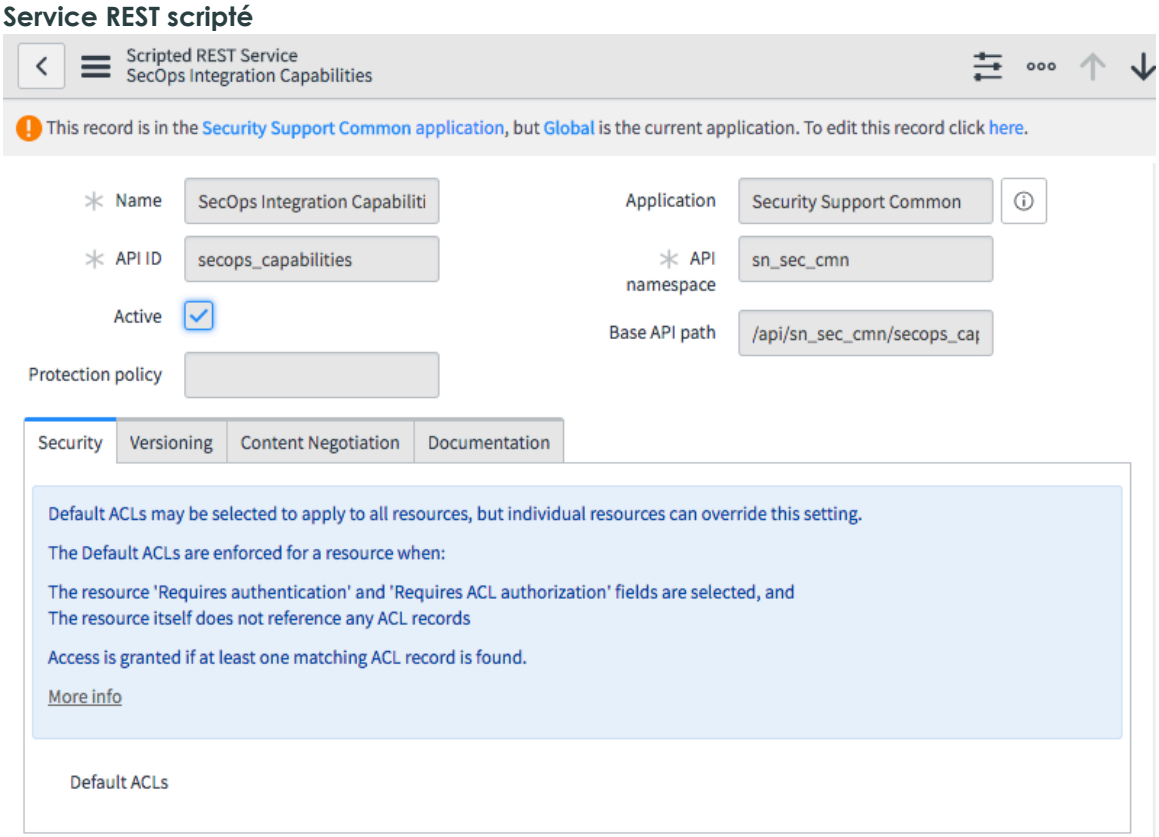
Les scripts écrits dans presque tous les langages (Python, par exemple) peuvent être utilisés avec les API pour effectuer des processus spécifiques au client. Les scripts doivent être écrits dans un langage capable d'effectuer un appel HTTP Post orienté vers l'extérieur. Par exemple, si vous avez une application Java, vous devez utiliser une bibliothèque, telle que le package `java.net.HttpUrlConnection` , pour construire un appel HTTP et transmettre une chaîne JSON comme corps pour le message.

L'API est uniquement utilisée pour ajouter des données qui ont été collectées en dehors de notre système. Par exemple, si vous avez entré un script Python VT et que vous avez reçu des données de VT, vous pouvez renvoyer ces données à l'instance SN.

Authentification

Toutes les opérations au sein des définitions d'API utilisent l'authentification de plateforme fournie par le Fonctionnalité d'opération des API REST scriptées . Pour y accéder, accédez à **Services web du système** > **Services Web basés sur un script** > **API REST basées sur un script** et localisez l'API des **options d'intégration SecOps** .

Service REST scripté



L'utilisateur et le domaine de l'utilisateur sont facilement disponibles dans le contexte de l'API. Les enregistrements peuvent être liés à un utilisateur, un chemin d'audit doit être établi et la séparation de domaine peut être réalisée. En outre, étant donné que vous êtes authentifié en tant qu'utilisateur spécifique, vous pouvez utiliser Utilisation de GlideRecordSecure pour empêcher tout accès non autorisé aux données.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisation

Pour protéger le processus de création d'enregistrement des utilisateurs extérieurs à l'application Opérations de sécurité , vous devez disposer du rôle sn_sec_cmn.api_write . Seuls les utilisateurs disposant de ce rôle peuvent accéder aux API.

Paramètres de demande de configuration

Les paramètres de demande suivants sont disponibles.

Nom	Par défaut	Description
ignore_mandatory_fields	faux	Si la valeur est définie sur vrai, l'enregistrement est conservé même si les champs obligatoires ne sont pas renseignés.
include_wrap	faux	Si la valeur est définie sur vrai, la réponse inclut la couche standard fournie par l'instance pour les API REST basées sur un script.
simple_response	faux	Si la valeur est définie sur vrai, la réponse indique uniquement si l'opération a réussi.

Réponses d'erreur

Les erreurs suivantes peuvent se produire.

Message d'erreur	Quand cela se produit-il ?	Solution
Accès insuffisant	L'utilisateur ne dispose pas du rôle sn_sec_cmn.api_write.	Ajoutez le rôle à l'utilisateur.
Corps de publication non valide	Le corps de la demande est vide ou est un objet vide.	Conforme à la définition de l'API.
Aucun champ fourni	Les champs de données fournis pour conserver sont vides.	Conforme à la définition de l'API.
Champs obligatoires manquants : x,y,z	Les champs obligatoires sont manquants.	Conformez-vous à la définition de table de la table cible ou définissez **ignore_mandatory_fields** sur vrai.
Impossible de conserver l'enregistrement	Impossible de conserver l'enregistrement analysé.	Échec de l'insertion de GlideRecord, une analyse plus approfondie est requise.
Erreur inconnue	Se produit si aucun chemin d'erreur connu n'a été suivi.	Une analyse plus approfondie est nécessaire.

Cas d'utilisation de l'enrichissement de CI

À l'aide de vos scripts tiers, vous pouvez écrire dans la table Enrichissement des éléments de configuration [sn_sec_cmn_ci_enrichment_result] pour l'enrichissement de CI. Les

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

enregistrements d'enrichissement sont basés sur les options existantes qui fournissent des informations détaillées sur un enregistrement provenant d'une source tierce.

Des exemples de demande et de réponses pour le cas d'utilisation d'enrichissement de CI sont affichés ici.

Créer une demande d'enrichissement de CI


```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```


Créer-Réponse pour l'enrichissement de CI


```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```


Cas d'utilisation de l'enrichissement des observables

À l'aide de vos scripts tiers, vous pouvez écrire dans la table Résultat de l'enrichissement des observables `[sn_ti_observable_enrichment_result]` pour l'enrichissement des observables. Les enregistrements d'enrichissement sont basés sur les options existantes qui fournissent des informations détaillées sur un enregistrement provenant d'une source tierce.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Des exemples de demande et de réponses pour le cas d'utilisation d'enrichissement des observables sont affichés ici.

Créer une demande d'enrichissement des observables


```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```


Créer-Réponse pour l'enrichissement des observables


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```


Remarque : En plus d'enrichir les enregistrements existants, vous pouvez également Opérations de sécurité Mappage des données d'enrichissement ajouter de nouveaux enregistrements à des tables en transmettant une **enrichment_mapping_id** pour un mappage d'enrichissement existant et une chaîne **de raw_data** correspondante qui peut être analysée par le processus de mappage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation de la recherche de menaces

À l'aide de vos scripts tiers, vous pouvez écrire dans la table Résultat de la recherche de menace [sn_ti_lookup_result] pour obtenir les résultats de la recherche de menace. Les enregistrements de recherche sont basés sur les options existantes qui fournissent des informations détaillées sur un enregistrement provenant d'une source tierce.

Des exemples de demande et de réponses pour le cas d'utilisation de recherche de menaces sont affichés ici.

Créer une demande pour les recherches de menaces


```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer-Réponse pour les recherches de menaces


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


Options d'intégration

Le Options d'intégration cadre de travail fournit une architecture cohérente pour prendre en charge l'interopérabilité avec les intégrations tierces. Cette interface et ce modèle de données abstraits isolent les intégrations des changements apportés à l'application principale et garantissent une expérience cohérente pour les types d'intégrations similaires.

Chaque option d'intégration est conservée dans la table Aptitude d'intégration `[sn_sec_cmn_integration_capability]`. Les workflows d'aptitude d'intégration ne peuvent pas être exécutés seuls et nécessitent le lancement d'un workflow d'implémentation. Tout module d'extension fournissant une implémentation de la fonctionnalité ajoute son implémentation à la table enfant : Implémentation de l'aptitude d'intégration `[sn_sec_cmn_integration_capability_implementation]`.

L'implémentation spécifie le workflow à exécuter, l'intégration connexe (ID de module d'extension) et l'aptitude qu'elle implémente. Ces flux de travail peuvent être exécutés en parallèle à l'aide du lanceur de flux de travail parallèle. Toutefois, l'exécution séquentielle est l'option par défaut dans le système de base. Si nécessaire, vous pouvez modifier l'ordre d'exécution.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Security Operations Integration - Aptitude de demande de bloc

L'option Blocage bloque les observables associées à un incident de sécurité sur un pare-feu, un proxy web ou un autre point de contrôle à l'aide de workflows d'implémentation. Cette option est utilisée au cours des enquêtes de réponse à un incident pour contenir une menace identifiée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'option Demande de bloc dispose d'un workflow, Security Operations Integration - Workflow de demande de bloc, qui exécute la demande de blocage. Ce workflow accepte une liste d'observables, détecte toutes les options d'implémentation et exécute la demande en fonction du workflow configuré.

L'aptitude utilise également d'autres implémentations :

- Workflow du lanceur de pare-feu Security Operations Integration Palo Alto Networks
- Security Operations Palo Alto Networks : workflow de vérification et de blocage de la valeur

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Exécuter une demande de bloc

Bloque la communication avec les observables associés à un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

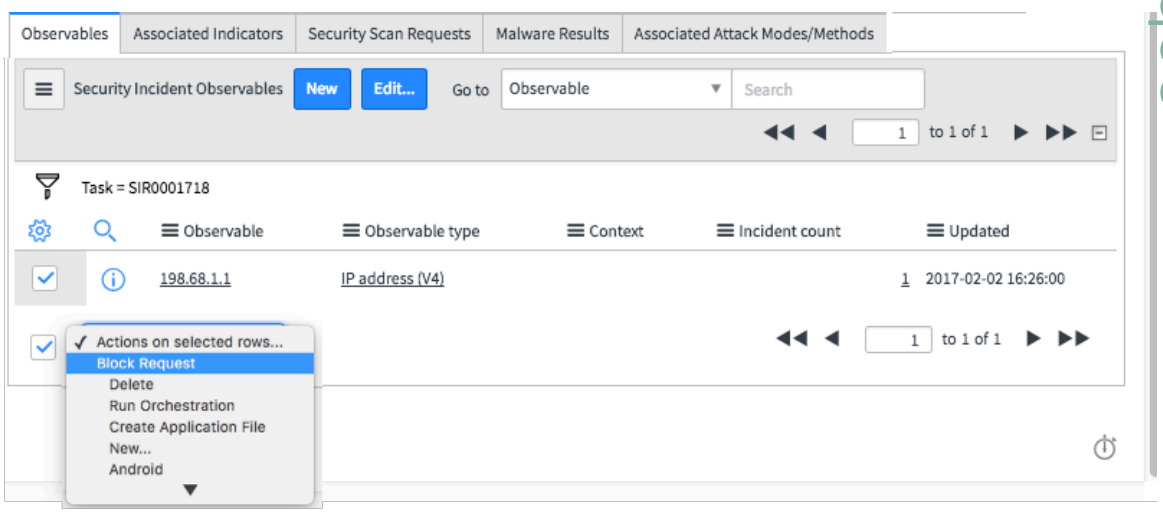
Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Le workflow **Security Operations Integration - Demande de bloc**peut être déclenché à partir d'un formulaire d'observable ou de la liste connexe **Observables d'incident de sécurité** sur un incident de sécurité.

Cet exemple montre une demande de bloc à partir d'un incident de sécurité.

Procédure

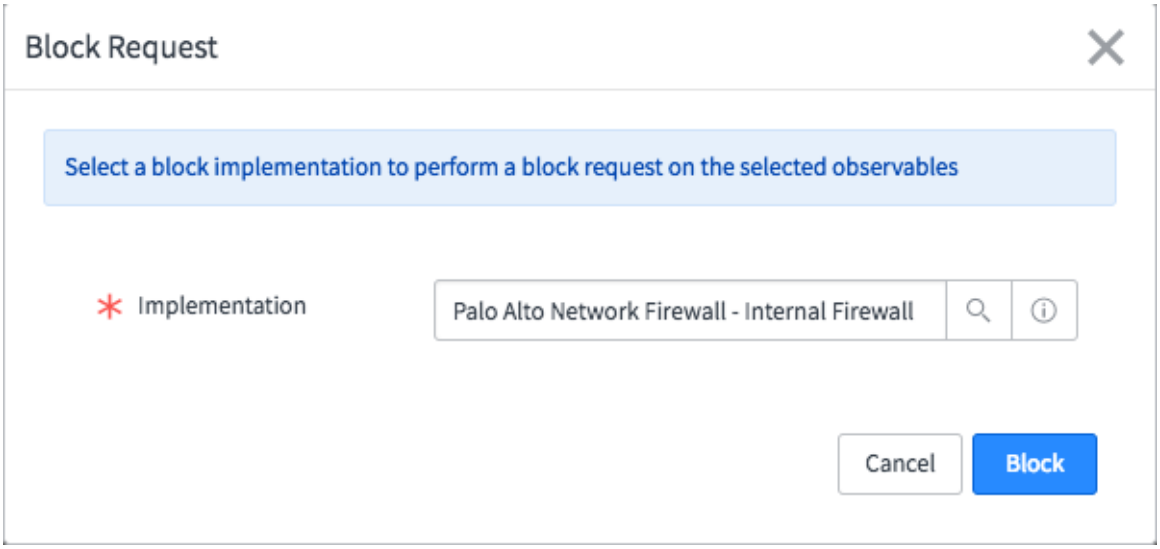
1. Accédez à un incident de sécurité.
2. Sélectionnez des observables dans l'onglet **Liste connexe** .
3. Cliquez sur **Bloquer la demande** dans le menu déroulant **Actions sur les lignes sélectionnées.**



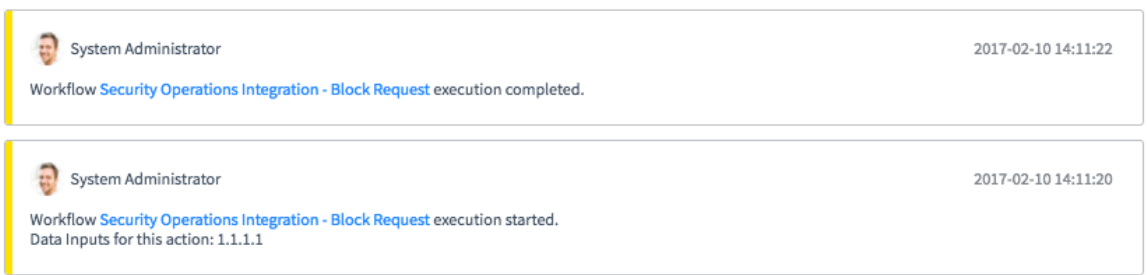
La boîte de dialogue s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Choisissez l'implémentation.
5. Cliquez sur **Bloquer**.
   L'audit d'exécution du workflow est affiché dans la section Notes de travail.



Security Operations Integration - Workflow de demande de bloc

Le workflow Security Operations Integration - Block Request est un workflow de haut niveau indépendant des intégrations. Il bloque les observables associés à un incident de sécurité. Utilisez-le pour réaliser une intégration telle que Palo Alto Networks - Firewall.

Avant de commencer

Rôle requis : sn_si.analyst

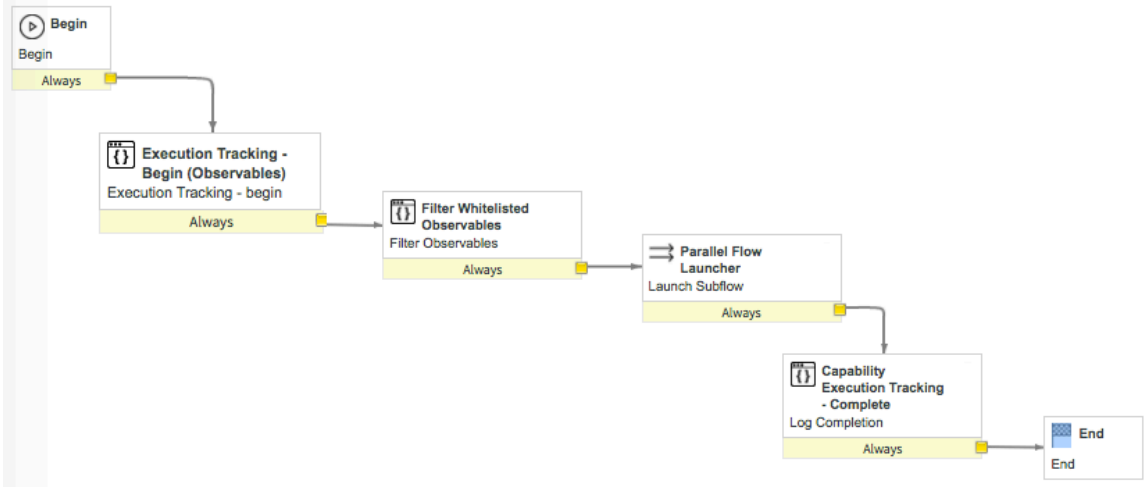
Pourquoi et quand exécuter cette tâche

Le workflow **Intégration de Security Operations - Demande de bloc**peut être déclenché sur un formulaire d'observable ou à partir de la liste connexe **Observables d'incident de sécurité** sur un incident de sécurité. Sur une liste, il se trouve dans le menu d'action déroulant. Sur un formulaire, il s'agit d'un lien connexe. Le blocage d'une demande n'est disponible que lorsqu'une implémentation est installée pour l'option de demande de blocage.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demande de bloc



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Security Operations Integration - Aptitude de recherche et de suppression d'e-mails

L'option de recherche et de suppression d'e-mail renvoie le nombre d'e-mails de menace à partir d'une recherche de serveur de messagerie et, éventuellement, renvoie des détails pour chaque e-mail trouvé. Une fois la recherche d'e-mails terminée, vous pouvez supprimer les e-mails.

L'option de recherche et de suppression d'e-mail dispose d'un workflow qui exécute les processus de recherche et de suppression d'e-mails.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit. En outre, si aucune des implémentations des aptitudes **de recherche et de suppression d'e-mail** n'est active, le lien connexe de **recherche d'e-mail** sur un incident de sécurité n'est pas affiché.

Security Operations Integration - Workflow de recherche et de suppression d'e-mail

Le workflow Intégration des opérations de sécurité : recherche et suppression d'e-mails renvoie le nombre d'e-mails de menace issus d'une recherche de serveur de messagerie et, éventuellement, renvoie des détails pour chaque e-mail trouvé. Une fois la recherche d'e-mails terminée, vous pouvez supprimer les e-mails.

Avant de commencer

Rôle requis : sn_si.analyst

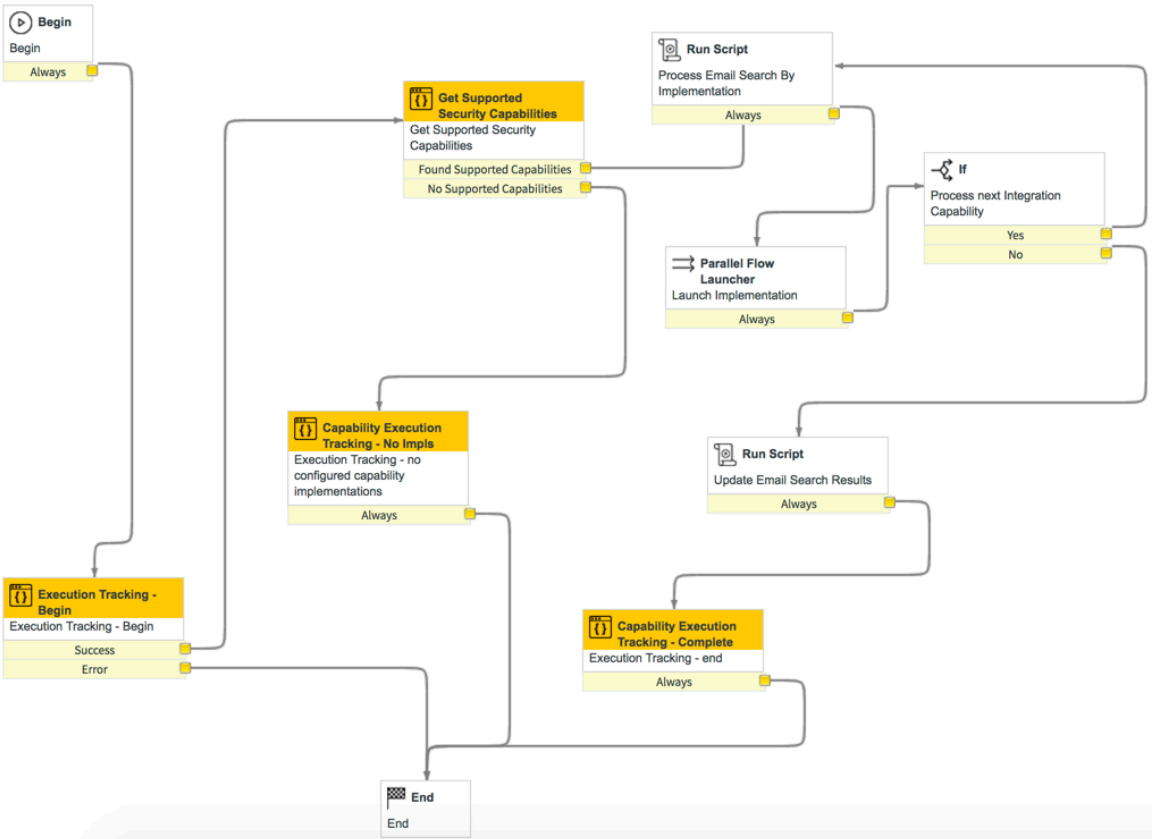
Pourquoi et quand exécuter cette tâche

L'exécution de la requête de recherche peut prendre un certain temps. Une fois le décompte reçu, une approbation est requise pour supprimer les e-mails d'un serveur de messagerie.

Ce workflow est déclenché par les boutons **Supprimer des serveurs de messagerie** et **Rechercher sur les serveurs de messagerie** du formulaire **Recherche d'e-mail** lors d'un incident de sécurité. Pour plus d'informations, consultez Rechercher et supprimer les e-mails d'hameçonnage.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche et suppression d'e-mail



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Les activités de processus du workflow comprennent :

Activité de suivi des exécutions Commencer (recherche de courrier)

L'activité d'exécution de l'aptitude Suivi des exécutions - Commencer (recherche de courrier) crée un enregistrement de suivi des exécutions et marque l'état de l'enregistrement comme démarré. Cette activité est utilisée par tous les workflows d'aptitude et d'implémentation pour suivre leur état.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	L'enregistrement de suivi des exécutions a été créé.
Échec	Impossible de créer l'enregistrement de suivi de l'exécution.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
capabilityId	Identificateur système de l'option d'intégration en cours d'exécution.
ID implémentation	Identificateur système de l'implémentation de l'option d'intégration en cours d'exécution.
taskId	Identificateur système pour toute tâche associée au workflow.
ID workflowContextId	Identificateur système de l'enregistrement de contexte de workflow associé. Fourni par le système.
nom du workflow	Nom du workflow. Fourni par le système.
parentCapabilityExcutionId	Identificateur système de l'enregistrement d'audit qui a lancé le workflow d'implémentation. Uniquement requis pour les workflows d'implémentation de l'option d'intégration, tels que Splunk, Elasticsearch.
emailsearchId (en anglais seulement)	Sysid de l'enregistrement de recherche d'e-mail dans la table Recherche d'e-mail [sn_sec_cmn_email_search].

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
CapabilityExecutionId	Identificateur système de l'enregistrement de suivi de l'exécution.

- Activité Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité

Security Operations Integration - Enrichir la capacité CI

L'option Enrichir le CI vous permet d'enrichir les données des éléments de configuration associés à un incident de sécurité.

L'option **Enrichir le CI** dispose d'un workflow, Security Operations Integration - Workflow d'enrichissement de CI. Lorsque le workflow d'aptitude s'exécute, il exécute des workflows supplémentaires pour les implémentations activées. Vous pouvez spécifier une implémentation à utiliser pour effectuer l'enrichissement sur les CI sélectionnés, ou vous pouvez effectuer l'enrichissement en utilisant toutes les implémentations.

Remarque : Ces données enrichies ne sont pas le type de données que vous souhaiteriez stocker dans votre CMDB, car il s'agit de données médico-légales spécifiques à une enquête donnée, par exemple, l'exécution d'un memdump à partir d'un CI. Au lieu de cela, les données sont stockées dans la table Enrichissement des éléments de configuration [sn_sec_cmn_ci_enrichment_result].

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Operations Integration - Workflow d'enrichissement de CI

Le workflow Intégration des opérations de sécurité - Enrichissement de CI vous permet d'enrichir les données des éléments de configuration (CI) associés à un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

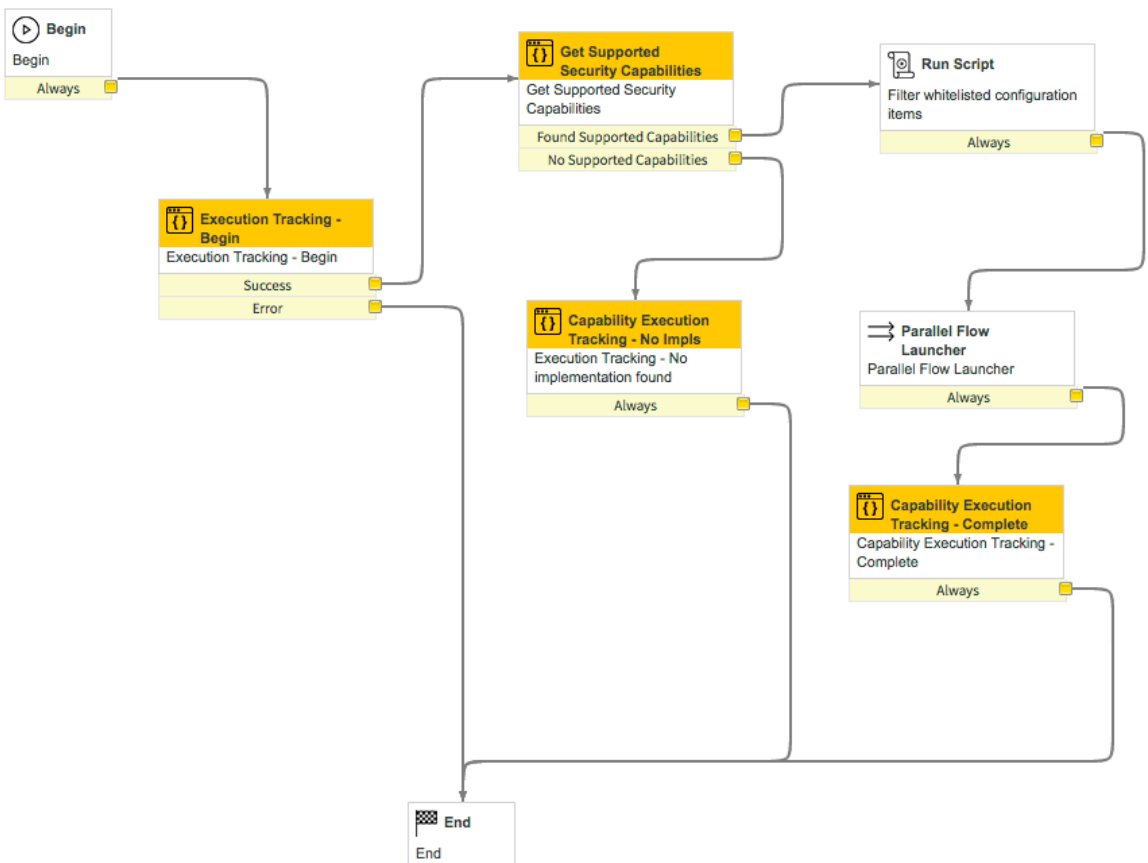
Le déclenchement de ce workflow se fait Réponse aux incidents de sécurité de deux manières.

- en sélectionnant un ou plusieurs CI dans l'onglet **Éléments de configuration** (sous le lien connexe **Éléments affectés**) et en sélectionnant **Exécuter l'enrichissement de CI** dans la liste de choix **Actions sur les lignes sélectionnées** .
- en ouvrant un enregistrement de CI et en cliquant sur le lien connexe **Exécuter l'enrichissement de CI** .

L'une ou l'autre méthode vous permet ensuite de spécifier les implémentations à utiliser pour enrichir les CI sélectionnés. Les workflows d'implémentation associés sont exécutés pour effectuer l'enrichissement.

Remarque : Le système de base n'inclut pas de workflow d'implémentation pour cette option. Pour enrichir les CI, vous devez créer votre propre workflow d'implémentation.

Enrichissement de CI



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les activités de processus du workflow comprennent :

- Suivi des exécutions : démarrer l'activité
- Security Operations Integration - Workflow d'enrichissement de CI
- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité
- Activité Obtenir les options de sécurité prises en charge

Intégration de Security Operations : aptitude d'enrichissement des observables

L'option Enrichir les observables permet d'enrichir les éléments observables à l'aide d'informations issues de différentes sources tierces qui utilisent des workflows d'implémentation. Cette option est utilisée au cours des enquêtes de réponse à un incident pour contenir une menace identifiée.

L'option Enrichir les observables dispose d'un workflow, Workflow Security Operations Integration - Enrichir les observables. Lorsque le workflow d'aptitude s'exécute, il exécute des workflows supplémentaires pour les implémentations activées. Vous pouvez spécifier une implémentation à utiliser pour effectuer l'enrichissement sur les observables sélectionnés, ou vous pouvez effectuer l'enrichissement à l'aide de toutes les implémentations qui correspondent aux types d'observables pris en charge.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Workflow Security Operations Integration - Enrichir les observables

Le sous-flux Intégration de Security Operations - Enrichir les observables vous permet d'enrichir les éléments observables à l'aide d'informations issues de différentes sources à l'aide de Concepteur de flux d'implémentation.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Ce workflow peut être déclenché de deux Réponse aux incidents de sécurité manières ou Renseignements sur les menaces de deux façons.

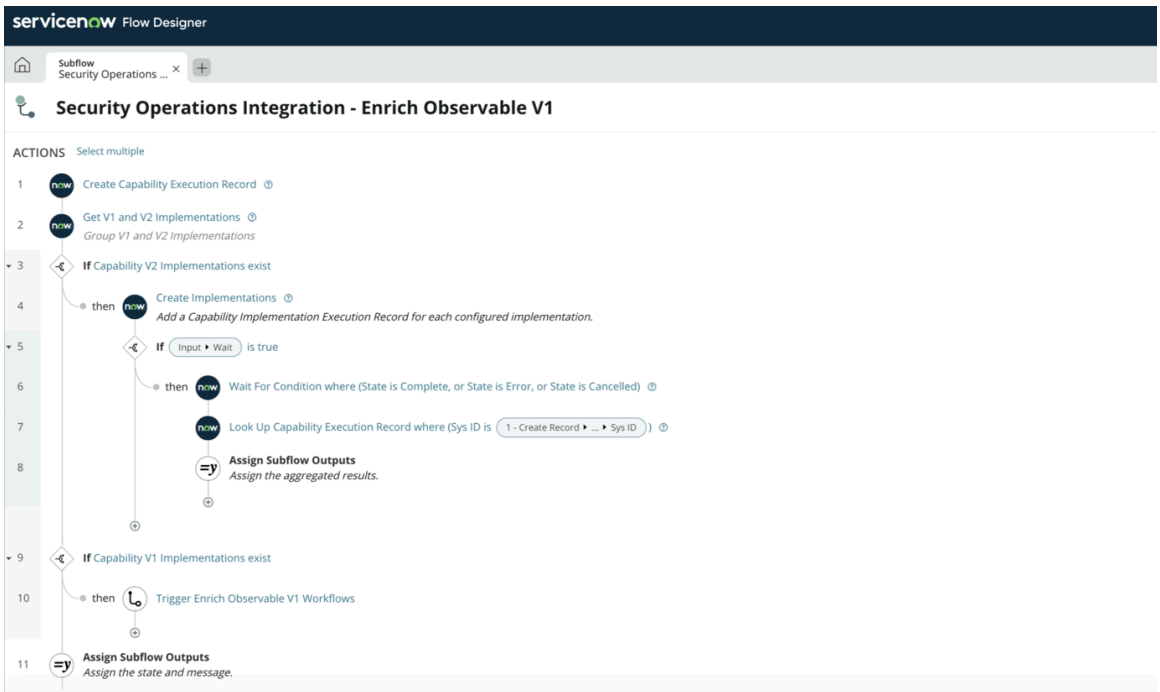
- en sélectionnant un ou plusieurs observables dans la liste Observables et en sélectionnant **Exécuter l'enrichissement de l'observable** dans la liste **de choix Actions sur les lignes sélectionnées** .
- en ouvrant un enregistrement d'observable et en cliquant sur le lien connexe **Exécuter l'enrichissement de l'observable** .

L'une ou l'autre méthode vous permet ensuite de spécifier les implémentations à utiliser pour enrichir les observables sélectionnés. Les workflows d'implémentation associés sont exécutés pour effectuer l'enrichissement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enrichir les observables



Les activités spécifiques à ce flux sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Les activités de processus du workflow comprennent :

- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité
- Activité Obtenir les options de sécurité prises en chargeSuivi de l'exécution de l'aptitude : aucune implémentation de l'activité

Security Operations Integration - Aptitude Obtenir les statistiques réseau

L'option Obtenir les statistiques réseau récupère une liste des connexions réseau actives à partir d'un hôte ou d'un point de terminaison. Il peut être utilisé pour enrichir les incidents au cours des enquêtes. Cette aptitude est déclenchée automatiquement lorsqu'un élément de configuration est ajouté à un incident de sécurité.

L'option **Obtenir les statistiques réseau** dispose d'un workflow Workflow Security Operations Integrations - Obtenir les statistiques réseau qui accepte un ou plusieurs CI et tâches. Le workflow itère sur chaque implémentation et chaque CI et invoque à nouveau le workflow d'implémentation.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Workflow Security Operations Integrations - Obtenir les statistiques réseau

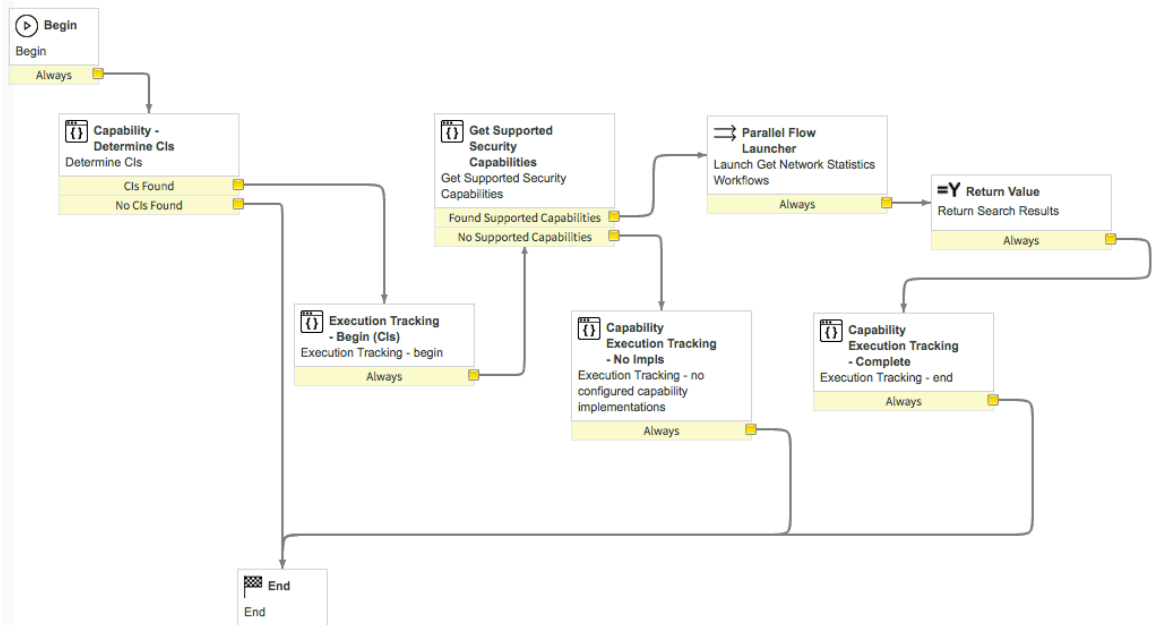
Le workflow Intégrations Security Operations - Obtenir les statistiques réseau récupère une liste des connexions réseau actives à partir d'un hôte ou d'un point de terminaison.

Avant de commencer
Rôle requis : sn_si.analyst

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche
Ce workflow s'exécute automatiquement lorsqu'un élément de configuration est ajouté à un incident de sécurité.

Obtenir les statistiques réseau



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Les activités du workflow comprennent :

- Aptitude : déterminer l'activité des CI
-

.

Suivi des exécutions - Activité de début (CI)

L'activité de workflow Suivi de l'exécution - Début (CI) démarre le processus d'audit pour un Opérations de sécurité workflow d'intégration qui fonctionne sur les éléments de configuration (CI).

L'activité **Suivi des exécutions - Début (CI)** peut être utilisée avec n'importe quel workflow de CI pour commencer à enregistrer la progression du workflow dans un audit.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Un enregistrement d'audit est créé.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
capabilityId	Identificateur système de l'option d'intégration en cours d'exécution.
isImpl	Marqueur qui spécifie si l'audit est effectué pour un workflow d'option d'intégration ou un workflow d'implémentation d'aptitude d'intégration. Les valeurs possibles sont les suivantes : • faux : désigne un audit sur un workflow abstrait d'aptitude d'intégration tel que la recherche de perceptions. (par défaut.) • vrai : désigne un audit sur un workflow d'implémentation d'option d'intégration. Par exemple, Splunk ou Elasticsearch.
taskId	Identificateur système pour toute tâche associée au workflow.

ciList	Un ou plusieurs éléments de configuration (CI) contre lesquels effectuer l'action souhaitée au format suivant :
	`["sysId", "sysId"]`
	ou
	`"sysId"`
	Utilisé comme entrée de workflow.

ID workflowContextId	Identificateur système de l'enregistrement de contexte de workflow associé. Fourni par le système.
nom du workflow	Nom du workflow. Fourni par le système.
parentCapabilityExcutionId	Identificateur système de l'enregistrement d'audit qui a lancé le workflow d'implémentation. Requis uniquement pour les workflows d'implémentation d'aptitude d'intégration tels que Splunk, Elasticsearch.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
CapabilityExecutionId	Identificateur système de l'enregistrement d'audit.

Les activités de processus du workflow comprennent :

- Activité Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow Security Incident Response - Obtenir les statistiques réseau

Le champ **Réponse aux incidents de sécurité** > **Obtenir les statistiques réseau** workflow récupère les statistiques réseau d'une ressource Windows affectée lorsqu'elle est ajoutée à un incident de sécurité à l'état **Analyse** .

Avant de commencer

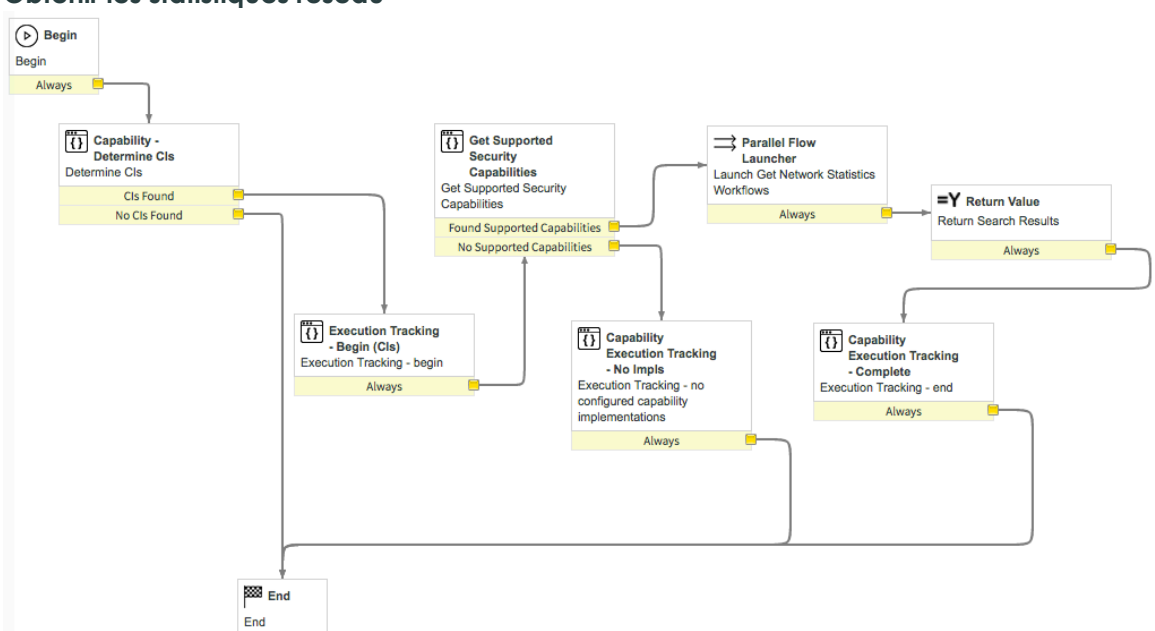
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Pour les nouveaux incidents de sécurité contenant des éléments de configuration, le workflow s'exécute automatiquement lorsque l'état passe à **Analyse**.

Les incidents de sécurité existants sont automatiquement mis à jour lorsque vous êtes dans l'état **Analyse** et que vous ajoutez un nouvel élément de configuration.

Obtenir les statistiques réseau



Les activités de processus du workflow comprennent :

- Obtenir l'activité FQDN de l'élément de configuration
- Déterminer le script Shell par système d'exploitation
- Si l'instruction est exécutée par Powershell
- Suivi des exécutions : démarrer l'activité
- Obtenir les statistiques réseau via l'activité netstat
- Suivi d'exécution de l'aptitude : activité d'échec
- Créer une activité d'enregistrements de données d'enrichissement
- Suivi d'exécution de l'aptitude : activité d'échec - Renvoie l'ID d'enrichissement.
- Suivi d'exécution de l'aptitude : terminer l'activité

Procédure

1. Ouvrez un incident de sécurité.
2. Mettez à jour **l'état** sur **Analyse**, si nécessaire.
3. Ajoutez un élément de configuration (ordinateur, serveur ou similaire).

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Mettre à jour**.
   Orchestration de la réponse aux incidents de sécurité fournit des informations statistiques sur le réseau dans le **Liens connexes** > **Enrichissements des incidents de sécurité** onglet. Pour plus d'informations, reportez-vous à la section Opérations de sécurité Mappage des données d'enrichissement.

   Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Security Operations Integration - Obtenir l'aptitude Processus en cours d'exécution

L'option Obtenir les processus en cours d'exécution récupère une liste des processus en cours sur un élément de configuration (CI) à partir d'un point de terminaison ou d'un hôte. Cette option sert à enrichir les incidents au cours des enquêtes.

L'option Obtenir les processus en cours d'exécution comporte deux workflows d'implémentation :

- Intégration de Security Operations Carbon Black : workflow Obtenir les processus en cours d'exécution
- Intégration des commandes système Security Operations : workflow Obtenir les processus en cours d'exécution

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Security Operations : workflow Obtenir les processus en cours d'exécution

Le workflow Opérations de sécurité : obtenir l'exécution des processus est un workflow de haut niveau indépendant des intégrations. Il récupère une liste des processus en cours d'exécution sur un élément de configuration (CI) à partir d'un hôte. Utilisez-le pour réaliser une intégration, telle que Carbon Black, ou pour un incident de sécurité Windows.

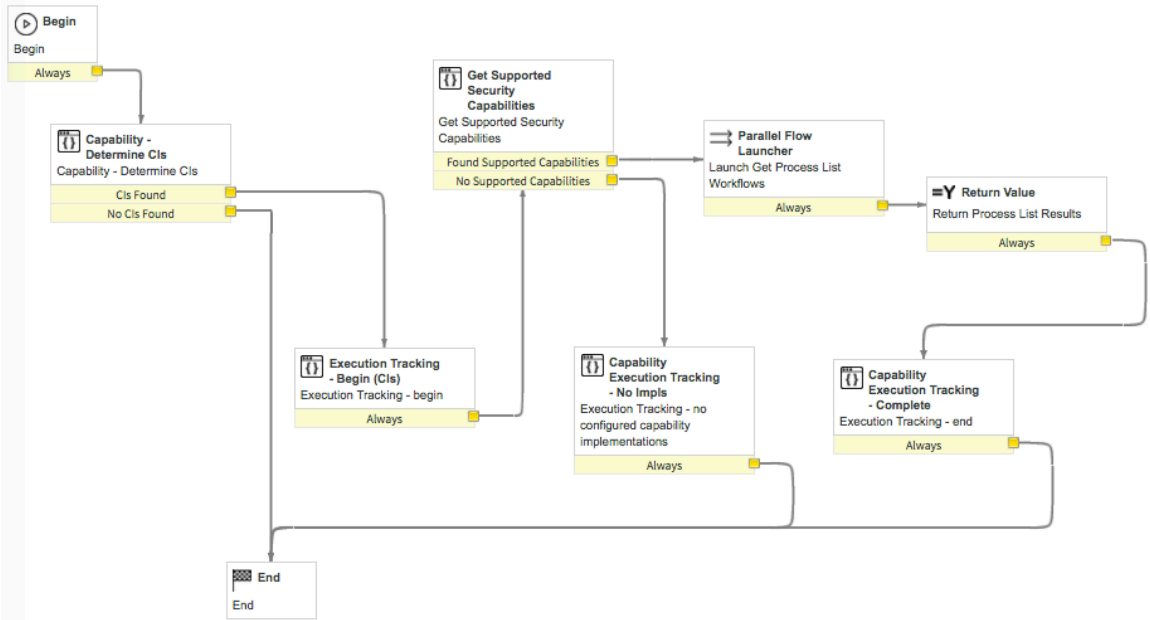
Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Les activités de processus du workflow comprennent :

- Aptitude : déterminer l'activité des CI
- Suivi des exécutions - Activité de début (CI)
- Activité Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité
- Lanceur de flux parallèle : renvoie les résultats de la recherche dans un tableau.
- Suivi d'exécution de l'aptitude : terminer l'activité

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Obtenir l'exécution des processus



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Intégration de Security Operations Carbon Black : workflow Obtenir les processus en cours d'exécution

L'intégration de Security Operations Carbon Black - Get Running Processes est l'implémentation de l'intégration Carbon Black lancée par le workflow Security Operations Integration - Get Running Process.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Les activités de processus du workflow comprennent :

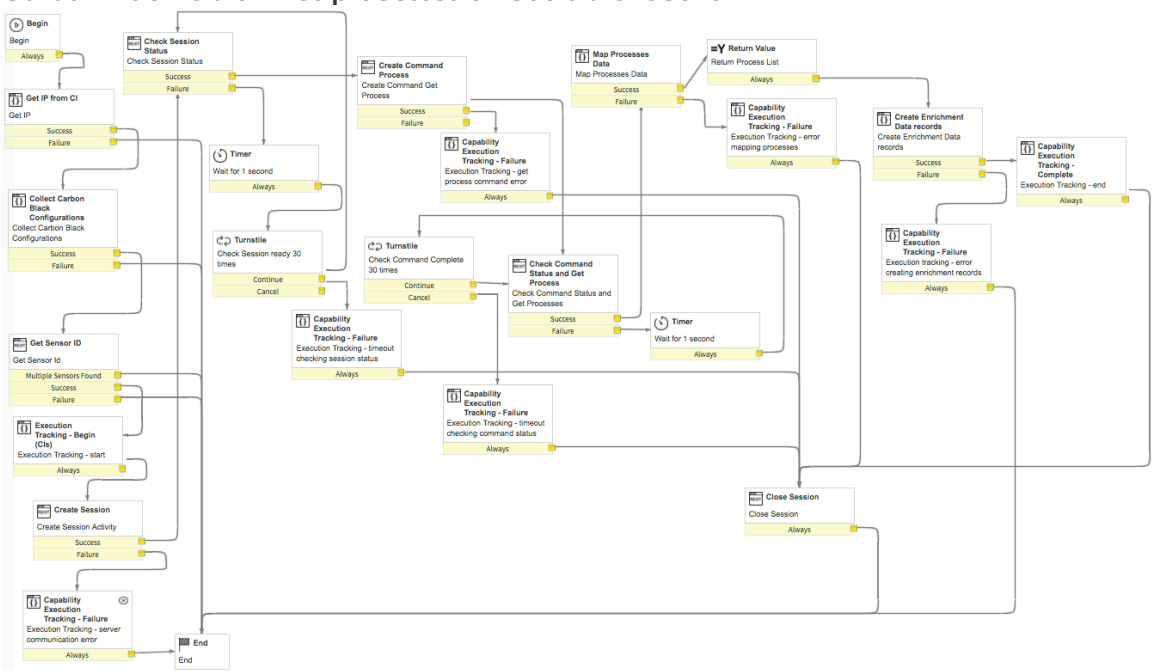
- Obtenir l'adresse IP à partir de l'activité du CI
- Collecter l'activité Configurations Carbon Black
- Obtenir l'activité d'ID de capteur
- Suivi des exécutions : démarrer l'activité
- Créer une session
- Suivi d'exécution de l'aptitude : activité d'échec
- Activité Vérifier l'état de la session
- Activité du workflow du minuteur : attend 1 seconde
- Activité du workflow du tourniquet : vérifier que la session est prête 30 fois
- Créer une activité de processus de commande
- Vérifier l'état des commande et obtenir l'activité du processus
- Processus de mappage Activité des données et liste des processus de retour
- Créer une activité d'enregistrements de données d'enrichissement

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Suivi d'exécution de l'aptitude : terminer l'activité
- Fermer l'activité de la session

Carbon Black Obtenir les processus en cours d'exécution



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Collecter l'activité Configurations Carbon Black

L'activité de workflow Collecter les configurations Carbon Black rassemble les informations de configuration à utiliser dans le workflow.

L'activité Collecter les configurations Carbon Black rassemble les informations de configuration Carbon Black à utiliser dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Configuration réussie.
Échec	Une erreur s'est produite lors de la tentative de vérification de la configuration. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Il n'existe aucune variable d'entrée pour cette activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
endpoint_base	URL de base de l'API d'intégration tierce.
use_mid_server	Détermine si l'activité REST utilise le MID Server pour interagir avec Carbon Black ou non.
api_token	Clé API d'intégration tierce.

Vérifier l'état du MID Server

Détermine si le Serveur MID identifié dans le champ **Hôte du Serveur MID** de la configuration de l'intégration est en cours d'exécution. Si le champ est défini sur **N'importe lequel**, l'activité vérifie qu'un Serveur MID est opérationnel.

L'activité Vérifier l'état du serveur MID peut être utilisée avec n'importe quel workflow pour vérifier la présence d'un serveur MID en cours d'exécution dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	État de session renvoyé.
Échec	Erreur d'état de session. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
CapabilityExecutionId	ID de l'option en cours d'exécution.
nom du workflow	Nom du workflow en cours d'exécution.
mid_server_host	Serveur MID identifié dans la configuration de l'intégration

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
mid_server_live	Identifie si le MID Server identifié dans le champ **Hôte du serveur MID** de la configuration de l'intégration est en cours d'exécution. Si le champ est défini sur **N'importe lequel**, l'activité vérifie qu'un Serveur MID est opérationnel.

Obtenir l'activité d'ID de capteur

L'activité de workflow Obtenir l'ID de capteur rassemble les identificateurs de capteurs à utiliser dans le workflow.

L'activité Obtenir l'ID de capteur peut être utilisée avec n'importe quel workflow pour recueillir des informations de capteur à utiliser dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Identificateurs de capteur trouvés.
Échec	Aucun capteur n'a été trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
api_token	Clé API Carbon Black.
use_mid_server	Détermine si l'activité REST utilise le MID Server pour interagir avec Carbon Black ou non.
endpoint_base	URL de base de l'API Carbon Black.
ci_ip_address	Adresse IP de l'élément de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code d'erreur HTTP et un message.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
Type d'élément de tableau	Variables d'API.
sensor_detail	Description du capteur Carbon Black au format JSON.

Créer une activité de session

L'activité de workflow Créer une session établit une session Carbon Black à utiliser dans le workflow.

L'activité Créer une session peut être utilisée avec n'importe quel workflow pour créer une session Carbon Black dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Session créée.
Échec	Session non créée. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l'API Carbon Black.
sensor_id	Identificateur de capteur.
use_mid_server	Détermine si l'activité REST utilise le MID Server pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code d'erreur HTTP et un message.
output	Variables d'API

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activité Vérifier l'état de la session

Détermine l'état d'une session Carbon Black dans le workflow.

L'activité Vérifier l'état de la session peut être utilisée avec n'importe quel workflow pour vérifier l'état de la session Carbon Black dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	État de session renvoyé.
Échec	Erreur d'état de session. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l'API Carbon Black.
session_id	Identificateur de session.
use_mid_server	Détermine si l'activité REST utilise le MID Server pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code d'erreur HTTP et un message.
output	Informations sur les processus en cours d'exécution de Carbon Black.

Créer une activité de processus de commande

L'activité de workflow Créer un processus de commande crée un processus de commande Carbon Black à utiliser dans le workflow.

L'activité Créer un processus de commande peut être utilisée avec n'importe quel workflow pour créer un processus de commande Carbon Black dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Processus de commande créé.
Échec	Processus de commande non créé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l'API Carbon Black.
session_id	Identificateur de session.
command_id	Identificateur de commande.
use_mid_server	Détermine si l'activité REST utilise le MID Server pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code d'erreur HTTP et un message.
output	Variables d'API

Vérifier l'état des commande et obtenir l'activité du processus

Vérifie l'état de la commande Carbon Black et récupère les processus à utiliser dans le workflow.

Les activités Vérifier l'état de la commande et Obtenir le processus peuvent être utilisées avec n'importe quel workflow pour vérifier l'état d'une commande Carbon Black et obtenir des processus dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	État de commande renvoyé et processus créés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats (suite)

Résultat	Description
Échec	État de la commande ou erreur de processus. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l'API Carbon Black.
session_id	Identificateur de session.
command_id	Identificateur de commande.
use_mid_server	Détermine si l'activité REST utilise le MID Server pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code d'erreur HTTP et un message.
output	Variables d'API

Processus de mappage Activité des données

Les cartes d'activité du flux de travail des processus de carte Carbon Black traitent les données au sein du flux de travail.

L'activité Données des processus de mappage peut être utilisée avec n'importe quel workflow pour mapper les processus Carbon Black.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Processus mappés
Échec	Processus non mappés. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
affected_ci	Élément de configuration affecté.
implementation_id	Identificateur d'implémentation.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
output	Données de renvoi formatées sur les processus en cours d'exécution utilisés par le workflow abstrait.
processus	Liste des processus dans un tableau.

Suivi d'exécution de l'aptitude : terminer l'activité

L'activité Suivi de l'exécution de l'aptitude - Terminer le workflow met à jour l'enregistrement d'audit lorsque le workflow est terminé.

L'activité Suivi de l'exécution de l'aptitude : terminer peut être utilisée avec n'importe quel workflow pour enregistrer l'achèvement du workflow.

Remarque : Le tableau de **valeurs de retour** de l'activité principale **Lanceur parallèle** contient un tableau des résultats de tous les workflows d'intégration exécutés et invite à terminer correctement le suivi des exécutions.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	L'état de l'enregistrement d'audit est défini sur **Terminé**.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
CapabilityExecutionId	Identificateur système de l'enregistrement d'audit. Ce champ était la sortie de l'une des activités de début d'audit.
nom du workflow	Nom du workflow. Fourni par le système.
message	Message d'achèvement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Il n'y a pas de variables de sortie.

Fermer l'activité de la session

Ferme une session Carbon Black dans le workflow.

L'activité Fermer la session peut être utilisée avec n'importe quel workflow pour fermer une session Carbon Black.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Session fermée.
Échec	Session non fermée. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l'API Carbon Black.
session_id	Identificateur de session.
use_mid_server	Détermine si l'activité REST utilise le MID Server pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code d'erreur HTTP et un message.
output	Variables d'API

Intégration des commandes système Security Operations : workflow Obtenir les processus en cours d'exécution

Le workflow Intégration des commandes du système des opérations de sécurité : obtenir l'exécution des processus récupère les processus en cours d'un élément de configuration

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

lorsqu'il est ajouté ou mis à jour dans un incident de sécurité Windows ou Unix à l'état **Analyse**.

Avant de commencer
Rôle requis : sn_si.analyst

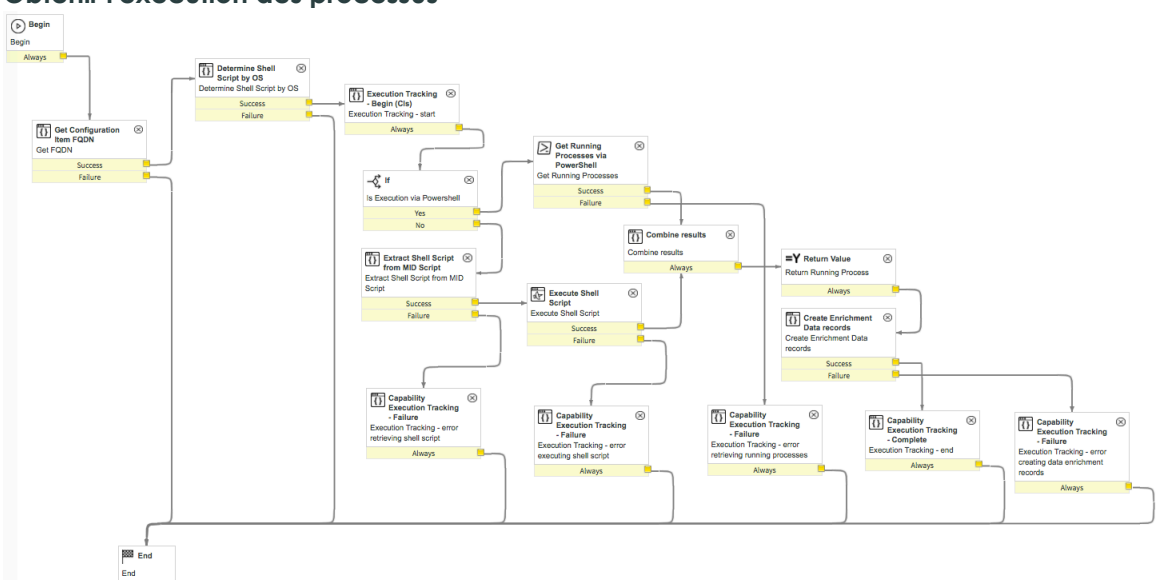
Pourquoi et quand exécuter cette tâche
Pour les nouveaux incidents de sécurité, le workflow s'exécute automatiquement lorsque vous soumettez l'incident avec un élément de configuration sélectionné, lorsque l'état passe automatiquement à **Analyse**. S'il reste à l'état **Brouillon** , il ne s'exécute pas.

Les incidents de sécurité existants sont automatiquement mis à jour lorsque vous êtes dans l'état **Analyse** et que vous ajoutez un nouvel élément de configuration.

Les activités de processus du workflow comprennent :

- Obtenir l'activité FQDN de l'élément de configuration
- Déterminer le script Shell par activité du système d'exploitation
- Suivi des exécutions : démarrer l'activité
- Obtenir les processus en cours d'exécution via PowerShell
- Activité Exécuter le script Shell
- Suivi d'exécution de l'aptitude : activité d'échec
- Extraire le script Shell de l'activité de script MID
- Combiner les résultats et les valeurs de retour dans un tableau
- Créer une activité d'enregistrements de données d'enrichissement
- Suivi d'exécution de l'aptitude : terminer l'activité

Obtenir l'exécution des processus



Procédure
1. Ouvrez un incident de sécurité.
2. Mettez à jour **l'état** sur **Analyse**, si nécessaire.
3. Ajoutez un élément de configuration (ordinateur, serveur ou similaire).
4. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Orchestration de la réponse aux incidents de sécurité fournit des informations sur le processus en cours dans le **Lien connexe** > **Enrichissements des incidents de sécurité**onglet. Pour plus d'informations, consultez Opérations de sécurité Mappage des données d'enrichissement.

Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Activité de combinaison des résultats

L'activité de workflow Combiner les résultats fusionne les résultats d'intégrations tierces pour les utiliser dans le workflow.

L'activité Combiner les résultats peut être utilisée avec n'importe quel workflow pour exécuter un script shell de MID Server dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Résultats combinés.
Échec	Échec de la combinaison. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
entréeA	Jeu de résultats A
entréeB	Jeu de résultats B
implementation_id	Identificateur d'implémentation.
affected_ci	Élément de configuration

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
résultat	Jeu de résultats A ou Jeu de résultats B en fonction de celui qui est rempli.

Activité Exécuter le script Shell

L'activité de workflow Exécuter le script shell exécute un script shell de MID Server dans le workflow.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'activité Exécuter le script shell peut être utilisée avec n'importe quel workflow pour exécuter un script shell de MID Server dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Script de l'interpréteur de commandes trouvé
Échec	Aucun script shell trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
target	IP ou nom de domaine complet (FQDN) du CI cible.
valeur script	Script, en tant que valeur de chaîne, exécuté sur un système Unix.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
réponse	Sortie brute. Données des processus en cours d'exécution.

Extraire le script Shell de l'activité de script MID

L'activité de workflow Extraire le script shell du script MID extrait un script shell de MID Server à utiliser dans le workflow.

L'activité Extraire le script shell du script MID peut être utilisée avec n'importe quel workflow pour extraire un script shell de MID Server à inclure dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Script de l'interpréteur de commandes trouvé
Échec	Aucun script shell trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
sysId	Identificateur système

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
valeur script	Script, en tant que valeur de chaîne, exécuté sur un système Unix.

Obtenir l'exécution des processus via l'activité PowerShell

L'activité de workflow Obtenir l'ID de capteur rassemble les processus en cours d'exécution à l'aide de PowerShell pour les utiliser dans le workflow.

L'activité de workflow Obtenir l'exécution des processus via PowerShell peut être utilisée avec n'importe quel workflow pour récupérer les processus à inclure dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Processus trouvés
Échec	Aucun processus trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
target	IP ou nom de domaine complet (FQDN) du CI cible.
Script de traitement	Script ECC exécuté sur un système Windows.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
réponse	Sortie brute. Données des processus en cours d'exécution.

Intégration de Security Operations : capacité Isoler l'hôte

L'option **Isoler l'hôte** limite les connexions du système à d'autres périphériques. Isoler l'hôte est exécuté sur un élément de configuration (CI).

L'option **Isoler l'hôte** dispose d'un workflow qui accepte un ou plusieurs CI et, éventuellement, Workflow Opérations de sécurité - Isoler l'hôte une implémentation. Vous pouvez spécifier une implémentation à utiliser pour isoler l'hôte ou pour que le workflow tente d'isoler l'hôte à l'aide de toutes les implémentations.

Remarque : Bien qu'il ne soit pas intégré à une option, un workflow Intégration de Security Operations Carbon Black : workflow de suppression de l'isolement de l'hôte est disponible pour l'orchestration afin de rétablir la communication avec un hôte isolé.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Exécuter Isoler l'hôte

Isoler l'hôte restreint les connexions du système à d'autres périphériques.

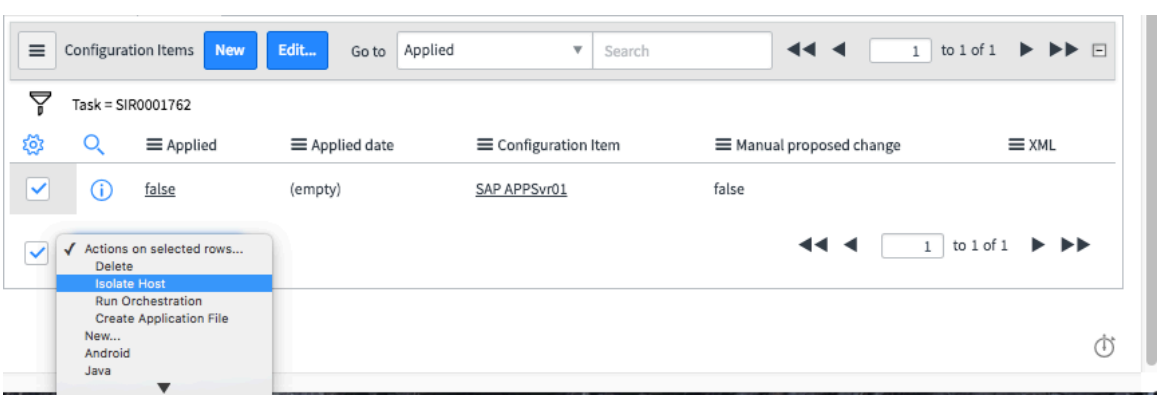
Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Le workflow **Intégration des opérations de sécurité - Isoler l'hôte ou le point de terminaison**peut être déclenché à partir de la liste connexe sur un incident de sécurité.

Procédure

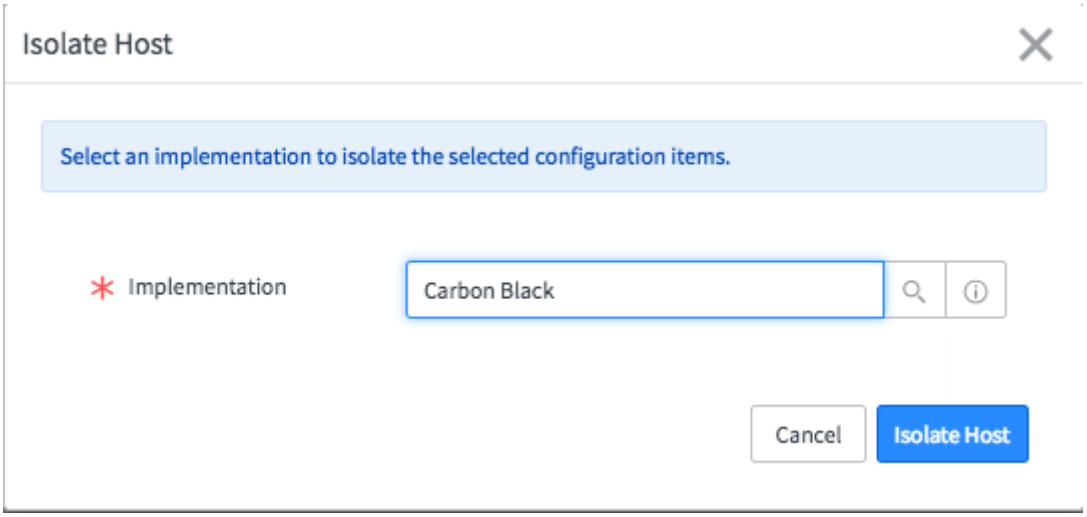
1. Accédez à un incident de sécurité.
2. Sélectionnez **des éléments de configuration** dans l'onglet **Liste connexe** .
3. Cliquez sur **Isoler l'hôte** dans le menu déroulant **Actions sur les lignes sélectionnées.**



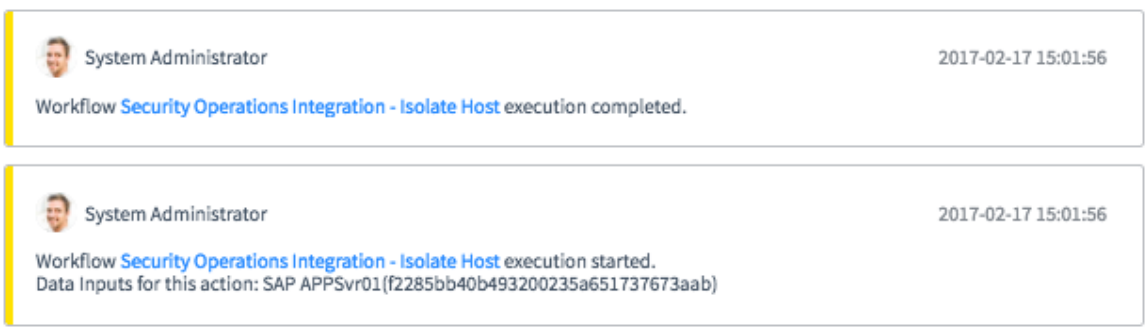
La boîte de dialogue s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Choisissez l'implémentation.
5. Cliquez sur **Isoler l'hôte**.
   L'audit d'exécution du workflow est affiché dans la section Notes de travail.



Workflow Opérations de sécurité - Isoler l'hôte

Le workflow **Opérations de sécurité - Isoler l'hôte** est un workflow de haut niveau indépendant des intégrations. Il utilise les requêtes configurées pour rechercher un ensemble d'éléments de configuration. Utilisez-le pour réaliser une intégration, telle que Carbon Black.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Ce workflow est déclenché à partir de l'onglet **Éléments de configuration** d'une liste connexe d'incidents de sécurité.

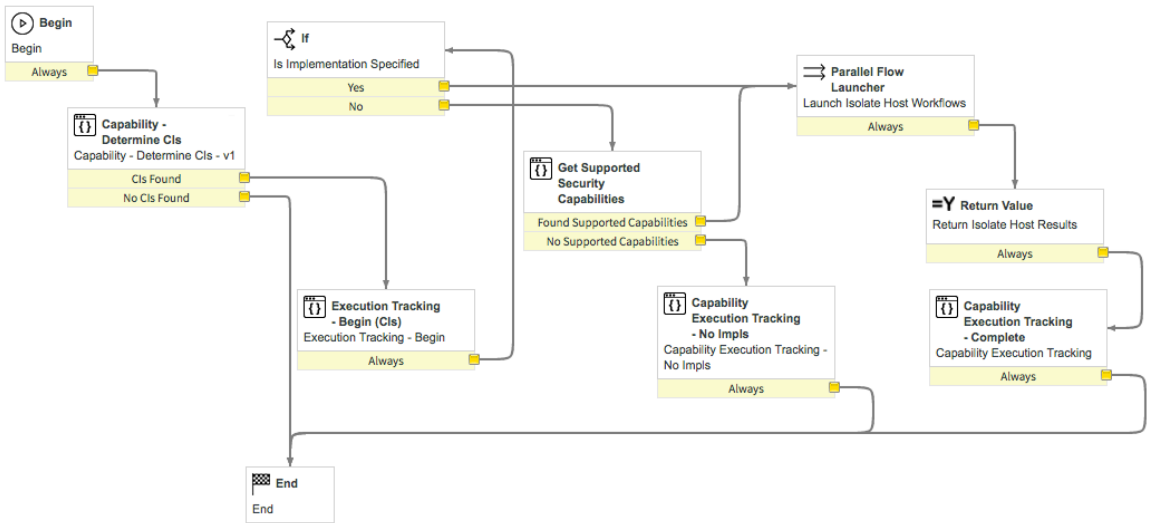
Les activités de processus du workflow comprennent :

- Aptitude : déterminer l'activité des CI
- Suivi des exécutions - Activité de début (CI)
- Activité Obtenir les options de sécurité prises en charge
- Lanceur de flux parallèle : lancer le workflow approprié. Stockez les résultats dans un tableau.
- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité
- Suivi d'exécution de l'aptitude : activité d'échec

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Isoler l'hôte



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Intégration de Security Operations Carbon Black : workflow Isoler l'hôte

L'intégration de Security Operations Carbon Black - Isoler l'hôte est l'implémentation de l'intégration Carbon Black lancée par le workflow Intégration de Security Operations - Isoler l'hôte.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Les activités de processus du workflow comprennent :

- Suivi des exécutions - Activité de début (CI)
- Obtenir l'adresse IP à partir du CI
- Recueillir les configurations Carbon Black
- Suivi d'exécution de l'aptitude : activité d'échec
- Obtenir l'ID de capteur
- Activer l'isolement réseau activité activée
- Mettre à jour le capteur ; renvoie le résultat Isoler l'hôte.
- Suivi d'exécution de l'aptitude : terminer l'activité

Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Obtenir l'activité d'ID de capteur

L'activité de workflow Obtenir l'ID de capteur rassemble les identificateurs de capteurs à utiliser dans le workflow.

L'activité Obtenir l'ID de capteur peut être utilisée avec n'importe quel workflow pour recueillir des informations de capteur à utiliser dans le workflow.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Identificateurs de capteur trouvés.
Échec	Aucun capteur n'a été trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
api_token	Clé API Carbon Black.
use_mid_server	Détermine si l'activité REST utilise le MID Server pour interagir avec Carbon Black ou non.
endpoint_base	URL de base de l'API Carbon Black.
ci_ip_address	Adresse IP de l'élément de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code d'erreur HTTP et un message.
Type d'élément de tableau	Variables d'API.
sensor_detail	Description du capteur Carbon Black au format JSON.

Activer l'isolement réseau activité activée

L'activité de workflow Activer l'isolement réseau active l'isolement réseau.

L'activité Activer l'isolement réseau peut être utilisée avec n'importe quel workflow pour activer l'isolement réseau.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Isolement réseau activé.
Échec	L'isolement réseau ne peut pas être activé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
sensor_detail	Description du capteur Carbon Black au format JSON.
Désactiver	Détermine si l'hôte est isolé ou supprime l'isolement de l'hôte. Vrai = désactiver l'isolement Faux = l'isolement reste activé

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
sensor_detail	Description du capteur Carbon Black au format JSON.

Mettre à jour l'activité du capteur

L'activité de workflow Mettre à jour le capteur met à jour le capteur pour isoler les hôtes ou les points de terminaison.

L'activité Mettre à jour le capteur peut être utilisée avec n'importe quel workflow pour isoler des hôtes ou des points de terminaison.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Capteur mis à jour.
Échec	Impossible de mettre à jour le capteur. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
api_token	Clé API Carbon Black.
use_mid_server	Détermine si l'activité REST utilise le MID Server pour interagir avec Carbon Black ou non.
endpoint_base	URL de base de l'API Carbon Black.
sensor_id	Identificateur de capteur.
sensor_detail	Description du capteur Carbon Black au format JSON.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code d'erreur HTTP et un message.

Intégration de Security Operations Carbon Black : workflow de suppression de l'isolement de l'hôte

Le workflow **Security Operations Carbon Black Integration - Remove Host Isolation débloque** la communication avec un hôte ou un point de terminaison spécifié dans un système Carbon Black.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

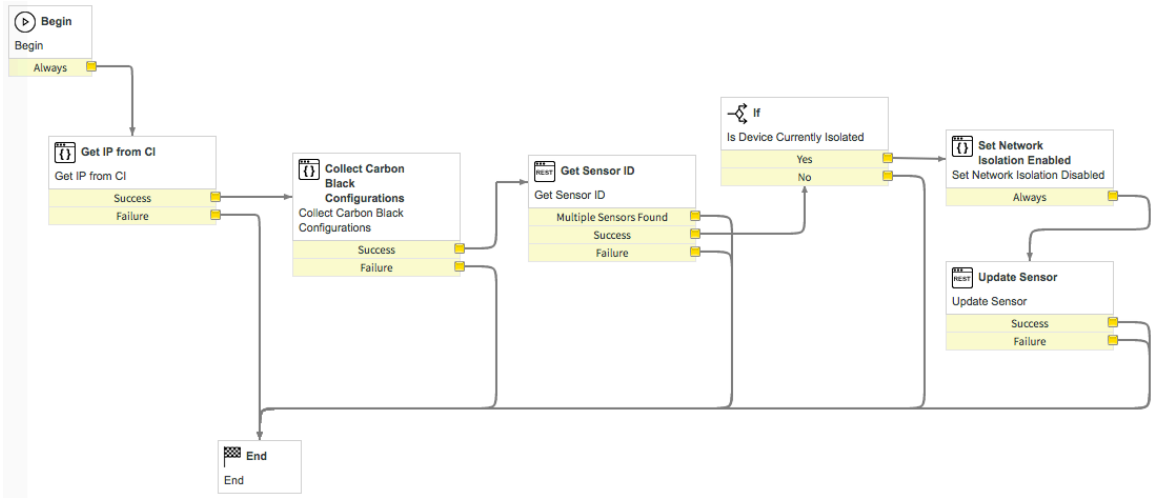
Ce workflow ne fait pas partie d'une aptitude et a besoin d'une orchestration personnalisée pour s'exécuter.
Les activités de processus du workflow comprennent :

- Obtenir l'adresse IP à partir de l'activité du CI
- En cas de réussite Collecter l'activité Configurations Carbon Black
- Obtenir l'activité d'ID de capteurObtenir l'ID de capteur
- Si l'appareil prend en charge l'isolement et que l'appareil n'estActiver l'isolement réseau activité activée pas isolé à désactivé.
- Mettre à jour l'activité du capteur- renvoie le résultat Isoler l'hôte.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration Carbon Black - Supprimer l'isolement de l'hôte



Intégration de Security Operations : aptitude Publier dans la liste de surveillance

L'option Publier dans la liste de surveillance ajoute les observables et les indicateurs associés à un incident de sécurité dans une liste de surveillance tierce qui surveille les événements de sécurité et génère des alertes. Cette option est utilisée dans le cadre de la réponse à un incident au cours des enquêtes.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Workflow Security Operations Integration - Publier dans la liste de surveillance

Le workflow **Intégrations pour opérations de sécurité - Publier dans la liste de surveillance** est un workflow de haut niveau indépendant des intégrations. Il ajoute des observables aux listes de surveillance tierces qui prennent en charge l'aptitude. Utilisez-la pour réaliser une intégration.

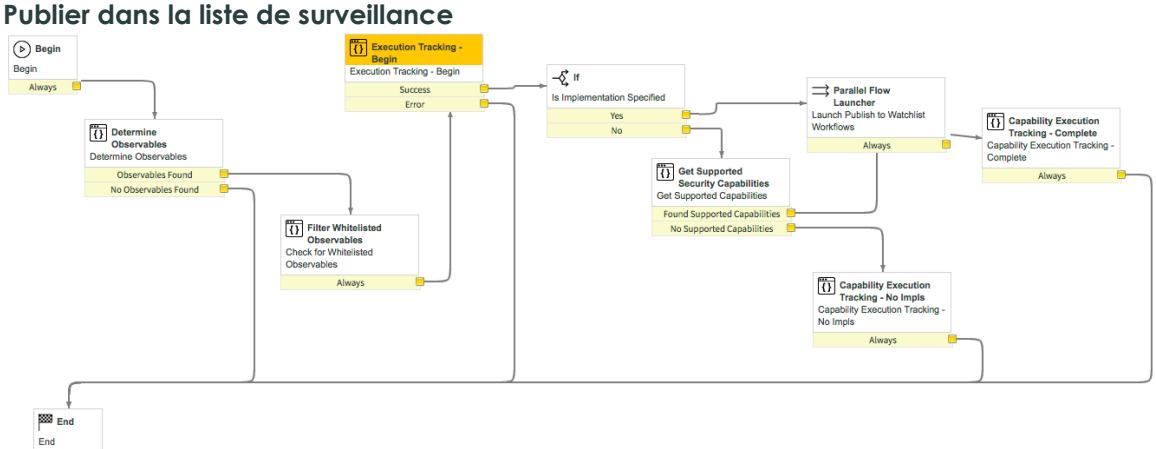
Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Ce workflow est visible et s'exécute uniquement lorsqu'une intégration est disponible. Il est déclenché à partir de l'onglet **Observables** ou **Indicateurs associés** d'un incident de sécurité.

Publier dans la liste de surveillance



Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Les activités de processus du workflow comprennent :

- Activité Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité
- Filtrer l'activité des observables sur liste d'autorisation

Intégration de Security Operations : fonctionnalité de recherche de perceptions

L'option **de recherche de perceptions** accepte un ensemble d'observables, trouve toutes les intégrations qui prennent en charge une recherche de perceptions, puis exécute ces recherches.

L'option de recherche de perceptions dispose d'un workflow, Security Operations Integration - Workflow de recherche de perceptions, qui exécute la recherche de perceptions. Ce workflow accepte une liste d'observables, trouve toutes les options d'implémentation, crée les requêtes en fonction des configurations de recherche de perceptions et exécute les recherches en fonction du workflow configuré. Une fois la recherche terminée, une note est ajoutée aux notes de travail de l'incident, indiquant si des observations ont été trouvées et, le cas échéant, combien.

Pour afficher les configurations de recherche de perceptions, naviguez vers **Security Operations** > **Intégrations** > **Configurations de la recherche de perceptions**.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Créer des enregistrements de configuration de recherche d'observations

Créez plusieurs enregistrements de configuration de recherche de perceptions et utilisez-les lors de l'interrogation de plusieurs magasins de journaux ou de la modification des paramètres de recherche.

Avant de commencer

Rôle requis : sn_si.admin

- Le module complémentaire CIM doit être installé sur l'instance Splunk.
- Les recherches enregistrées et les requêtes sur place ne sont prises en charge que pour Splunk Integration.

Pourquoi et quand exécuter cette tâche

Vous pouvez également créer des enregistrements de configuration de recherche de perceptions pour appeler des recherches enregistrées dans le magasin de journaux d'entreprise Splunk.

Remarque : Les requêtes de configuration de recherche s'appuient sur les données du journal Splunk pour être conformes au modèle d'information commun (CIM) Splunk.

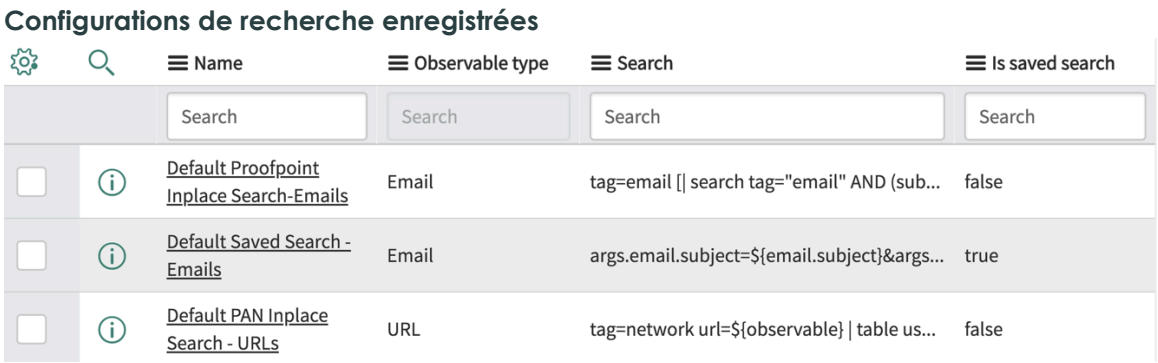
Avec les configurations de recherche enregistrées, vous pouvez :

- Créez des recherches personnalisées qui combinent plusieurs enregistrements d'événements.
- Concevez des recherches efficaces et efficientes.
- Utiliser des entrées paramétrées dans la recherche enregistrée Splunk.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le système de base inclut les exemples de configurations, comme illustré dans cette image :



La recherche enregistrée et les requêtes de configuration sur place sont des exemples de requêtes et peuvent être remplacées par des paramètres appropriés pour votre environnement. Créez des configurations de recherche enregistrées supplémentaires selon vos besoins. Lorsque vous définissez une configuration de recherche enregistrée, le nom et les paramètres de la requête de recherche doivent correspondre à la configuration enregistrée définie sur votre instance Splunk. Si le nom et les paramètres ne sont pas les mêmes, vous risquez de ne pas voir de résultats précis lorsque vous effectuez une recherche d'observations.

Remarque : Sur votre instance Splunk, accédez à la page Recherches, rapports et alertes et localisez votre requête de recherche enregistrée. Cliquez sur le lien **Autorisations** pour accéder à la page Autorisations. Sélectionnez la case d'option **Toutes les applications** et activez l'option **Autorisation de lecture** pour **Tout le monde**. Cela modifiera la valeur de la colonne Partage de Privé à Application pour votre requête de recherche enregistrée. Si cette option n'est pas définie, la requête de recherche enregistrée peut ne pas renvoyer de résultats.

Pour vérifier si la configuration de recherche enregistrée correspond à la configuration définie sur votre instance Splunk :

1. Accédez à la **Paramètres** > **Recherches, rapports et alertes**.
2. Définissez **tous lescontextes de l'application**.

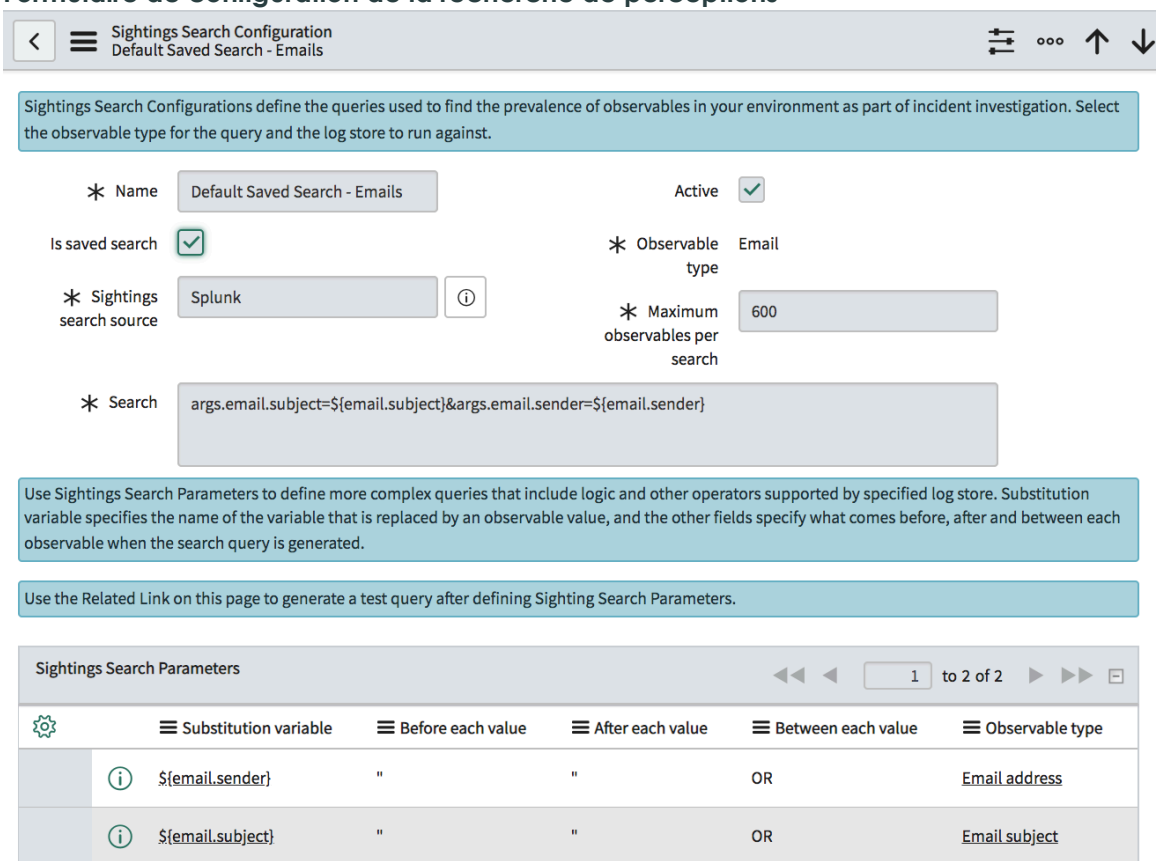
   Une liste des rapports de recherche s'affiche.
3. Confirmez que la requête de recherche enregistrée figure dans la liste.

Par exemple, le formulaire de configuration de recherche de perceptions contient l'adresse e-mail et l'expéditeur d'e-mail comme paramètres de recherche :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de configuration de la recherche de perceptions



Dans votre instance Splunk, définissez la recherche enregistrée avec le même nom, la recherche enregistrée par défaut : e-mails, et les mêmes paramètres de recherche pour l'adresse e-mail et l'objet de l'e-mail. Si le nom et les paramètres de recherche ne sont pas les mêmes, la recherche de perceptions ne génère pas de résultat précis.

Procédure

1. Accédez à la **Security Operations** > **Intégrations** > **Configuration de la recherche de perceptions** et créez un nouvel enregistrement (voir la table des descriptions de champ).

Formulaire de configuration de la recherche de perceptions

Champ	Description
Nom	Nom de la configuration.
Est une recherche enregistrée	La configuration de recherche enregistrée est créée si vous sélectionnez cette option.
Source de recherche de perceptions	La source de la recherche d'observations. Sélectionnez le magasin de journaux Splunk comme source.
Actif	Option pour l'état de la recherche enregistrée. Seules les configurations de recherche actives peuvent être utilisées pour effectuer une recherche de perceptions.
Type d'observable	Le type d'observable peut être n'importe quel type d'observable tel qu'une adresse IP, une valeur de hachage, une URL, un nom de domaine, etc.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nombre maximum d'observables par recherche	Nombre maximal d'observables à renvoyer à partir de la recherche.
Rechercher	La chaîne de recherche par défaut est `$(observable),` mais vous pouvez définir votre propre requête de recherche en spécifiant les paramètres pris en charge par le magasin de journaux Splunk.

2. Cliquez sur **Envoyer**.

Résultats
Vous avez créé un enregistrement de configuration de recherche de perceptions.

Que faire ensuite
Après avoir défini la requête de recherche, cliquez sur **Générer une requête de test de recherche de détections**, puis spécifiez une liste de valeurs observables pour générer une requête de test basée sur cette configuration de recherche enregistrée.

Exécuter une recherche d'observations

Déterminer la prévalence d'une menace dans le temps ou tester les efforts de rattrapage ou d'éradication. Vous pouvez sélectionner un ou plusieurs observables et la plage de dates pour votre recherche à partir d'un incident de sécurité. Les résultats sont inclus dans la liste connexe **Observables de l'incident de sécurité** .

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
L'option de recherche de perceptions dispose d'un workflow, Security Operations Integration - Workflow de recherche de perceptions, qui exécute la recherche de perceptions. Ce workflow accepte une liste d'observables, trouve toutes les options d'implémentation, crée les requêtes en fonction des configurations de recherche de perceptions et exécute les recherches en fonction du workflow configuré.

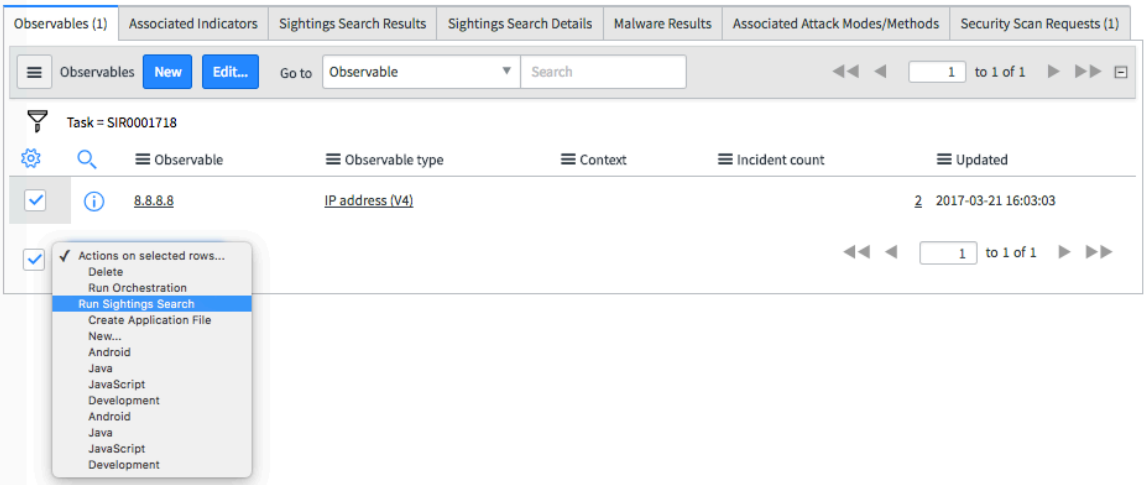
Remarque : Une implémentation active doit être configurée. La recherche de perceptions prend en charge l'enrichissement des incidents Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger et QRadar. Si aucune implémentation n'est disponible, les actions d'aptitude, telles que **Exécuter la recherche de perceptions**, ne sont pas affichées dans les menus produit.

Procédure

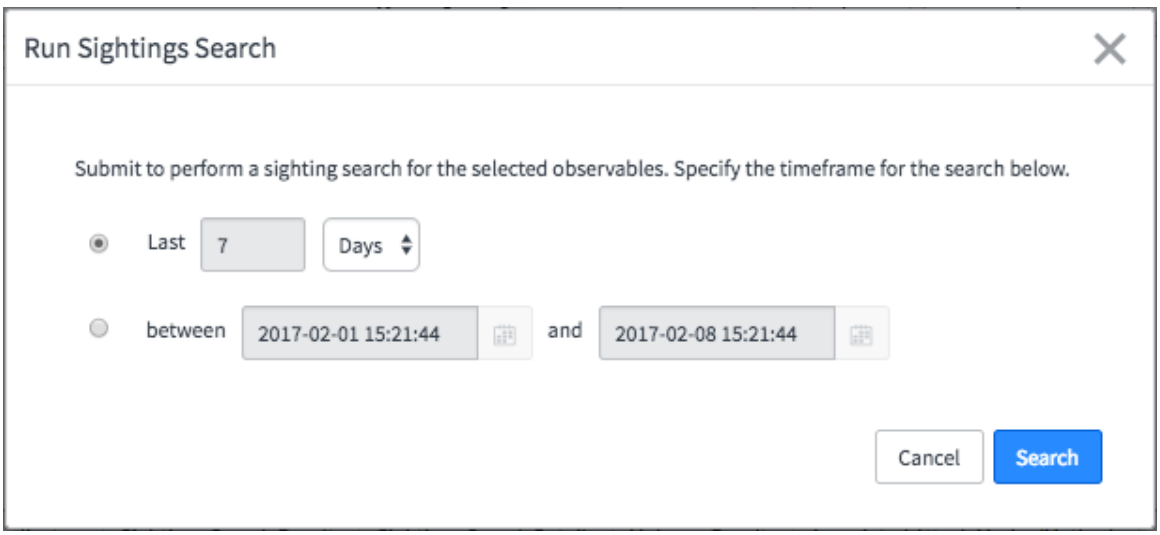
1. Accédez à un incident de sécurité.
2. Cliquez sur le lien connexe **Afficher IoC** .
3. Sélectionnez **des observables** dans l'onglet Liste connexe.
4. Sélectionnez les observables sur lesquels vous souhaitez effectuer une recherche de perceptions.
5. Cliquez sur **Exécuter la recherche de perceptions** dans le menu déroulant **Actions sur les lignes sélectionnées.**

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La boîte de dialogue Exécuter la recherche de perceptions s'ouvre.



Remarque : Les valeurs saisies dans la boîte de dialogue remplacent les valeurs de configuration d'aptitude pour cette exécution.

6. Choisissez le nombre de jours ou une plage de dates pour rechercher des données.

Option	Description
Dernier	Nombre d'heures ou de jours avant la création de l'incident à rechercher. La valeur par défaut est de 7 jours. La limite est de 99 heures ou jours.
entre	Plage de dates à rechercher. Les dates par défaut sont les suivantes : Date et heure d'ouverture de l'incident. Date et heure sept jours avant l'ouverture de l'incident.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : **Le dernier** est le nombre d'heures ou de jours avant la création de l'incident à rechercher. La valeur par défaut est de 7 jours. La limite est de 99 heures ou jours.

7. Cliquez sur **Rechercher**.
   Un enregistrement de recherche de perceptions est créé. Les données agrégées et les perceptions associées sont affichées dans l'incident de sécurité sous les **onglets Résultats de recherche de perceptions** et **Détails de la recherche de perceptions** .

Remarque : Les données des résultats de recherche de perceptions peuvent être partagées avec Trusted Security Circle, à l'exception des données brutes dans le cas d'implémentations configurées pour inclure des données brutes.

Résultats de recherche de perceptions

Résultat	Description
Numéro	L'identificateur de la recherche de perceptions.
Nombre d'observables	Nombre d'observables recherchés par la requête.
Perceptions internes	Nombre de perceptions internes.
Perceptions externes	Nombre de perceptions externes. (Reçu de Threat Sharing.)
Éléments de configuration correspondants	Nombre d'éléments de configuration qui correspondaient à un enregistrement existant dans votre CMDB pour chaque observable trouvé dans votre environnement.
Plage de dates de démarrage	Il est temps de commencer à chercher des observations.
Plage de dates de fin	Il est temps d'arrêter de chercher des observations.
Mis à jour	Date et heure de la dernière modification.

Note: Si l'implémentation utilisée pour la recherche de perceptions est configurée pour inclure des données brutes et qu'au moins une observation est trouvée, une pièce jointe contenant des échantillons de données brutes apparaît en haut de l'incident de sécurité.

Détails de la recherche de perception

Détail	Description
Recherche de perception	L'identificateur de la recherche de perceptions.
Observable	Observable recherché par requête.
Type d'observable	Type d'observable recherché par la requête.
Perceptions internes	Nombre agrégé de perceptions internes.
Perceptions externes	Nombre agrégé de perceptions externes. (Reçu de Threat Sharing.)
Mis à jour	Date et heure de la dernière modification.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Operations Integration - Workflow de recherche de perceptions

Le workflow Security Operations Integration - Recherche de perceptions est un workflow de haut niveau indépendant des intégrations. Elle utilise les requêtes configurées pour rechercher un ensemble d'observables en fonction des intégrations configurées qui prennent en charge l'aptitude. Utilisez-le pour réaliser une intégration telle que Splunk ou Elasticsearch.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Si un incident de sécurité est associé à un observable, ce workflow est déclenché lorsque vous cliquez sur **Exécuter la recherche de perception** dans le menu déroulant **Actions sur les lignes sélectionnées...** dans l'onglet **Observables d'incident de sécurité** .

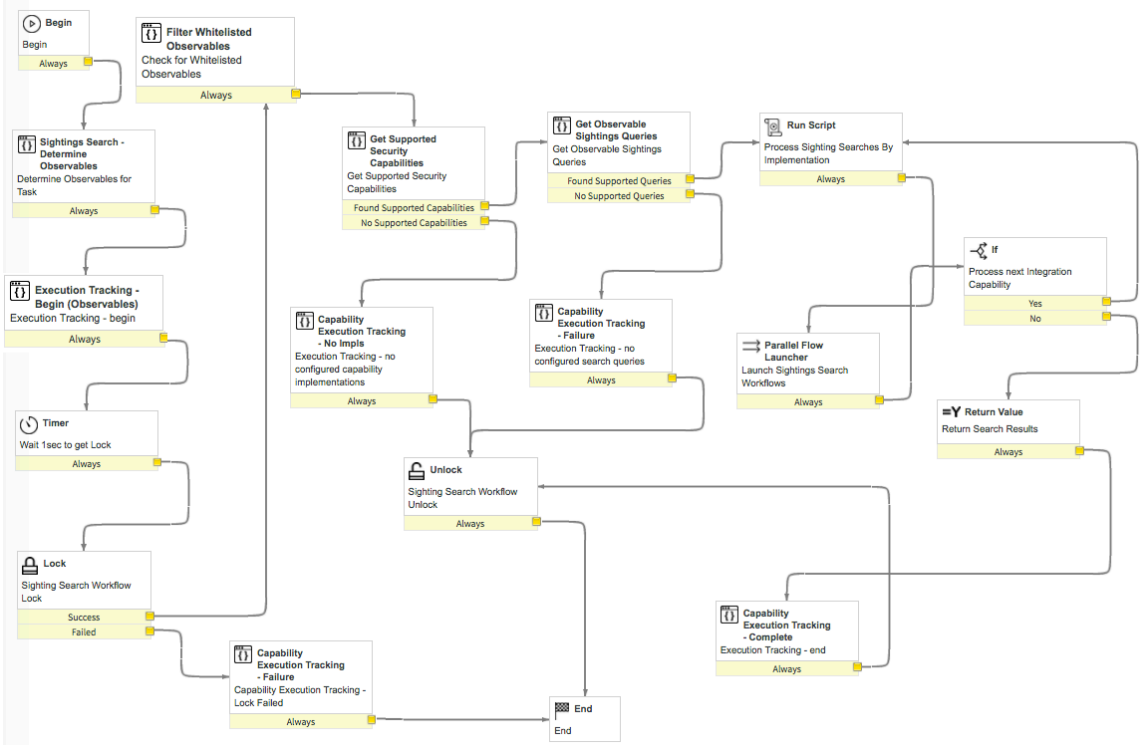
Les activités de processus du workflow comprennent :

- Déterminer l'activité des observables
- Suivi des exécutions : démarrer l'activité
- Activité du workflow du minuteur : attend une seconde pour obtenir un verrou.
- Verrouiller l'activité du workflow
- Filtrer les éléments observables sur la liste d'autorisation
- Activité Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité
- Déverrouiller workflow activité
- Obtenir des observations d'observables Activité de requête
- Suivi d'exécution de l'aptitude : activité d'échec
- Exécuter le script workflow activité
- Lanceur de flux parallèle
- Si activité de workflow Si activité de workflow : itérez jusqu'à ce que tous les workflows appropriés se soient exécutés et stockez les résultats dans un tableau.
- Suivi d'exécution de l'aptitude : terminer l'activité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche de perceptions



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Recherche de perceptions : déterminer l'activité des observables

L'activité **du workflow Recherche de perceptions - Déterminer les observables** détermine les observables à inclure dans le workflow.

L'activité **Recherche de perceptions - Déterminer les observables** peut être utilisée avec n'importe quel workflow pour déterminer les observables à inclure dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Observables trouvés
Échec	Aucun observable trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
task_sys_id	Identificateur de tâche (mappe l'incident de sécurité aux observables).
observables	Adresses IP, hachage, URL, noms de domaines.
workflow_current_sys_id	Identificateur système de l'enregistrement actuel. (Utilisé uniquement si `task_sys_id`, les entrées d'observables ne sont pas disponibles.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
observables	Observables filtrés

Activité de perceptions observables persistantes

L'activité de workflow **Perceptions observables persistantes** récupère les observables de l'intégration tierce.

L'activité **Observations observables persistantes** peut être utilisée avec n'importe quel workflow pour enregistrer les observables trouvés dans l'intégration tierce.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Observables récupérés.
Échec	Une erreur s'est produite lors de la tentative de collecte des observables. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
Réponse sur les perceptions	
taskId	Identificateur de tâche.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
réponse	

Obtenir des observations d'observables Activité de requête

L'activité de workflow **Obtenir des requêtes de perceptions d'observables** récupère les requêtes de la configuration d'intégration.

L'activité **Obtenir des requêtes de perceptions d'observables** peut être utilisée avec n'importe quel workflow pour obtenir des requêtes à envoyer à l'implémentation spécifiée à l'aide du **lanceur de flux parallèle**.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Requêtes trouvées.
Échec	Une erreur s'est produite lors de la tentative d'obtention de requêtes. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
observables	Liste des observables filtrés.
Options	Liste des options prises en charge.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
requêtes	Chaîne de recherche.
queryCount	Nombre de requêtes à exécuter.

Opérations de sécurité : workflow de recherche de perceptions Arcsight Logger

Le workflow de recherche de perceptions ArcSight Logger - Opérations de sécurité est l'implémentation de l'intégration Splunk lancée par le **workflow de recherche de perceptions Intégration de Security Operations - Recherche de perceptions**.

Traduction automatique

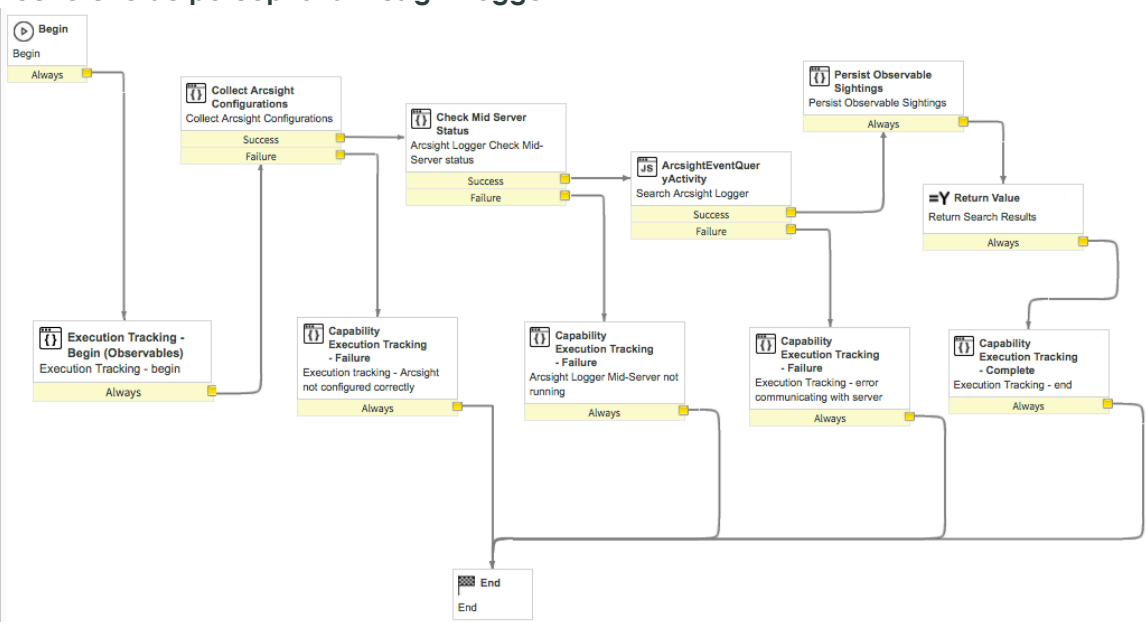
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si_analyst

Pourquoi et quand exécuter cette tâche
Les activités de processus du workflow comprennent :

- Suivi des exécutions : démarrer l'activité
- Activité de collecte des configurations ArcSight
- Suivi d'exécution de l'aptitude : activité d'échec
- Activité de requête d'événement ArcSight
- Vérifie si le MID Server est en cours d'exécution ou non.
- Activité de requête d'événement ArcSight
- Activité de perceptions observables persistantes - renvoie les résultats de recherche dans un tableau.
- Suivi d'exécution de l'aptitude : terminer l'activité

Recherche de perceptions Arcsight Logger



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Activité de collecte des configurations ArcSight

L'activité **de workflow Collecter les configurations ArcSight** rassemble des informations de configuration à utiliser dans le workflow.

L'activité **Collecter les configurations ArcSight peut** être utilisée avec n'importe quel workflow pour collecter les paramètres de configuration de HPE Security ArcSight Logger.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Configuration réussie.
Échec	Une erreur s'est produite lors de la tentative de vérification de la configuration. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
observables	Liste des observables ou Trusted Security Circle de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
endpoint_base	URL de base de l'API d'intégration tierce.
link_endpoint_base	Lien vers une interface de recherche ArcSight Logger, lorsqu'elle est disponible.
use_default_workflows	Détermine l'utilisation du workflow qui a été installé avec le module d'extension. Les valeurs possibles sont les suivantes : • vrai : utiliser le workflow • Faux : ne pas utiliser le workflow
arcsight_username	Nom d'utilisateur HPE Security ArcSight Logger
arcsight_password	Mot de passe HPE Security ArcSight Logger
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce. .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.
all_peers	Détermine s'il faut rechercher tous les autres enregistreurs connectés au réseau.

Activité de requête d'événement ArcSight

L'activité de workflow **ArcSight Event Query** recherche des indicateurs malveillants dans les journaux d'événements ArcSight.

L'activité **ArcSight Event Query** peut être utilisée avec n'importe quel workflow pour effectuer des recherches dans les journaux d'événements HPE Security ArcSight Logger.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Requête réussie.
Échec	Une erreur s'est produite lors de la tentative de vérification de la requête. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
utilisateur	Nom d'utilisateur du système HPE Security ArcSight Logger.
mot de passe	Mot de passe du système HPE Security ArcSight Logger.
observables	Liste des observables ou Trusted Security Circles de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
base_url	URL de base de l'API d'intégration tierce.
link_base_url	Lien vers une interface de recherche ArcSight Logger, lorsqu'elle est disponible.
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
all_peers	Détermine s'il faut rechercher tous les autres enregistreurs connectés au réseau.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
output	Sortie de la requête au format JSON.

Security Operations - Workflow de recherche de perceptions Elasticsearch

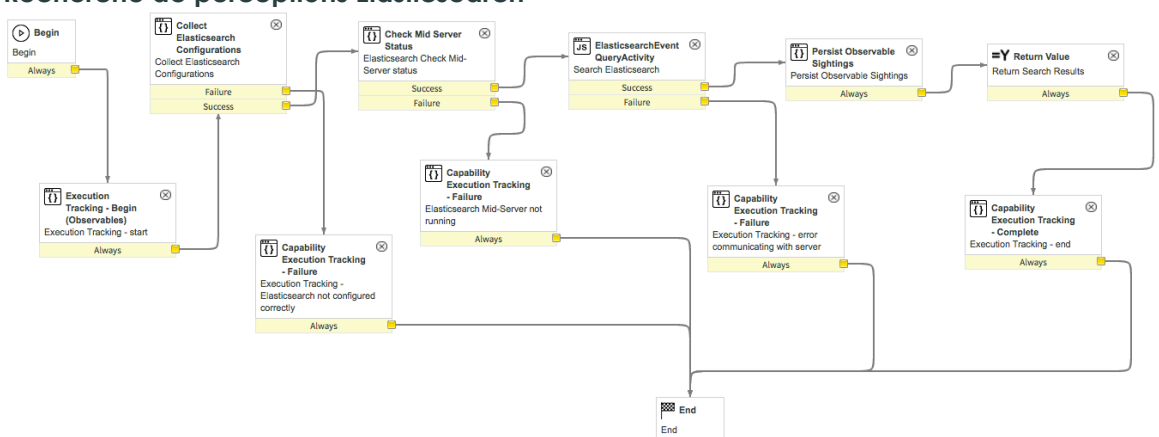
Le workflow Security Operations - Elasticsearch Sightings Search est l'implémentation d'Elasticsearch lancée par le workflow **Security Operations Integration - Sightings Search** .

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Les activités de processus du workflow comprennent :

- Suivi des exécutions : démarrer l'activité
- Collecter l'activité Elasticsearch Configurations
- Vérifie si le MID Server est en cours d'exécution ou non.
- Suivi d'exécution de l'aptitude : activité d'échec
- Activité QueryActivity d'événement Elasticsearch
- Activité de perceptions observables persistantes - renvoie les résultats de recherche dans un tableau.
- Suivi d'exécution de l'aptitude : terminer l'activitéSuivi de l'exécution de l'aptitude : aucune implémentation de l'activité

Recherche de perceptions Elasticsearch



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Collecter l'activité Elasticsearch Configurations

L'activité **de workflow Collecter les configurations Elasticsearch** rassemble les informations de configuration à utiliser dans le workflow.

L'activité **Collecter les configurations Elasticsearch** peut être utilisée avec n'importe quel workflow pour collecter les paramètres de configuration Elasticsearch.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Configuration réussie. .
Échec	Une erreur s'est produite lors de la tentative de vérification de la configuration. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
observables	Liste des observables ou Trusted Security Circles de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
endpoint_base	URL de base de l'API d'intégration tierce.
link_endpoint_base	[Facultatif] Lien vers une instance Kibana, lorsqu'il est disponible
use_default_workflows	Détermine l'utilisation du workflow qui a été installé avec le module d'extension. Les valeurs possibles sont les suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
	• vrai : utiliser le workflow • Faux : ne pas utiliser le workflow
elastic_username	Nom d'utilisateur Elasticsearch
elastic_password	Mot de passe Elasticsearch
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce. .
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Activité QueryActivity d'événement Elasticsearch

L'activité de workflow de **requête d'événement Elasticsearch** recherche des indicateurs malveillants dans les journaux d'événements Elasticsearch.

L'activité QueryActivity d'événement Elasticsearch peut être utilisée avec n'importe quel workflow pour effectuer des recherches dans les journaux d'événements Elasticsearch.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Requête réussie.
Échec	Une erreur s'est produite lors de la tentative de vérification de la requête. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
utilisateur	Nom d'utilisateur du système Elasticsearch.
mot de passe	Mot de passe du système Elasticsearch.
observables	Liste des observables ou Trusted Security Circles de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
base_url	URL de base de l'API d'intégration tierce.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
link_base_url	[Facultatif] Lien vers une instance Kibana, lorsqu'il est disponible
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
output	Sortie de la requête au format JSON.

Security Operations - Workflow de recherche d'observations McAfee ESM

Le workflow Recherche de perceptions Security Operations - McAfee ESM est l'implémentation de l'intégration Splunk lancée par le **workflow Intégration de Security Operations - Recherche de perceptions**.

Avant de commencer
Rôle requis : sn_si_analyst

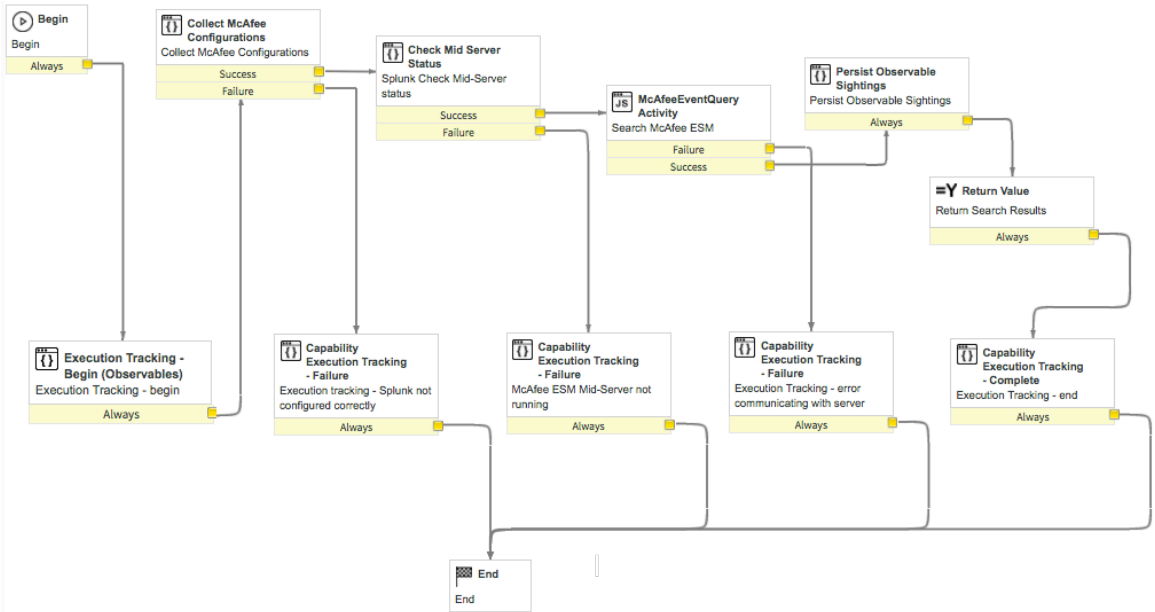
Pourquoi et quand exécuter cette tâche
Les activités de processus du workflow comprennent :

- Suivi des exécutions : démarrer l'activité
- Collecter l'activité McAfee Configurations
- Suivi d'exécution de l'aptitude : activité d'échec
- Activité de requête d'événement McAfee ESM
- Vérifie si le MID Server est en cours d'exécution.
- Activité de perceptions observables persistantes - renvoie les résultats de recherche dans un tableau.
- Suivi d'exécution de l'aptitude : terminer l'activité

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche d'observations McAfee ESM



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Collecter l'activité McAfee Configurations

L'activité **de workflow Collecter les configurations McAfee** rassemble des informations de configuration à utiliser dans le workflow.

L'activité **Collecter les configurations McAfee** peut être utilisée avec n'importe quel workflow pour collecter les paramètres de configuration de McAfee ESM.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Configuration réussie. .
Échec	Une erreur s'est produite lors de la tentative de vérification de la configuration. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
observables	Liste des observables ou Trusted Security Circles de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
endpoint_base	URL de base de l'API d'intégration tierce.
link_endpoint_base	Lien vers une interface Web McAfee, lorsqu'elle est disponible.
use_default_workflows	Détermine l'utilisation du workflow qui a été installé avec le module d'extension. Les valeurs possibles sont les suivantes : • vrai : utiliser le workflow • Faux : ne pas utiliser le workflow
elastic_username	Nom d'utilisateur McAfee
elastic_password	Mot de passe McAfee
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce. .
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Activité de requête d'événement McAfee ESM

L'activité de workflow **de requête d'événement McAfee ESM** recherche des indicateurs malveillants dans les journaux d'événements McAfee ESM.

L'activité **de requête d'événement McAfee ESM** peut être utilisée avec n'importe quel workflow pour effectuer des recherches dans les journaux d'événements HPE Security ArcSight Logger.

Résultats

Les résultats possibles pour cette activité sont les suivants :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Requête réussie.
Échec	Une erreur s'est produite lors de la tentative de vérification de la requête. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
utilisateur	Nom d'utilisateur du système McAfee ESM.
mot de passe	Mot de passe du système McAfee ESM.
observables	Syntaxe de recherche. `$(observable)` est la valeur par défaut.
base_url	URL de base de l'API d'intégration tierce.
link_base_url	Lien vers une interface Web McAfee, lorsqu'elle est disponible.
observables	Liste des observables ou Trusted Security Circles de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
output	Sortie de la requête au format JSON.

Security Operations - Workflow de recherche de perceptions QRadar

Le workflow Security Operations - QRadar Sightings Search est l'implémentation de l'intégration IBM QRadar lancée par le **workflow Security Operations Integration - Sightings Search**.

Avant de commencer

Rôle requis : sn_si_analyst

Pourquoi et quand exécuter cette tâche

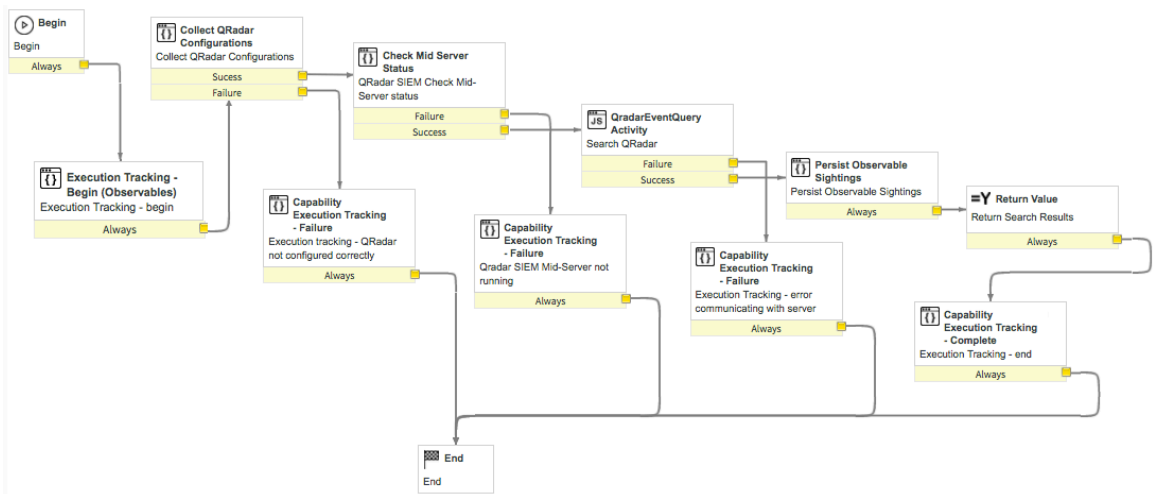
Les activités de processus du workflow comprennent :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Suivi des exécutions : démarrer l'activité
- Activité de collecte des configurations QRadar
- Suivi d'exécution de l'aptitude : activité d'échec
- Vérifie si le MID Server est en cours d'exécution.
- Événement QRadar Activité QueryActivity
- Activité de perceptions observables persistantes - renvoie les résultats de recherche dans un tableau.
- Suivi d'exécution de l'aptitude : terminer l'activité

Recherche d'observations QRadar



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Activité de collecte des configurations QRadar

L'activité **de workflow Collecter les configurations QRadar** rassemble des informations de configuration à utiliser dans le workflow.

L'activité **Collecter les configurations QRadar** peut être utilisée avec n'importe quel workflow pour collecter les paramètres de configuration IBM QRadar.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Configuration réussie. .
Échec	Une erreur s'est produite lors de la tentative de vérification de la configuration. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
observables	Liste des observables ou Trusted Security Circles de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
endpoint_base	URL de base de l'API d'intégration tierce.
link_endpoint_base	Lien vers une IBM QRadar instance, lorsqu'il est disponible.
use_default_workflows	Détermine s'il faut utiliser ou non le workflow installé avec le module d'extension. Les valeurs possibles sont true et false..
elastic_username	Nom d'utilisateur Qradar
elastic_password	Mot de passe QRadar
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce. .
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Événement QRadar Activité QueryActivity

L'activité de workflow **QRadar Event Query** recherche des indicateurs malveillants dans les journaux d'événements QRadar.

L'activité QueryActivity de l'événement QRadar peut être utilisée avec n'importe quel workflow pour effectuer des recherches dans les journaux d'événements Elasticsearch.

Résultats

Les résultats possibles pour cette activité sont les suivants :

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Requête réussie.
Échec	Une erreur s'est produite lors de la tentative de vérification de la requête. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
utilisateur	Nom d'utilisateur du système QRadar.
mot de passe	Mot de passe du système QRadar.
observables	Liste des observables ou Trusted Security Circles de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
base_url	URL de base de l'API d'intégration tierce.
link_base_url	Lien vers une IBM QRadar instance, lorsqu'il est disponible.
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
output	Sortie de la requête au format JSON.

Security Operations Integration : workflow de recherche d'observations Splunk

Le workflow Security Operations - Splunk Sightings Search est l'implémentation de l'intégration Splunk lancée par le **workflow Security Operations Integration - Sightings Search**.

Avant de commencer
Rôle requis : sn_si_analyst

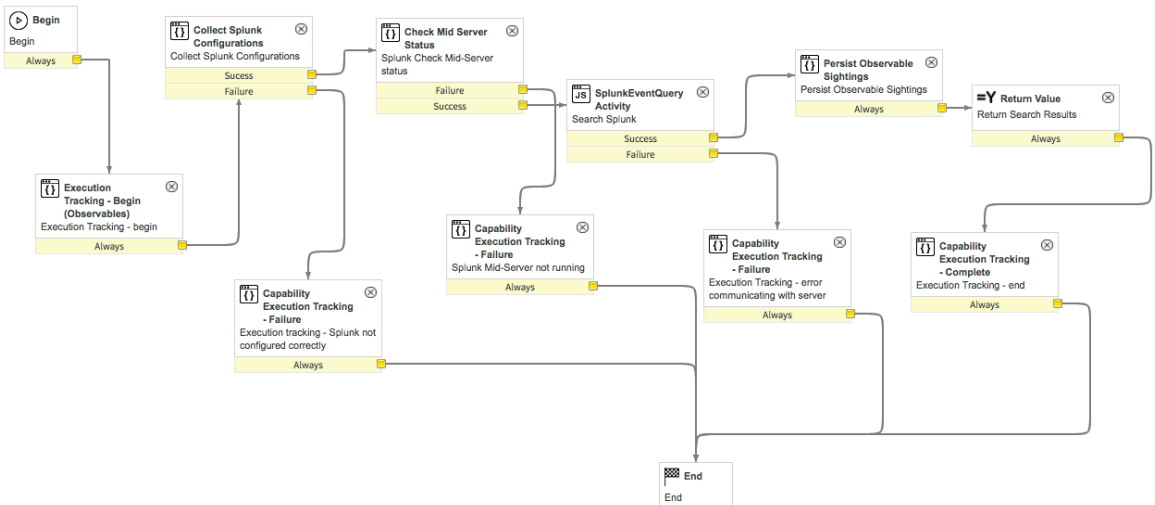
Pourquoi et quand exécuter cette tâche
Les activités de processus du workflow comprennent :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Suivi des exécutions : démarrer l'activité
- Activité de collecte des configurations Splunk
- Suivi d'exécution de l'aptitude : activité d'échec
- Vérifie si le MID Server est en cours d'exécution ou non.
- Activité de requête d'événement Splunk
- Activité de perceptions observables persistantes - renvoie les résultats de recherche dans un tableau.
- Suivi d'exécution de l'aptitude : terminer l'activité

Recherche d'observations Splunk



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Activité de collecte des configurations Splunk

L'activité **de workflow Collecter les configurations Splunk** rassemble des informations de configuration à utiliser dans le workflow.

L'activité **Collecter la configuration Splunk** peut être utilisée avec n'importe quel workflow pour collecter les paramètres de configuration Splunk.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Configuration réussie.
Échec	Une erreur s'est produite lors de la tentative de vérification de la configuration. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
observables	Liste des observables ou Trusted Security Circle de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
endpoint_base	URL de base de l'API d'intégration tierce.
link_endpoint_base	Liens vers l'interface Web, lorsqu'ils Splunk sont disponibles.
use_default_workflows	Détermine l'utilisation du workflow qui a été installé avec le module d'extension. Les valeurs possibles sont les suivantes : • vrai : utiliser le workflow • Faux : ne pas utiliser le workflow
elastic_username	Nom d'utilisateur Splunk.
elastic_password	Mot de passe Splunk.
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Activité de requête d'événement Splunk

L'activité de workflow de **requête d'événement Splunk** recherche des indicateurs malveillants dans les journaux d'événements Splunk.

L'activité QueryActivity d'événement Splunk peut être utilisée avec n'importe quel workflow pour effectuer des recherches dans les journaux d'événements Splunk.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Splunk
Échec	Une erreur s'est produite lors de la tentative de vérification de la requête Splunk. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
utilisateur	Nom d'utilisateur du système Splunk.
mot de passe	Mot de passe du système Splunk.
observables	Liste des observables ou Trusted Security Circle de la tâche d'incident de sécurité à rechercher. Renvoyé au format JSON.
base_url	URL du point de terminaison d'intégration Splunk.
link_base_url	Lien vers l'interface Web, lorsqu'il Splunk est disponible.
source	Source de la demande d'exécution du workflow. Les entrées prises en charge sont : Trusted Security Circles ou la tâche d'incident de sécurité.
max_rows	Nombre maximal de lignes à renvoyer à partir de la requête. La limite dépend de l'intégration tierce.
days_to_search	Jours pour rechercher à partir du jour actuel dans l'envers. La valeur par défaut est 7.
requête	Syntaxe de recherche. `$(observable)` est la valeur par défaut.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
output	Sortie de la requête au format JSON.

Afficher les résultats de recherche d'observations

Vous pouvez consulter les résultats de la recherche de perceptions à la recherche d'indicateurs malveillants internes et externes.

Avant de commencer

Rôle requis : sn_si.analyst

Traduction automatique

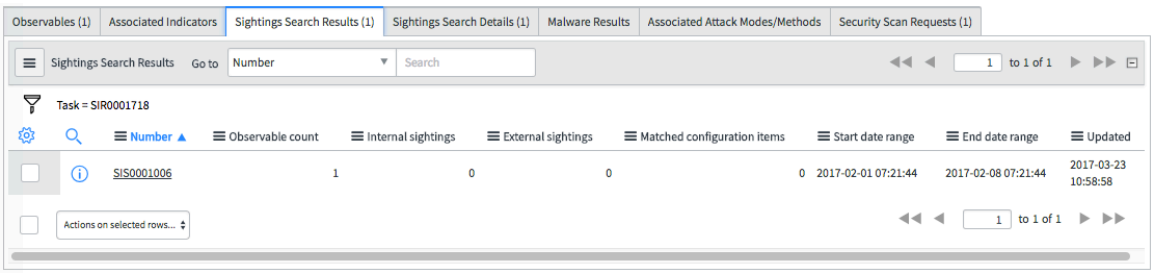
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

.

Procédure

1. Accédez à un incident de sécurité.
2. Sélectionnez l'onglet **Résultats de la recherche de perceptions** dans le groupe Afficher la liste connexe **IoC** pour afficher la liste des recherches de perceptions.



Remarque : Ces données peuvent être partagées avec Trusted Security Circle.

Résultats de recherche de perceptions

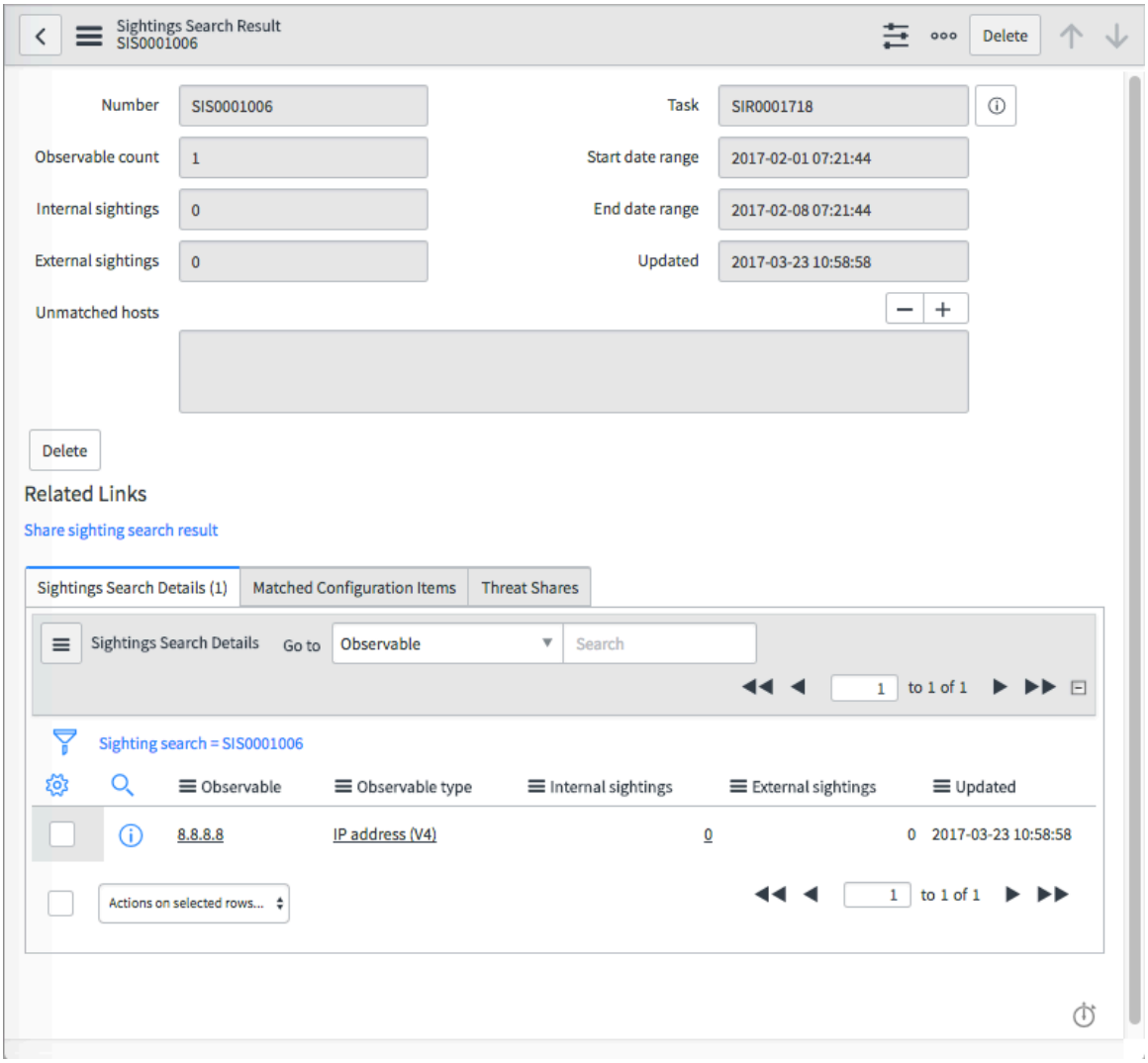
Résultat	Description
Numéro	Identificateur de recherche de perceptions.
Nombre d'observables	Nombre d'observables recherchés.
Perceptions internes	Nombre agrégé de perceptions internes.
Perceptions externes	Nombre agrégé de perceptions externes. (Reçu de Threat Sharing.)
Éléments de configuration correspondants	Nombre agrégé d'éléments de configuration qui correspondent à un enregistrement existant dans votre `CMDB`.
Plage de dates de démarrage	Il est temps de commencer à chercher des observations.
Plage de dates de fin	Il est temps d'arrêter de chercher des observations.
Mis à jour	Date et heure de la dernière modification.

Pour afficher les détails d'une recherche unique :

3. Cliquez sur une recherche de perceptions dans la liste **des résultats de recherche de perceptions** .
   Le formulaire Résultats de la recherche de perceptions s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Formulaire de résultats de recherche de perceptions

Détail	Description
Numéro	Identificateur de recherche de perceptions internes.
Nombre d'observables	Nombre d'observables recherchés par cette requête.
Perceptions internes	Nombre de perceptions internes pour cette recherche.
Perceptions externes	Nombre de perceptions externes pour cette recherche. (Reçu de Trusted Security Circle.)
Hôtes sans correspondance	Liste des éléments de configuration potentiels pour cette recherche qui n'ont pas été mis en correspondance avec des enregistrements de votre `CMDB`.
Tâche	Identificateur de tâche d'incident de sécurité.
Plage de dates de démarrage	Heure à laquelle la recherche d'observations a commencé.
Plage de dates de fin	Heure à laquelle la recherche d'observations s'est arrêtée.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détail	Description
Mis à jour	Date et heure de la dernière modification.
Détails de la recherche de perception	Type, nombre d'observations et date de modification.
Éléments de configuration correspondants	Nombre d'éléments de configuration qui correspondaient à un enregistrement existant dans votre `CMDB`. Répertorie le CI et la perception.
Partages de menaces	Liste des menaces partagées avec Trusted Security Circle.

Partager les résultats de recherche de perceptions

Vous pouvez partager des détails ou des résultats sur les perceptions locales associés à une recherche particulière avec votre cercle de sécurité de confiance.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

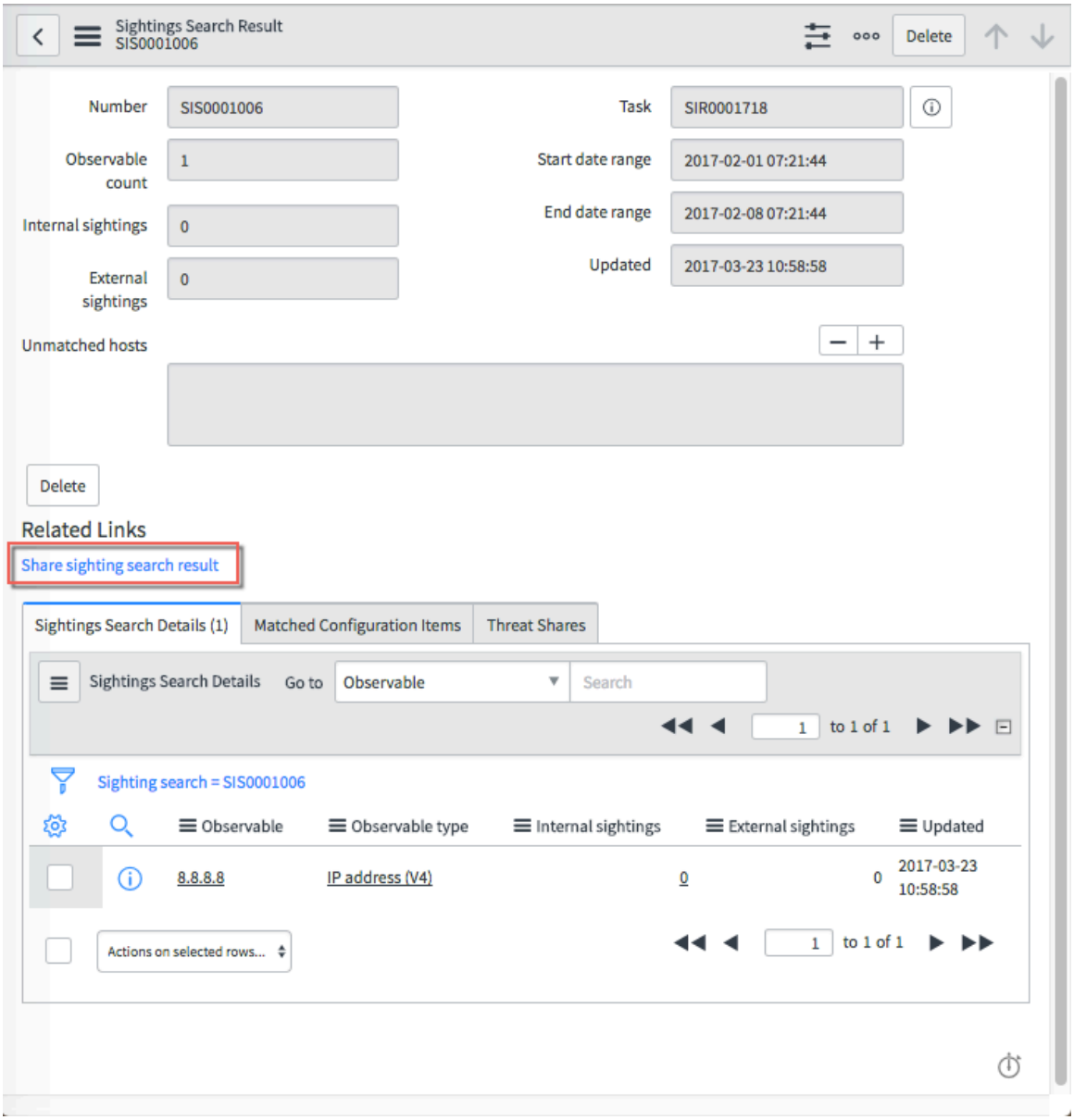
Le partage peut être automatisé à l'aide des propriétés de Security Incident **Response** suivantes.

- Partager automatiquement les résultats d'une recherche de perceptions avec le cercle de confiance ServiceNow par défaut
- Inclure les observables sans perceptions locales lors du partage automatique des résultats de recherche de perceptions
- Répondre par des perceptions locales chaque fois qu'un partage de menace est reçu d'un cercle de confiance

Procédure

1. Accédez à un incident de sécurité.
2. Cliquez sur la liste connexe **Afficher IoC** et sélectionnez l'onglet **Résultats de recherche de perceptions** pour afficher la liste des recherches de perceptions.
3. Cliquez sur un résultat de recherche d'observations.

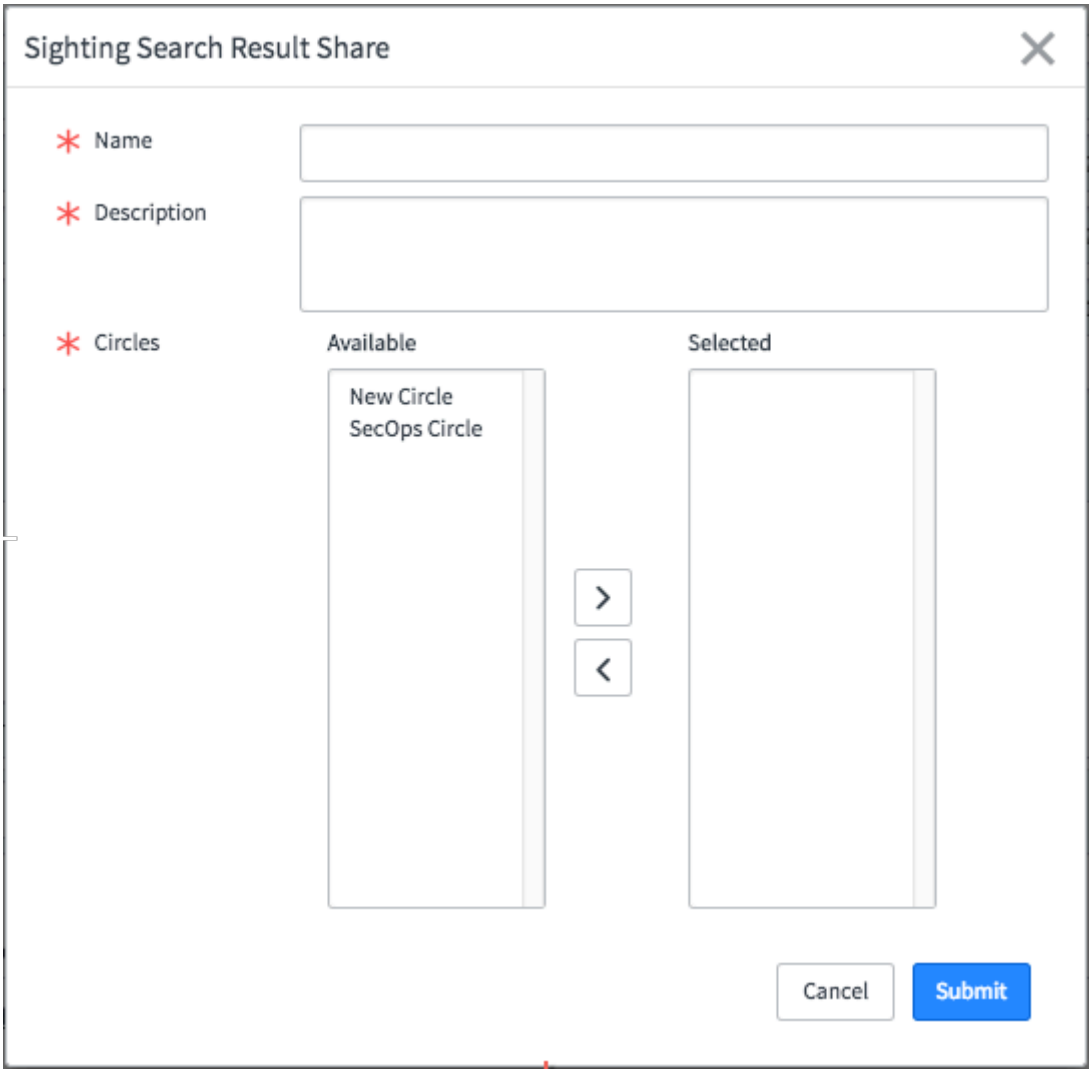
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sur le formulaire **Résultats de recherche de perceptions**, cliquez sur le lien connexe **Partager les résultats de recherche de perceptions** .
La boîte de dialogue Partage des résultats de recherche de perception s'affiche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Entrez un **nom** pour cet enregistrement de partage observable.

6. Saisissez une **description**des observables à partager.

7. Choisissez **des cercles** avec lesquels partager les observables.

8. Cliquez sur **Envoyer**.
Le ou les observables sont partagés avec le cercle de confiance spécifié.

Partager les observables à partir d'un incident de sécurité

Les observables peuvent être partagés à partir d'un incident de sécurité avec Réponse aux incidents de sécurité les membres de votre cercle de confiance.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à un incident de sécurité.

2. Sélectionnez l'onglet **Observables** dans le groupe Afficher la liste connexe **IoC** .

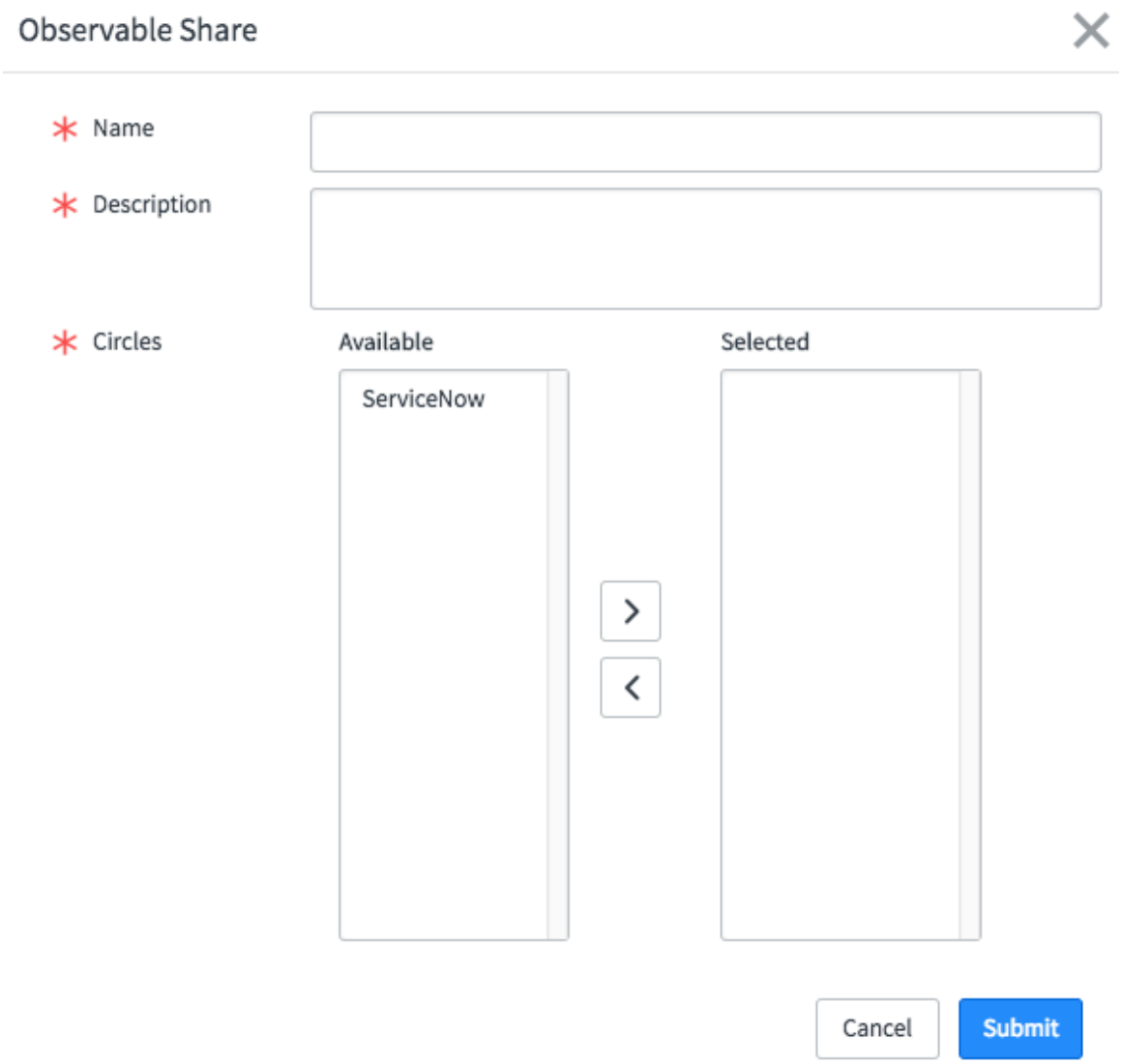
3. Cliquez sur un observable.

4. Sur le formulaire **Observable** , cliquez sur le lien connexe **Partager l'observable** .

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La boîte de dialogue Observable Share (Partage observable) s'affiche.



5. Entrez un **nom** pour cet enregistrement de partage de menaces.
6. Entrez une **description**des observables sélectionnés.
7. Choisissez **des cercles** avec lesquels partager les observables.
8. Cliquez sur **Envoyer**.
   Le ou les observables sont partagés avec le cercle de confiance spécifié.
9. Vous pouvez afficher les enregistrements de partage de menaces en cliquant sur l'onglet **Partages de menaces** .
10. Si l'un des observables partagés contient des observations, les observations sont également partagées et peuvent être visualisées en cliquant sur l'onglet **Observations** .

Afficher les détails de la recherche d'observations

Passez en revue les détails agrégés de toutes les recherches d'observations.

Avant de commencer
Rôle requis : sn_si.analyst

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

.

Procédure

1. Accédez à un incident de sécurité.
2. Sélectionnez l'onglet Détails de la **recherche de perceptions** dans le groupe Afficher la liste connexe **IoC** pour afficher la liste des recherches de perceptions.

Remarque : Ces données peuvent être partagées avec Trusted Security Circle.

Détails de la recherche de perception

Détail	Description
Observable	Liste de tous les observables recherchés par la requête.
Type d'observable	
Perceptions internes	Nombre de perceptions internes pour toutes les recherches.
Perceptions externes	Nombre de perceptions externes pour toutes les recherches. (Reçu de Threat Sharing.)
Recherche de perception	Identificateur de recherche de perceptions.
Mis à jour	Date et heure de la dernière modification.

Security Operations Integration - Aptitude Recherche de menace

L'option **Recherches de menace** effectue des recherches de renseignements sur les menaces pour déterminer si un ou plusieurs éléments observables sont associés à des menaces de sécurité connues.

L'option **Recherches de menaces** dispose d'un workflow, Workflow de recherche de menaces - Intégration des opérations de sécurité. Lorsque le workflow d'aptitude s'exécute, il exécute des workflows supplémentaires pour les implémentations activées. Vous pouvez spécifier une implémentation à utiliser pour effectuer une recherche sur les observables sélectionnés, ou vous pouvez effectuer la recherche en utilisant toutes les implémentations.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus produit.

Workflow de recherche de menaces - Intégration des opérations de sécurité

Le workflow **d'aptitude Intégration des opérations de sécurité - Recherche de menace** accède aux implémentations de recherche de menaces disponibles et exécute les workflows d'implémentation associés à chacune d'entre elles pour effectuer des recherches de menaces sur les observables sélectionnés.

Avant de commencer

Rôle requis : sn_ti.write

Pourquoi et quand exécuter cette tâche

Ce workflow peut être déclenché de cette manière.

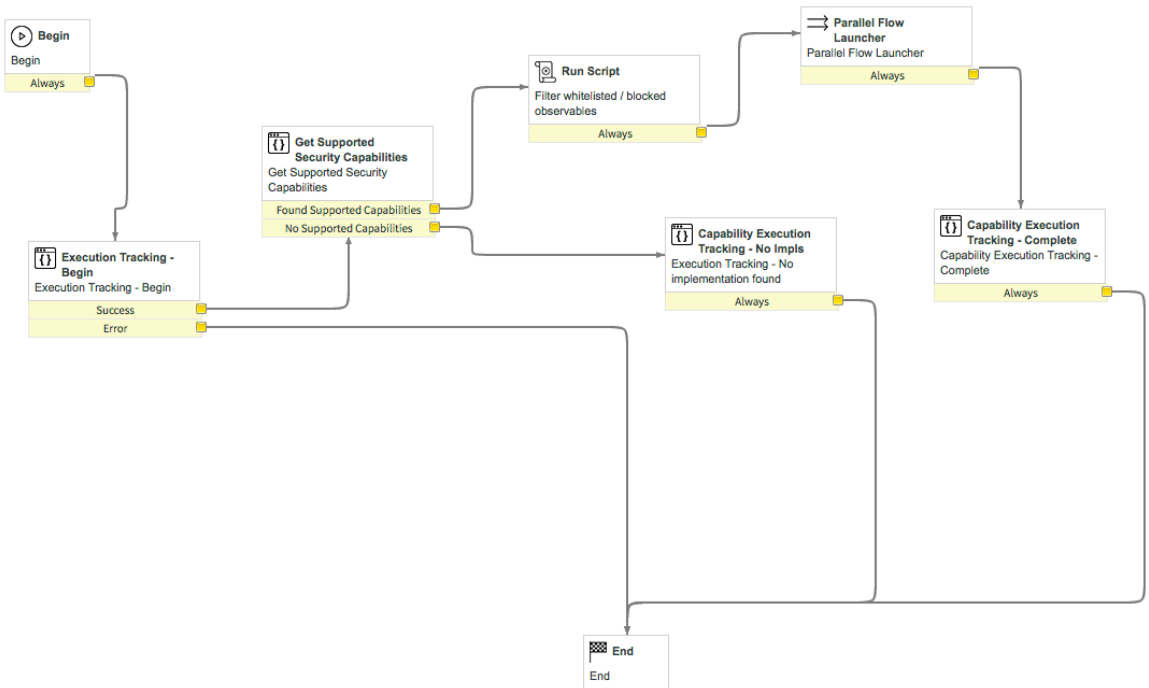
Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- en sélectionnant un ou plusieurs observables dans la liste Observables et en sélectionnant **Exécuter une recherche de menace** dans la liste de choix **Actions sur les lignes sélectionnées** .
- en ouvrant un enregistrement d'observable et en cliquant sur le lien connexe **Exécuter la recherche de menace** .
- À partir de la liste connexe Observables dans un incident de sécurité.

Chaque méthode vous permet ensuite de spécifier les implémentations de recherche à utiliser pour analyser les observables sélectionnés. Les workflows d'implémentation associés sont exécutés pour effectuer les recherches.

Recherche de menace



Les activités spécifiques à ce workflow sont décrites ici. Pour plus d'informations sur d'autres activités, voir Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité.

Les activités de processus du workflow comprennent :

- Activité Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité

Modifier l'ordre d'exécution du workflow

Les implémentations d'option d'intégration spécifient le workflow à exécuter. Dans le système de base, les workflows sont exécutés séquentiellement, dans l'ordre spécifié dans l'implémentation. Vous pouvez modifier l'ordre selon vos besoins.

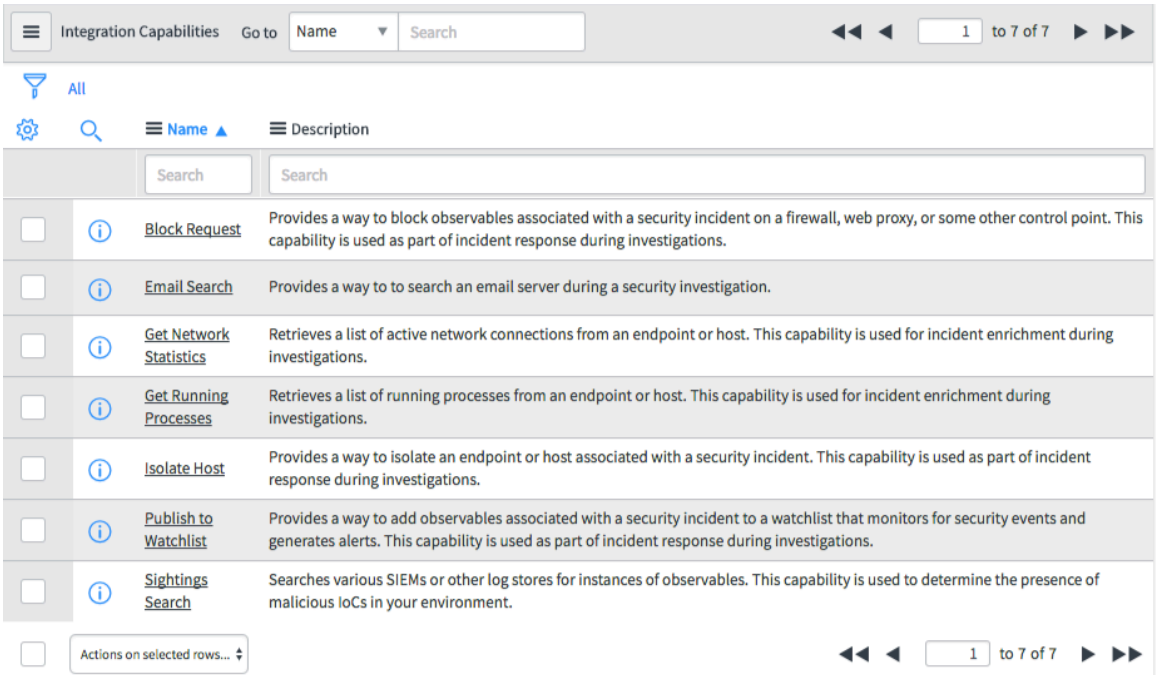
Avant de commencer

Rôle requis : sn_sec_cmn.write

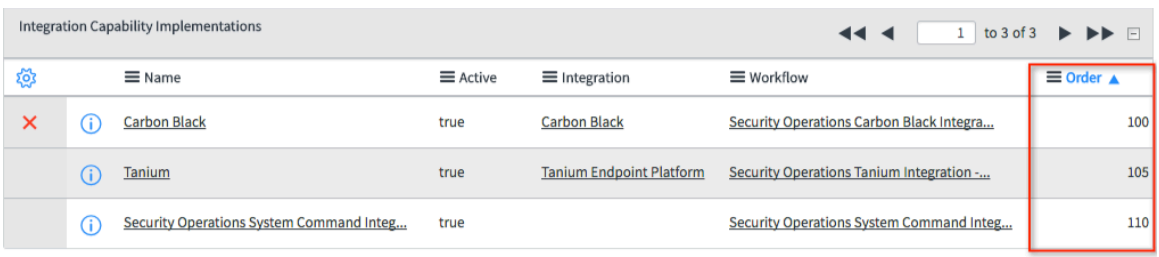
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

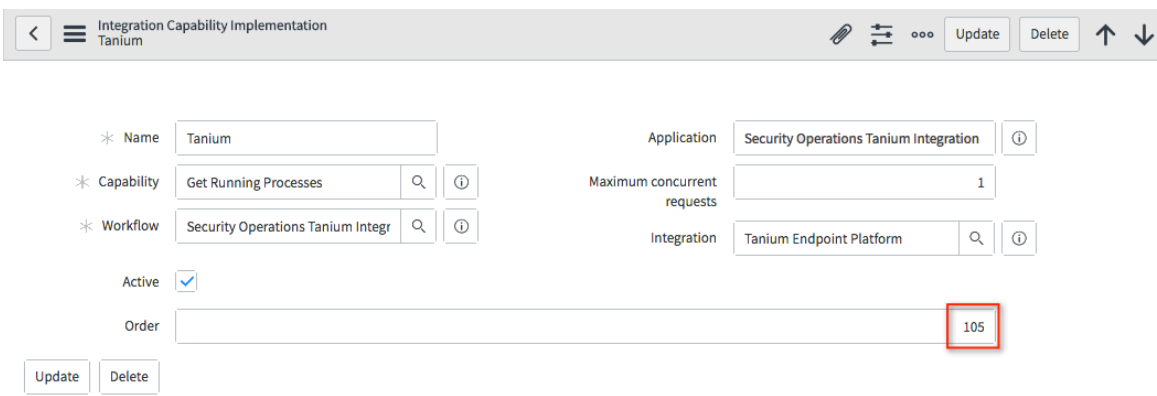
1. Accédez à la **Tout** > **Security Operations** > **Intégrations** > **Options d'intégration**.



2. Sélectionnez l'option d'intégration dont vous souhaitez modifier l'ordre d'exécution.



3. Sélectionnez l'implémentation que vous souhaitez modifier.



4. Modifiez la **commande** sur un nombre supérieur ou inférieur.
Les numéros inférieurs ont une priorité d'exécution plus élevée.

5. Cliquez sur **Envoyer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflows d'intégration et activités d'orchestration courants pour Opérations de sécurité

La plupart des workflows associés aux intégrations tierces incluent les mêmes activités. Par exemple, les activités de début et de fin de traitement.

Suivi des exécutions : démarrer l'activité

L'activité Suivi de l'exécution - Démarrer le workflow démarre le processus d'audit pour un Opérations de sécurité workflow d'intégration qui fonctionne sur les observables.

L'activité Suivi des exécutions - Début peut être utilisée avec n'importe quel workflow pour commencer à enregistrer la progression du workflow dans un audit.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Un enregistrement d'audit est créé.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
capabilityId	Identificateur système de l'option d'intégration en cours d'exécution.
isImpl	Marqueur qui spécifie si l'audit est effectué pour un workflow d'option d'intégration ou un workflow d'implémentation d'aptitude d'intégration. Les valeurs possibles sont les suivantes : • faux : désigne un audit sur un workflow abstrait d'aptitude d'intégration tel que la recherche de perceptions. (par défaut.) • vrai : désigne un audit sur un workflow d'implémentation d'option d'intégration. Par exemple, Splunk ou Elasticsearch.
taskId	Identificateur système pour toute tâche associée au workflow.
liste observablelist	Un ou plusieurs SysID d'observables pour effectuer l'action souhaitée. Utilisé comme entrée de workflow.
ID workflowContextId	Identificateur système de l'enregistrement de contexte de workflow associé. Fourni par le système.
nom du workflow	Nom du workflow. Fourni par le système.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
parentCapabilityExcutionId	Identificateur système de l'enregistrement d'audit qui a lancé le workflow d'implémentation. Requis uniquement pour les workflows d'implémentation de l'option d'intégration tels que Splunk, Elasticsearch et VirusTotal.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
CapabilityExecutionId	Identificateur système de l'enregistrement d'audit.

- Activité Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité

Suivi d'exécution de l'aptitude : terminer l'activité

L'activité Suivi de l'exécution de l'aptitude - Terminer le workflow met à jour l'enregistrement d'audit lorsque le workflow est terminé.

L'activité Suivi de l'exécution de l'aptitude : terminer peut être utilisée avec n'importe quel workflow pour enregistrer l'achèvement du workflow.

Remarque : Le tableau de **valeurs de retour** de l'activité principale **Lanceur parallèle** contient un tableau des résultats de tous les workflows d'intégration exécutés et invite à terminer correctement le suivi des exécutions.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	L'état de l'enregistrement d'audit est défini sur **Terminé**.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
CapabilityExecutionId	Identificateur système de l'enregistrement d'audit. Ce champ était la sortie de l'une des activités de début d'audit.
nom du workflow	Nom du workflow. Fourni par le système.
message	Message d'achèvement.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Il n'y a pas de variables de sortie.

Suivi d'exécution de l'aptitude : activité d'échec

L'activité de workflow Suivi de l'exécution de l'aptitude - Défaillance enregistre une défaillance dans l'enregistrement d'audit.

L'activité Suivi de l'exécution de l'aptitude - Défaillance peut être utilisée avec n'importe quel workflow pour enregistrer une condition de défaillance.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	L'état de l'enregistrement d'audit est défini sur **Erreur** et un message indiquant l'erreur est enregistré.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
CapabilityExecutionId	Identificateur système de l'enregistrement d'audit. Il s'agit du résultat de n'importe quelle activité de début d'audit.
errorMessage	Message indiquant le motif de l'échec.
nom du workflow	Nom du workflow. Fourni par le système.

Variables de sortie

Il n'y a pas de variables de sortie.

Aptitude : déterminer l'activité des CI

L'activité de workflow Aptitude - Déterminer les CI détermine les éléments de configuration (CI) à inclure dans le workflow.

L'activité Aptitude - Déterminer les CI peut être utilisée avec n'importe quel workflow pour déterminer les CI à inclure dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Éléments de configuration trouvés.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats (suite)

Résultat	Description
Échec	Aucun CI trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
task_sys_id	Identificateur de tâche (mappe l'incident de sécurité aux CI).
cis_affected	Éléments de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
cis_affected	CI filtrés
task_sys_id	Identificateur de tâche (mappe l'incident de sécurité aux CI).

Créer une activité d'enregistrements de données d'enrichissement

L'activité **de workflow Créer des enregistrements de données d'enrichissement** crée ou met à jour des enregistrements d'enrichissement à utiliser dans le workflow.

L'activité **Créer des enregistrements de données d'enrichissement** peut être utilisée avec n'importe quel workflow pour mettre à jour des enregistrements d'enrichissement dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Enregistrement d'enrichissement mis à jour.
Échec	Enregistrement d'enrichissement non mis à jour. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
task_id	Identificateur de tâche.
contenu	Contenu brut (données des processus en cours).
enrichment_mapping_id	Identificateur de mappage d'enrichissement.
ci_id	Identificateur d'élément de configuration.
reference_value	Inutilisé.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
résultat	GlideRecords créé à l'aide du script enrichmentUtils.

Obtenir l'activité FQDN de l'élément de configuration

Le champ **Orchestration commune de sécurité** > **Obtenir le FQDN de l'élément de configuration** Activité du workflow Récupère le nom de domaine complet (FQDN) d'un élément de configuration. Cette activité peut accélérer le processus d'investigation et de correction.

L'activité Obtenir le nom de domaine complet de l'élément de configuration peut être utilisée avec n'importe quel workflow pour récupérer le nom de domaine complet (FQDN) d'un élément de configuration.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
cmdb_ci.id [chaîne]	L'identificateur système (sys_id) d'un enregistrement d'élément de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
FQDN [chaîne]	Nom de domaine complet (FQDN) de l'élément de configuration.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarques supplémentaires

Le champ fqdn de l'élément de configuration doit être renseigné.

Déterminer l'activité des observables

L'activité de workflow **Déterminer les observables** détermine les observables à inclure dans le workflow

L'activité **Déterminer les observables** peut être utilisée avec n'importe quel workflow pour déterminer les observables à inclure dans le workflow.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Observables trouvés
Échec	Aucun observable trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
task_sys_id	Identificateur de tâche (mappe l'incident de sécurité aux observables).
observables	Adresses IP, hachage, URL, noms de domaines.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
observables	Observables filtrés

Activité Obtenir les options de sécurité prises en charge

L'activité de workflow Obtenir les options prises en charge récupère le nom et le nombre d'intégrations actives qui prennent en charge l'option demandée.

L'activité Obtenir les options prises en charge peut être utilisée avec n'importe quel workflow pour déterminer quelles options sont prises en charge.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Intégration prenant en charge l'aptitude trouvée.
Échec	Une erreur s'est produite lors de la tentative de recherche d'une intégration active prenant en charge l'option. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
capabilityName	Nom de l'option.
taskId	Identificateur système pour toute tâche associée au workflow.
domainId	Identificateur système pour tout domaine associé au workflow.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
supportedCapabilities	Liste des intégrations qui prennent en charge l'option.
Nombre d'options	Nombre d'intégrations prenant en charge l'option.

Suivi de l'exécution de l'aptitude : aucune implémentation de l'activité

L'activité de workflow Suivi de l'exécution de l'aptitude - Aucune implémentation de l'aptitude crée un enregistrement d'erreur lorsqu'aucune implémentation de l'aptitude d'intégration n'est trouvée.

L'activité Suivi de l'exécution de l'aptitude : aucune implémentation peut être utilisée avec n'importe quel workflow d'aptitude d'intégration abstrait pour gérer la condition d'erreur lorsqu'aucune implémentation d'aptitude configurée n'est disponible.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	L'état de l'enregistrement de suivi des exécutions est défini sur **Erreur** et un message indiquant l'erreur est enregistré.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
CapabilityExecutionId	Identificateur système de l'enregistrement d'audit. Sortie de l'activité utilisée pour démarrer le suivi des exécutions.
nom du workflow	Nom du workflow. Fourni par le système.

Variables de sortie

Il n'y a pas de variables de sortie.

Créer une activité de recherche de conformité

L'activité Créer une recherche de conformité crée une recherche de conformité pour les e-mails dans le(s) serveur(s) Exchange désigné(s) à l'aide des requêtes de recherche définies et renvoie le nom de la recherche de conformité créée.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
search_query	Requête de recherche obligatoire utilisée pour trouver des e-mails dans le serveur Exchange dans toutes les boîtes aux lettres.
Emplacement Exchange	Champ d'emplacement obligatoire utilisé pour effectuer des recherches dans l'ensemble de l'emplacement défini. Les valeurs possibles sont les suivantes : • Tout • Nom de boîte de réception spécifique
targetId	Champ d'identificateur d'hôte cible obligatoire où se trouve le serveur Exchange.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
réponse	Nom de la recherche de conformité créée.

Conditions de sortie

Les conditions de sortie possibles pour cette activité sont les suivantes :

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions de sortie

Variable	Description
Échec de la création de la recherche	Lorsque la création de la recherche échoue en raison d'une exception dans le serveur Exchange.
Recherche créée avec succès	Lorsque la création de la recherche est réussie.
Échec de la création de la recherche en raison d'une erreur d'analyse	Lorsque la création d'une recherche échoue en raison d'un problème d'analyse.
Erreur	Lorsqu'une exception se produit dans l'activité du workflow.

Obtenir l'adresse IP à partir de l'activité du CI

Cette activité du workflow détermine l'adresse IPV4 associée à un élément de configuration (CI).

L'activité **Obtenir l'adresse IP à partir du CI** peut être utilisée avec n'importe quel workflow pour récupérer l'adresse IPv4 d'un CI.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
ci_sys_id [chaîne]	Identificateur système de l'élément de configuration

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
ip_addr [chaîne]	Adresse IPv4. Si l'adresse IP ne peut pas être déterminée, cette valeur est vide.

Conditions de sortie

Les résultats possibles pour cette activité sont les suivants :

Conditions

Condition	Description
Réussite	Une adresse IPv4 a été renvoyée.
Échec	Une adresse IPv4 n'a pas pu être déterminée.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Obtenir les statistiques réseau via l'activité netstat

L'activité de workflow Security Common Orchestration - Get Network Statistics via netstat récupère les statistiques réseau d'une ressource affectée sur un système Windows. Cette activité peut accélérer le processus d'investigation et de correction.

L'activité Obtenir les statistiques réseau via netstat peut être utilisée avec n'importe quel workflow pour récupérer des statistiques réseau à partir d'un système Windows. La machine est interrogée avec la commande **netstat** incluant les paramètres **-a** et **-o** . Pour améliorer les données de sortie, la commande **get-process** est également invoquée.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Les statistiques du réseau ont été récupérées au format JSON.
Échec	Une erreur s'est produite lors de la tentative de récupération des statistiques réseau. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Variable	Description
cible [chaîne]	Nom de domaine complet (FQDN) ou adresse IP du système cible.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
Réponse [chaîne]	Une chaîne JSON représentant les processus en cours d'exécution sur l'ordinateur cible. Les données JSON comprennent : pid Identificateur de processus _port local Port local pour la transaction réseau État État de la connexion TCP. **Remarque :** Ce champ est nul pour les connexions UDP. local_address

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
	Nom de domaine complet (FQDN) ou adresse IP local remote_address Nom de domaine complet (FQDN) ou adresse IP distant protocol TCP ou UDP remote_port Port distant de la transaction réseau chemin d'accès Chemin d'accès au fichier de l'exécutable du processus hachage Valeur de hachage de l'exécutable du processus. Le hachage est en SHA-256 pour PowerShell V4 ou une version ultérieure. Sinon, le hachage est en MD5.

Restrictions

Le MID Server doit prendre en charge PowerShell.

Le hachage SHA-256 nécessite PowerShell V4.

Obtenir les processus en cours d'exécution via l'activité WMI

L'activité de workflow**Obtenir les processus en cours d'exécution** récupère les processus en cours d'exécution d'un élément de configuration sur un système Windows. Cette activité peut accélérer le processus d'investigation et de correction.

L'activité **Obtenir les processus en cours d'exécution via WMI** peut être utilisée avec n'importe quel workflow pour récupérer les processus en cours d'exécution sur un système Windows.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
cible [chaîne]	Nom de domaine complet (FQDN) ou adresse IP du système cible.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
Réponse [chaîne]	Chaîne JSON représentant les processus en cours d'exécution sur le système cible. Les données JSON comprennent : pid Identificateur du processus name Nom du processus De plus, s'il est disponible : Propriétaire Nom du propriétaire du processus owner_sid L'identificateur système du propriétaire du processus owner_domain Domaine du propriétaire du processus chemin d'accès Chemin d'accès au fichier de l'exécutable du processus hachage Valeur de hachage de l'exécutable du processus. Le hachage est en SHA-256 pour PowerShell V4 ou une version ultérieure. Sinon, le hachage est en MD5.

Restrictions

Le MID Server doit prendre en charge **PowerShell**.

Le hachage SHA-256 nécessite PowerShell V4.

Vérifier l'activité d'état de la recherche de conformité

L'activité Vérifier l'état de la recherche de conformité vérifie l'état de la recherche de conformité créée sur le serveur Exchange et, si l'état est terminé, renvoie les informations relatives à la recherche d'e-mails trouvées pour la recherche de conformité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
targetId	Champ d'identificateur d'hôte cible obligatoire où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
réponse	Contient l'état de la recherche de conformité et le nombre d'e-mails trouvés sur le serveur Exchange pour la recherche de conformité.

Conditions de sortie

Les conditions de sortie possibles pour cette activité sont les suivantes :

Conditions de sortie

Variable	Description
Recherche en cours	Lorsque l'état de la recherche de conformité est en cours.
Recherche terminée : aucun e-mail de menace trouvé	Lorsque l'état de la recherche de conformité est terminé et qu'aucun e-mail n'est trouvé dans le cadre de la recherche de conformité.
Recherche terminée : e-mails de menace trouvés	Lorsque l'état de la recherche de conformité est terminé et que des e-mails sont trouvés dans le cadre de la recherche de conformité.
Erreur lors de la vérification de l'état	Lorsque la vérification de l'état échoue en raison d'une exception dans le serveur Exchange.
Erreur	Lorsqu'une exception se produit dans l'activité du workflow.

Mettre à jour l'activité des notes de travail de la tâche

L'activité **de workflow Security Common Orchestration - Mettre à jour les notes de travail de tâche** met à jour la section **Activité** (notes de travail) d'un enregistrement de tâche. Ceci est utile pour enregistrer des informations.

L'activité **Mettre à jour les notes de travail de la tâche** peut être utilisée avec n'importe quel workflow pour mettre à jour les notes de travail de n'importe quel enregistrement de tâche.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
task_id [chaîne]	L'identificateur système (sys_id) d'un enregistrement de tâche.
Contenu [chaîne]	Données écrites dans les notes de travail d'une tâche.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
Résultat [chaîne]	Indique si la mise à jour a réussi.

Déployer les informations de recherche sur l'activité d'incident de sécurité

L'option Déployer les informations de recherche sur l'activité d'incident de sécurité peut être utilisée avec n'importe quel workflow pour recueillir des informations à partir d'une recherche de menaces et générer un résumé du contenu, ainsi que l'ID de l'incident de sécurité d'origine dans les notes de travail de la tâche.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Résumé du rapport de recherche déployé jusqu'à l'incident de sécurité.
Échec	La tâche d'origine et le rapport de résumé de recherche sont vides.

Variables d'entrée

Variable	Description
scanID[chaîne]	Rechercher un identificateur.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
sild[chaîne]	Identificateur d'incident de sécurité.
Réponse [chaîne]	Résumé des résultats de recherche, y compris : valeur IoC, résultat, motif de la défaillance, référence de recherche, etc.

Mettre à jour un incident de sécurité avec le workflow des résultats de la recherche

Le workflow **Mettre à jour un incident de sécurité avec les résultats de recherche** met à jour les incidents de sécurité existants avec les résultats de recherche.

Avant de commencer

Rôle requis : sn_si.basic

Traduction automatique

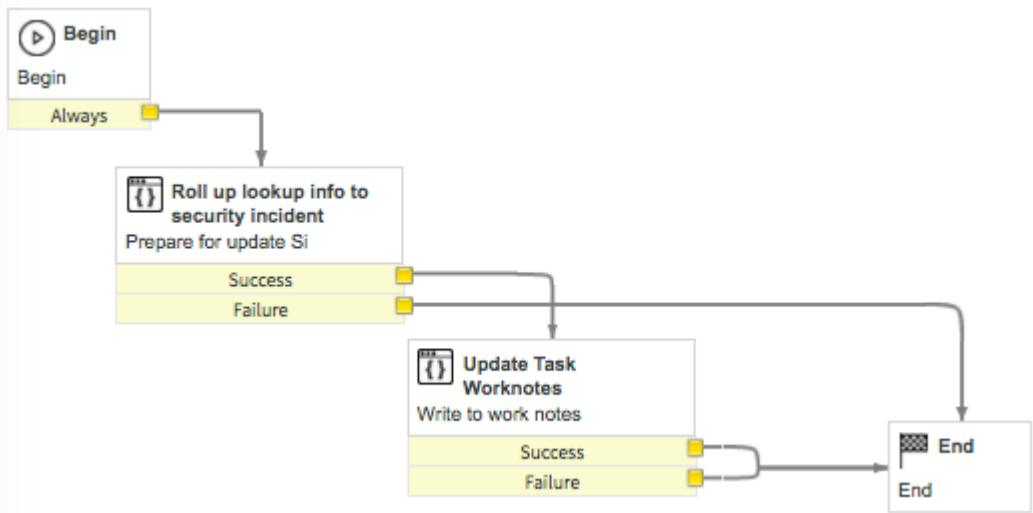
© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche
Ce workflow est déclenché par une règle métier sur la table de recherche, qui surveille quand le champ **Résultat** bascule sur Échec.

Les activités de processus du workflow comprennent :

Déployer les informations de recherche sur l'activité d'incident de sécurité

Mettre à jour l'activité des notes de travail de la tâche



Filtrer l'activité des observables sur liste d'autorisation

L'activité de workflow Observables sur liste d'autorisation filtrés supprime les observables qui peuvent être ignorés de la liste des observables. Cette activité peut accélérer le processus d'investigation et de correction.

L'activité Filtrer les éléments observables sur liste d'autorisation peut être utilisée avec n'importe quel workflow pour filtrer les observables avant d'effectuer toute action.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Liste de filtres créée.
Échec	Une erreur s'est produite lors de la tentative de filtrage des observables. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
observables	Liste des observables disponibles.

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
filteredObservables	Observables filtrés

Écrire le contenu à enregistrer en tant qu'activité de pièce jointe

Cette activité écrit le contenu transmis à partir d'une entrée et crée une pièce jointe désignée à un enregistrement donné.

L'activité **Écrire le contenu à enregistrer en tant que pièce jointe** peut être utilisée avec n'importe quel workflow pour écrire du contenu et le joindre à un enregistrement.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
nom de table [chaîne]	Nom de la table de l'enregistrement. Ce champ d'entrée est obligatoire.
SysId [chaîne]	L'identificateur système (sys_id) d'un enregistrement de tâche. Ce champ d'entrée est obligatoire.
charge utile	Contenu en texte brut à écrire en tant que pièce jointe. Ce champ d'entrée est obligatoire.
filename	Nom du fichier de la pièce jointe.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
Résultat [chaîne]	Indique si la mise à jour a réussi.

Obtenir l'adresse IP à partir de l'activité du CI

L'activité de workflow Obtenir l'adresse IP à partir du CI rassemble l'adresse IP à partir des éléments de configuration (CI) pour l'utiliser dans le workflow.

L'activité Obtenir l'adresse IP à partir du CI peut être utilisée avec n'importe quel workflow pour collecter des adresses IP d'éléments de configuration (CI) à utiliser dans le workflow.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Les résultats possibles pour cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Adresses IP trouvées.
Échec	Aucune adresse IP trouvée. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie d'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
ci_sys_id	Identificateur d'élément de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités suivantes.

Variables de sortie

Variable	Description
ip_addr	Adresses IP.

Opérations de sécurité Déclencheurs de workflow

Opérations de sécurité Les déclencheurs de workflow contiennent une condition sur une table. Tous les workflows associés à l'enregistrement de déclencheur de workflow s'exécutent lorsque la condition est remplie.

Créer des Opérations de sécurité déclencheurs de workflow

Créez un déclencheur de workflow qui contient une condition sur une table.

Avant de commencer
Opérations de sécurité contient plusieurs déclencheurs de workflow dans le système de base :

- Les modifications d'éléments de configuration sur un incident de sécurité actif

  Utilise l'intégration pour enrichir les données liées au CI au fur et à mesure que les éléments de configuration changent.

- Analyser à nouveau le groupe vulnérable

  Analyse à nouveau un groupe vulnérable à l'aide du Workflow Analyser la vulnérabilité, lorsque vous **fermez/ignorez** le groupe.

- Analyser à nouveau l'élément vulnérable

  Scanne à nouveau un élément vulnérable à l'aide du Workflow d'élément de vulnérabilité de l'analyse bouton **lorsque vous fermez/ignorez** l'élément.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles requis :

- À lire : sn_sec_cmn.read
- Pour créer ou mettre à jour : sn_sec_cmn.write
- À supprimer : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tout** > **Security Operations** > **Utilités** > **Déclencheurs de workflow**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

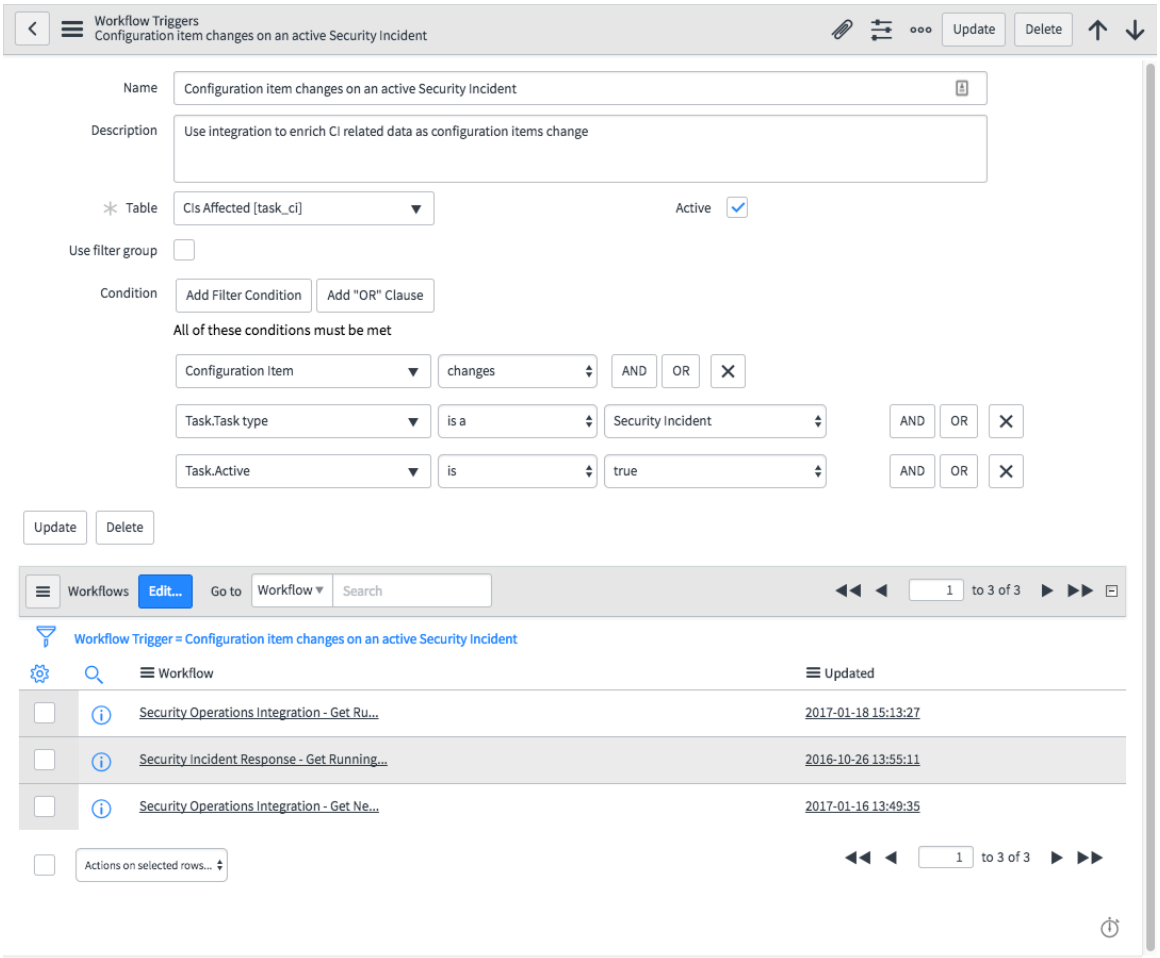
Déclencheurs de workflow

Champ	Description
Nom	Nom du déclencheur de workflow.
Description	Entrez une description pour le déclencheur de workflow.
Table	Table contenant le déclencheur de workflow. Si vous avez coché la case **Utiliser un groupe de filtres** et sélectionné un groupe de filtres, ce champ est par défaut la table associée au groupe de filtres sélectionné.
Condition	Utiliser le Créateur de conditions permettant de définir les critères du déclencheur de workflow. Si vous avez coché la case **Utiliser un groupe de filtres** et sélectionné un groupe **de** filtres, les champs Conditions ne s'affichent pas.
Actif	Cochez cette case pour activer le déclencheur de workflow.
Utiliser un groupe de filtres	Cochez cette case pour utiliser un groupe de filtres prédéfini ou créez un nouveau groupe de filtres pour définir les critères de déclencheur du workflow.
Groupe de filtres	Sélectionnez le groupe de filtres à utiliser pour définir les déclencheurs de workflow. Ce champ s'affiche uniquement si la case **Utiliser des groupes de filtres** est cochée.

4. Lorsque vous avez terminé vos saisies, faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'onglet **Workflows** s'affiche. Il contient des workflows qui sont exécutés lorsque toutes les conditions de filtre ou les conditions de groupe de filtres sont remplies.

5. Pour ajouter des workflows, procédez comme suit.
   a. Dans l'onglet **Workflows** , cliquez sur **Modifier**.
   b. Utilisez le créateur de conditions, si nécessaire, pour localiser les workflows que vous souhaitez sélectionner ou utilisez la zone de sélection pour sélectionner des workflows et les déplacer vers la liste des workflows.
   c. Cliquez sur **Enregistrer**.
   Les workflows sélectionnés sont ajoutés.
6. Cliquez sur **Mettre à jour**.

Orchestration de Security Operations

Les utilisateurs peuvent interagir et récupérer des données à partir de systèmes et d'environnements Windows ou UNIX à l'aide de packs d'activités et de workflows dans Orchestration des Opérations de sécurité.

Orchestration des Opérations de sécurité Gagnez du temps en éliminant les processus manuels et en obtenant des informations contextuelles pour corriger les incidents. Les Opérations de sécurité produits disposent de packs d'activités et de flux de travail standard qui sont inclus et activés dans chacun des modules d'extension.

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour créer et accéder à des activités d'orchestration supplémentaires qui ne sont pas disponibles avec les produits de l'offre Opérations de sécurité standard, achetez une licence d'orchestration complète.

- Orchestration de la réponse aux incidents de sécurité Flux de travail :
  - Workflow Security Incident Response - Obtenir les statistiques réseau
  - Intégration des commandes système Security Operations : workflow Obtenir les processus en cours d'exécution
  - Créer une demande de recherche pour le workflow des changements IoC
  - Security Operations Integration - Workflow de recherche et de suppression d'e-mail
- Orchestration des renseignements sur les menaces Flux de travail :
  - Renseignements sur les menaces - Exécuter le workflow de recherche IoC
  - Mettre à jour un incident de sécurité avec le workflow des résultats de la recherche
- Orchestration de la réponse aux vulnérabilités Flux de travail :
  - Workflow Analyser la vulnérabilité
  - Workflow d'élément de vulnérabilité de l'analyse

Traduction automatique

© 2024 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.